Alcatel-Lucent 7705

SERVICE AGGREGATION ROUTER OS | RELEASE 2.1

SERVICES GUIDE

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

OAM and SAA. 325

List of Tables

List of Figures

List of Acronyms

Acronym	Expansion
2G	second generation wireless telephone technology
3DES	triple DES (data encryption standard)
3G	third generation mobile telephone technology
5620 SAM	5620 Service Aware Manager
7705 SAR	7705 Service Aggregation Router
7710 SR	7710 Service Router
7750 SR	7750 Service Router
9500 MPR	9500 Microwave Packet Radio
ABR	available bit rate area border router
AC	alternating current attachment circuit
ACL	access control list
ACR	adaptive clock recovery
AFI	authority and format identifier
AIS	alarm indication signal
ANSI	American National Standards Institute
Apipe	ATM VLL
ARP	address resolution protocol
AS	autonomous system
ASAP	any service, any port
ASBR	autonomous system boundary router
ATM	asynchronous transfer mode
ATM PVC	ATM permanent virtual circuit

Acronym	Expansion
Batt A	battery A
B-bit	beginning bit (first packet of a fragment)
Bellcore	Bell Communications Research
BFD	bidirectional forwarding detection
BITS	building integrated timing supply
BOF	boot options file
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 continuity check
CCM	continuity check message
CE	customer edge circuit emulation
CEM	circuit emulation
CES	circuit emulation services
CESoPSN	circuit emulation services over packet switched network
CFM	connectivity fault management
CIDR	classless inter-domain routing
CIR	committed information rate
CLI	command line interface
CLP	cell loss priority

Acronym	Expansion
CoS	class of service
CPE	customer premises equipment
Cpipe	circuit emulation (or TDM) VLL
CPM	Control and Processing Module (CPM is used instead of CSM when referring to CSM filtering – to align with CLI syntax used with other SR products)
CPU	central processing unit
CRC	cyclic redundancy check
CRON	a time-based scheduling service (from chronos = time)
CSM	Control and Switching Module
CSNP	complete sequence number PDU
CSPF	constrained shortest path first
CV	connection verification customer VLAN (tag)
CW	control word
DC	direct current
DC-C	DC return - common
DC-I	DC return - isolated
DCE	data communications equipment
DCO	digitally controlled oscillator
DDoS	distributed DoS
DES	data encryption standard
DHCP	dynamic host configuration protocol
DIS	designated intermediate system
DNS	domain name server
DoS	denial of service

Acronym	Expansion
dot1p	IEEE 802.1p bits, found in Ethernet or VLAN ingress packet headers and used to map traffic to up to eight forwarding classes
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
EGP	exterior gateway protocol
EIA/TIA-232	electronic industries alliance/telecommunications industry association standard 232 (also known as RS-232)
ELER	egress label edge router
Epipe	Ethernet VLL
ERO	explicit route object
ESD	electrostatic discharge
ETE	end-to-end
ETH-CFM	Ethernet connectivity fault management (IEEE 802.1ag)
EVDO	evolution - data optimized
EXP bits	experimental bits
FC	forwarding class
FCS	frame check sequence

Acronym	Expansion
FDB	forwarding database
FDL	facilities data link
FEC	forwarding equivalence class
FF	fixed filter
FIB	forwarding information base
FIFO	first in, first out
FNG	fault notification generator
FRR	fast reroute
FTN	FEC-to-NHLFE
FTP	file transfer protocol
GigE	Gigabit Ethernet
GRE	generic routing encapsulation
GSM	Global System for Mobile Communications (2G)
HCM	high capacity multiplexing
HEC	header error control
HMAC	hash message authentication code
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
IEEE 1588v2	Institute of Electrical and Electronics Engineers standard 1588-2008
IES	Internet Enhanced Service
IETF	Internet Engineering Task Force

Acronym	Expansion
IGP	interior gateway protocol
ILER	ingress label edge router
ILM	incoming label map
IMA	inverse multiplexing over ATM
IOM	input/output module
IP	Internet Protocol
IPCP	Internet Protocol Control Protocol
Ipipe	IP interworking VLL
IS-IS	Intermediate System-to-Intermediate System
IS-IS-TE	IS-IS-traffic engineering (extensions)
ISO	International Organization for Standardization
LB	loopback
LBM	loopback message
LBR	loopback reply
LCP	link control protocol
LDP	label distribution protocol
LER	label edge router
LIB	label information base
LLF	link loss forwarding
LLID	loopback location ID
LSA	link-state advertisement
LSDB	link-state database
LSP	label switched path link-state PDU (for IS-IS)
LSR	label switch router link-state request

Acronym	Expansion
LSU	link-state update
LT	linktrace
LTM	linktrace message
LTN	LSP ID to NHLFE
LTR	linktrace reply
MA	maintenance association
MAC	media access control
MBB	make-before-break
MBS	maximum buffer space maximum burst size media buffer space
MBSP	Mobile Backhaul Service Provider
MC-MLPPP	multi-class multilink point-to-point protocol
MD	maintenance domain
MD5	message digest version 5 (algorithm)
MDA	media dependent adapter
ME	maintenance entity
MEF	Metro Ethernet Forum
MEN	Metro Ethernet network
MEP	maintenance association end point
MFC	multi-field classification
MHF	MIP half function
MIB	management information base
MIP	maintenance association intermediate point
MIR	minimum information rate
MLPPP	multilink point-to-point protocol

Acronym	Expansion
MP	merge point multilink protocol
MPLS	multiprotocol label switching
MPR	see 9500 MPR
MRRU	maximum received reconstructed unit
MRU	maximum receive unit
MSDU	MAC Service Data Unit
MS-PW	multi-segment pseudowire
MTSO	mobile trunk switching office
MTU	maximum transmission unit multi-tenant unit
MW	microwave
NBMA	non-broadcast multiple access (network)
NET	network entity title
NHLFE	next hop label forwarding entry
NHOP	next-hop
NNHOP	next next-hop
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)
NSAP	network service access point
NSSA	not-so-stubby area
NTP	network time protocol
OAM	operations, administration, and maintenance
OAMPDU	OAM protocol data units
OC3	optical carrier, level 3
OS	operating system

Acronym	Expansion
OSI	Open Systems Interconnection (reference model)
OSINLCP	OSI Network Layer Control Protocol
OSPF	Open Shortest Path First
OSPF-TE	OSPF-traffic engineering (extensions)
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
PLR	point of local repair
POP	point of presence
POS	packet over SONET
PPP	point-to-point protocol
PSN	packet switched network
PSNP	partial sequence number PDU
PTP	precision time protocol
PVC	permanent virtual circuit
PVCC	permanent virtual channel connection
PW	pseudowire
PWE3	pseudowire emulation edge-to-edge
QoS	quality of service
RADIUS	Remote Authentication Dial In User Service

Acronym	Expansion
RAN	Radio Access Network
RDI	remote defect indication
RED	random early discard
RESV	reservation
RIB	routing information base
RNC	Radio Network Controller
RRO	record route object
RS-232	recommended standard 232 (also known as EIA/TIA-232)
RSVP-TE	resource reservation protocol - traffic engineering
R&TTE	Radio and Telecommunications Terminal Equipment
RT	receive/transmit
RTM	routing 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
SCP	secure copy
SDH	synchronous digital hierarchy
SDI	serial data interface
SDP	service destination point
SE	shared explicit
SFP	small form-factor pluggable (transceiver)
SGT	self-generated traffic

Acronym	Expansion
SHA-1	secure hash algorithm
SIR	sustained information rate
SLA	Service Level Agreement
SNMP	Simple Network Management Protocol
SNPA	subnetwork point of attachment
SNTP	simple network time protocol
SONET	synchronous optical networking
S-PE	switching provider edge router
SPE	source provider edge router
SPF	shortest path first
SPT	shortest path tree
SR	service router (includes 7710 SR, 7750 SR)
SRLG	shared risk link group
SSH	secure shell
SSU	system synchronization unit
STM1	synchronous transport module, level 1
SVC	switched virtual circuit
TACACS+	Terminal Access Controller Access-Control System Plus
TCP	transmission control protocol
TDM	time division multiplexing
TE	traffic engineering
TFTP	trivial file transfer protocol
TLDP	targeted LDP
TLV	type length value
ToS	type of service
T-PE	terminating provider edge router

Acronym	**Expansion**
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
V.35	v-series recommendation 35
VC	virtual circuit
VCC	virtual channel connection
VCCV	virtual circuit connectivity verification
VCI	virtual circuit identifier
VID	VLAN ID
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
VRF	virtual routing and forwarding table
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), Resource Reservation Protocol for Traffic Engineering (RSVP-TE), 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 Maintenance (OAM) tools.
- 7705 SAR OS Quality of Service Guide

  This guide describes how to configure Quality of Service (QoS) policy management.
- 7705 SAR OS Routing Protocols Guide

  This guide provides an overview of dynamic routing concepts and describes how to configure them.

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://www.alcatel-lucent.com/support

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 57
VLL services	Apipe service	ATM VLL (Apipe) Services on page 108
	Cpipe service	Circuit Emulation VLL (Cpipe) Services on page 111
	Epipe service	Ethernet VLL (Epipe) Services on page 129
	Ipipe service	IP Interworking VLL (Ipipe) Services on page 144
Internet Enhanced Service	Configure in-band management of 7705 SAR over ATM links	Internet Enhanced Service on page 287

Table 1: 7705 SAR Configuration Process (Continued)

Area	Task	Reference
Diagnostics/Service verification	Diagnostics, monitoring, and troubleshooting	OAM and SAA on page 325 Tools on page 419
Reference	List of IEEE, IETF, and other proprietary entities	Standards and Protocol Support on page 447

Notes on 7705 SAR-8 and 7705 SAR-F

The 7705 SAR-8 and the 7705 SAR-F 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	

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

7705 SAR-8	7705 SAR-F	Notes
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 the T1/E1 ports on the 16-port T1/E1 ASAP Adapter card, except that the 16 T1/E1 ports on the 7705 SAR-F support multiple synchronization sources to support two timing references. On the 7705 SAR-8, the CLI indicates the MDA type for the 16-port T1/E1 ASAP Adapter card as `a16-chds1`. On the 7705 SAR-F, the CLI indicates the MDA type for the 7705 SAR-F ports as `a16-chds1v2`.
8-port Ethernet Adapter card	8 individual Ethernet ports on the faceplate	The –48 VDC versions of the 7705 SAR-8 support two versions of the 8-port Ethernet Adapter card, with version 2 having additional support for Synchronous Ethernet. The Ethernet ports on the 7705 SAR-F are equivalent to the Ethernet ports on version 2 of the 8-port Ethernet Adapter card and support multiple synchronization sources to support two timing references. The +24 VDC version of the 7705 SAR-8 only supports version 2 of the 8-port Ethernet Adapter card. On the 7705 SAR-8, the CLI indicates the MDA type for the 8-port Ethernet Adapter card as `a8-eth` or `a8-ethv2`. On the 7705 SAR-F, the CLI indicates the MDA type for the 7705 SAR-F Ethernet ports as `a8-ethv3`, to distinguish it from the actual version 2 of the 8-port Ethernet Adapter card.
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

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 36 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 2.1, SAP-to-SAP connections are supported for ATM, Ethernet, 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 108.
    - → 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 111.
    - → 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 129.
    - → IP interworking VLL (Ipipe) — a PWE3 IP service between two hosts connected by any combination of point-to-point access circuits (PPP/MLPPP) with routed IPv4 encapsulation and Ethernet interface SAPs; for example, Ethernet SAP to Ethernet SAP, PPP SAP to MLPPP SAP, or Ethernet SAP to MLPPP SAP. See IP Interworking VLL (Ipipe) Services on page 144.
- Internet Enhanced Service (IES)
    - → In Release 2.1, 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 287.

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

Table 3: Pseudowire Service Types

PW Service Type (EtherType)	Value
IP Layer 2 transport	0x000B
Ethernet tagged mode	0x0004
Ethernet raw	0x0005
PPP	0x0007
ATM N-to-one VCC cell mode (1)	0x0009
ATM N-to-one VPC cell mode	0x000A
SAToP E1	0x0011
SAToP T1	0x0012

Table 3: Pseudowire Service Types (Continued)

PW Service Type (EtherType)	Value
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. IP filter policies are supported on Epipes and Ipipes and on Management SAPs.

- 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.
- IP filter policies allow selective blocking or forwarding of traffic that matches criteria that is set in the policy. The action applies to traffic that enters from the ingress direction of a SAP.

  Filter policies, also referred to as access control lists (ACLs), control the traffic allowed into an Ethernet or IP SAP based on IP match criteria. Assigning a filter policy to a SAP is optional. Filter policies are identified by a unique filter policy ID. A filter policy must be created before it can be applied to a SAP. A single ingress filter policy can be associated with a SAP.

For more information on provisioning QoS policies, including queuing behaviors, refer to the 7705 SAR OS Quality of Service Guide. For information on configuring IP filter policies, refer to the 7705 SAR OS Router Configuration 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 37). 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, accounting policies, and IP filter policies (Epipes, Ipipes, and Management SAPs only) 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

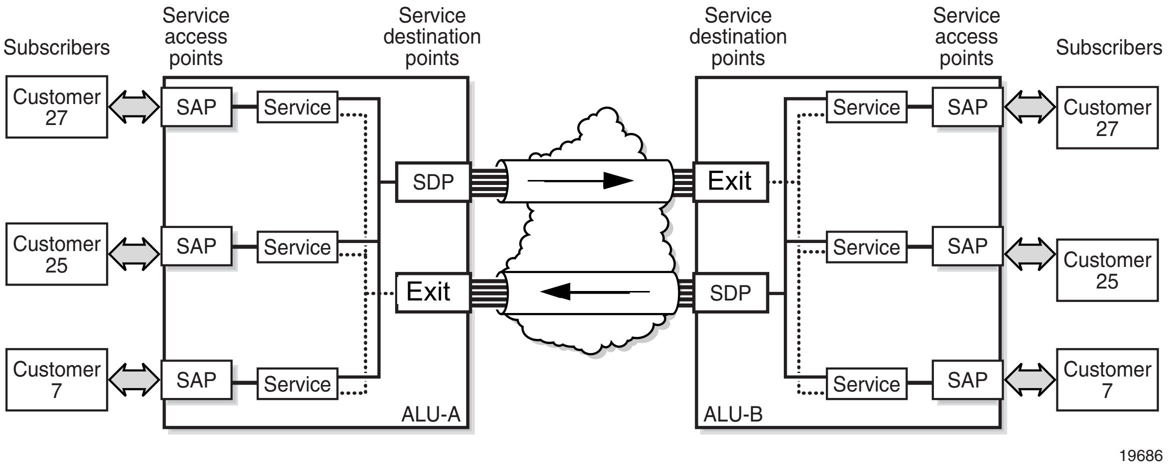
The basic (logical) service entities in the service model used to construct an end-to-end service are:

- 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



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 four types of VLL service: ATM VLL (Apipe), circuit emulation VLL (Cpipe), Ethernet VLL (Epipe), and IP interworking VLL (Ipipe) 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 56 for more information on identifiers.

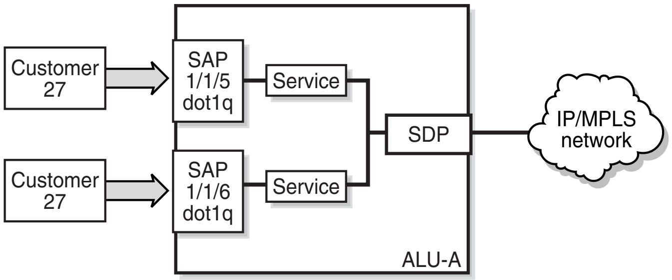
There are four VLL service types available on the 7705 SAR: Apipe, Cpipe, Epipe, and Ipipe. For each service type, the SAP has slightly different parameters. In general, SAPs are logical endpoints that are local to the 7705 SAR and are uniquely identified by:

- the physical Ethernet port, SONET/SDH 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, SONET/SDH port, or TDM channel group used for the service. It identifies the protocol that is used to provide the service. The 7705 SAR supports three SAP encapsulation types: Ethernet, SONET/SDH, 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.

Notes:

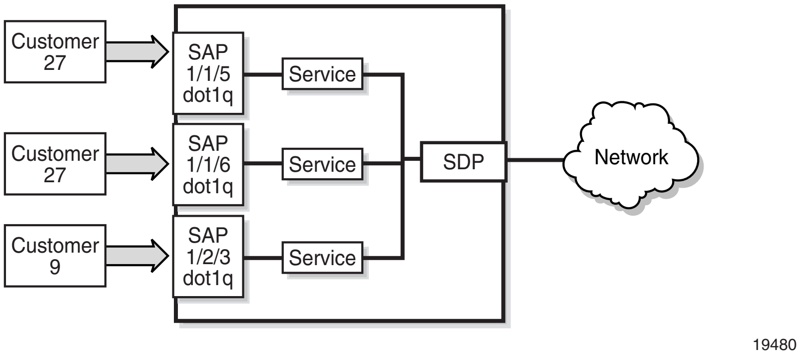
- Throughout this guide, the term “channel group” is often simplified to “channel”.
- Do not confuse the term “encapsulation ID” (described here) with the term “Encapsulation ID”, which is used with the SNMP and MIBs for the 7705 SAR.

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



SONET/SDH Encapsulations

The following service encapsulation option is available on SONET/SDH ports:

- atm — supports multiple services for one customer

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 × DS0)) and unstructured cem service (structure-agnostic TDM over packet (SAToP)) are supported.

- ipcp — supports a single IP service per TDM channel group on channelized interfaces. This is typically used for router interconnection using the point-to-point protocol (PPP).

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
SONET/SDH	atm
TDM	cem
TDM	atm
TDM	ipcp

SAP Configuration Considerations

In addition to being an entry or exit point for 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
    - → Ingress filter policy (for Epipes, Ipipes, and Management SAPs only)

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 in the following list. 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.

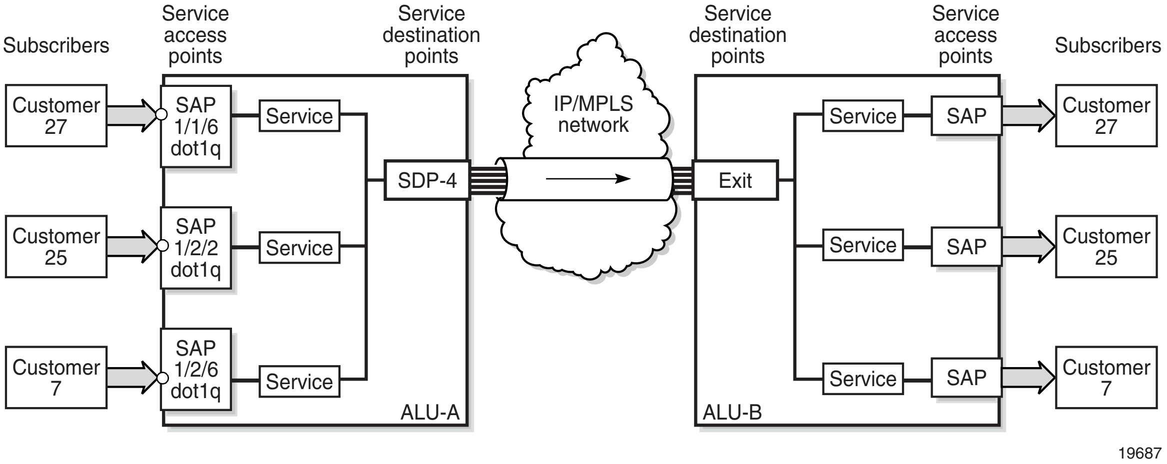
An SDP has the following characteristics.

- 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.
- An SDP can be used to provide PW redundancy, where up to four spoke SDPs can be assigned to a service endpoint that acts as the managing entity to ensure service connection. See Pseudowire Redundancy on page 158.

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



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 2.1, 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 154 for more information.

The following ways of configuring an MPLS tunnel are supported:

- LDP signaled
- RSVP-TE 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 51), 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. Up to 64 GRE tunnels are supported per chassis.

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

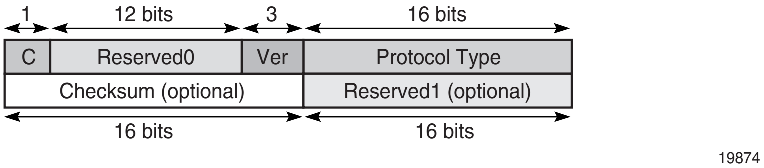


Table 5: GRE Header Descriptions

Field	Description
C	Specifies whether there is a checksum in the header If set to 1, both the checksum and reserved1 fields must be present 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. 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.
Reserved0	Indicates whether the header contains optional fields 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
Ver	Always set to 000 for GRE 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
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

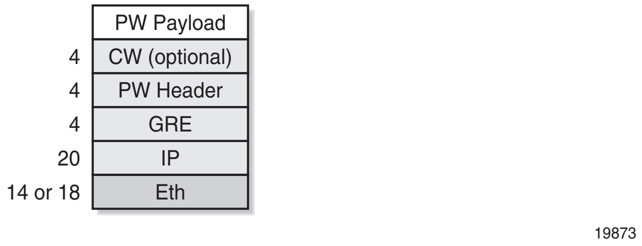


Table 6: GRE Pseudowire Payload Packet Descriptions

Field	Description
Eth	This field is the Layer 2 transport header In Release 2.1, 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 158
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 2102 octets. For more information on MTU, see MTU Settings on page 154.

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 328 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 63.

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.

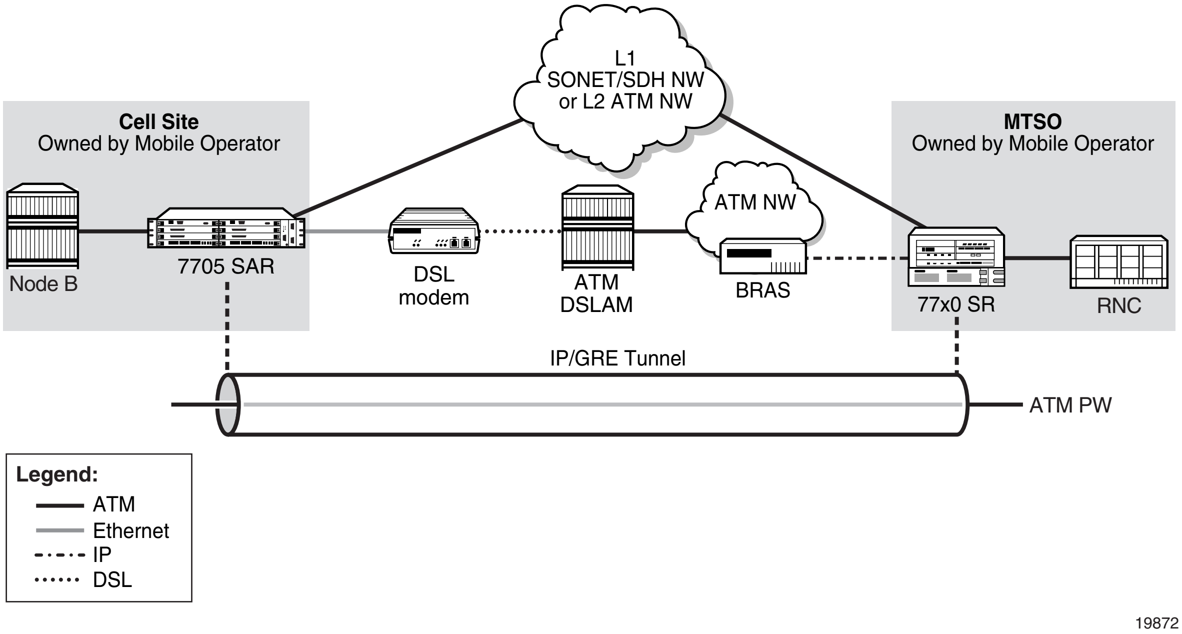
HSDPA Offload

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 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 midsized 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



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 encapsulation configuration. One endpoint of a SAP connection can be an IMA group, while the other endpoint can be on a single ATM port.

ATM SAP-to-SAP connections are also supported between any two OC3/STM1 ports and between any T1/E1 ASAP port and OC3/STM1 port, as long as both SAPs support ATM.

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 325. 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.

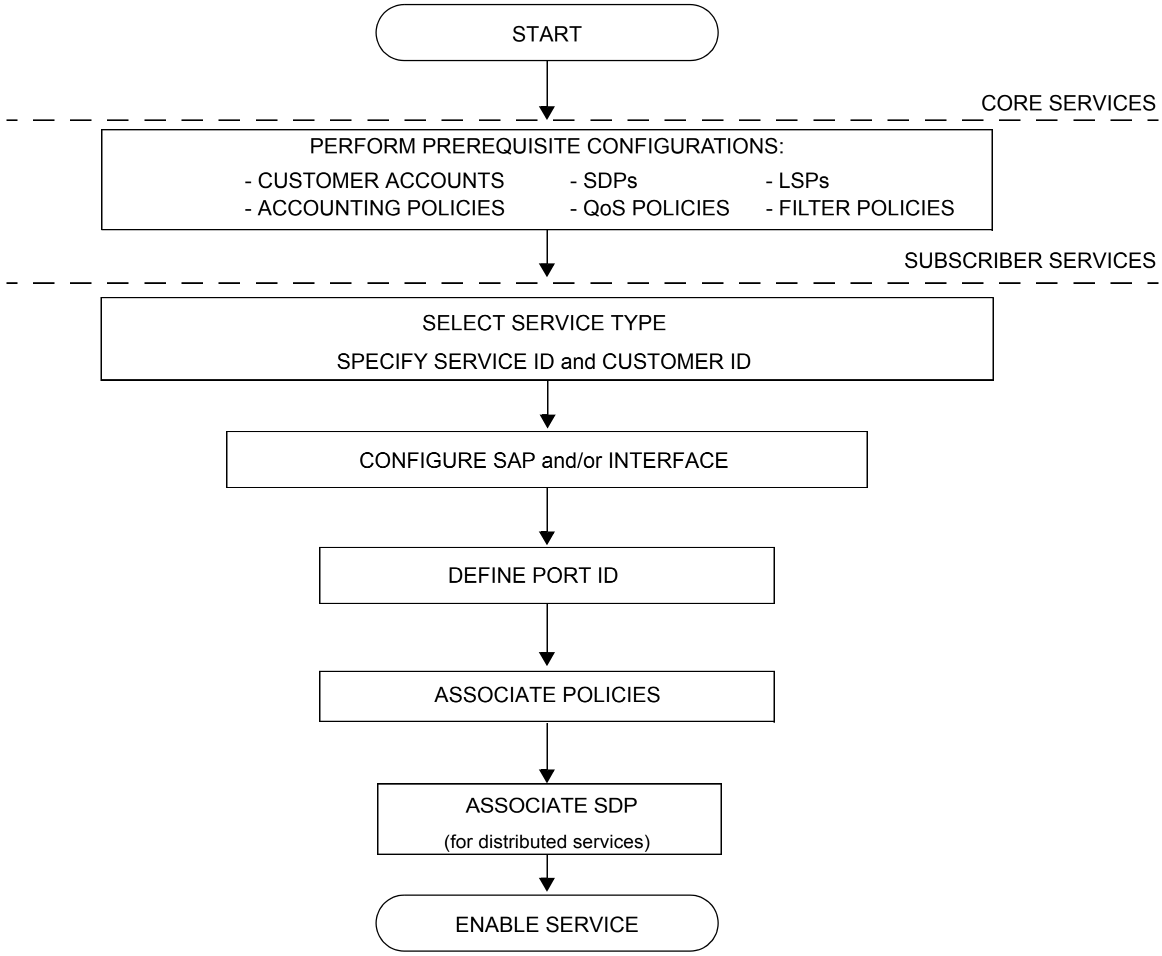
Core tasks include the following items:

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

Subscriber services tasks include the following items:

- create Apipe, Cpipe, Epipe, or Ipipe services or IES
- configure SAPs
- bind SDPs
- create exclusive QoS policies
- assign IP filter policies to Epipes, Ipipes, and/or Management SAPs

Figure 8: Service Creation and Implementation Flow Chart



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 447.

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

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 61
- Service Destination Points (SDPs)
  → Configuring SDPs on page 62
- Service Types
  → ATM VLL (Apipe) Services on page 108
  → Circuit Emulation VLL (Cpipe) Services on page 111
  → Ethernet VLL (Epipe) Services on page 129
  → Internet Enhanced Service on page 287
- Service Access Points (SAPs)
  → Configuring Apipe SAP Parameters on page 167
  → Configuring Cpipe SAP parameters on page 170
  → Configuring Epipe SAP Parameters on page 174
  → Configuring IES SAP Parameters on page 297

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
                        filter ip 1
                        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
```

ETH-CFM (802.1ag)

Ethernet Connectivity Fault Management (ETH-CFM) is defined in the IEEE 802.1ag standard, which specifies protocols, procedures, and managed objects in support of transport fault management, including discovery and verification of the path, and detection and isolation of a connectivity fault for each Ethernet service instance.

CFM uses Ethernet frames and can be distinguished by its Ethertype and special Ethernet multicast addresses. CFM frames are only processed by IEEE MAC bridges. For Ethertype and Ethernet multicast address values, see Dot1ag CFM Frame Format on page 138.

With CFM, interoperability can be achieved between different vendor equipment in the service provider network, up to and including customer premises bridges.

Table 7 provides Ethernet OAM terminology definitions.

Table 7: Ethernet OAM Terminology

Term	Expansion	Definition
MA	Maintenance Association	A grouping of MEs that need to be managed as part of a given service An MA is uniquely identified by its combination of *md-index*, MD level and *ma-index*, where *md-index* and *ma-index* are user-configured values
MD	Maintenance Domain	A set of Ethernet network elements or ports that are controlled by an operator, where boundaries are set by MEPs
MD level	Maintenance Domain level	A user-configured value of 0 to 7 representing a level of hierarchy within a CFM architecture. The value 7 is the highest MD level and 0 is the lowest. The MD level is transmitted as part of the Ethernet CFM frame. A CFM message is said to have a higher MD level when its MD level value is higher than the MD value configured on the 7705 SAR.
ME	Maintenance Entity	An Ethernet port or endpoint that is managed as part of dot1ag OAM. An endpoint can be an SAP or a spoke SDP.
MEP	Maintenance Association End Point	An edge point that can terminate, respond to, or initiate the OAM messages for a configured MA-MD combination A MEP is identified by its MEP ID, which is a unique combination of *md-index* and *ma-index*, where *md-index* and *ma-index* are user-configured values
MIP	Maintenance Association Intermediate Point	An intermediate point that can respond to OAM messages initiated by MEPs in the same MD. Connectivity fault management (CFM) messages destined for other MIPs or the destination MEP are transparent to MIPs. MIPs are not supported in Release 2.1 of the 7705 SAR

MDs, MD Levels, MAs, and MEPs

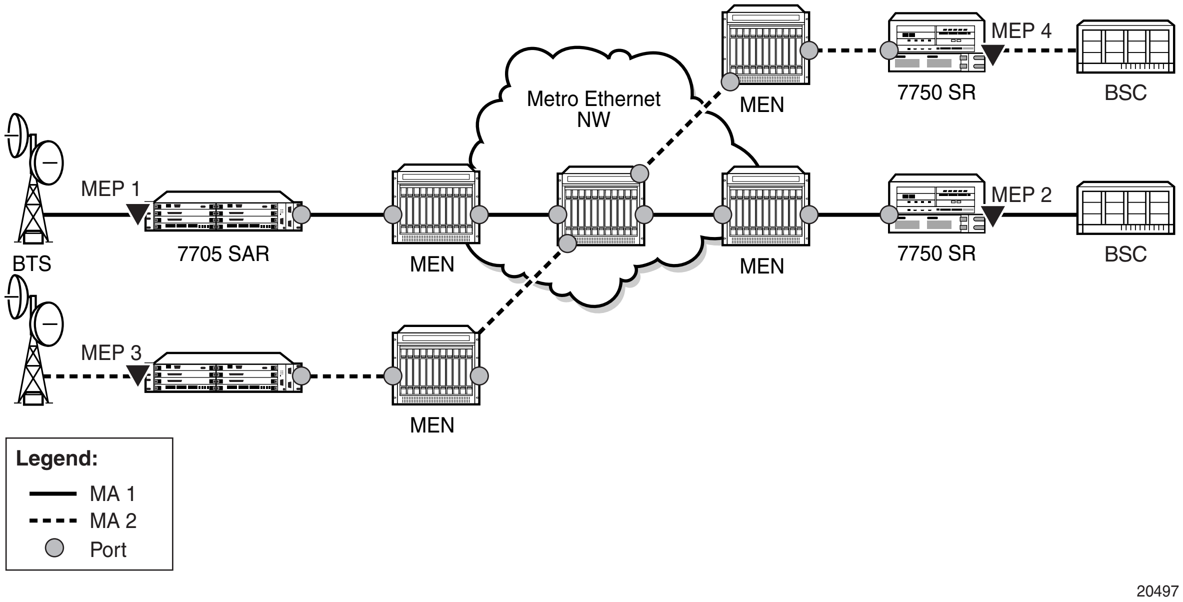
A maintenance domain (MD) identifies a set of network elements that have a common CFM OAM purpose. An MD can be divided into subsets of maintenance domain levels (MD levels) by assigning MD level values.

Maintenance association end points (MEPs) are configured as part of Ethernet SAPs or spoke SDPs and can generate or terminate CFM OAM messages. MEPs only communicate within the same MD level. The configured value of an MD level (0 to 7, inclusive) is carried in the CFM PDU to inform management entities (MEs) of the maintenance association (MA) to which the CFM PDU belongs.

A maintenance association (MA) has a pair of MEPs (one local and one remote MEP), where each MEP is configured with the same MD index, MD level, and MA index (this combination is called the MA-ID). The MA itself is configured with a value for a bridge identifier, which maps to a service ID. The MA is used to verify the integrity of a single service instance. Figure 9 depicts a high-level view of MEPs in a CFM-enabled network. Two MAs are shown. Also shown are maintenance association intermediate points (MIPs); however, MIPs are not supported in Release 2.1 of the 7705 SAR.

For more information on MEP support on Ethernet SAPs and spoke SDPs, see ETH-CFM (802.1ag) on page 138.

Figure 9: MEPs and MAs



The following functions are supported:

- CFM can be enabled or disabled on a SAP or spoke SDP basis
- eight MD levels can be assigned
- the following MD name formats are supported:
    - → none – no MD name
    - → DNS name
    - → MAC address and 2-octet integer
    - → character string
- MAs for each MD level can be configured, modified, or deleted
    - → each MA is defined by a unique combination of MD index, MD level, and MA index. This unique combination of values is called the MA identifier (MA-ID).
    - → the following MA name formats are supported:
        - primary VLAN ID (VID)
        - character string
        - 2-octet integer
        - RFC 2685, Virtual Private Networks Identifier
    - → when a VID is used as the MA name, CFM will not support VLAN translation because the unique MA-ID must match all the MEPs
    - → the default format for an MA name is a 2-octet integer; integer value 0 means that the MA is not attached to a VID
- down MEPs with a MEP-ID on a SAP or spoke SDP for each MD level (both associations for a down MEP are with the same Bridge Port; this is described in Section 19.2.1 of IEEE Standard 802.1ag-2007) can be configured, modified, or deleted. Each MEP is uniquely identified by its MEP index and MA-ID combination.
- MEP creation on a SAP is allowed only for Ethernet ports (with null or q-tag encapsulations)

Loopback (LB)

A Loopback Message (LBM) is generated by a MEP and sent to its peer MEP. Its function is similar to IP or MPLS ping in that it verifies Ethernet connectivity between the nodes on a per-request basis. That is, it is non-periodic and is only initiated by a user request.

For more information on ETH-CFM loopbacks, see ETH-CFM (802.1ag) on page 337.

Linktrace (LT)

A Linktrace Message (LTM) is originated by a MEP and targeted to a peer MEP in the same MA and within the same MD level. Its function is similar to IP traceroute. The peer MEP responds with a Linktrace Reply (LTR) message after successful inspection of the LTM.

For more information on ETH-CFM linktrace, see ETH-CFM (802.1ag) on page 337.

Continuity Check (CC)

A Continuity Check Message (CCM) is a multicast frame that is generated by a MEP and sent to its remote MEPs in the same MA. The CCM does not require a reply message. To identify faults, the receiving MEP maintains a MEP database with the MAC addresses of the remote MEPs with which it expects to maintain connectivity checking. The MEP database can be provisioned manually. If there is no CCM from a monitored remote MEP in a preconfigured period, the local MEP raises an alarm.

For more information on ETH-CFM continuity checking, see ETH-CFM (802.1ag) on page 337.

Configuring ETH-CFM Parameters

The following example displays an 802.1ag configuration. The first set of commands occurs at the global level. The second set occurs at the Epipe service level.

```
*A:ALU-1>config>eth-cfm# info
----------------------------------------------
        domain 1 name "kanata_MD" level 5
            association 1 format string name "kanata_MA"
                bridge-identifier 2
                exit
                ccm-interval 60
                remote-mepid 125
            exit
        exit
----------------------------------------------

*A:ALU-1>config>service>epipe# info
----------------------------------------------
            shutdown
            sap 1/5/1 create
                eth-cfm
                    mep 1 domain 1 association 1 direction down
                        shutdown
                    exit
                exit
            exit
            spoke-sdp 1:11 create
                eth-cfm
                    mep 2 domain 1 association 1 direction down
                        shutdown
                    exit
                exit
            exit
----------------------------------------------
```

Applying ETH-CFM Parameters

Apply ETH-CFM parameters to a SAP and a spoke SDP on an Epipe, as shown below.

In Release 2.1, the 7705 SAR only supports MEPs in the down MEP direction. In addition, the MAC address for a MEP on an Epipe cannot be changed. For a MEP on a SAP, the MAC address is the port MAC address. For a MEP on a spoke SDP, the MAC address is the system MAC address.

CLI Syntax:

```
config>service>epipe>sap
eth-cfm
     mep mep-id domain md-index association ma-index
        [direction {up |down}]
        ccm-enable
        ccm-ltm-priority priority
        low-priority-defect {allDef | macRemErrXcon |
          remErrXcon | errXcon | xcon | noXcon}
        [no] shutdown
```

CLI Syntax:

```
config>service>epipe>spoke-sdp
eth-cfm
     mep mep-id domain md-index association ma-index
        [direction {up |down}]
        ccm-enable
        ccm-ltm-priority priority
        low-priority-defect {allDef | macRemErrXcon |
          remErrXcon | errXcon | xcon | noXcon}
        [no] shutdown
```

CLI Syntax:

```
oam
     eth-cfm linktrace ieee-address mep mep-id domain md-
        index association ma-index [ttl ttl-value]
     eth-cfm loopback ieee-address mep mep-id domain md-
        index association ma-index [send-count send-count]
        [size size][priority priority]
```

Global Service Command Reference

Command Hierarchies

- Global Service Configuration Commands
  - → Customer Commands
  - → SDP Commands
  - → SAP Commands
  - → ETH-CFM 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
        — ipipe
            — sap sap-id [create]
            — no sap sap-id
        — ies
            — interface ip-int-name [create]
                — sap sap-id [create]
                — no sap sap-id
```

ETH-CFM Commands

```
config
    — eth-cfm
        — domain md-index [format {dns | mac | string}] name md-name level level
        — no domain md-index
            — association ma-index [format {integer | string | vid | vpn-id}] name ma-name
            — no association ma-index
                — [no] bridge-identifier bridge-id
                    — vlan vlan-id
                    — no vlan
                — ccm-interval {10ms | 100ms | 1 | 10 | 60 | 600}
                — no ccm-interval
                — [no] remote-mepid mep-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]
```

Command Descriptions

- Global Service Configuration Commands on page 79
- Show Commands on page 96

Global Service Configuration Commands

Generic Commands

description

Syntax **description** *description-string*
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 *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.

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** *customer-id* [**create**]
no customer *customer-id*

Context config>service

Description 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.

Each *customer-id* must be unique and the **create** keyword must follow each new **customer** *customer-id* entry.

To edit a customer's parameters, enter the existing **customer** *customer-id* without the **create** keyword.

Default **customer 1** always exists on the system and cannot be deleted.

The **no** form of this command removes a *customer-id* and all associated information. Before removing a *customer-id*, all references to that customer in all services must be deleted or changed to a different customer ID.

Parameters *customer-id* — specifies the ID number to be associated with the customer, expressed as an integer

Values 1 to 2147483647

contact

Syntax **contact** *contact-information*
no contact

Context config>service>customer

Description 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.

The **no** form of this command removes the contact information from the customer ID.

Default No contact information is associated with the *customer-id*.

Parameters *contact-information* — 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.

phone

Syntax [**no**] **phone** *phone-number*

Context config>service>customer

Description This command adds telephone number information for a customer ID.

The **no** form of this command removes the phone number value from the customer ID.

Default No telephone number information is associated with a customer.

Parameters *phone-number* — 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** *sdp-id* [**gre** | **mpls**] [**create**]
no sdp *sdp-id*

Context config>service

Description This command creates or edits an SDP. SDPs must be explicitly configured.

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.

The 7705 SAR supports both generic routing encapsulation (GRE) and multiprotocol label switching (MPLS) tunnels. 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.

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.

If *sdp-id* 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.

If *sdp-id* 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 *sdp-id*, an error is generated and the context of the CLI is not changed to the specified *sdp-id*.

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 *sdp-id* does not exist, an error is generated.

Default **none**

Parameters *sdp-id* — the SDP identifier

Values 1 to 17407

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.

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.

adv-mtu-override

Syntax [**no**] **adv-mtu-override**

Context config>service>sdp

Description 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.

The **no** form of this command disables the VC-type MTU override.

Default **no adv-mtu-override**

far-end

Syntax **far-end** *ip-address*
no far-end

Context config>service>sdp

Description 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.

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.

If the SDP uses GRE for the destination encapsulation, the local 7705 SAR might not know whether the *ip-address* is actually a system IP interface address on the far-end service router.

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.

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**).

The **no** form of this command removes the currently configured destination IP address for the SDP. The *ip-address* 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 *lsp-name* associations with the SDP to be removed.

Default **none**

Parameters *ip-address* — the system address of the far-end 7705 SAR for the SDP

Values a.b.c.d

ldp

Syntax [**no**] **ldp**

Context config>service>sdp

Description This command enables LDP-signaled LSPs on MPLS-encapsulated SDPs.

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.

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.

Default **no ldp** (disabled)

lsp

Syntax [**no**] **lsp** *lsp-name*

Context config>service>sdp

Description This command creates an association between an LSP and an MPLS SDP. This command is implemented only on MPLS-type encapsulated SDPs.

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.

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.

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 *lsp-name* may be shut down, causing the association with the SDP to be operationally down (the LSP will not be used by the SDP).

LSP SDPs also require that the TLDP signaling be specified and that the SDP keepalive parameter be enabled and not timed out.

The **no** form of this command deletes an LSP association from an SDP. If the *lsp-name* does not exist as an association or as a configured LSP, no error is returned. An *lsp-name* must be removed from all SDP associations before the *lsp-name* can be deleted from the system. The SDP must be administratively disabled (**shutdown)** before the last *lsp-name* association with the SDP is deleted.

Default No LSP names are defined.

Parameters *lsp-name* — 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 *lsp-name* does not already exist as a defined LSP, an error message is generated. If the *lsp-name* does exist and the LSP **to** IP address matches the SDP **far-end** IP address, the association is created.

metric

Syntax **metric** *metric*
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 *metric* — specifies the SDP metric

Values 1 to 17407

path-mtu

Syntax **path-mtu** *bytes*
no path-mtu

Context config>service>sdp

Description This command configures the Maximum Transmission Unit (MTU) in bytes that the SDP can transmit to the far-end router without packet dropping or IP fragmentation overriding the default SDP-type path MTU.

The default SDP-type **path-mtu** can be overridden on a per-SDP basis.

Dynamic maintenance protocols on the SDP may override this setting.

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.

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.

Default The default **path-mtu** defined on the system for the type of SDP is used.

Parameters *bytes* — specifies the number of bytes in the path MTU

Values 576 to 9194

signaling

Syntax **signaling** {**off** | **tldp**}

Context config>service>sdp

Description 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.

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.

Default **tldp**

Parameters **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).

tldp — ingress and egress signaling auto-labeling is enabled

vlan-vc-etype

Syntax **vlan-vc-etype** *0x0600..0xffff*
no vlan-vc-etype [*0x0600..0xffff*]

Context config>service>sdp

Description 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.

Default **no vlan-vc-etype** *(0x8100)*

Parameters *0x0600..0xffff* — 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 *orig-sdp-id* (1)	Orig-SDP Non-Existent	Down
keepalive request not sent due to administratively down *orig-sdp-id*	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** *seconds*
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** *seconds* value to the default setting.

Parameters *seconds* — the time period in seconds between SDP keepalive messages, expressed as a decimal integer

Default 10

Values 1 to 3600

hold-down-time

Syntax **hold-down-time** *seconds*
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 *sdp-id* will immediately be brought operationally down. If a keepalive response is received that indicates the error has cleared, the *sdp-id* 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 *seconds* — the time in seconds, expressed as a decimal integer, the *sdp-id* 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 *sdp-id*.

Default 10

Values 0 to 3600

max-drop-count

Syntax **max-drop-count** *count*
no max-drop-count

Context config>service>sdp>keep-alive

Description 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.

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.

The **no** form of this command reverts the **max-drop-count** *count* value to the default settings.

Parameters *count* — 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** *octets*
no message-length

Context config>service>sdp>keep-alive

Description This command configures the size of SDP monitoring keepalive request messages transmitted on the SDP.

The **no** form of this command reverts the **message-length** *octets* value to the default setting.

Parameters *octets* — 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

ETH-CFM Configuration Commands

eth-cfm

Syntax **eth-cfm**

Context config

Description This command enables the context to configure 802.1ag Connectivity Fault Management (CFM) parameters.

domain

Syntax **domain** *md-index* [**format** {**dns** | **mac** | **string**}] **name** *md-name* **level** *level*
no domain *md-index*

Context config>eth-cfm

Description This command configures CFM domain parameters.

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

Parameters *md-index* — specifies the Maintenance Domain (MD) index value

Values 1 to 4294967295

format {**dns | mac | string**} **—** specifies a value that represents the type (format)

dns: specifies the DNS name format

mac: X:X:X:X:X:X-u

X: [0 to FF] hex

u: [0 to 65535] decimal

string: specifies an ASCII string

Default string

md-name **—** specifies a generic Maintenance Domain (MD) name

Values 1 to 43 characters

level **—** specifies the integer identifying the maintenance domain level (MD level). Higher numbers correspond to higher-level maintenance domains (those with the greatest physical reach) with the highest values for customers' CFM packets. Lower numbers correspond to lower-level maintenance domains (those with more limited physical reach) with the lowest values for single bridges or physical links.

Values 0 to 7

association

Syntax **association** *ma-index* [**format** {**integer** | **string** | **vid** | **vpn-id**}] **name** *ma-name*
no association *ma-index*

Context config>eth-cfm>domain

Description This command configures the Maintenance Association (MA) for the domain.

Parameters *ma-index* — specifies the MA index value

Values 1 to 4294967295

format {integer | string | vid | vpn-id} — specifies a value that represents the type (format)

integer: 0 to 65535 (integer value 0 means the MA is not attached to a VID)

string: raw ASCII

vid: 0 to 4095

vpn-id: RFC 2685, Virtual Private Networks Identifier

xxx:xxxx, where x is a value between 00 and FF (for example 00164D:AABBCCDD)

Default integer

ma-name **—** specifies the part of the maintenance association identifier that is unique within the maintenance domain name

Values 1 to 45 characters

bridge-identifier

Syntax [**no**] **bridge-identifier** *bridge-id*

Context config>eth-cfm>domain>association

Description This command configures the service ID for the domain association. The *bridge-id* should be configured to match the *service-id* of the service where MEPs for this association will be created. For example, for Epipe service-id 2, set the bridge-id to 2. Note that there is no verification that the service with a matching *service-id* exists.

Parameters *bridge-id* — specifies the bridge ID for the domain association

Values 1 to 2147483647

vlan

Syntax **vlan** *vlan-id*
no vlan

Context config>eth-cfm>domain>association>bridge-identifier

Description This command configures the bridge-identifier primary VLAN ID. Note that it is informational only, and no verification is done to ensure that MEPs on this association are on the configured VLAN.

Parameters *vlan-id* — specifies a VLAN ID monitored by MA

Values 0 to 4094

ccm-interval

Syntax **ccm-interval** {**10ms** | **100ms** | **1** | **10** | **60** | **600**}
no ccm-interval

Context config>eth-cfm>domain>association

Description This command configures the CCM transmission interval for all MEPs in the association, in milliseconds and seconds.

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

Default **10 seconds**

remote-mepid

Syntax [**no**] **remote-mepid** *mep-id*

Context config>eth-cfm>domain>association

Description This command configures the remote maintenance association endpoint MEP identifier.

Parameters *mep-id* — maintenance association endpoint identifier of a remote MEP whose information from the MEP database is to be returned

Values 1 to 8191

Show Commands

customer

Syntax **customer** *customer-id*

Context show>service

Description This command displays service customer information.

Parameters *customer-id* — displays only information for the specified customer ID

Default all customer IDs display

Values 1 to 2147483647

Output The following output is an example of customer information, and Table 9 describes the fields.

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#
```

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

sdp

Syntax **sdp** [*sdp-id* | **far-end** *ip-address*] [**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 *sdp-id* — the SDP ID for which to display information

Default all SDPs

Values 1 to 17407

ip-address — displays only SDPs matching with the specified far-end IP address

Default SDPs with any far-end IP address

detail — displays detailed SDP information

Default SDP summary output

keep-alive-history — displays the last fifty SDP keepalive events for the SDP

Default SDP summary output

Output The following output is an example of service SDP information, and Table 10 describes the fields.

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#
```

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

Table 10: Show Service SDP Output Fields (Continued)

Label	Description
Opr Oper State	Specifies the operating state of the SDP
Deliver Delivery	Specifies the type of delivery used by the SDP: GRE or MPLS
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

Table 10: Show Service SDP Output Fields (Continued)

Label	Description
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
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

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 — thsse virtual circuit identifier

Values 1 to 4294967295

ip-address — displays only services matching with the specified far-end IP address

Default services with any far-end IP address

Output The following output is an example of service SDP-using information, and Table 11 describes the fields.

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#
```

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
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

service-using

Syntax **service-using** [**epipe**] [**apipe**] [**cpipe**] [**sdp** *sdp-id*] [**customer** *customer-id*]

Context show>service

Description This command displays the services matching certain usage properties.

If no optional parameters are specified, all services defined on the system are displayed.

Parameters **epipe** — displays matching Epipe services

apipe — displays matching Apipe services

cpipe — displays matching Cpipe services

sdp-id — displays only services bound to the specified SDP ID

Default services bound to any SDP ID

Values 1 to 17407

customer-id — displays services only associated with the specified customer ID

Default services associated with a customer

Values 1 to 2147483647

Output The following outputs are examples of service-using information, and Table 12 describes the fields.

Sample Output all services used in system

```
*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 services by service type (epipe)

```
*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#
```

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

Table 12: Show Service service-using Output Fields (Continued)

Label	Description
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

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

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:

- Common Configuration Tasks on page 164
- Configuring VLL Components on page 165
  - → Creating an Apipe Service on page 165
- Service Management Tasks on page 185

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 10). 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.

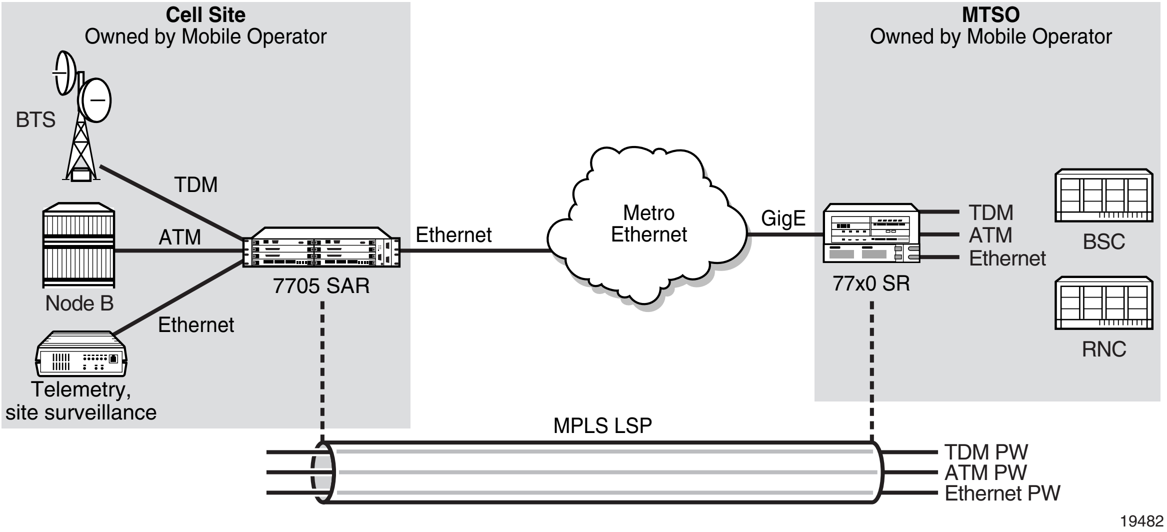
The 7705 SAR receives standard UNI/NNI cells on the ATM service access point (SAP), which are then encapsulated into a pseudowire packet using N-to-1 cell mode encapsulation in accordance with RFC 4717.

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 150 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 10: ATM VLL for End-to-End ATM Service



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 encapsulation configuration. One endpoint of a SAP connection can be an IMA group, while the other endpoint can be on a single ATM port.

ATM SAP-to-SAP connections are also supported between any two OC3/STM1 ports and between any T1/E1 ASAP port and OC3/STM1 port, as long as both SAPs support ATM.

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 and OC3/STM1 Clear Channel 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 158 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:

- Common Configuration Tasks on page 164
- Configuring VLL Components on page 165
  - → Creating a Cpipe Service on page 170
- Service Management Tasks on page 185

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). 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 × 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 (encapsulation, channel group size, and CAS).

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 × 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 × 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 with and without CAS for DS1 and E1.

When CESoPSN with CAS is selected, the ABCD bits are coded into the T1 or E1 multiframe packets, transported within the TDM PW, and reconstructed in the T1 or E1 multiframe at the far end for each timeslot.

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 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 11, 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.

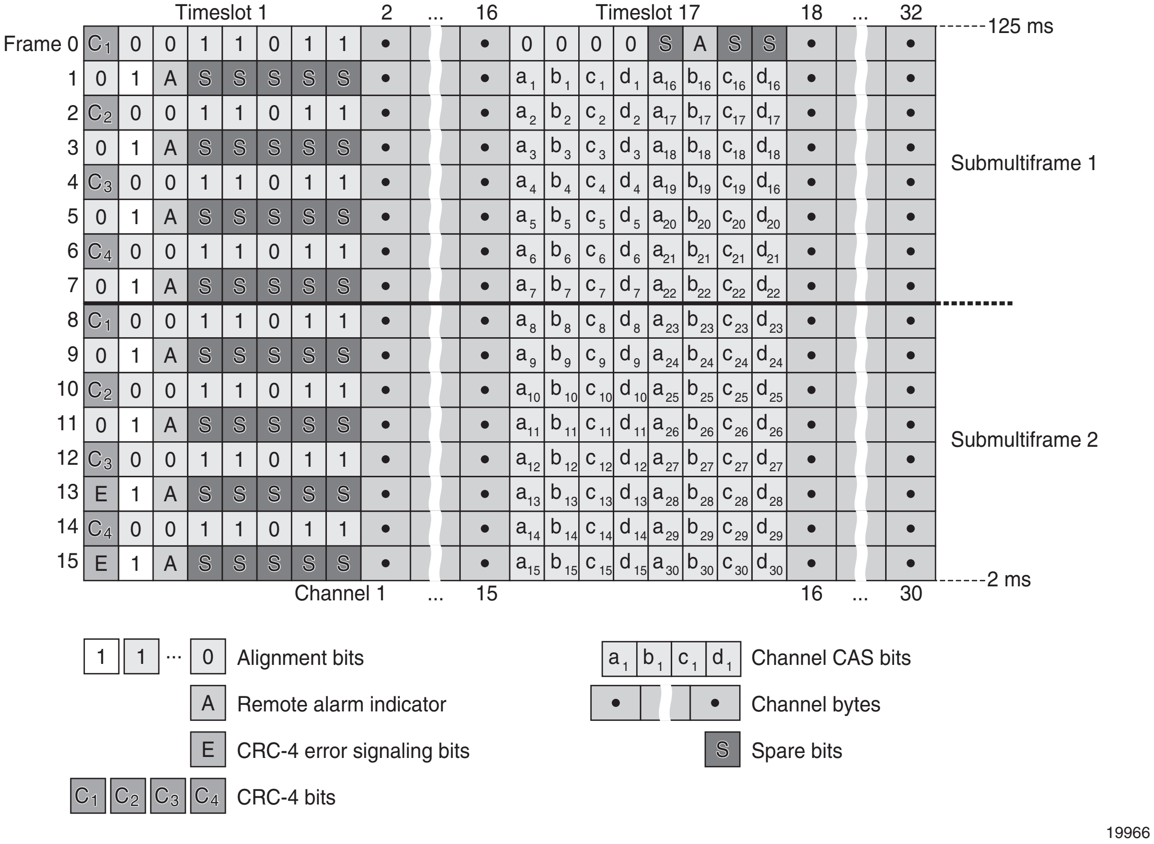
For T1 CAS, the signaling bits are transferred using Robbed Bit Signaling (RBS), where the least significant bit in the channel is used periodically to transport these bits instead of voice data.

T1 CAS is supported when ESF or SF framing is configured. ESF framing uses a 24-frame multiframe and transfers all four signaling bits (ABCD). SF framing uses a 12-frame multiframe and transfers only the AB bits. The signaling bits are carried in the least significant bit of the following frames:

- A bit in frame 6
- B bit in frame 12
- C bit in frame 18
- D bit in frame 24

Table 13 shows the structure of a T1 ESF multiframe that uses RBS. The structure of a T1 SF multiframe is based on 12 frames and only the A and B bits are available.

Figure 11: E1 Framing for CAS Support in an E1 Multiframe



	Timeslot 1								2	...	16	Timeslot 17								18	...	32
Frame 0	C_1	0	0	1	1	0	1	1	•		•	0	0	0	0	S	A	S	S	•		•
1	0	1	A	S	S	S	S	S	•		•	a_1	b_1	c_1	d_1	a_{16}	b_{16}	c_{16}	d_{16}	•		•
2	C_2	0	0	1	1	0	1	1	•		•	a_2	b_2	c_2	d_2	a_{17}	b_{17}	c_{17}	d_{17}	•		•
3	0	1	A	S	S	S	S	S	•		•	a_3	b_3	c_3	d_3	a_{18}	b_{18}	c_{18}	d_{18}	•		•
4	C_3	0	0	1	1	0	1	1	•		•	a_4	b_4	c_4	d_4	a_{19}	b_{19}	c_{19}	d_{16}	•		•
5	0	1	A	S	S	S	S	S	•		•	a_5	b_5	c_5	d_5	a_{20}	b_{20}	c_{20}	d_{20}	•		•
6	C_4	0	0	1	1	0	1	1	•		•	a_6	b_6	c_6	d_6	a_{21}	b_{21}	c_{21}	d_{21}	•		•
7	0	1	A	S	S	S	S	S	•		•	a_7	b_7	c_7	d_7	a_{22}	b_{22}	c_{22}	d_{22}	•		•
8	C_1	0	0	1	1	0	1	1	•		•	a_8	b_8	c_8	d_8	a_{23}	b_{23}	c_{23}	d_{23}	•		•
9	0	1	A	S	S	S	S	S	•		•	a_9	b_9	c_9	d_9	a_{24}	b_{24}	c_{24}	d_{24}	•		•
10	C_2	0	0	1	1	0	1	1	•		•	a_{10}	b_{10}	c_{10}	d_{10}	a_{25}	b_{25}	c_{25}	d_{25}	•		•
11	0	1	A	S	S	S	S	S	•		•	a_{11}	b_{11}	c_{11}	d_{11}	a_{26}	b_{26}	c_{26}	d_{26}	•		•
12	C_3	0	0	1	1	0	1	1	•		•	a_{12}	b_{12}	c_{12}	d_{12}	a_{27}	b_{27}	c_{27}	d_{27}	•		•
13	E	1	A	S	S	S	S	S	•		•	a_{13}	b_{13}	c_{13}	d_{13}	a_{28}	b_{28}	c_{28}	d_{28}	•		•
14	C_4	0	0	1	1	0	1	1	•		•	a_{14}	b_{14}	c_{14}	d_{14}	a_{29}	b_{29}	c_{29}	d_{29}	•		•
15	E	1	A	S	S	S	S	S	•		•	a_{15}	b_{15}	c_{15}	d_{15}	a_{30}	b_{30}	c_{30}	d_{30}	•		•
							Channel 1			...	15									16	...	30

Table 13: T1 Framing for CAS (RBS) Support in a T1 ESF Multiframe

Frame Number	F Bit				Bit Numbers in Each Channel Timeslot		Signaling Channel Designation (4)
	Bit Number within Multiframe	Assignments					
		FAS (1)	DL (2)	CRC (3)	For Character Signal (4)	For Signaling (4)	
1	1	–	m	–	1-8	–	
2	194	–	–	e1	1-8	–	
3	387	–	m	–	1-8	–	
4	580	0	–	–	1-8	–	
5	773	–	m	–	1-8	–	
6	966	–	–	e2	1-7	8	A
7	1159	–	m	–	1-8	–	
8	1352	0	–	–	1-8	–	
9	1545	–	m	–	1-8	–	
10	1738	–	–	e3	1-8	–	
11	1931	–	m	–	1-8	–	
12	2124	1	–	–	1-7	8	B
13	2317	–	m	–	1-8	–	
14	2510	–	–	e4	1-8	–	
15	2703	–	m	–	1-8	–	
16	2896	0	–	–	1-8	–	
17	3089	–	m	–	1-8	–	
18	3282	–	–	e5	1-7	8	C
19	3475	–	m	–	1-8	–	
20	3668	1	–	–	1-8	–	
21	3861	–	m	–	1-8	–	
22	4054	–	–	e6	1-8	–	
23	4247	–	m	–	1-8	–	
24	4440	1	–	–	1-7	8	D

Notes:
1. FAS = frame alignment signal (....001011.....)
2. DL = 4 kb/s data link (m represents message bits)
3. CRC = CRC-6 block check field (e1 to e6 represent check bits)
4. Only applicable for CAS

TDM PW Encapsulation

TDM circuits are MPLS-encapsulated as per RFC 4533 (SAToP) and RFC 5086 (CESoPSN) (see Figure 12 and Figure 13).

Figure 12: SAToP MPLS Encapsulation

```
0               1               2               3
     0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |                           ...                                 |
    |                    MPLS Label Stack                           |
    |                           ...                                 |
    +=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
    |                   SAToP Control Word                          |
    +=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
    |                       OPTIONAL                                |
    +--                                                           --+
    |                                                               |
    +--                                                           --+
    |                 Fixed RTP Header (see [RFC 3550])             |
    +=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
    |                  Packetized TDM data (Payload)                |
    |                            ...                                |
    |                            ...                                |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 13: CESoPSN MPLS Encapsulation

```
 0               1               2               3
     0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |                           ...                                 |
    |                    MPLS Label Stack                           |
    |                           ...                                 |
    +=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
    |                  CESoPSN Control Word                         |
    +=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
    |                       OPTIONAL                                |
    +--                                                           --+
    |                                                               |
    +--                                                           --+
    |                 Fixed RTP Header (see [RFC 3550])             |
    +=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
    |                  Packetized TDM data (Payload)                |
    |                            ...                                |
    |                            ...                                |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

For GRE tunnels, the same encapsulations shown in Figure 13 are used, but GRE tunnel headers are used instead of MPLS tunnel headers.

Figure 14 shows the format of the CESoPSN TDM payload (with and without CAS) for packets carrying trunk-specific n × 64 kb/s service.

Figure 14: CESoPSN Packet Payload Format for Trunk-Specific n x 64 kb/s (with and without CAS transport)

```
              0 1 2 3 4 5 6 7                               0 1 2 3 4 5 6 7
  ---------- +-+-+-+-+-+-+-+-+                ---------- +-+-+-+-+-+-+-+-+
             |   Timeslot 1  |                           |   Timeslot 1  |
             +-+-+-+-+-+-+-+-+                           +-+-+-+-+-+-+-+-+
             |   Timeslot 2  |                           |   Timeslot 2  |
Frame #1     |      ...      |              Frame #1     |      ...      |
             |   Timeslot n  |                           |   Timeslot n  |
  ---------- +-+-+-+-+-+-+-+-+                ---------- +-+-+-+-+-+-+-+-+
  ---------- +-+-+-+-+-+-+-+-+                ---------- +-+-+-+-+-+-+-+-+
             |   Timeslot 1  |                           |   Timeslot 1  |
             +-+-+-+-+-+-+-+-+                           +-+-+-+-+-+-+-+-+
             |   Timeslot 2  |                           |   Timeslot 2  |
Frame #2     |      ...      |              Frame #2     |      ...      |
             |   Timeslot n  |                           |   Timeslot n  |
  ---------- +-+-+-+-+-+-+-+-+                ---------- +-+-+-+-+-+-+-+-+
...          |      ...      |              ...          |      ...      |
  ---------- +-+-+-+-+-+-+-+-+                ---------- +-+-+-+-+-+-+-+-+
             |   Timeslot 1  |                           |   Timeslot 1  |
             +-+-+-+-+-+-+-+-+                           +-+-+-+-+-+-+-+-+
             |   Timeslot 2  |                           |   Timeslot 2  |
Frame #m     |      ...      |              Frame #m     |      ...      |
             |   Timeslot n  |                           |   Timeslot n  |
  ---------- +-+-+-+-+-+-+-+-+                ---------- +-+-+-+-+-+-+-+-+
Nibbles 1,2  |A B C D|A B C D|
  ---------- +-+-+-+-+-+-+-+-+
Nibbles 3,4  |A B C D|A B C D|
  ---------- +-+-+-+-+-+-+-+-+
Nibble n     |A B C D| (pad) |
(odd) & pad  +-+-+-+-+-+-+-+-+


     (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 24 for T1 or 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 T1/E1 CES with CAS on page 122 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 × 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 T1/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 64 and 1514 octets and must be a multiple of 32. The payload packet size affects the packet efficiency and packetization delay. Table 14 shows the default values for packet size and packetization delay. See Packet Payload Size on page 124 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 14: 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 × 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 15 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 µs.

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

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

Table 15 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 ≤ N ≤ 4, the default is 32 frames/packet
- for 5 ≤ N ≤ 15, the default is 16 frames/packet
- for N ≥ 16, the default is 8 frames/packet

Table 15: Default and Minimum Payload Size for CESoPSN without CAS

	Default Values			Minimum Values		
Number of Timeslots (N)	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

Table 15: 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)
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
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 T1/E1 CES with CAS

Structured circuit emulation with CAS is supported for T1 and E1 circuits.

Structured CES with CAS service is configured by choosing `cesopsn-cas` as the `vc-type` when creating a Cpipe service. The DS1 or 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 DS1 or E1 with CAS. Refer to the 7705 SAR OS Interface Configuration Guide for information on configuring signal mode.

For n × 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 16 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 14 to see the structure of the CES with CAS payload.

CES fragmentation is not supported.

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.

Table 16: Payload Size for T1 and E1 CESoPSN with CAS

Number of Timeslots	T1			E1		
	Number of Frames per Packet	Payload Size (Octets)	Packetization Delay (ms)	Number of Frames per Packet	Payload Size (Octets)	Packetization Delay (ms)
1	24	24	3.00	16	16	2.00
2	24	48	3.00	16	32	2.00
3	24	72	3.00	16	48	2.00
4	24	96	3.00	16	64	2.00
5	24	120	3.00	16	80	2.00
6	24	144	3.00	16	96	2.00
7	24	168	3.00	16	112	2.00
8	24	192	3.00	16	128	2.00
9	24	216	3.00	16	144	2.00
10	24	240	3.00	16	160	2.00
11	24	264	3.00	16	176	2.00
12	24	288	3.00	16	192	2.00
13	24	312	3.00	16	208	2.00
14	24	336	3.00	16	224	2.00
15	24	360	3.00	16	240	2.00
16	24	384	3.00	16	256	2.00
17	24	408	3.00	16	272	2.00
18	24	432	3.00	16	288	2.00
19	24	456	3.00	16	304	2.00
20	24	480	3.00	16	320	2.00
21	24	504	3.00	16	336	2.00
22	24	528	3.00	16	352	2.00
23	24	552	3.00	16	368	2.00

Table 16: Payload Size for T1 and E1 CESoPSN with CAS (Continued)

Number of Timeslots	T1			E1		
	Number of Frames per Packet	Payload Size (Octets)	Packetization Delay (ms)	Number of Frames per Packet	Payload Size (Octets)	Packetization Delay (ms)
24	24	576	3.00	16	384	2.00
25	NA	NA	NA	16	400	2.00
26	NA	NA	NA	16	416	2.00
27	NA	NA	NA	16	432	2.00
28	NA	NA	NA	16	448	2.00
29	NA	NA	NA	16	464	2.00
30	NA	NA	NA	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 1 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 ≤ N ≤ 4, the default is 16 ms
- for 5 ≤ N ≤ 15, the default is 8 ms
- for N ≥ 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 15. Table 17 describes the bit fields. Refer to Pseudowire Control Word on page 158 for more information.

Figure 15: Control Word Bit Structure

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|0|0|0|0|L|R| M |FRG|    LEN    |       Sequence number         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Table 17: 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.

Table 17: Control Word Bit Descriptions (Continued)

Bit(s)	Description
M (Modifier)	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: • When L bit = 0, and 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 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, 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
    - → Ethernet SAP-to-SAP
    - → Control Word
    - → MTU
    - → Raw and Tagged Modes
    - → IP Filters
    - → ETH-CFM (802.1ag)

Epipe configuration information is found under the following topics:

- Common Configuration Tasks on page 164
- Configuring VLL Components on page 165
    - → Creating an Epipe Service on page 173
- Service Management Tasks on page 185

Epipe Service Overview

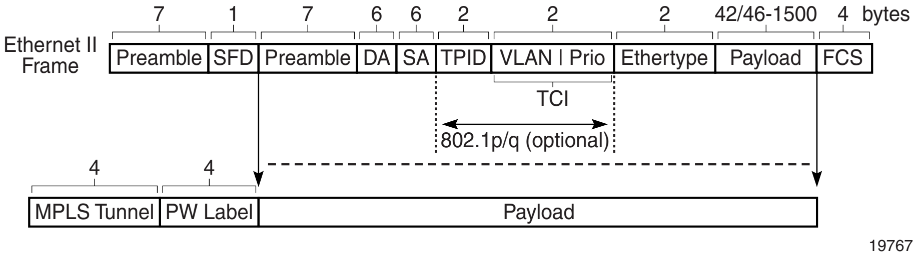
An Ethernet pseudowire (PW) is used to carry Ethernet/802.3 protocol data units (PDUs) over an MPLS or IP network, allowing service providers to offer emulated Ethernet services over existing MPLS or IP networks. For the 7705 SAR, Ethernet emulation is a point-to-point service.

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

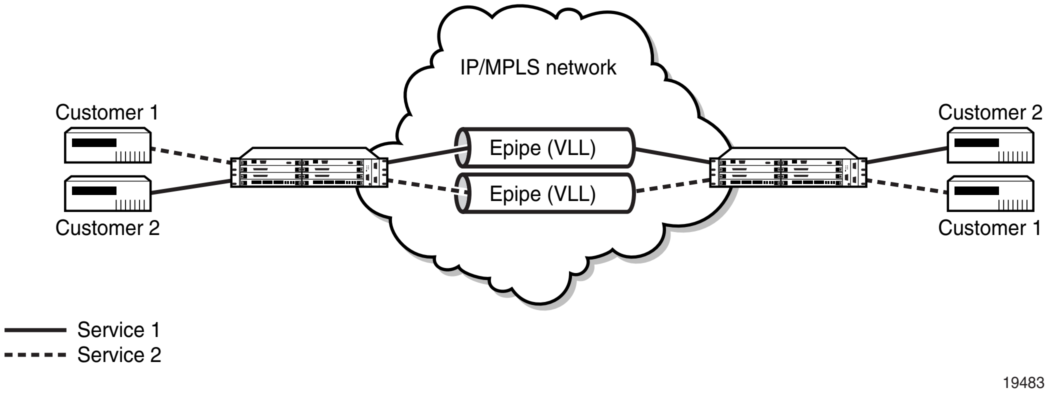
Figure 16: Ethernet VLL Frame with MPLS Encapsulation



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 a 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 17: 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.

Ethernet SAP-to-SAP

Ethernet VLLs can be configured with both endpoints (SAPs) on the same 7705 SAR. This is referred to as Ethernet SAP-to-SAP or local Ethernet service. Ethernet SAP-to-SAP provides local Ethernet switching between two Ethernet endpoints on the 7705 SAR.

An Ethernet SAP-to-SAP connection is set up on the 7705 SAR and a pseudowire is configured between the two endpoints.

When the port encapsulation is null, there is no change to the VLAN tags on the ingress and egress frame headers, if VLAN tags are present.

When the port encapsulation is dot1q, the VLAN tag is removed from the ingress frame header and a new VLAN tag is inserted into the egress frame header. No VLAN tag is inserted into the egress frame header if the SAP has a VLAN ID of 0.

Control Word

Ethernet VLL supports an optional control word (CW). Refer to Pseudowire Control Word on page 158 for more information.

MTU

The largest maximum transmission unit (MTU) supported on an Ethernet port is 2012 bytes for null encapsulated ports and 2106 bytes for dot1q encapsulated ports. 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 154 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 20 (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 18 and Table 19 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 2.1 of the 7705 SAR.

Table 18: 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 19: Egress SAP Tagging Rules

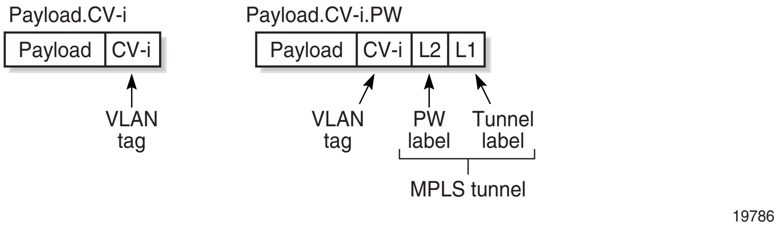
Egress SAP Type (1)	VC Type (Epipe)	
	Raw (Ethernet)	**Tagged (VLAN)**
Null	No operation	Pop (VC tag)
Dot1q	Push (SAP tag) (2)	Pop (VC tag) Push (SAP tag) (3)

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 20 shows the VLAN ID translation operation (from ingress to egress) for the various packet types. In Table 20, 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 18 shows two examples using the more familiar representation of a packet format, where the packet starts on the right-hand side.

Figure 18: Ethernet Frame Representations



➡ **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 20: 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

IP Filters

In Release 2.1 of the 7705 SAR, IP filters are applied to ingress pseudowire SAPs (Epipes and Ipipes) as well as to ingress network interfaces and Management SAPs.

Ethernet pseudowires are generally used to transparently switch traffic across an MPLS network to the far end. However, in some cases, the traffic that is switched over the network, consuming valuable bandwidth, is just discarded at the other end of the pseudowire. As well, with the 7705 SAR expanding into areas such as vertical markets, and with local area networks being connected to the 7705 SAR Ethernet ports, an increasing amount of traffic must stay local and not pass through the MPLS network to the far end. By using IP filters at the access ingress, operators can determine what traffic is passed through the pseudowire and therefore use the network links more efficiently.

IP filters can also be used for security purposes, by allowing access only to designated services (for example, allowing e-mail and FTP services while disallowing Telnet services) at the origin of the traffic.

IP filter policies specify either a forward or a drop action for packets, based on information specified in the match criteria. You can create up to 16 IP unique filter policies per adapter card and up to 96 IP filters per node. Within each filter policy, you can create up to 64 matching entries.

The filters for the adapter cards are assigned to the network interfaces, the IP pseudowires, and the Ethernet pseudowires. A filter can be assigned to multiple entities of the same type but cannot be assigned to different entities on the same card (with the exception of network interfaces). The filter can be assigned to any entity on another adapter card.

For example, a filter policy defined as filter-5 can be applied to numerous IP pseudowires on an adapter card but cannot be applied to Ethernet pseudowires or to network interfaces on that card. Because up to 16 unique filter policies are supported per card, using the same filter policy multiple times on entities of the same type counts as using one filter policy (leaving 15 more policies per card). The filter policy defined as filter-5 can also be used on any entity on another adapter card.

Configuration of filter policies is similar for network interfaces, Management SAPs, and Ethernet and IP pseudowire SAPs. This guide describes the assignment of filter policies to SAPs. Refer to the 7705 SAR OS Router Configuration Guide for information on configuring filter policies and assigning them to network interfaces.

ETH-CFM (802.1ag)

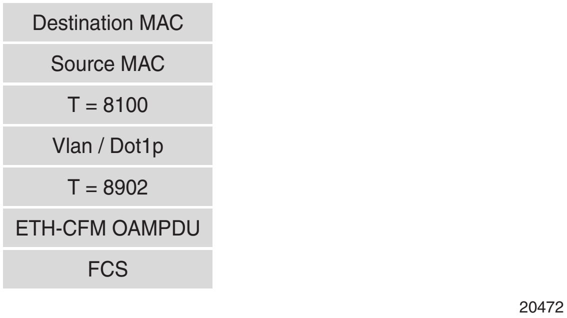
The 7705 SAR conforms to the IEEE 802.1ag (dot1ag) standard for Ethernet Connectivity Fault Management (ETH-CFM). Dot1ag CFM OAMPDUs use a standard Ethernet frame. The following ETH-CFM (802.1ag) topics are discussed:

- Dot1ag CFM Frame Format
- MEP Support on Ethernet SAPs
- MEP Support on Ethernet Spoke SDPs
- Loopback (LB)
- Linktrace (LT)
- Continuity Check (CC)

Dot1ag CFM Frame Format

Figure 19 shows the dot1ag CFM frame format. The parts of the frame are described below.

Figure 19: Dot1ag CFM Frame Format



Source and Destination Addresses

The source and destination MAC addresses of the CFM message must match at the send and the receive routers. For example, in Figure 23 (Dot1ag Down MEPs on Spoke SDPs), a 7705 SAR-initiated CFM message would have the spoke SDP MAC address of the 7705 SAR as the source MAC address and the spoke SDP MAC address of SR as the destination MAC address.

An exception to the matching source-destination MAC address requirement occurs for trace and continuity messages, where the destination MAC address is set to a multicast group address. The designated multicast group address for CCM and linktrace is 01-80-C2-00-00-3*x*; where *x* represents the maintenance domain (MD) number. For example, a CCM message destined for 01-80-C2-00-00-31 corresponds to MD level 1.

CCM packets using source-destination multicast MAC addresses are for user-initiated messages only (that is, loopbacks).

Ethertype (T)

If dot1q encapsulation is not configured, then the Ethertype value is 8902 and there is no VLAN tag. If dot1q encapsulation is configured, the VLAN tag (Ethertype value 8100) is present and is followed by the Ethertype value of 8902, which indicates CFM messages.

VLAN/dot1p

This is the VLAN dot1p identifier. If null encapsulation is configured (for Ethernet SAPs or spoke-SDP bindings to a VC-type [ether or vlan]), the frame will be tagged with NULL.

Ethernet dot1ag CFM OAMPDU

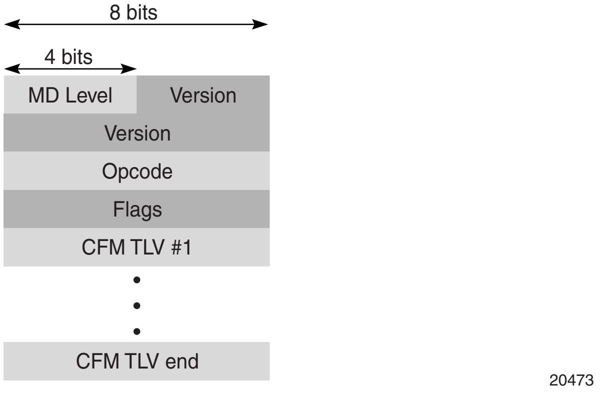
As shown in Figure 20, each dot1ag CFM OAMPDU contains the following fields:

- maintenance domain (MD) level: user-configured value, 0 to 7
- version: current version is 0
- opcodes: as defined in IEEE 802.1ag standard
- flags: as defined in IEEE 802.1ag standard
- one or more TLVs, which include:
  - → Continuity Check Message (CCM)
  - → Loopback Message (LBM)
  - → Loopback Reply (LBR)
  - → Linktrace Message (LTM)
  - → Linktrace Reply (LTR)

FCS

This is the frame check sequence field.

Figure 20: CFM Message



MEP Support on Ethernet SAPs

Maintenance association endpoints (MEPs) with down OAMPDU transmission direction (a down MEP) on Ethernet access ports are supported on the 7705 SAR in Release 2.1. Figure 21 shows that the 7705 SAR can terminate and respond to CFM messages received from connected devices, such as base stations, when port B is a down MEP. A CFM message coming from port A would be terminated on port B of the 7705 SAR. Conversely, port B on the 7705 SAR can generate and send a CFM message towards port A.

Figure 21: MEP on Ethernet Access

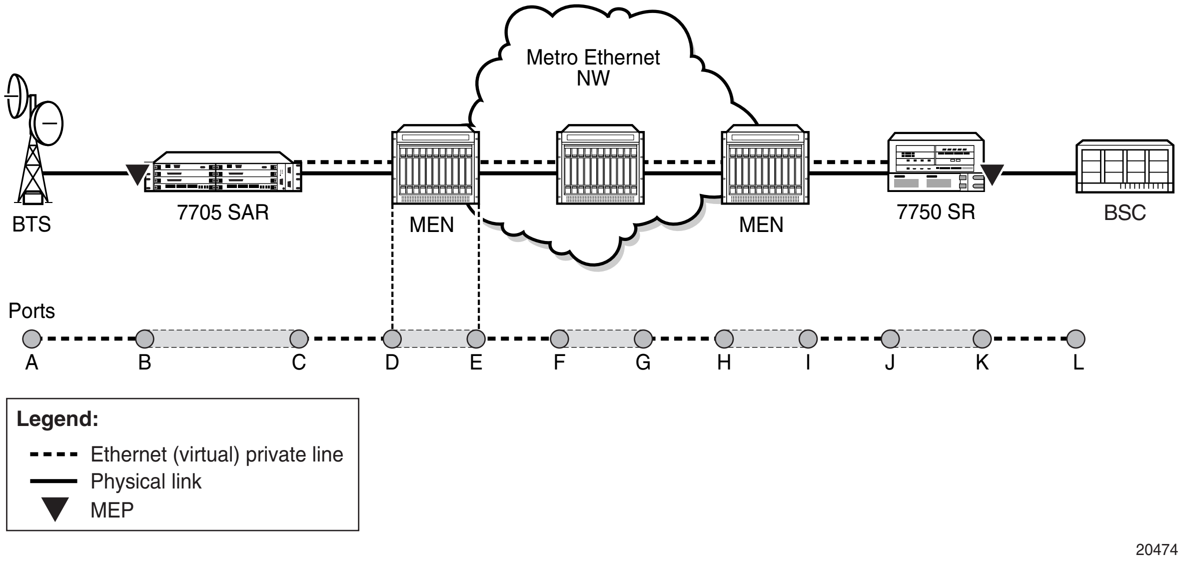
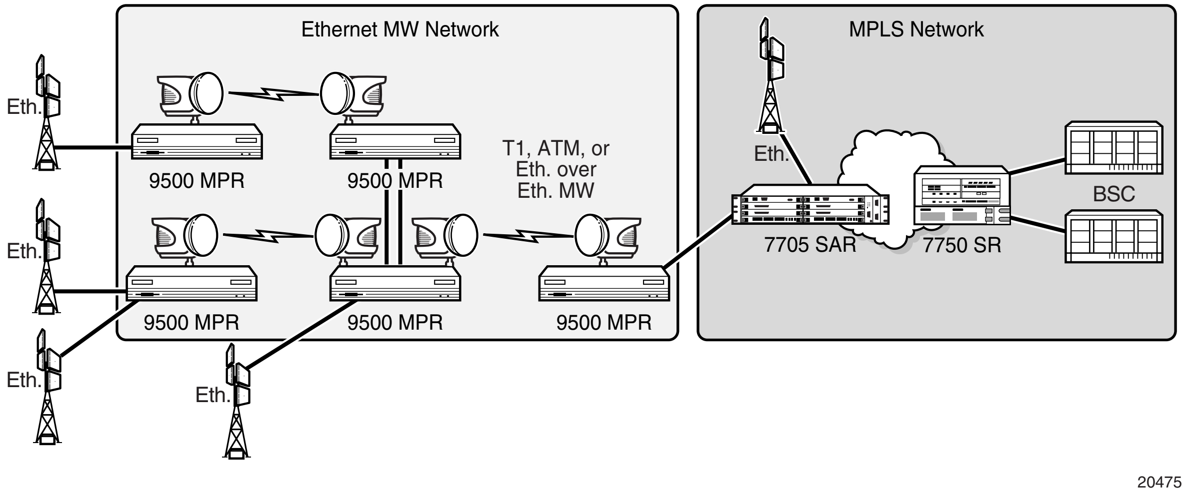


Figure 22 shows how a down MEP at an Ethernet SAP might be used. In this example, an Ethernet network connects to an access Ethernet port on the 7705 SAR and there are multiple SAPs on that port (that is, multiple endpoints). Since CFM offers OAM capabilities on a per-service basis, which in this case means per SAP (or endpoint), each service can run CFM. Note that if BSC end devices were directly connected to the 7705 SAR (and a VLAN is not used to separate services from each other), EFM would offer capabilities similar to CFM for Ethernet OAM.

In the example shown in Figure 22, separate dot1ag instances initiated on the 9500 MPR nodes can be used to ensure Ethernet layer connectivity on a per-base-station basis. All the traffic from these base stations is aggregated and switched to a single port on the 7705 SAR. Each base station is recognized through a different VLAN, where the VLANs are bound to different services. CFM with down MEP OAMPDU traffic direction at the Ethernet SAP offers the flexibility to run OAM tests on a per-base-station basis.

Figure 22: Down MEP at Ethernet SAP



MEP Support on Ethernet Spoke SDPs

Maintenance association endpoints (MEPs) on Ethernet spoke SDP endpoints are supported on the 7705 SAR. Figure 23 illustrates a MEP on an Ethernet spoke SDP.

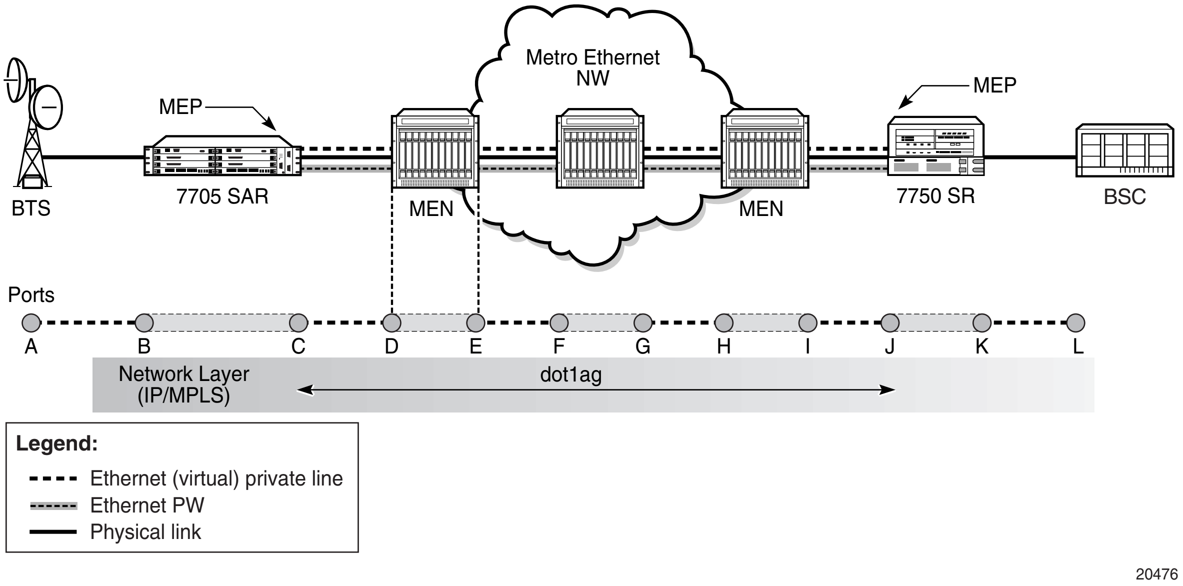
CFM messages can be generated and switched across an Ethernet PW. CFM messages that are received and have an MD that matches the value configured on the 7705 SAR are extracted and processed. Any received CFM messages with an MD level that does not match the configured value are not terminated and are switched transparently to the Ethernet SAP.

Down MEPs on Ethernet spoke SDPs on the 7705 SAR support the following:

- termination of the CFM messages destined for the MEP-ID of the 7705 SAR
- termination of CFM messages at the user-configured domain only
- discarding of OAMPDUs at a lower MD level than the configured one (an alarm message is raised)
- transparent pass-through of upper layer CFM messages
  - → MD of the CFM messages that are higher than the one configured on the 7705 SAR

Forwarding of CFM messages with the same MD level is not supported in Release 2.1 of the 7705 SAR (that is, MIP functionality). Only down MEP functionality is supported on Ethernet spoke SDP (that is, termination of CFM messages that are ingress from the Ethernet PW, or generation of CFM packets that are destined for the SR spoke SDP MEP-ID).

Figure 23: Dot1ag Down MEPs on Spoke SDPs



In Figure 23, assuming that the MEP is enabled both on the SR and the 7705 SAR spoke SDP endpoints, the 7705 SAR can generate CFM messages and can terminate any received CFM messages that are destined for the 7705 SAR MEP-ID and have a matching configured domain. Any 7705 SAR-generated CFM packets would traverse the Ethernet PW and would be processed first by the SR node. The Ethernet PW running between the 7705 SAR and the SR generates a pipe-like connectivity; thus, no intermediate Ethernet node can process the CFM messages. All the CFM messages are transported over Ethernet PWs, and PW termination only takes place on SR and 7705 SAR endpoints.

Loopback (LB)

A Loopback Message (LBM) is generated by a MEP to its peer MEP. Its function is similar to IP or MPLS ping in that it verifies Ethernet connectivity between the nodes on a per-request basis. That is, it is non-periodic and is only initiated by a user request.

For more information on ETH-CFM loopbacks, see ETH-CFM (802.1ag) on page 337 of this document.

Linktrace (LT)

A Linktrace Message (LTM) is originated by a MEP and targeted to a peer MEP in the same MA and within the same MD level. Its function is similar to IP traceroute. The peer MEP responds with a Linktrace Reply (LTR) message after successful inspection of the LTM.

For more information on ETH-CFM linktrace, see ETH-CFM (802.1ag) on page 337 of this document.

Continuity Check (CC)

A Continuity Check Message (CCM) is a multicast frame that is generated by a MEP and sent to its remote MEPs in the same MA, which assists fault isolation. The CCM does not require a reply message. To identify faults, the receiving MEP maintains a MEP database with the MAC addresses of the remote MEPs with which it expects to maintain connectivity checking. The MEP database can be provisioned manually. If there is no CCM from a monitored remote MEP in a preconfigured period, the local MEP raises an alarm.

For more information on ETH-CFM continuity checking, see ETH-CFM (802.1ag) on page 337 of this document.

IP Interworking VLL (Ipipe) Services

This section provides information about the Ipipe service.

Topics in this section include:

- Ipipe Service Overview
  - → IP Interworking VLL Datapath
  - → Control Word
  - → IP Filters

Ipipe configuration information is found under the following topics:

- Common Configuration Tasks on page 164
- Configuring VLL Components on page 165
  - → Creating an Ipipe Service on page 179
- Service Management Tasks on page 185

Ipipe Service Overview

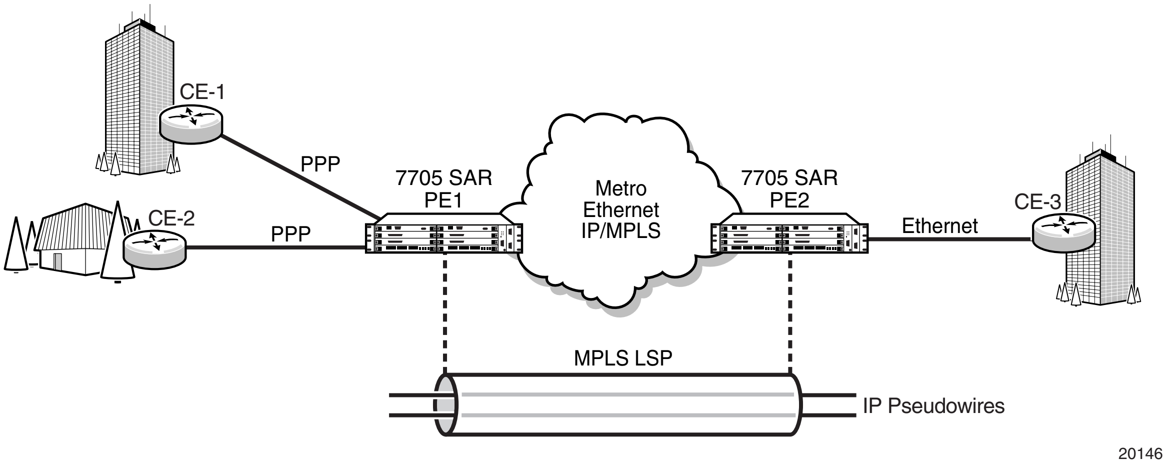
An Ipipe pseudowire (IP PW) enables service interworking between different link layer technologies and network interworking between connections with the same link layer technologies. IP PWs provide an efficient means to connect Layer 3 IP traffic to the IP/MPLS network, even without access to VLANs.

An Ipipe is a point-to-point Layer 2 service where the customer data is encapsulated and transported across an MPLS or IP network. An Ipipe service transparently forwards all packets received on one SAP to the other SAP. No native IP routing of customer packets occurs.

IP interworking allows connections to be created with any combination of PPP, MLPPP, and Ethernet SAPs, but the payload must always be IP. Ipipes can be used to transport IP payloads more efficiently than Epipes because an Ipipe service does not need to forward the Ethernet header information.

Figure 24 provides an example of IP connectivity between a host attached to a point-to-point access circuit (PPP) with routed PDU IPv4 encapsulation and a host attached to an Ethernet interface. Both hosts are on the same LAN segment.

Figure 24: IP Pseudowires Between SAR Nodes



A PPP interface makes use of RFC 1332, *The PPP Internet Protocol Control Protocol (IPCP)*, PPP IPCP encapsulation of an IPv4 packet. The PW uses the IP Layer 2 transport pseudowire encapsulation type.

IP Interworking VLL Datapath

In order to be able to forward IP packets between CE 1 and CE 3 in Figure 24, PE 2 is manually configured with both CE 1 and CE 3 IP addresses. These are host addresses and are entered in the /32 format. PE 2 maintains an ARP cache context for each IP interworking VLL and responds to ARP request messages received on the Ethernet SAP. PE 2 responds with the Ethernet SAP configured MAC address as a proxy for any ARP request for the CE 1 IP address. PE 2 silently discards any ARP request messages received on the Ethernet SAP for addresses other than CE 1. Likewise, PE 2 silently discards any ARP request messages with source IP addresses other than CE 3. In all cases, PE 2 keeps track of the association of IP to MAC addresses for ARP requests it receives over the Ethernet SAP. All entries are subject to aging.

In order to forward unicast frames destined for CE 3, PE 2 needs to know the MAC address of CE 3. If there is no entry in the ARP cache, PE 2 sends an ARP request message for the CE 3 MAC address over the Ethernet SAP.

IP broadcast and IP multicast packets are sent on the Ethernet SAP using the broadcast or direct-mapped multicast MAC address.

In order to forward unicast frames destined for CE 1, PE 2 validates the MAC destination address of the received Ethernet frame. It should match that of the Ethernet SAP. PE 2 then removes the Ethernet header and encapsulates the IP packet directly into a pseudowire with or without the optional control word. PE 1 removes the pseudowire encapsulation and forwards the IP packet over the SAP using PPP encapsulation.

When a packet reaches the access egress and the configured SAP is over a VLAN, the node pushes (inserts) the appropriate VLAN tag into the Ethernet frame header before forwarding the Ethernet frame out of the port. Ethernet frames at the access egress can also be marked with appropriate dot1 priority bits if the dot1 priority QoS profile is assigned to the forwarding class configuration.

Ethernet frames mapped to an Ipipe service can have a maximum of two VLAN tags. Frames with more than two VLAN tags are dropped at the Ipipe access ingress SAP.

At access ingress, PE 1 performs proxy PPP negotiation and provides the IP address of the remote CE 3 device to CE 1 during IPCP negotiation using the IP-Address option.

A PE does not flush the ARP cache unless the SAP goes administratively or operationally down. The PE with the Ethernet SAP sends unsolicited ARP requests to refresh the ARP cache according to the refresh interval. ARP requests are staggered at an increasing rate if no reply is received to the first unsolicited ARP request. The refresh interval is configurable using the `mac-refresh` CLI command.

Control Word

IP interworking VLL supports an optional control word (CW). Refer to Pseudowire Control Word on page 158 for more information.

IP Filters

In Release 2.1 of the 7705 SAR, IP filters are applied to ingress pseudowire SAPs (Epipes and Ipipes) as well as to ingress network interfaces and Management SAPs.

IP pseudowires are generally used to transparently switch traffic across an MPLS network to the far end. However, in some cases, the traffic that is switched over the network, consuming valuable bandwidth, is just discarded at the other end of the pseudowire. As well, with the 7705 SAR expanding into areas such as vertical markets, and with local area networks being connected to the 7705 SAR Ethernet ports, an increasing amount of traffic must stay local and not pass through the MPLS network to the far end. By using IP filters at the access ingress, operators can determine what traffic is passed through the pseudowire and therefore use the network links more efficiently.

Another use for IP filters is in cases where a customer router is connected to an access port on the 7705 SAR with ppp/mlppp encapsulation. The service provider may want to filter incoming traffic from the customer at the boundaries of the network.

IP filters can also be used for security purposes, by allowing access only to designated services (for example, allowing e-mail and FTP services while disallowing Telnet services) at the origin of the traffic.

IP filter policies specify either a forward or a drop action for packets, based on information specified in the match criteria. You can create up to 16 IP unique filter policies per adapter card and up to 96 IP filters per node. Within each filter policy, you can create up to 64 matching entries.

The filters for the adapter cards are assigned to the network interfaces, the IP pseudowires, and the Ethernet pseudowires. A filter can be assigned to multiple entities of the same type but cannot be assigned to different entities on the same card (with the exception of network interfaces). The filter can be assigned to any entity on another adapter card.

For example, a filter policy defined as filter-5 can be applied to numerous IP pseudowires on an adapter card but cannot be applied to Ethernet pseudowires or to network interfaces on that card. Because up to 16 unique filter policies are supported per card, using the same filter policy multiple times on entities of the same type counts as using one filter policy (leaving 15 more policies per card). The filter policy defined as filter-5 can also be used on any entity on another adapter card.

Configuration of filter policies is similar for network interfaces, Management SAPs, and Ethernet and IP pseudowire SAPs. This guide describes the assignment of filter policies to SAPs. Refer to the 7705 SAR OS Router Configuration Guide for information on configuring filter policies and assigning them to network interfaces.

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
- IP Filter Policies
- MTU Settings
- Pseudowire Control Word
- Pseudowire Redundancy

Service Support

ATM VLL service is supported on any port of the 4-port OC3/STM1 Clear Channel Adapter card when the port is configured for ATM and 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.

IP interworking VLL service is supported on the 7705 SAR-8 on any Ethernet port on the 8-port Ethernet Adapter card and on PPP/MLPPP connections on the T1/E1 ASAP Adapter card.

IP interworking VLL service is supported on the 7705 SAR-F on any 10/100 Base-T Ethernet or Gigabit Ethernet SFP ports and on PPP/MLPPP connections on any T1/E1 ASAP port.

The 7705 SAR supports a combined total of 1536 VLLs for ATM, Ethernet, TDM, and IP interworking VLLs.

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

Table 21 lists the limits for VLL service types.

Table 21: Maximum Number of Supported VLL services

	7705 SAR-8	7705 SAR-F
Total PWs per node	1536	384
Total IP PWs per node	5 x 256	256
Total PWs per T1/E1 ASAP card	192 (1)	192 (1)
Total PWs per Ethernet card	256 (2)	256 (2)
Total PWs per Ethernet port	128	128
Total PWs per 4-port OC3/STM1 card	512	—

Notes:
1. PWs can be any combination of Apipes, Cpipes, and or Ipipes.
2. PWs can be any combination of Epipes and/or Ipipes.

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

The 7705 SAR 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
- Ipipe

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 151). The value of N is always 1.

The supported PW service types 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. Cpipes support SAP-to-SAP and SAP-to-spoke SDP binding with a default service MTU of 1514 bytes.

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

Ipipe

Ipipe service supports Ethernet null, Ethernet dot1q, IPCP, and PPP/MLPPP SAP encapsulation over IP or MPLS. Ipipes support SAP-to-spoke SDP binding with a default service MTU of 1500 bytes.

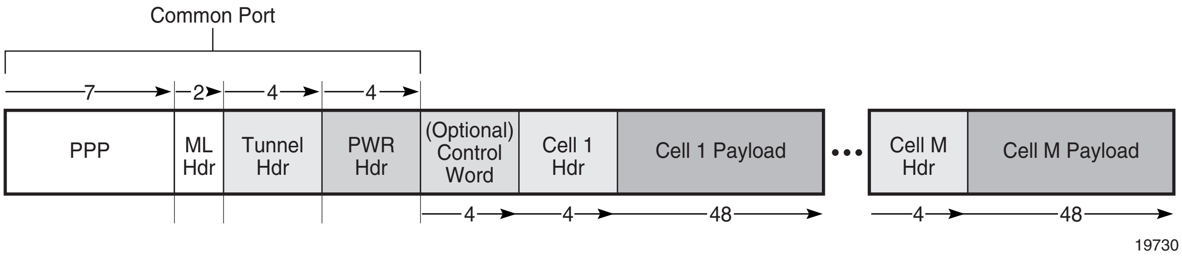
Ipipe service supports 0x000B (IP Layer2 Transport) PW service type.

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 2.1, N is not user-configurable and N = 1 is the only value supported. Figure 25 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 25: 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 158 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, Epipe, and Ipipe services, service ingress QoS policies only create the unicast queues defined in the policy.

With Apipe, Cpipe, Epipe, and Ipipe 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, Epipe, or Ipipe service. QoS policies on Apipes cannot perform any classification.

IP Filter Policies

The 7705 SAR supports ingress IP filter policies on Epipe and Ipipe SAPs. Configuration of IP filter policies for Epipes and Ipipes is similar to configuring IP filters for network interfaces and Management SAPs. Refer to the 7705 SAR OS Router Configuration Guide for information on configuring IP filters.

MTU Settings

There are several MTU values that must be set properly for a VLL service (Apipe, Cpipe, Epipe, or Ipipe) to work from end to end. Figure 26 locates the MTU point for each value. Table 22 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:

SAP MTU ≥ Service MTU ≤ Path MTU

Figure 26: MTU Points on the 7705 SAR

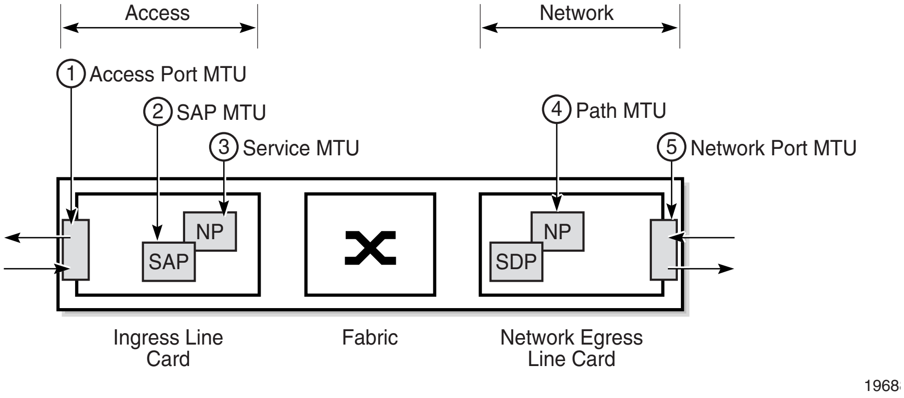


Table 22: MTU Points and Descriptions

Key	MTU Point	Description
1	Access port MTU	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: • **Null:** 1514 bytes (payload = 1500 bytes, L2 header = 14 bytes) • **dot1q:** 1518 bytes (payload = 1500 bytes, L2 header = 18 bytes)
2	SAP MTU	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.
3	Service MTU	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 26, NP stands for network processor. 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 T1/E1 CES with CAS on page 122 for more information.
4	Path MTU	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). If the network port SDP binding is Ethernet, then the following equations hold: • 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	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.

Table 23 aids in calculating MTU values for various configurations and operating scenarios.

Note: Ethernet QinQ is not supported in this release and is shown in this table for reference purposes only.

Table 23: MTU Calculator — Service Creation (Worst Case)

		Service Creation													NW
		Access Port Default MTU		SAP				Network Port MTU							
													Epipe over MPLS Encap	Epipe/Ipipe over GRE	LSR
		TDM/ ATM	Eth	Epipe	Ipipe	Apipe	Cpipe	PPP	ML-PPP	Eth Null	Eth dot1q	MPLS Label	Best Case	Worst Case	Worst Case
	Max Payload			2048	2048	1514	1514						40	2048	2084
	RTP Header						12								
	Control Word			4	4	4	4							4	
SDP Encap: GRE/MPLS	IP Header for GRE Encap			20	20	20	20							20	
	GRE/MPLS Header			4	4	4	4						4	4	4
	PW Header			4	4	4	4						4	4	
	VCCV Type 2 /sdp-ping			4	4	4	4					4		4	
	Fast Reroute Label											4			
	LDP over RSVP											4			
Physical Media (T11/E1 ASAP and Ethernet Adapter cards)	Eth Null		1514												
	Eth dot1q		1518								4			4	4
	Eth QinQ		1522												
	Eth Type									2	2			2	2
	Eth-SA									6	6			6	6
	Eth-DA									6	6			6	6
	TDM/ATM	1572	1572												
	PPP Protocol							2	2				2		
	ML Sequence								3						
	ML Preamble								1						
	Total			**2084**	**2084**	**1550**	**1562**	**2**	**6**	**14**	**18**		**50**	**2102**	**2106**

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 24 shows the values that are expected to match.

Table 24: Matching MTU or Payload Values for Signaled VLL Services

	Apipe	Cpipe	Epipe	Ipipe
Payload size (bytes)		Yes		
Bit rate		Yes		
Maximum number of ATM cells	Yes			
Service MTU			Yes	Yes
Must match at both ends	Yes	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, CESoPSN, and IP PW).

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 2.1 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).

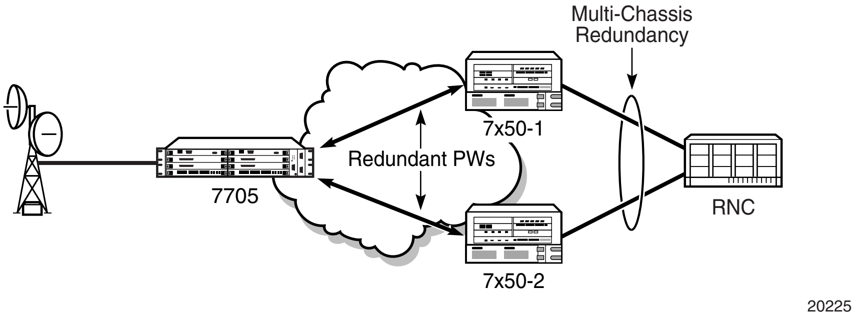
Pseudowire Redundancy

Pseudowire (PW) redundancy protects a PW and any services on the PW against endpoint failures. This differs from LSP redundancy and FRR, which offer protection against link and node failures within the backhaul network.

As shown in Figure 27, in order to provide redundant PWs, the 7705 SAR must signal PWs to two endpoints at the MTSO (7x50-1 and 7x50-2), which is done using two spoke SDPs on the 7705 SAR. This configuration removes any single point of failure from a given network. If 7x50-1 loses all of its connectivity to the network or to the RNC, then the 7705 SAR can reroute the PW traffic to 7x50-2, which switches traffic to the RNC.

Note that for end-to-end protection, PW redundancy must operate with the multi-chassis (MC) redundancy feature running on the 7x50 SR nodes.

Figure 27: Pseudowire Redundancy



PW redundancy applies to all VLL services available on the 7705 SAR: Apipe, Cpipe, Epipe, and Ipipe.

PW Redundancy Operation

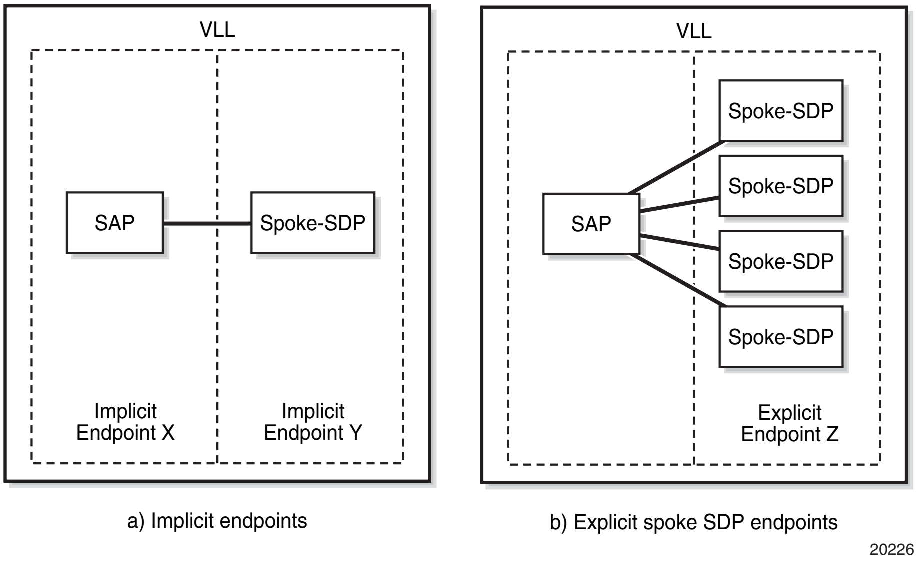
PW redundancy on the 7705 SAR is similar to a point-to-multipoint implementation for PWs (in the ingress to the egress direction). A single SAP can be bound to more than one spoke SDP; conversely, traffic from multiple spoke SDPs can all be switched to the same SAP. To implement PW redundancy, a PW service on the 7705 SAR must be able to accommodate more than one spoke SDP on the spoke SDP side. This is achieved using the concept of endpoints.

An endpoint can be thought of as a container for a single SAP, a single spoke SDP, or multiple spoke SDPs. Figure 28 illustrates the model for a redundant VLL service based on the endpoints. Endpoints are implicit or explicit objects.

Implicit endpoints are transparent to the user and are not user-configurable. As shown in Figure 28a, implicit endpoints mean that one endpoint is a SAP and another endpoint is a spoke SDP. Endpoints are considered implicit if the `endpoint` command is not used in the `config>service>xpipe>spoke-sdp` context, where `xpipe` refers to any of the VLL services.

Explicit endpoints are user-configurable and apply when there are multiple spoke SDPs. As shown in Figure 28b, explicit endpoints mean that there can be multiple spoke SDPs associated with the endpoint. An endpoint created explicitly can have up to four spoke SDPs associated with it. The explicit endpoint method is used for PW redundancy. Explicit endpoints are user-configurable.

Figure 28: Implicit and Explicit Endpoint Objects



a) Implicit endpoints

b) Explicit spoke SDP endpoints

The 7705 SAR supports the following types of endpoint objects:

- SAP — there can be only one SAP per PW endpoint (Endpoint X in Figure 28a)
- Spoke SDP — from the perspective of a 7705 SAR, if there is only one SDP endpoint, then it is a spoke SDP endpoint and it is implicitly defined. In other words, there can be only one implicitly defined spoke SDP per PW endpoint (Endpoint Y in Figure 28a).
- Primary spoke SDP — there can be only one explicitly defined primary spoke SDP per PW endpoint (one of the spoke SDPs at Endpoint Z in Figure 28b). If a primary spoke SDP is defined, then there can be up to three secondary spoke SDPs per endpoint and the service can be revertive.
- Secondary spoke SDP — there can be up to four explicitly defined secondary spoke SDPs per endpoint if no primary spoke SDP is defined; otherwise, there can be up to three. Secondary spoke SDPs are assigned a precedence value that is used by the 7705 SAR OS to determine which secondary PW becomes active when the currently active PW fails (see Selecting the Active Spoke SDP for PW Redundancy Configuration).

Multiple spoke SDPs can be established between a 7705 SAR and any SR platform. For example, multiple spoke SDPs on a 7705 SAR can connect to a 7750 SR. In this case, the 7750 SR must be configured to use multi-chassis backup in conjunction with multi-segment PWs; that is, the 7750 SR nodes at the far end must support multi-chassis redundancy.

A PW service endpoint can only use a single active spoke SDP for transmission at any given time. A PW SAP can receive traffic from any of the endpoint spoke SDPs assigned to the service.

7705 SAR nodes support user-initiated manual switchover of the VLL path to the primary path or any of the secondary paths using the `force-switchover` command under the `tools>perform>service-id` context. A manual switchover is useful during planned outages such as node upgrade procedures.

Selecting the Active Spoke SDP for PW Redundancy Configuration

There are two main scenarios for configuring PW redundancy. One scenario uses a primary spoke SDP and provides revertive behavior. The other scenario uses only secondary spoke SDPs for non-revertive behavior.

Primary and Secondary Spoke SDPs

If a primary spoke SDP is defined, up to three secondary spoke SDPs can also be defined. The VLL service always uses the primary endpoint PW and only switches to a secondary PW when the primary PW is down. The PW service switches the path back to the primary PW when the primary PW is back up. The user can configure a timer to delay reverting back to the primary path or to never revert back. When the primary PW goes down, the 7705 SAR OS selects the secondary spoke SDP that is operationally up and has the highest precedence setting.

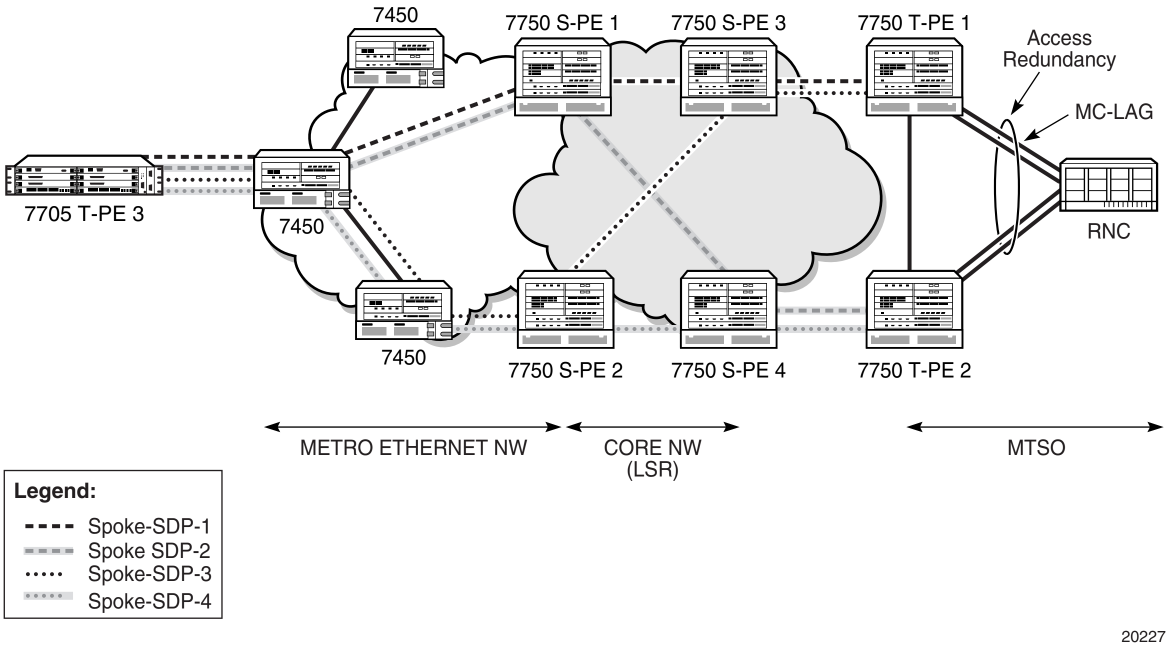
Secondary Spoke SDPs Only

If a primary spoke SDP is not defined, up to four secondary spoke SDPs can be defined. The user can configure the precedence of each secondary PW to indicate the order in which secondary PWs are activated. The secondary PW with the highest precedence is selected first. If two or more secondary spoke SDPs are assigned the same precedence, the 7705 SAR OS selects the secondary path that is operationally up and has the lowest spoke SDP identifier. There is no revertive behavior between secondary paths, which means that a secondary path will not switch to another secondary path of higher precedence if one becomes available.

The use of four secondary spoke SDPs is illustrated in Figure 29, where:

- spoke SDP-1 goes over S-PE-1 to T-PE1 (red path) (S-PE is a switching PE and T-PE is a terminating PE)
- spoke SDP-2 goes over S-PE-1 to T-PE2 (green path)
- spoke SDP-3 goes over S-PE-2 to T-PE1 (violet path)
- spoke SDP-4 goes over S-PE-2 to T-PE2 (orange path)

Figure 29: Pseudowire Redundancy with Four Spoke SDPs



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:

Common Configuration Tasks

The following list 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)
    - → Optional – select ingress IP filter policies (for Epipes and Ipipes only)
- Define spoke SDP parameters.
    - → Optional – select egress and ingress vc label parameters
    - → Optional – explicitly assign spoke SDP endpoints for pseudowire (PW) redundancy applications
- 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
- Ipipe
  - → Creating an Ipipe Service
  - → Configuring Ipipe SAP Parameters
  - → Configuring Ipipe SDP Bindings
- Configuring Ingress and Egress SAP Parameters
- Using the Control Word
- Configuring PW Redundancy

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>apipe# description “apipe test”
A:ALU-41config>service>apipe# service-mtu 1400
A:ALU-41config>service>apipe# no shutdown
A:ALU-41config>service>apipe#
```

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 182.

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

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 62.

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 182.

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 62.

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
-------------------------------------------
```

Configuring Epipe SAP Parameters

The 7705 SAR supports distributed Epipe service and local (SAP-to-SAP) Epipe service. A distributed Epipe consists of two SAPs on different nodes. A local Epipe consists of both SAPs on the same 7705 SAR. 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 182. For SAP ETH-CFM configuration information, see Configuring ETH-CFM Parameters on page 72.

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
               eth-cfm
               ingress
                  filter [ip ip-filter-id]
                  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 1/1/3:21 create
config>service>epipe>sap# ingress
config>service>epipe>sap>ingress# filter ip 1
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 1/1/4:550 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 1/1/3:21 create
                ingress
                    filter ip 1
                    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 1/1/4:550 create
                ingress
                    qos 654
              exit
              egress
                    qos 432
              exit
            exit
        exit
...
----------------------------------------------
ALU-2>config>service#
```

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

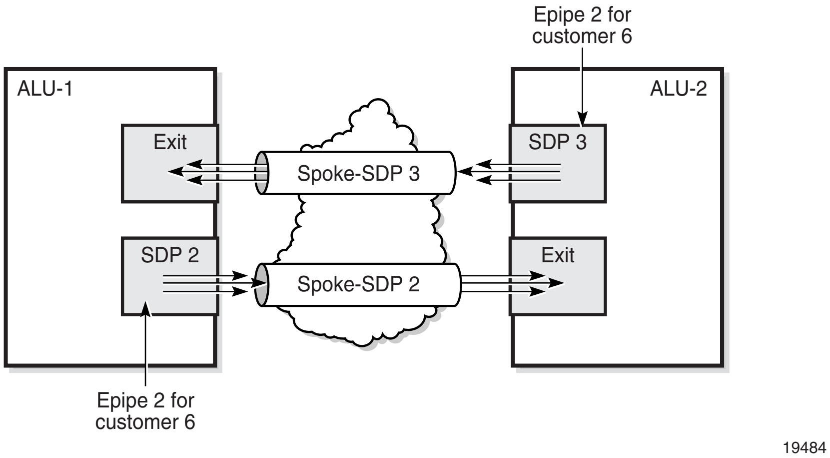
The following example displays an Ethernet SAP-to-SAP configuration:

```
A:ALU-4>config>service# info
-------------------------------------
...
        epipe 2 customer 1 create
            description "Ethernet sap2sap"
               sap 1/1/1:1000
               sap 1/2/1:50
            no shutdown
        exit
...
-------------------------------------
```

Configuring Epipe SDP Bindings

Figure 30 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 30: SDPs — Unidirectional Tunnels



Use the following CLI syntax to create a spoke SDP binding with an Epipe service. For SDP configuration information, see Configuring SDPs on page 62. For spoke SDP ETH-CFM configuration information, see Configuring ETH-CFM Parameters on page 72.

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
           eth-cfm
           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 174).

```
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
                    filter ip 1
                    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
...
----------------------------------------------
```

Creating an Ipipe Service

Use the following CLI syntax to create an Ipipe service.

CLI Syntax: `config>service# ipipe service-id [customer customer-id] [vpn vpn-id]`

```
              description description-string
              no shutdown
```

The following example displays an Ipipe configuration example:

```
A:ALU-1>config>service# info
-------------------------------------------
...
        ipipe 202 customer 1 create
            description "eth_ipipe"
            no shutdown
        exit
-------------------------------------------
A:ALU-1>config>service#
```

Configuring Ipipe SAP Parameters

The following displays an Ipipe SAP configuration example:

```
A:ALU-48>config>service# info
----------------------------------------------
...
        ipipe 202 customer 1 create
            sap 1/1/2:444 create
                description "eth_ipipe"
                ce-address 31.31.31.1
            exit
             spoke-sdp 16:516 create
                ce-address 31.31.31.2
            exit
            no shutdown
        exit
...
----------------------------------------------
A:ALU-48>config>service#
```

The following displays a PPP to Ethernet local Ipipe example:

Example:

```
config>service# ipipe 206 customer 1 create
config>service>ipipe$ sap 1/1/2:447 create
config>service>ipipe>sap$ description "eth_ppp_ipipe"
config>service>ipipe>sap$ ce-address 33.33.33.1
config>service>ipipe>sap$ no shutdown
config>service>ipipe>sap$ exit
config>service>ipipe# spoke-sdp 15:516 create
config>service>ipipe>sap>spoke-sdp$ ce-address 33.33.33.2
config>service>ipipe>sap-spoke-sdp$ exit
config>service>ipipe>$ exit
config>service>ipipe# no shutdown
config>service>ipipe# exit
config>service#
```

The following displays the output:

```
A:ALU-48>config>service# info
----------------------------------------------
ipipe 206 customer 1 create
            sap 1/1/2:447 create
                description "eth_ppp_ipipe"
                ce-address 33.33.33.1
            exit
            spoke-sdp 15:516 create
                ce-address 33.33.33.2
             exit
           exit
            no shutdown
        exit
exit
----------------------------------------------
```

Configuring Ipipe SDP Bindings

The following displays an Ipipe SDP configuration example:

```
A:ALU-48>config>service# info
----------------------------------------------
...
        sdp 16 mpls create
            far-end 4.4.4.4
            ldp
            path-mtu 1600
            keep-alive
                shutdown
            exit
            no shutdown
        exit
...
        ipipe 207 customer 1 create
            shutdown
            sap 1/1/2:449 create
                description "Remote_Ipipe"
                ce-address 34.34.34.1
            exit
            spoke-sdp 16:516 create
                ce-address 34.34.34.2
            exit
        exit
...

----------------------------------------------
A:ALU-48>config>service#
```

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 QoS SAP parameters can be applied to distributed Epipe and Ipipe service SAPs, and to Apipe, and Cpipe service SAPs.

By default, there are no IP filters associated with interfaces or services. IP filter policies can be applied to ingress Epipe and Ipipe 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# filter ip 1
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
                    filter ip 1
                    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, Epipe, and Ipipe 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, Epipe, or Ipipe services, use the `no control-word` command.

Example:

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

Configuring PW Redundancy

For PW redundancy, create an explicit endpoint and then assign a primary spoke SDP and up to three secondary spoke SDPs, or up to four secondary spoke SDPs with no primary spoke SDP, to that endpoint.

CLI Syntax:

```
config>service# cpipe service-id [customer customer-id]
[create]
            endpoint endpoint-name [create]
            spoke-sdp sdp-id:vc-id endpoint endpoint-name
               [create]
               precedence precedence-value
            no shutdown
```

Example:

```
config>service# cpipe 2100
config>service>cpipe$ endpoint “Endpoint_Y” create
config>service>cpipe$ spoke-sdp 1:100 endpoint
   “Endpoint_Y” create
config>service>cpipe>spoke-sdp$ precedence primary
config>service>cpipe$ spoke-sdp 2:200 endpoint
   “Endpoint_Y” create
config>service>cpipe>spoke-sdp$ precedence 1
no shutdown
```

The following example displays the PW redundancy configuration output for a Cpipe service.

```
*A:7705:Dut-C>config>service>cpipe# info
----------------------------------------------
            endpoint "Endpoint_Y" create
            exit
            spoke-sdp 1:100 endpoint "Endpoint_Y" create
                precedence primary
            exit
            spoke-sdp 2:200 endpoint "Endpoint_Y" create
                precedence 1
            exit
----------------------------------------------------
*A:7705:Dut-C>config>service>cpipe#
```

Service Management Tasks

The service management tasks are similar for Apipe, Cpipe, Epipe, and Ipipe 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, Epipe, and Ipipe 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, Epipe, and Ipipe 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, Epipe, and Ipipe 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, Epipe, and Ipipe 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
  - → Ipipe 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
                    — [no] endpoint endpoint-name
                            — description description-string
                            — no description
                            — revert-time [revert-time | infinite]
                            — no revert-time
                    — 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] [no-endpoint] (see Note)
                    — spoke-sdp sdp-id:vc-id [create] endpoint endpoint-name
                    — 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
```

```
                          — [no] egress
                                    — vc-label egress-vc-label
                                    — no vc-label [egress-vc-label]
                          — [no] ingress
                                    — vc-label ingress-vc-label
                                    — no vc-label [ingress-vc-label]
                          — precedence [precedence-value | primary]
                          — no precedence
                          — [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
                         — [no] endpoint endpoint-name
                                   — description description-string
                                   — no description
                                   — revert-time [revert-time | infinite]
                                   — no revert-time
                         — 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] [no-endpoint] (see Note)
— spoke-sdp sdp-id:vc-id [create] endpoint endpoint-name
— no spoke-sdp sdp-id:vc-id
        — [no] control-word
        — [no] egress
                — [no] vc-label egress-vc-label
        — [no] ingress
                — [no] vc-label ingress-vc-label
        — precedence [precedence-value | primary]
        — no precedence
        — [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
                    — [no] endpoint endpoint-name
                            — description description-string
                            — no description
                            — revert-time [revert-time | infinite]
                            — no revert-time
                    — 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
                            — eth-cfm
                                    — mep mep-id domain md-index association ma-index
                                      [direction {up | down}]
                                    — no mep mep-id domain md-index association ma-index
                                            — [no] ccm-enable
                                            — ccm-ltm-priority priority
                                            — [no] ccm-ltm-priority
                                            — low-priority-defect {allDef | macRemErrXcon |
                                              remErrXcon | errXcon | xcon | noXcon}
                                            — [no] shutdown
                            — ethernet
                                    — [no] llf
                            — ingress
                                    — filter ip ip-filter-id
```

```
                    — no filter [ip ip-filter-id]
                    — 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-endpoint]
            — spoke-sdp sdp-id:vc-id [vc-type {ether | vlan}] [create] endpoint endpoint-name
            — no spoke-sdp sdp-id:vc-id
                — [no] control-word
                — egress
                    — vc-label egress-vc-label
                    — no vc-label [egress-vc-label]
                — eth-cfm
                    — mep mep-id domain md-index association ma-index
                      [direction {up | down}]
                    — no mep mep-id domain md-index association ma-index
                        — [no] ccm-enable
                        — ccm-ltm-priority priority
                        — [no] ccm-ltm-priority
                        — low-priority-defect {allDef | macRemErrXcon |
                          remErrXcon | errXcon | xcon | noXcon}
                        — [no] shutdown
                — ingress
                    — vc-label ingress-vc-label
                    — no vc-label [ingress-vc-label]
                — [no] shutdown
                — precedence [precedence-value | primary]
                — no precedence
                — vlan-vc-tag 0..4094
                — no vlan-vc-tag [0..4094]
```

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

Ipipe Service Configuration Commands

```
config
    — service
        — ipipe service-id [customer customer-id] [create] [vpn vpn-id]
        — [no] ipipe service-id
            — description description-string
            — no description
            — [no] endpoint endpoint-name
                — description description-string
                — no description
                — revert-time [revert-time | infinite]
                — no revert-time
            — sap sap-id [create]
            — no sap sap-id
                — accounting-policy acct-policy-id
```

    - **no accounting-policy**
    - **ce-address** *ip-address*
    - **no ce-address**
    - **no collect-stats**
    - **description** *description-string*
    - **no description**
    - **egress**
        - **qos** *policy-id*
        - **no qos**
    - **ingress**
        - **filter ip** *ip-filter-id*
        - **no filter** [**ip** *ip-filter-id*]
        - **qos** *policy-id*
        - **no qos**
    - [**no**] **ipcp**
        - [**no**] **assign-peer-ce-addr**
        - [**no**] **dns** *ip-address-1* [**secondary** *ip-address-2*]
    - [**no**] **mac** *ieee-address*
    - **mac-refresh** *refresh-interval*
    - **no mac-refresh**
    - [**no**] **shutdown**
- **service-mtu** *octets*
- **no service-mtu**
- [**no**] **shutdown**
- **spoke-sdp** *sdp-id*:*vc-id* [**create**] [**no-endpoint**]
- **spoke-sdp** *sdp-id*:*vc-id* [**create**] **endpoint** *endpoint-name*
- **no spoke-sdp** *sdp-id*:*vc-id*
    - **ce-address** *ip-address*
    - **no ce-address**
    - [**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**
    - **precedence** [*precedence-value* | **primary**]
    - **no precedence**

Show Commands

```
show
    — eth-cfm
            — association [ma-index] [detail]
            — cfm-stack-table
            — cfm-stack-table [port [port-id [vlan vlan-id] | sdp sdp-id[:vc-id]] [level 0..7] [direction
              down]
            — domain [md-index] [association ma-index | all-associations] [detail]
            — mep mep-id domain md-index association ma-index [loopback] [linktrace]
    — service
            — egress-label start-label [end-label]
            — id service-id
                    — all
                    — base
                    — endpoint endpoint-name
                    — 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
                    — arp
                    — 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
```

Command Descriptions

- VLL Service Configuration Commands on page 199
- Show Commands on page 232
- Clear Commands on page 285

VLL Service Configuration Commands

Generic Commands

description

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

Context config>service>apipe
config>service>apipe>endpoint
config>service>apipe>sap
config>service>cpipe
config>service>cpipe>endpoint
config>service>cpipe>sap
config>service>epipe
config>service>epipe>endpoint
config>service>epipe>sap
config>service>epipe>spoke-sdp
config>service>ipipe
config>service>ipipe>endpoint
config>service>ipipe>sap
config>service>ipipe>spoke-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 *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.

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
config>service>ipipe
config>service>ipipe>sap
config>service>ipipe>spoke-sdp

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 can 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** *service-id* [**customer** *customer-id*] [**create**] [**vpn** *vpn-id*] [**vc-type** {**atm-vcc | atm-vpc**}]
no apipe *service-id*

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 *service-id* — 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 *service-id* must be the same number used for every 7705 SAR on which this service is defined.

Values 1 to 2147483647

create — keyword used to create an Apipe. The **create** keyword requirement can be enabled/disabled in the **environment>create** context

customer-id **—** 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-id — specifies the VPN ID number that 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.

Values 1 to 2147483647

Default **null (0)**

vc-type — specifies a 15-bit value that defines the type of the VC signaled to the peer. Its values are defined in *draft-ietf-pwe3-iana-allocation* and it defines both the signaled VC type as well as the resulting datapath encapsulation over the Apipe.

Values atm-vcc, atm-vpc

Default atm-vcc

cpipe

Syntax [**no**] **cpipe** *service-id* [**customer** *customer-id*] [**create**] [**vpn** *vpn-id*] [**vc-type** {**satop-e1** | **satop-t1** | **cesopsn** | **cesopsn-cas**}]

Context config>service

Description This command configures a circuit emulation service utilizing MPLS or GRE encapsulation. The **vc-type** defines the type of unstructured or structured circuit emulation service to be configured. All other parameters (**service-id**, **customer**) have common usage with other service types.

Default **no cpipe**

Parameters *service-id* — 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 *service-id* must be the same number used for every 7705 SAR on which this service is defined.

Values 1 to 2147483647

customer-id **—** 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

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

vpn-id **—** specifies the VPN ID number that 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.

Values 1 to 2147483647

Default **null** (0)

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.

Values satop-e1: unstructured E1 circuit emulation service

satop-t1: unstructured DS1 circuit emulation service

cesopsn: basic structured n × 64 kb/s circuit emulation service

cesopsn-cas: structured n × 64 kb/s circuit emulation service with signaling

Default **cesopsn**

epipe

Syntax [**no**] **epipe** *service-id* [**customer** *customer-id*] [**create**] [**vpn** *vpn-id*]

Context config>service

Description 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.

No MAC learning or filtering is provided (or needed) on an Epipe.

When a service is created, the **customer** keyword and *customer-id* must be specified, which associates the service with a customer. The *customer-id* 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.

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 *service-id* — 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 *service-id* must be the same number used for every 7705 SAR on which this service is defined.

Values 1 to 2147483647

customer-id **—** 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

create — keyword used to create an Epipe. The **create** keyword requirement can be enabled/disabled in the **environment>create** context

vpn-id — specifies the VPN ID number that 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)

ipipe

Syntax **ipipe** *service-id* [**customer** *customer-id*] [**create**] [**vpn** *vpn-id*]
no ipipe *service-id*

Context config>service

Description This command configures an IP interworking service. An Ipipe can connect an Ethernet or PPP/MLPPP SAP over an MPLS or IP network to a remote Ethernet or PPP/MLPP SAP.

Parameters *service-id* — 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 *service-id* must be the same number used for every 7705 SAR on which this service is defined.

Values 1 to 2147483647

customer-id **—** 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

create — keyword used to create an Ipipe. The **create** keyword requirement can be enabled/disabled in the **environment>create** context.

vpn-id **—** specifies the VPN ID number that 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)

endpoint

Syntax [**no**] **endpoint** *endpoint-name*

Context config>service>apipe
config>service>cpipe
config>service>epipe
config>service>ipipe

Description This command provides access to the service endpoint context.

Parameters *endpoint-name* — specifies an endpoint name (up to 32 alphanumeric characters)

revert-time

Syntax **revert-time** [*revert-time* | **infinite**]
no revert-time

Context config>service>apipe>endpoint
config>service>cpipe>endpoint
config>service>epipe>endpoint
config>service>ipipe>endpoint

Description This command configures the time to wait before reverting back to the primary spoke SDP defined on this service endpoint, after having switched over to a backup spoke SDP after a failure of the primary spoke SDP.

Parameters *revert-time* — specifies the time, in seconds, to wait before reverting to the primary SDP

Values 0 to 600

infinite — causes the endpoint to be non-revertive

service-mtu

Syntax **service-mtu** *octets*
no service-mtu

Context config>service>apipe
config>service>cpipe
config>service>epipe
config>service>ipipe

Description This command configures the service payload (Maximum Transmission Unit – MTU), in octets, for the service. This MTU value overrides the service-type default MTU.

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.

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.

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
ipipe: 1500

Table 25 displays MTU values for specific VC types.

Table 25: 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** *sap-id* [**create**]
no sap *sap-id*

Context config>service>apipe
config>service>cpipe
config>service>epipe
config>service>ipipe

Description This command creates a SAP within a service. Each SAP must be unique.

All SAPs must be explicitly created with the **create** keyword. If no SAPs are created within a service or an IP interface, a SAP will not exist on that object.

To edit SAP parameters, enter an existing SAP without the **create** keyword.

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** *port-id* context using the **mode access** command. Fractional TDM ports are always access ports. Refer to the 7705 SAR OS Interface Configuration Guide.

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.

The following SAP types are supported:

- 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)
- PPP IPCP encapsulation of an IPv4 packet for Ipipe service (RFC 1332)
- MLPPP bundle
- Ethernet SAPs supporting null and dot1q for Ipipe service

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.

Default **no sap**

Special Cases

A default SAP has the following format: port-id:*. 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).

Parameters *sap-id* — specifies the physical port identifier portion of the SAP definition

The *sap-id* can be configured in one of the formats described in Table 26.

Table 26: SAP ID Configurations

Type	Syntax	Example
port-id	*slot*/*mda*/*port*[.*channel*]	1/1/5
null	[*port-id* | *bundle-id*]	*port-id*: 1/1/3 *bundle-id*: bundle-ppp-1/1.1
dot1q	[*port-id* | *bundle-id*]:qtag1	*port-id*:qtag1: 1/1/3:100 *bundle-id*: bundle-ppp-1/1.1
atm	[*port-id* | *bundle-id*][:vpi/vci |vpi]	port-id: 1/1/1.1 *bundle-id*: 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
ipcp	slot/mda/port.channel	1/2/2.4

Values *sap-id*:

null	[*port-id* | *bundle-id*]	
dot1q	[*port-id* | *bundle-id*]:*qtag1*	
atm	[*port-id* | *bundle-id*][:*vpi*/*vci* |*vpi* |*vpi1.vpi2*]	
cem	*slot/mda/port.channel*	
ipcp	*slot/mda/port.channel*	
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	

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 specificially defined, the default value is 0.

Values qtag1: 0 to 4094

The values depend on the encapsulation type configured for the interface. Table 27 describes the allowed values for the port and encapsulation types.

Table 27: Port and Encapsulation Values

Port Type	Encap-Type	Allowed Values	Comments
Ethernet	Null	—	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.

mac

Syntax [**no**] **mac** *ieee-address*

Context config>service>ipipe>sap

Description This command assigns a specific MAC address to an Ipipe Ethernet SAP.

The **no** form of this command returns the MAC address of the SAP to the default value.

Default The default is the physical MAC address associated with the Ethernet interface where the SAP is configured.

Parameters *ieee-address* — specifies the 48-bit MAC address in the form aa:bb:cc:dd:ee:ff or aa-bb-cc-dd-ee-ff where aa, bb, cc, dd, ee, and ff are hexadecimal numbers

mac-refresh

Syntax	**mac-refresh** *refresh-interval* **no mac-refresh**
Context	config>service>ipipe>sap
Description	This command specifies the interval between ARP requests sent on an Ipipe Ethernet SAP. When the SAP is first enabled, an ARP request will be sent to the attached CE device and the received MAC address will be used in addressing unicast traffic to the CE. Although this MAC address will not expire while the Ipipe SAP is enabled and operational, it is verified by sending periodic ARP requests at the specified interval. The **no** form of this command restores **mac-refresh** to the default value.
Default	14400
Parameters	*refresh-interval* — specifies the interval, in seconds, between ARP requests sent on an Ipipe Ethernet SAP **Values** 0 to 65535

ipcp

Syntax	[**no**] **ipcp**
Context	config>service>ipipe>sap
Description	This command enables the context to configure IPCP. Within this context, IPCP extensions can be configured to define the remote IP address and DNS IP address to be signaled via IPCP on the associated PPP interface. This command is only applicable if the associated SAP is a PPP/MLPPP interface.

assign-peer-ce-addr

Syntax	[**no**] **assign-peer-ce-addr**
Context	config>service>ipipe>sap>ipcp
Description	This command assigns the IP address, defined by the **config>service>ipipe>sap>ce-address** command, to the far end of the associated PPP/MLPPP link via IPCP extensions. This command is only applicable if the associated SAP or port is a PPP/MLPPP interface with an IPCP encapsulation.
Default	**no assign-peer-ce-addr**

dns

Syntax [**no**] **dns** *ip-address-1* [**secondary** *ip-address-2*]

Context config>service>ipipe>sap>ipcp

Description This command defines the dns address(es) to be assigned to the far end of the associated PPP/MLPPP link via IPCP extensions. This command is only applicable if the associated SAP or port is a PPP/MLPPP interface with an IPCP encapsulation.

Default **no dns**

Parameters *ip-address-1* — specifies a unicast IPv4 address for the primary DNS server to be signaled to the far end of the associated PPP/MLPPP link via IPCP extensions

ip-address-2 — specifies a unicast IPv4 address for the secondary DNS server to be signaled to the far end of the associated PPP/MLPPP link via IPCP extensions

ethernet

Syntax **ethernet**

Context config>service>epipe>sap

Description Use this command to configure Ethernet properties for the SAP.

llf

Syntax [**no**] **llf**

Context config>service>epipe>sap>ethernet

Description This command enables Link Loss Forwarding (LLF) on an Ethernet port. LLF can only be enabled on Ethernet ports configured for null encapsulation.

LLF provides an end-to-end OAM fault notification for Ethernet VLL service. When LLF is enabled and there is a local fault on the pseudowire or service, or a remote fault on the SAP or pseudowire, the Ethernet port is brought down. Using label withdrawal or T-LDP status bits, LLF signals to connected equipment that the VLL is down. LLF stops signaling when the fault disappears.

The **no** form of the command disables LLF.

SAP cem Commands

cem

Syntax **cem**

Context config>service>cpipe>sap

Description This command configures the circuit emulation service parameters on a Cpipe.

This command is blocked for all SAPs except for E1, DS1 and n × 64 kb/s channels configured for encap-type cem.

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** *value* | **payload-size** *size*

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 The default value varies depending on the SAP bandwidth, as follows:

- 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 *value* — This parameter describes the size of the receive jitter buffer, expressed in milliseconds. The range of supported values is 2 to 250 ms. Setting the value to 0 sets the default (depends on SAP bandwidth). The buffer size must be set to at least 3 times the value of the packetization delay and no greater than 32 times the value of the packetization delay.

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%).

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 14. For CESoPSN without CAS, see Table 15. For CESoPSN with CAS, see Table 16.

Parameters *size* — 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).

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. Note that the configured value of the **service-mtu** size takes the extra CAS bytes into account. See Structured T1/E1 CES with CAS on page 122 for details.

For CESoPSN, the payload size may be specified as the number of bytes to be included in the packet.

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.

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.

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 **On: stray, malformed, pktloss, overrun and underun**

Off: rpktloss, rfault, rrdi

Parameters **stray —** reports the reception of packets not destined for this CES circuit

malformed — reports the reception of packets not properly formatted as CES packets

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** *acct-policy-id*
no accounting-policy

Context config>service>apipe>sap
config>service>cpipe>sap
config>service>epipe>sap
config>service>ipipe>sap

Description This command creates the accounting policy context that can be applied to a SAP. An accounting policy must be defined before it can be associated with a SAP. If the *policy-id* does not exist, an error message is generated.

A maximum of one accounting policy can be associated with a SAP at one time. Accounting policies are configured in the **config>log** context.

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

Default **no accounting-policy**

Parameters *acct-policy-id* — the accounting *policy-id* 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
config>service>ipipe>sap

Description 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.

When the **no collect-stats** command is issued, the statistics are still accumulated by the CSM. However, the CPU will not obtain the results and write them to the billing file. If a subsequent **collect-stats** command is issued, the counters written to the billing file include all the traffic while the **no collect-stats** command was in effect.

Default **collect-stats**

ETH-CFM Service Commands

eth-cfm

Syntax **eth-cfm**

Context config>service>epipe>spoke-sdp
config>service>epipe>sap

Description This command enables the context to configure ETH-CFM parameters.

mep

Syntax **mep** *mep-id* **domain** *md-index* **association** *ma-index* [**direction** {**up** | **down**}]
no mep *mep-id* **domain** *md-index* **association** *ma-index*

Context config>service>epipe>sap>eth-cfm
config>service>epipe>spoke-sdp>eth-cfm

Description This command provisions an 802.1ag maintenance association endpoint (MEP).

In Release 2.1, the 7705 SAR only supports MEPs in the down MEP direction.

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

Parameters *mep-id* — specifies the maintenance association endpoint identifier

Values 1 to 81921

md-index — specifies the maintenance domain (MD) index value

Values 1 to 4294967295

ma-index — specifies the MA index value

Values 1 to 4294967295

down — specifies the direction in which the maintenance association (MEP) faces on the bridge port (down sends continuity check messages away from the MAC relay entity)

ccm-enable

Syntax [**no**] **ccm-enable**

Context config>service>epipe>spoke-sdp>eth-cfm>mep
config>service>epipe>sap>eth-cfm>mep

Description This command enables the generation of CCM messages.

The **no** form of the command disables the generation of CCM messages.

ccm-ltm-priority

Syntax **ccm-ltm-priority** *priority*
no ccm-ltm-priority

Context config>service>epipe>spoke-sdp>eth-cfm>mep
config>service>epipe>sap>eth-cfm>mep

Description This command specifies the priority value for CCMs and LTMs transmitted by the MEP.

The **no** form of the command removes the priority value from the configuration.

Default **highest priority on the bridge-port**

Parameters *priority* — specifies the priority of CCM and LTM messages

Values 0 to 7

low-priority-defect

Syntax **low-priority-defect** {**allDef** | **macRemErrXcon** | **remErrXcon** | **errXcon** | **xcon** | **noXcon**}

Context config>service>epipe>spoke-sdp>eth-cfm>mep
config>service>epipe>sap>eth-cfm>mep

Description This command specifies the lowest priority defect that is allowed to generate a fault alarm.

Default **remErrXcon**

Parameters **allDef** — DefRDICCM, DefMACstatus, DefRemoteCCM, DefErrorCCM, and DefXconCCM

macRemErrXcon — DefMACstatus, DefRemoteCCM, DefErrorCCM, and DefXconCCM

remErrXcon — only DefRemoteCCM, DefErrorCCM, and DefXconCCM

errXcon — only DefErrorCCM and DefXconCCM

xcon — only DefXconCCM

noXcon — no defects DefXcon or lower are to be reported

SAP QoS and IP Filter Policy Commands

egress

Syntax **egress**

Context config>service>apipe>sap
config>service>cpipe>sap
config>service>epipe>sap
config>service>ipipe>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
config>service>ipipe>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.

filter

Syntax **filter ip** *ip-filter-id*
no filter [**ip** *ip-filter-id*]

Context config>service>epipe>sap>ingress
config>service>ipipe>sap>ingress

Description This command associates an IP filter policy with an ingress Epipe or Ipipe SAP.

Filter policies control the forwarding and dropping of packets based on IP matching criteria. Only one filter can be applied to a SAP at a time.

The *ip-filter-id* must already be defined before the **filter** command is executed. If the filter policy does not exist, the operation will fail and an error message will be displayed.

The **no** form of the command removes any configured filter ID association with the SAP. The filter policy cannot be deleted until it is removed from all SAPs where it is applied.

Default **no filter**

Parameters *ip-filter-id* — the IP filter policy ID number

Values 1 to 65535

qos

Syntax **qos** *policy-id*
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
config>service>ipipe>sap>egress
config>service>ipipe>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 *policy-id* 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 the 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** *sdp-id*:*vc-id* [**create**] [**no-endpoint**]
spoke-sdp *sdp-id*:*vc-id* [**create**] **endpoint** *endpoint-name*
no spoke-sdp *sdp-id*:*vc-id*

Context config>service>apipe
config>service>cpipe
config>service>ipipe

Description This command binds a service to an existing Service Destination Point (SDP). The syntax for an epipe spoke SPD has additional parameters. See spoke-sdp on page 222 for the epipe syntax.

A spoke SDP is treated as 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 on which it was received.

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.

The SDP must already be defined in the **config>service>sdp** context in order to associate an SDP with a service. If the **sdp** *sdp-id* is not already configured, an error message is generated. If the *sdp-id* does exist, a binding between that *sdp-id* and the service is created.

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.

The **endpoint** command allows multiple spoke SDPs to be associated with the endpoint, providing PW redundancy capability. The endpoint must be defined using the **create** command before multiple spoke SDPs can be associated with the endpoint. The **no-endpoint** command removes the endpoint and the spoke SDP associations.

The **no** form of the **spoke-sdp** 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.

Default **no *sdp-id* is bound to a service**

Parameters *sdp-id* — uniquely identifies the SDP

Values 1 to 17407

vc-id — identifies the virtual circuit

Values 1 to 4294967295

endpoint-name **—** specifies the name of the service endpoint

no-endpoint — removes a spoke SDP association

spoke-sdp

Syntax
spoke-sdp *sdp-id*:*vc-id* [**vc-type** {**ether** | **vlan**}] [**create**] [**no-endpoint**]
spoke-sdp *sdp-id*:*vc-id* [**vc-type** {**ether** | **vlan**}] [**create**] **endpoint** *endpoint-name*
no spoke-sdp *sdp-id*:*vc-id*

Context config>service>epipe

Description This command binds an Epipe service to an existing Service Destination Point (SDP). The syntax for an apipe, cpipe, or ipipe spoke SPD has additional parameters. See spoke-sdp on page 221 for the apipe, cpipe, or ipipe syntax.

A spoke SDP is treated as 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 on which it was received.

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.

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** *sdp-id* is not already configured, an error message is generated. If the *sdp-id* does exist, a binding between that *sdp-id* and the service is created.

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.

The **endpoint** command allows multiple spoke SDPs to be associated with the endpoint, providing PW redundancy capability. The endpoint must already be defined in the **config>service>epipe** context in order to associate multiple spoke SDPs with the endpoint.

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.

Default **no *sdp-id* is bound to a service**

Parameters *sdp-id* — uniquely identifies the SDP

Values 1 to 17407

vc-id — identifies the virtual circuit

Values 1 to 4294967295

vc-type — 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 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.

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 — 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 — 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.

endpoint-name **—** specifies the name of the service endpoint

no-endpoint — removes a spoke SDP association

egress

Syntax **egress**

Context config>service>apipe>spoke-sdp
config>service>cpipe>spoke-sdp
config>service>epipe>spoke-sdp
config>service>ipipe>spoke-sdp

Description This command configures the egress SDP context.

ingress

Syntax **ingress**

Context config>service>apipe>spoke-sdp
config>service>cpipe>spoke-sdp
config>service>epipe>spoke-sdp
config>service>ipipe>spoke-sdp

Description This command configures the ingress SDP context.

precedence

Syntax **precedence** [*precedence-value* **| primary**]
no precedence

Context config>service>apipe>spoke-sdp
config>service>cpipe>spoke-sdp
config>service>epipe>spoke-sdp
config>service>ipipe>spoke-sdp

Description This command specifies the precedence of the spoke SDP when there are multiple spoke SDPs associated with one service endpoint. One SDP binding can be assigned to be the primary SDP binding, leaving three bindings for secondary bindings, or, if no primary spoke SDP is defined, up to four secondary spoke SDPs can be configured. When an SDP binding goes down, the next highest precedence SDP binding will begin to forward traffic.

The **no** form of the command returns the precedence value to the default.

Default 4

Parameters *precedence-value* — specifies the spoke SDP precedence

Values 1 to 4 (where 1 is the highest precedence)

primary — makes the specified spoke SDP the primary spoke SDP (primary is indicated on the CLI display as the value 0)

vc-label

Syntax **vc-label** *egress-vc-label*
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
config>service>ipipe>spoke-sdp>egress

Description This command configures the egress VC label.

Parameters *egress-vc-label* — indicates a specific connection

Values 16 to 1048575

vc-label

Syntax	**vc-label** *ingress-vc-label* **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 config>service>ipipe>spoke-sdp>ingress
Description	This command configures the ingress VC label.
Parameters	*ingress-vc-label* — indicates a specific connection **Values** 2048 to 18431

vlan-vc-tag

Syntax	**vlan-vc-tag** *0..4094* **no vlan-vc-tag** [*0..4094*]
Context	config>service>epipe>spoke-sdp
Description	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. 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. The **no** form of this command disables the command
Default	**no vlan-vc-tag**
Parameters	*0..4094* — specifies a valid VLAN identifier to bind an 802.1Q VLAN tag ID

ce-address

Syntax

ce-address *ip-address*
no ce-address

Context

config>service>ipipe>sap
config>service>ipipe>spoke-sdp

Description

This command specifies the IP address of the CE device associated with an Ipipe SAP or spoke SDP. In the case of a SAP, it is the address of the CE device directly attached to the SAP. For a spoke SDP, it is the address of the CE device reachable through that spoke SDP (for example, attached to the SAP on the remote node). The address must be a host address (no subnet addresses are accepted) as there must be only one CE device attached to an Ipipe SAP. The CE address specified at one end of an Ipipe will be used in processing ARP messages at the other endpoint, as the router acts as a proxy for ARP messages.

Default

none

Parameters

ip-address — specifies the IP address of the CE device associated with an Ipipe SAP

control-word

Syntax

control-word
no control-word

Context

config>service>apipe>spoke-sdp
config>service>cpipe>spoke-sdp
config>service>epipe>spoke-sdp
config>service>ipipe>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.

.

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 2.1, 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.

max-cells

Syntax **max-cells** *cell-count*
no max-cells [*cell-count*]

Context config>service>apipe>spoke-sdp>cell-concatenation

Description 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.

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.

The **no** form of this command sets max-cells to the value “1”, indicating that no concatenation will be performed.

Parameters *cell-count* — 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** *delay-time*
no max-delay [*delay-time*]

Context config>service>apipe>spoke-sdp>cell-concatenation

Description 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.

The **no** form of this command resets max-delay to its default value.

Parameters *delay-time* — 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, a value of 1 equals 100 µs, and a value of 400 equals 40000 µs, or 40 ms.

Values 1 to 400

Default 400

ATM Commands

atm

Syntax **atm**

Context config>service>apipe>sap

Description 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:

- configuring ATM port or ATM port-related functionality on T1/E1 ASAP Adapter cards or OC3/STM1 Adapter cards
- configuring ATM-related configuration for ATM-based SAPs that exist on T1/E1 ASAP Adapter cards or on OC3/STM1 Adapter cards

If ATM functionality is not supported for a given context, the command returns an error.

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** *traffic-desc-profile-id*
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 This command enables the context to configure OAM functionality for a PVCC delimiting a SAP.

The T1/E1 ASAP Adapter card and OC3/STM1 Adapter card support the generation of F4 (VP) and F5 (VC) AIS cells when the Apipe service is operationally down. When the Apipe service is operationally up, OAM cells are transported over the Apipe and are transparent to the 7705 SAR. This capability is in accordance with ITU-T Recommendation I.610 - B-ISDN Operation and Maintenance.

alarm-cells

Syntax [**no**] **alarm-cells**

Context config>service>apipe>sap>atm>oam

Description 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.

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.

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.

Default **enabled**

Show Commands

all

Syntax **all**

Context show>service>id

Description This command displays detailed information for all aspects of the service.

Output The following output is an example of service-id all information, and Table 28 describes the fields. Following the table are output examples for:

- Sample Output (Apipe ATMVpc Service)
- Sample Output (Cpipe Service)
- Sample Output (Epipe Service)
- Sample Output (Ipipe 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     Signaling         : TLDP
Last Mgmt Change   : 03/28/2008 19:49:51
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
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.
===============================================================================
```

Table 28: 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 28: 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 28: 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, IacIngressFault, 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 28: 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
`Dot1ag Configuration Information`	
`Md-index`	Displays the value of the MD index
`Direction`	Displays the direction of the MEP
`Ma-index`	Displays the value of the MA index
`Admin`	Displays the administrative state of the MEP (enabled or disabled)
`MepId`	Displays the MEP-ID
`CCM-Enable`	Displays the status of the Continuity Check Message (CCM)
`LowestDefectPri`	Displays a configured value that defects are evaluated against
`HighestDefect`	Displays the highest defect
`Defect Flags`	Indicates the defect flags
`Mac Address`	Displays the MAC address (the MAC address for a spoke SDP is the system MAC address; for a SAP, it is the port MAC address)
`CcmLtmPriority`	Displays the priority of the CCM Linktrace Message (LTM)
`CcmTx`	Displays the number of CCM transmissions
`CcmSequenceErr`	Displays the number of CCM sequence errors
`LbRxReply`	Displays the number of received loopback (LB) replies
`LbRxBadOrder`	Displays the number of LB replies that have been received in the wrong order
`LbRxBadMsdu`	Displays the number of LB replies that have been received with the wrong destination MAC address (MSDU = MAC Service Data Unit)
`LbTxReply`	Displays the number of LBRs (loopback replies) transmitted out this MEP
`LbNextSequence`	Displays the sequence number of the next LB transmission

Table 28: Show Service-ID All Command Output Fields (Continued)

Label	Description
`LtNextSequence`	Displays the sequence number of the next Linktrace (LT) message transmitted
`LtRxUnexplained`	Displays the number of the unexplained Linktrace (LT) messages
`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 `max-cells` 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 `max-delay` 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 28: 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
`IPIPE Service Destination Point specifics`	
`Precedence`	Specifies the precedence level of the SDP binding
`IpipeSdpBindCeIpAd*`	Specifies the IP address of the Ipipe spoke-sdp
`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

Table 28: Show Service-ID All Command Output Fields (Continued)

Label	Description
`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
`IPIPE Service Access Points specifics`	
`Ipipe SAP ARP Entry Info`	Displays the MAC address of the connected CE address after being resolved through the ARP mechanism
`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 28: 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` *n*	Specifies the index of the ingress QoS queue of this SAP, where *n* 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` *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

Table 28: 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 124)
`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 28: 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

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
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
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
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 : 03/11/2008 19:58:19      Signaling         : TLDP
Last Mgmt Change   : 03/31/2008 20:41:13
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         : 100                      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


-------------------------------------------------------------------------------
CPIPE Service Destination Point specifics
-------------------------------------------------------------------------------
Local Bit-rate     : 10                       Peer Bit-rate     : n/a
Local Payload Size : 160                      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   : Yes                      Peer RTP Header   : No
Local Differential : No                       Peer Differential : No
Local Timestamp    : 0                        Peer Timestamp    : 0
-------------------------------------------------------------------------------
Number of SDPs : 1
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
Service Access Points
-------------------------------------------------------------------------------
```

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

===============================================================================
Service Detailed Information
===============================================================================
Service Id        : 2
Service Type      : Epipe
Customer Id       : 1
Last Status Change: 07/13/2009 18:50:40
Last Mgmt Change  : 07/13/2009 18:50:40
Admin State       : Down                Oper State        : Down
MTU               : 1514
Vc Switching      : False
SAP Count         : 1                   SDP Bind Count    : 1
-------------------------------------------------------------------------------
Service Destination Points(SDPs)
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
 Sdp Id 1:11  -(10.10.10.10)
-------------------------------------------------------------------------------
SDP Id             : 1:11                     Type              : Spoke
VC Type            : Ether                    VC Tag            : n/a
Admin Path MTU     : 0                        Oper Path MTU     : 0
Far End            : 10.10.10.10              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 : 07/13/2009 18:50:40      Signaling         : TLDP
Last Mgmt Change   : 07/13/2009 18:50:40      Force Vlan-Vc     : Disabled
Endpoint           : N/A                      Precedence        : 4
Class Fwding State : Down
Flags              : SvcAdminDown SdpOperDown
                     NoIngVCLabel NoEgrVCLabel
                     PathMTUTooSmall
Time to RetryReset : 476014240 seconds        Retries Left      : -1
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
-------------------------------------------------------------------------------
Dot1ag Configuration Information
```

```
-------------------------------------------------------------------------------
Md-index           : 1                        Direction          : Down
Ma-index           : 1                        Admin              : Disabled
MepId              : 2                        CCM-Enable         : Disabled
LowestDefectPri    : macRemErrXcon            HighestDefect      : none
Defect Flags       : None
Mac Address        : a4:58:ff:00:00:00        CcmLtmPriority     : 7
CcmTx              : 0                        CcmSequenceErr     : 0
LbRxReply          : 0                        LbRxBadOrder       : 0
LbRxBadMsdu        : 0                        LbTxReply          : 0
LbNextSequence     : 1                        LtNextSequence     : 1
LtRxUnexplained    : 0

Associated LSP LIST :
No LSPs Associated

-------------------------------------------------------------------------------
Number of SDPs : 1
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
Service Access Points
-------------------------------------------------------------------------------

-------------------------------------------------------------------------------
SAP 1/5/1
-------------------------------------------------------------------------------
Service Id         : 2
SAP                : 1/5/1                    Encap              : null
Admin State        : Up                       Oper State         : Down
Flags              : ServiceAdminDown
                     PortOperDown
Multi Svc Site     : None
Last Status Change : 07/13/2009 18:50:40
Last Mgmt Change   : 07/13/2009 18:50:40
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          : 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                        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
-------------------------------------------------------------------------------
Dot1ag Configuration Information
-------------------------------------------------------------------------------
Md-index          : 1                        Direction         : Down
Ma-index          : 1                        Admin             : Disabled
MepId             : 1                        CCM-Enable        : Disabled
LowestDefectPri   : macRemErrXcon            HighestDefect     : none
Defect Flags      : None
Mac Address       : 00:00:00:00:00:00
CcmTx             : 0                        CcmSequenceErr    : 0
LbRxReply         : 0                        LbRxBadOrder      : 0
LbRxBadMsdu       : 0                        LbTxReply         : 0
LbNextSequence    : 1                        LtNextSequence    : 1
LtRxUnexplained   : 0

-------------------------------------------------------------------------------
Service Endpoints
-------------------------------------------------------------------------------
No Endpoints found.
===============================================================================
A:ALU-1>show>service>id#
```

Sample Output (Ipipe Service)

```
*A:ALU-A# show service id 1301 all

===============================================================================
Service Detailed Information
===============================================================================
Service Id        : 1301
Service Type      : Ipipe
Description       : Default ipipe description for service id 1301
Customer Id       : 1
Last Status Change: 01/20/2009 16:44:14
Last Mgmt Change  : 01/20/2009 16:02:02
Admin State       : Up                  Oper State        : Up
MTU               : 1514
Vc Switching      : False
SAP Count         : 1                   SDP Bind Count    : 1
-------------------------------------------------------------------------------
Service Destination Points(SDPs)
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
 Sdp Id 123:1301  -(10.20.1.3)
-------------------------------------------------------------------------------
Description     : Default sdp description
SDP Id            : 123:1301                Type              : Spoke
VC Type           : Ipipe                   VC Tag            : 0
Admin Path MTU    : 0                       Oper Path MTU     : 1516
Far End           : 10.20.1.3               Delivery          : LDP

Admin State       : Up                      Oper State        : Up
Acct. Pol         : None                    Collect Stats     : Disabled
Ingress Label     : 131069                  Egress Label      : 131069
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 : 01/20/2009 16:05:49    Signaling         : TLDP
Last Mgmt Change  : 01/20/2009 16:02:02
Endpoint          : N/A                     Precedence        : 4
Class Fwding State : Down
Flags             : None
Time to RetryReset : 1 seconds              Retries Left      : 213236003
Mac Move          : Ukwn                    Blockable Level   : Unknown
Peer Pw Bits      : None
Peer Fault Ip     : None
Peer Vccv CV Bits  : lspPing
Peer Vccv CC Bits  : mplsRouterAlertLabel

Ipipe Sdp Bind Info :
IpipeSdpBindCeIpAd*: 88.1.10.4

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.     : 600                     I. Dro. Pkts.     : 0
I. Fwd. Octs.     : 60000                   I. Dro. Octs.     : 0
```

```
E. Fwd. Pkts.      : 21817053                E. Fwd. Octets    : 1919900664
-------------------------------------------------------------------------------
Number of SDPs : 1
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
Service Access Points
-------------------------------------------------------------------------------

-------------------------------------------------------------------------------
SAP 1/2/8:11
-------------------------------------------------------------------------------
Service Id         : 1301
SAP                : 1/2/8:11                Encap             : q-tag
Description        : Default sap description for service id 1301
Admin State        : Up                      Oper State        : Up
Flags              : None
Multi Svc Site     : None
Last Status Change : 01/20/2009 16:44:14
Last Mgmt Change   : 01/21/2009 16:31:04
Sub Type           : regular
Dot1Q Ethertype    : 0x8100                  QinQ Ethertype    : 0x8100

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
Q Frame-Based Acct : Disabled

Acct. Pol          : Default                 Collect Stats     : Enabled
Ce IP Address      : 88.1.10.3
SAP MAC Address    : 00:1a:f0:bd:ab:b0       Mac Refresh Inter*: 14400

-------------------------------------------------------------------------------
Ipipe SAP ARP Entry Info
-------------------------------------------------------------------------------
88.1.10.3       00:00:15:b9:6b:73 dynamic 03h52m50s


-------------------------------------------------------------------------------
QOS
-------------------------------------------------------------------------------
Ingress qos-policy : 13                      Egress qos-policy : 13
Shared Q plcy      : n/a                     Multipoint shared : Disabled
-------------------------------------------------------------------------------
Sap Statistics
-------------------------------------------------------------------------------
Last Cleared Time     : 01/21/2009 14:19:23

                        Packets                 Octets
Forwarding Engine Stats
Dropped               : 0                       0
Off. HiPrio           : 19961282                1556979996
Off. LowPrio          : 1840167                 143533026

Queueing Stats(Ingress QoS Policy 13)
Dro. HiPrio           : 0                       0
Dro. LowPrio          : 0                       0
```

```
For. InProf           : 10730245                836959110
For. OutProf          : 11071204                863553912

Queueing Stats(Egress QoS Policy 13)
Dro. InProf           : 0                       0
Dro. OutProf          : 0                       0
For. InProf           : 0                       0
For. OutProf          : 600                     46800
-------------------------------------------------------------------------------
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

Ingress Queue 2 (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

Ingress Queue 3 (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

Ingress Queue 4 (Unicast) (Priority)
Off. HiPrio           : 6582217                 513412926
Off. LoPrio           : 0                       0
Dro. HiPrio           : 0                       0
Dro. LoPrio           : 0                       0
For. InProf           : 4932647                 384746466
For. OutProf          : 1649570                 128666460

Egress Queue 1
For. InProf           : 0                       0
For. OutProf          : 0                       0
Dro. InProf           : 0                       0
Dro. OutProf          : 0                       0

Egress Queue 2
For. InProf           : 0                       0
For. OutProf          : 200                     15600
Dro. InProf           : 0                       0
Dro. OutProf          : 0                       0

Egress Queue 3
For. InProf           : 0                       0
```

```
For. OutProf          : 200                       15600
Dro. InProf           : 0                         0
Dro. OutProf          : 0                         0

Egress Queue 4
For. InProf           : 0                         0
For. OutProf          : 200                       15600
Dro. InProf           : 0                         0
Dro. OutProf          : 0                         0

-------------------------------------------------------------------------------
Service Endpoints
-------------------------------------------------------------------------------
No Endpoints found.
===============================================================================
*A:ALU-A#
```

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 The following output is an example of service-id base information, and Table 29 describes the fields.

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
===============================================================================
```

Table 29: 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

Table 29: Show Service-ID Base Output Fields (Continued)

Label	Description
`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
`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

egress-label

Syntax **egress-label** *start-label* [*end-label*]

Context show>service

Description This command displays services using the range of egress 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 ldp bindings** command to display dynamic labels.

Parameters *start-label* — indicates the starting egress 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 egress label value for which to display services using the label range

Default the *start-label* value

Values 2049 to 131071

Output The following output is an example of service egress-label information, and Table 30 describes the fields.

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
-------------------------------------------------------------------------------
```

Table 30: 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

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 The following output is an example of service ingress-label information, and Table 31 describes the fields.

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#
```

Table 31: 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

endpoint

Syntax **endpoint** *endpoint-name*

Context show>service>id

Description This command displays the endpoint configuration status of the active spoke SDP and lists the primary and secondary spoke SDPs used by the service.

Output The following output is an example of service-id endpoint information, and Table 32 describes the fields.

Sample Output

```
*A:7705:Dut-C>show>service>id# endpoint Endpoint_Y

===============================================================================
Service 6 endpoints
===============================================================================
Endpoint name                 : Endpoint_Y
Revert time                   : 0
Act Hold Delay                : 0
Ignore Standby Signaling      : false
Suppress Standby Signaling    : true
Tx Active                     : none
Tx Active Up Time             : 0d 00:00:00
Revert Time Count Down        : N/A
Tx Active Change Count        : 0
Last Tx Active Change         : 02/12/2009 19:16:37
-------------------------------------------------------------------------------
Members
-------------------------------------------------------------------------------
Spoke-sdp                     : 6:6 Precedence:0
Spoke-sdp                     : 7:7 Precedence:1
===============================================================================
*A:7705:Dut-C>show>service>id# info
```

Table 32: Service-ID Endpoint Output Fields

Label	Description
`Service endpoints`	
`Endpoint name`	Identifies the endpoint
`Revert time`	Displays the revert time setting for the active spoke SDP
`Act Hold Delay`	Not applicable
`Ignore Standby Signaling`	Indicates whether standby signaling is ignored `True` — standby signaling is ignored `False` — standby signaling is not ignored

Table 32: Service-ID Endpoint Output Fields (Continued)

Label	Description
`Suppress Standby Signaling`	Indicates whether standby signaling is suppressed `True` — standby signaling is suppressed `False` — standby signaling is not suppressed
`Tx Active`	Identifies the actively transmitting spoke SDP
`Tx Active Up Time`	Indicates the length of time that the active spoke SDP has been up
`Revert Time Count Down`	Not applicable
`Tx Active Change Count`	Indicates the number of times that there has been a change of active spoke SDPs
`Last Tx Active Change`	Indicates the date and time when a different spoke SDP became the actively transmitting spoke SDP
`Members`	
`Spoke-sdp`	Identifies the primary and secondary spoke SDPs that are associated with this endpoint and shows their precedence value (0 precedence indicates the primary spoke SDP)

labels

Syntax **labels**

Context show>service>id

Description This command displays the labels being used by the service.

Output The following output is an example of service-id labels information, and Table 33 describes the fields.

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#
```

Table 33: 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

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 *sap-id* — identifies the SAPs for the service in the form *slot*/*mda*/*port*[.*channel*]

detail — displays detailed information for the SAP

Output The following output is an example of service-id SAP information, and Table 34 describes the fields. Following the table are output examples for:

- Sample Output (Epipe)
- Sample Output (Ipipe)

Sample Output (Apipe)

```
*A:ALU-12>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
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           : 21900                   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           : 10950                   10950
For. OutProf          : 10950                   10950

Queueing Stats(Egress QoS Policy 1)
Dro. InProf           : 0                       n/a
Dro. OutProf          : n/a                     n/a
For. InProf           : 21900                   21900
For. OutProf          : n/a                     n/a
-------------------------------------------------------------------------------
Sap per Queue stats
-------------------------------------------------------------------------------
                        Packets                 Octets

Ingress Queue 1 (Unicast) (Priority)
Off. HiPrio           : 21900                   n/a
Off. LoPrio           : n/a                     n/a
Dro. HiPrio           : 0                       n/a
Dro. LoPrio           : n/a                     n/a
For. InProf           : 10950                   10950
For. OutProf          : 10950                   10950

Egress Queue 1
For. InProf           : 21900                   21900
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
===============================================================================

*A:ALU-12>show>service>id#
```

Table 34: Service-ID SAP Output 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 SeviceAdminDown, 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

Table 34: Service-ID SAP Output Fields (Continued)

Label	Description
`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
`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

Table 34: Service-ID SAP Output Fields (Continued)

Label	Description
`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 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
`Dot1ag Configuration Information`	
`Md-index`	Displays the value of the MD index
`Direction`	Displays the direction of the MEP
`Ma-index`	Displays the value of the MA index
`Admin`	Displays the administrative state of the MEP (enabled or disabled)
`MepId`	Displays the MEP-ID
`CCM-Enable`	Displays the status of the Continuity Check Message (CCM)

Table 34: Service-ID SAP Output Fields (Continued)

Label	Description
`LowestDefectPri`	Displays a configured value that defects are evaluated against
`HighestDefect`	Displays the highest defect
`Defect Flags`	Indicates the defect flags
`Mac Address`	Displays the MAC address (the MAC address for a spoke SDP is the system MAC address; for a SAP, it is the port MAC address)
`CcmLtmPriority`	Displays the priority of the CCM Linktrace Message (LTM)
`CcmTx`	Displays the number of CCM transmissions
`CcmSequenceErr`	Displays the number of CCM sequence errors
`LbRxReply`	Displays the number of received loopback (LB) replies
`LbRxBadOrder`	Displays the number of LB replies that have been received in the wrong order
`LbRxBadMsdu`	Displays the number of LB replies that have been received with the wrong destination MAC address (MSDU = MAC Service Data Unit)
`LbTxReply`	Displays the number of LBRs (loopback replies) transmitted out this MEP
`LbNextSequence`	Displays the sequence number of the next LB transmission
`LtNextSequence`	Displays the sequence number of the next Linktrace (LT) message transmitted
`LtRxUnexplained`	Displays the number of the unexplained Linktrace (LT) messages
`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

Table 34: Service-ID SAP Output Fields (Continued)

Label	Description
`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 124)
`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
`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

Table 34: Service-ID SAP Output Fields (Continued)

Label	Description
`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

Sample Output (Epipe)

```
*A:csasim2>show>service>id# sap 1/3/1 detail

===============================================================================
Service Access Points(SAP)
===============================================================================
Service Id         : 3
SAP                : 1/3/1                    Encap             : q-tag
Admin State        : Up                       Oper State        : Down
LLF Admin State    : Up                       LLF Oper State    : Clear
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                     Oper MTU          : 1518
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          : 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     : 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#
```

Sample Output (Ipipe)

```
*A:ALU-12# show service id 1301 sap 1/2/8:11 detail

===============================================================================
Service Access Points(SAP)
===============================================================================
Service Id         : 1301
SAP                : 1/2/8:11                Encap             : q-tag
Description        : Default sap description for service id 1301
Admin State        : Up                      Oper State        : Up
Flags              : None
Multi Svc Site     : None
Last Status Change : 01/20/2009 16:44:14
```

```
Last Mgmt Change   : 01/21/2009 16:31:04
Sub Type           : regular
Dot1Q Ethertype    : 0x8100                  QinQ Ethertype    : 0x8100

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
Q Frame-Based Acct : Disabled

Acct. Pol          : Default                 Collect Stats     : Enabled
Ce IP Address      : 88.1.10.3
SAP MAC Address    : 00:1a:f0:bd:ab:b0       Mac Refresh Inter*: 14400

-------------------------------------------------------------------------------
Ipipe SAP ARP Entry Info
-------------------------------------------------------------------------------
88.1.10.3       00:00:15:b9:6b:73 dynamic 03h50m24s



-------------------------------------------------------------------------------
QOS
-------------------------------------------------------------------------------
Ingress qos-policy : 13                      Egress qos-policy : 13
Shared Q plcy      : n/a                     Multipoint shared : Disabled
-------------------------------------------------------------------------------
Sap Statistics
-------------------------------------------------------------------------------
Last Cleared Time     : 01/21/2009 14:19:23

                        Packets                 Octets
Forwarding Engine Stats
Dropped               : 0                       0
Off. HiPrio           : 20683584                1613319552
Off. LowPrio          : 1840167                 143533026

Queueing Stats(Ingress QoS Policy 13)
Dro. HiPrio           : 0                       0
Dro. LowPrio          : 0                       0
For. InProf           : 11271525                879178950
For. OutProf          : 11252226                877673628

Queueing Stats(Egress QoS Policy 13)
Dro. InProf           : 0                       0
Dro. OutProf          : 0                       0
For. InProf           : 0                       0
For. OutProf          : 600                     46800
-------------------------------------------------------------------------------
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

Ingress Queue 2 (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

Ingress Queue 3 (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

Ingress Queue 4 (Unicast) (Priority)
Off. HiPrio          : 7304519                 569752482
Off. LoPrio          : 0                       0
Dro. HiPrio          : 0                       0
Dro. LoPrio          : 0                       0
For. InProf          : 5473927                 426966306
For. OutProf         : 1830592                 142786176

Egress Queue 1
For. InProf          : 0                       0
For. OutProf         : 0                       0
Dro. InProf          : 0                       0
Dro. OutProf         : 0                       0

Egress Queue 2
For. InProf          : 0                       0
For. OutProf         : 200                     15600
Dro. InProf          : 0                       0
Dro. OutProf         : 0                       0

Egress Queue 3
For. InProf          : 0                       0
For. OutProf         : 200                     15600
Dro. InProf          : 0                       0
Dro. OutProf         : 0                       0

Egress Queue 4
For. InProf          : 0                       0
For. OutProf         : 200                     15600
Dro. InProf          : 0                       0
Dro. OutProf         : 0                       0
===============================================================================
* indicates that the corresponding row element may have been truncated.

*A:ALU-12#
```

sap-using

Syntax **sap-using** [**sap** *sap-id*]
sap-using [**ingress** | **egress**] **atm-td-profile** *td-profile-id*
sap-using [**ingress** | **egress**] **qos-policy** *qos-policy-id*

Context show>service

Description This command displays SAP information.

If no optional parameters are specified, the command displays a summary of all defined SAPs.

The optional parameters restrict output to only SAPs matching the specified properties.

Parameters **ingress** — specifies matching an ingress policy

egress — specifies matching an egress policy

qos-policy-id — identifies the ingress or egress QoS Policy for which to display matching SAPs

Values 1 to 65535

td-profile-id — displays SAPs using this traffic description

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 The following output is an example of service SAP-using information, and Table 35 describes the fields.

Sample Output

```
*A:ALU-48# show service sap-using
===============================================================================
Service Access Points
===============================================================================
PortId              SvcId      Ing.   Ing.     Egr.   Egr.    Adm  Opr
                               QoS    Fltr     QoS    Fltr
-------------------------------------------------------------------------------
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
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.  Ing.    Egr.  Egr.    Adm  Opr
                                  QoS   Fltr    QoS   Fltr
-------------------------------------------------------------------------------
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.  Ing.    Egr.  Egr.   Adm  Opr
                            QoS   Fltr    QoS   Fltr
------------------------------------------------------------------------------
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#
```

Table 35: Show Service SAP-Using 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

sdp

Syntax **sdp** [*sdp-id* | **far-end** *ip-address*] [**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 *sdp-id* — Displays only information for the specified SDP ID.

Values 1 — 17407

ip-address **—** Displays only SDPs matching the specified far-end IP address.

Default SDPs with any far-end IP address.

detail — Displays detailed SDP information.

Output The following output is an example of service-id SDP information, and Table 36 describes the fields.

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. Octs.     : 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#
```

Table 36: 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

Table 36: SDP Output Fields (Continued)

Label	Description
`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
`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, IacIngressFault, 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

Table 36: SDP Output Fields (Continued)

Label	Description
`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
`Dot1ag Configuration Information`	
`Md-index`	Displays the value of the MD index
`Direction`	Displays the direction of the MEP
`Ma-index`	Displays the value of the MA index
`Admin`	Displays the administrative state of the MEP (enabled or disabled)
`MepId`	Displays the MEP-ID
`CCM-Enable`	Displays the status of the Continuity Check Message (CCM)
`LowestDefectPri`	Displays a configured value that defects are evaluated against
`HighestDefect`	Displays the highest defect
`Defect Flags`	Indicates the defect flags
`Mac Address`	Displays the MAC address (the MAC address for a spoke SDP is the system MAC address; for a SAP, it is the port MAC address)
`CcmLtmPriority`	Displays the priority of the CCM Linktrace Message (LTM)
`CcmTx`	Displays the number of CCM transmissions

Table 36: SDP Output Fields (Continued)

Label	Description
`CcmSequenceErr`	Displays the number of CCM sequence errors
`LbRxReply`	Displays the number of received loopback (LB) replies
`LbRxBadOrder`	Displays the number of LB replies that have been received in the wrong order
`LbRxBadMsdu`	Displays the number of LB replies that have been received with the wrong destination MAC address (MSDU = MAC Service Data Unit)
`LbTxReply`	Displays the number of LBRs (loopback replies) transmitted out this MEP
`LbNextSequence`	Displays the sequence number of the next LB transmission
`LtNextSequence`	Displays the sequence number of the next Linktrace (LT) message transmitted
`LtRxUnexplained`	Displays the number of the unexplained Linktrace (LT) messages
`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 `max-cells` 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 `max-delay` 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

Table 36: SDP Output Fields (Continued)

Label	Description
`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

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 **id** *service-id*

Context clear>service
clear>service>statistics

Description This command clears commands for a specific service.

Parameters *service-id* — uniquely identifies a service

sap

Syntax **sap** *sap-id* {**all | cem | counters**}

Context clear>service>statistics

Description This command clears SAP statistics for a SAP.

Parameters *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

all — clears all SAP queue statistics and STP statistics

cem — clears all queue statistics associated with a acem 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

arp

Syntax **arp**

Context clear>service>id

Description This command clears the ARP entries from an Ipipe service.

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

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

In the HSDPA offload application (see HSDPA Offload on page 51), 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 2.1, 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 311 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 325.

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. 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:

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
                    — interface ip-int-name [create]
                    — no interface ip-int-name
                            — 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
                            — sap sap-id [create]
                            — no sap sap-id
                                    — 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
```

Command Descriptions

IES Management Configuration Commands

Generic Commands

description

Syntax **description** *description-string*
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 *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.

shutdown

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

Context config>service>ies
config>service>ies>interface
config>service>ies>interface>sap

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

IES — the default administrative status of an IES service is down. While the service is down, its associated interface is operationally down.

For example, if1) 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 transmited 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** *service-id* [**customer** *customer-id*] [**create**] [**vpn** *vpn-id*]
no ies *service-id*

Context config>service

Description This command enables Internet Enhanced Service (IES). IES in Release 2.1 of the 7705 SAR is used only for in-band management of the 7705 SAR over ATM links.

The **no** form of this command deletes the IES service instance with the specified *service-id*.

The service cannot be deleted until all the IP interfaces defined within the service ID have been shut down and deleted.

Parameters *service-id* — 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 *service-id* must be the same number used for every 7705 SAR on which this service is defined.

Values 1 to 2147483647

customer-id — 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.

Values 1 to 2147483647

vpn-id — 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.

Values 1 to 2147483647

Default null (0)

IES Interface Commands

interface

Syntax **interface** *ip-int-name* [**create**]
no interface *ip-int-name*

Context config>service>ies

Description 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.

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.

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.

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.

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.

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.

Default **no interface**

Parameters *ip-int-name* — 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.

Values 1 to 32 characters (must start with a letter)

If the *ip-int-name* already exists, the context is changed to maintain that IP interface. If the *ip-int-name* 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 *ip-int-name* does not exist, the interface is created and the context is changed to that interface for further command processing.

address

Syntax **address** {*ip-address*/*mask* | *ip-address netmask*}
no address

Context config>service>ies>interface *ip-int-name*

Description 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.

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.

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.

By default, no IP address or subnet association exists on an IP interface until it is explicitly created.

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.

Default **no address**

Parameters *ip-address* — the IP address of the IP interface. The *ip-address* 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.

Values 1.0.0.0 to 223.255.255.255

/ — the forward slash is a parameter delimiter that separates the *ip-address* portion of the IP address from the mask that defines the scope of the local subnet. No spaces are allowed between the *ip-address*, the “/”, and the *mask* parameter. If a forward slash does not immediately follow the *ip-address*, a dotted decimal mask must follow the prefix.

mask — 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 *ip-address* from the *mask* parameter. The *mask* 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.

Values 1 to 32 (mask length of 32 is reserved for system IP addresses)

netmask — the subnet mask in dotted decimal notation

Values 0.0.0.0 to 255.255.255.255 (network bits all 1 and host bits all 0)

bfd

Syntax **bfd** {*transmit-interval*} [**receive** *receive-interval*] [**multiplier** *multiplier*]
no bfd

Context config>service>ies>interface *ip-int-name*

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 *transmit-interval* — the number of milliseconds between transmitted control messages

Values 100 to 100000

Default 100

receive-interval — the number of milliseconds between received control messages

Values 100 to 100000

Default 100

multiplier — the number of control messages to be sent during the configured transmit and receive intervals

Values 3 to 20

Default 3

ip-mtu

Syntax **ip-mtu** *octets*
no ip-mtu

Context config>service>ies>interface>*ip-int-name*

Description This command configures the IP maximum transmit unit (packet size) for this interface.

The **no** form of the command returns the default value.

Parameters *octets* — the MTU for the interface

Values 512 to 1524

IES SAP Commands

sap

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

Context config>service>ies>interface *ip-int-name*

Description This command creates a SAP within an IES service. Each SAP must be unique.

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.

Enter an existing SAP without the **create** keyword to edit SAP parameters.

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** *port-id* 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.

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.

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.

Default **no sap**

Parameters *sap-id* — specifies the physical port identifier portion of the SAP definition

The *sap-id* can be configured in one of the formats described in Table 37.

Table 37: SAP ID Configurations

Type	Syntax	Example
port-id	*slot*/*mda*/*port*[.*channel*]	1/1/5
atm or ima group	[*port-id* | *bundle-id*][:*vpi*/*vci* | *vpi*]	*port-id*: 1/1/1.1 *bundle-id*: bundle-ima-1/1.1 vpi/vci: 16/32 vpi: 16

Values *sap-id*: atm [*port-id*][:*vpi*/*vci* | *vpi*]
IMA group [*bundle-id*][:*vpi*/*vci* | *vpi*]

port-id *slot/mda/port*[.*channel*]
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

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 *ip-int-name*>sap *sap-id*

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** *ip-filter-id*
no filter
no filter [**ip** *ip-filter-id*]

Context config>service>ies>interface *ip-int-name*>sap *sap-id*>ingress

Description 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.

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.

The **no** form of this command removes any configured filter ID association with the SAP.

Default **no filter**

Parameters *ip-filter-id* — 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 *ip-int-name*>sap *sap-id*

Description 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:

- 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

If ATM functionality is not supported for a given context, the command returns an error.

encapsulation

Syntax **encapsulation** *atm-encap-type*

Context config>service>ies>interface *ip-int-name*>sap *sap-id*>atm

Description This command configures an ATM VC SAP for encapsulation in accordance with RFC 2684, *Multiprotocol Encapsulation over ATM Adaptation Layer 5*.

In Release 2.1, the only supported encapsulation type is aal5mux-ip.

Ingress traffic that does not match the configured encapsulation is dropped.

Default **aal5mux-ip**

Parameters *atm-encap-type* — aal5mux-ip (routed IP encapsulation for a VC multiplexed circuit as defined in RFC 2684)

egress

Syntax **egress**

Context config>service>ies>interface *ip-int-name*>sap *sap-id*>atm

Description This command provides access to the context to configure egress ATM traffic policies for the SAP.

ingress

Syntax **ingress**

Context config>service>ies>interface *ip-int-name*>sap *sap-id*>atm

Description This command provides access to the context to configure ingress ATM traffic policies for the SAP.

traffic-desc

Syntax **traffic-desc** *traffic-desc-profile-id*
no traffic-desc

Context config>service>ies>interface *ip-int-name*>sap *sap-id*>atm>egress
config>service>ies>interface *ip-int-name*>sap *sap-id*>atm>ingress

Description This command assigns an ATM traffic descriptor profile to an egress or ingress 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.

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.

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 ATM VC SAPs.

Parameters *traffic-desc-profile-id* — 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 *ip-int-name*>sap *sap-id*>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 *ip-int-name*>sap *sap-id*>atm>oam

Description 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.

Layer 2 OAM AIS/RDI cells that are received on the IES SAP will cause the IP interface to be disabled.

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.

Default **enabled**

Show Commands

all

Syntax **all**

Context show>service>id

Description This command displays detailed information for all aspects of the service.

Output The following output is an example of service-id all information, and Table 38 describes the fields.

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
```

```
-------------------------------------------------------------------------------
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 232.

Table 38: 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
`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

Table 38: Show Service ID All Command Output Fields (Continued)

Label	Description
`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
`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)`	

Table 38: Show Service ID All Command Output Fields (Continued)

Label	Description
`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` *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 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

Table 38: Show Service ID All Command Output Fields (Continued)

Label	Description
`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
`AAL-5 Encap`	Specifies the AAL-5 encapsulation type — for Release 2.1, 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
`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 2.1, 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

Table 38: Show Service ID All Command Output Fields (Continued)

Label	Description
`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
`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

OAM and SAA

In This Chapter

This chapter provides information about the Operations, Administration and Maintenance (OAM) and Service Assurance Agent (SAA) commands available in the CLI for troubleshooting services.

Topics in this chapter include:

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.

ICMP Diagnostics

ICMP sends and receives control and error messages used to manage the behavior of the TCP/IP stack. ICMP provides:

- debugging tools and error reporting mechanisms to assist in troubleshooting an IP network
- the ability to send and receive error and control messages to far-end IP entities

Ping

Ping is used to determine if there is IP layer connectivity between the 7705 SAR and another node in the network.

Traceroute

Traceroute is used to determine the path that an IP packet takes from the 7705 SAR to a specified router.

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

LSP traceroute sends a packet to each transit 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 litigation 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 (Virtual Circuit Connectivity Verification) and VCCV trace, the VLL diagnostic capabilities for the 7705 SAR.

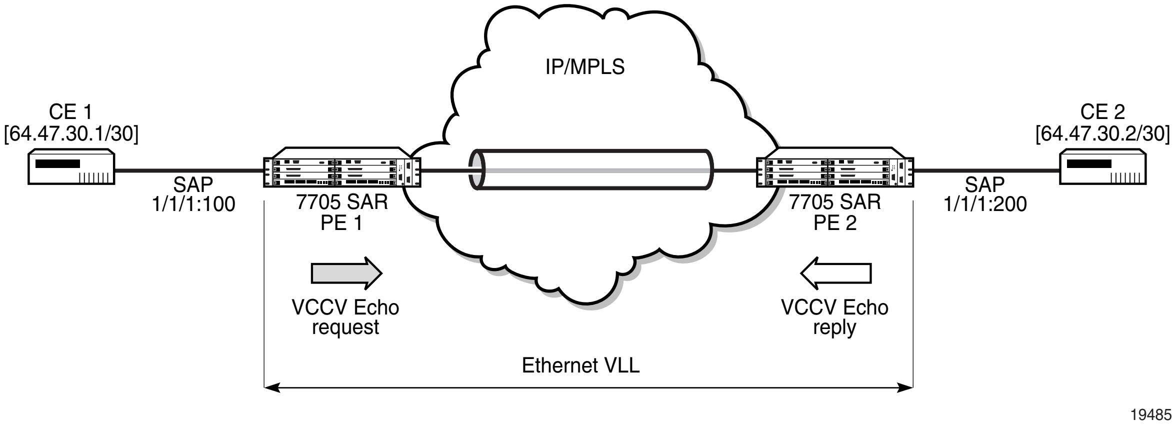
VCCV Ping

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 31). PE2 should be able to distinguish, on the receive side, VCCV control messages from user packets on that VLL.

Figure 31: VCCV Ping Application



VCCV-based PW tests are only supported on dynamically signaled PWs (not on statically signaled PWs).

There are three methods of encapsulating a VCCV message in a VLL, which translates into three types of control channels, as follows:

- Type 1 — in-band VCCV (special control word)

  Type 1 uses the OAM control word, which is shown in Figure 32.

  Figure 32: OAM Control Word Format

  ```
  0                   1                   2                   3
  0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
  |0 0 0 1| FmtID |   Reserved    |         Channel Type          |
  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
  ```

  In Figure 32, the first nibble is set to 0x1. The Format ID and the Reserved fields are set to 0 and the Channel Type is the code point associated with the VCCV IP control channel, as specified in the PWE3 IANA registry [RFC 4446]. The channel type value of 0x21 indicates that the Associated Channel carries an IPv4 packet.

  The use of the OAM control word assumes that the *draft-martini* control word is also used for the user packets. This means that if the control word is optional for a VLL and is not configured, the 7705 SAR PE node will only advertise the router alert label as the CC capability in the Label Mapping message.

  This method is supported by the 7705 SAR.

- Type 2 — out-of-band VCCV (router alert above the service label)

  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. This effectively means it will not troubleshoot the appropriate path.

  This method is supported on the 7705 SAR.

- Type 3 — TTL expiry VCCV (service label TTL = 1 and special control word)

  This method is not supported by the 7705 SAR.

When sending the label mapping message for the VLL, PE1 and PE2 must indicate which of the above OAM packet encapsulation methods (that is, which control channel type) they support. This is accomplished by including an optional VCCV TLV in the PW FEC interface parameter field. The format of the VCCV TLV is shown in Figure 33.

Note that the absence of the optional VCCV TLV in the Interface parameters field of the pseudowire FEC indicates the PE has no VCCV capability.

Figure 33: VCCV TLV

```
0                   1                   2                   3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
|     0x0c      |     0x04      |   CC Types    |   CV Types    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
```

In Figure 33, the Control Channel (CC) Type field is a bit mask used to indicate if the PE supports none, one, or many control channel types.

- 0x00 — none of the following VCCV control channel types are supported
- 0x01 — (Type 1, in-band) PWE3 OAM control word (see Figure 32)
- 0x02 — (Type 2, out-of-band) MPLS router alert label
- 0x04 — (Type 3, not supported on 7705 SAR) MPLS inner label TTL = 1

If both PE nodes support more than one of the CC types, then a 7705 SAR PE will make use of the CC type with the lowest type value. For instance, OAM control word (0x01) will be used in preference to the MPLS router alert label (0x02).

The Connectivity Verification (CV) Type field is a bit mask used to indicate the specific type of VCCV packets to be sent over the VCCV control channel. The possible values supported on the 7705 SAR are:

- 0x00 — none of the following VCCV packet types are supported
- 0x02 — LSP Ping.

  This value is used in VCCV ping application and applies to a VLL over an MPLS or a GRE SDP.

A VCCV ping is an LSP echo request message as defined in RFC 4379. 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:

- do not reply

  This mode is supported by the 7705 SAR.
- reply by an IPv4 UDP packet

  This mode is supported by the 7705 SAR.

- reply via an IPv4 UDP packet with router alert

  This mode is not supported by the 7705 SAR.

  ➡ **Note:** Do not confuse this mode, which sets the router alert bit in the IP header, with the CC type that makes use of the router alert label.

- 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 mode is supported by the 7705 SAR.

The VCCV ping reply has the same format as an LSP echo reply message as defined in RFC 4379. 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 that 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 RFC 5085.

VCCV Trace

VCCV-trace is similar to LSP-trace. VCCV-trace is used to trace the entire path of a pseudowire (PW) with a single command.

VCCV-trace is useful in multi-segment PW (MS-PW) applications where a single PW traverses one or more switched-PEs (S-PEs). VCCV-trace is an iterative process by which the initiating T-PE (that is, the 7705 SAR) sends successive VCCV-ping messages, each message having an incrementing TTL value, starting from TTL=1. The procedure for each iteration is the same as that for VCCV-ping, where each node in which the VC label TTL expires will check the FEC and reply with the FEC to the downstream S-PE or far-end T-PE (that is, the far-end 7705 SAR) node. The process is terminated when the reply is from the far-end T-PE (that is, the far-end 7705 SAR) or when a timeout occurs.

The results of a VCCV-trace can be displayed for a fewer number of pseudowire segments of the end-to-end MS-PW path. In this case, the `min-ttl` and `max-ttl` parameters should be configured accordingly. However, the T-PE or S-PE node will still probe all hops up to the `min-ttl` value in order to correctly build the FEC of the desired subset of segments.

In Release 2.1, VCCV-trace can only be issued from a 7705 SAR used as a T-PE.

Ethernet OAM Capabilities

Ethernet OAM capabilities on the 7705 SAR are discussed in the following sections:

- Ethernet OAM Overview
- ETH-CFM (802.1ag)
- EFM OAM (802.3ah)

Ethernet OAM Overview

Ethernet OAM capabilities on the 7705 SAR include:

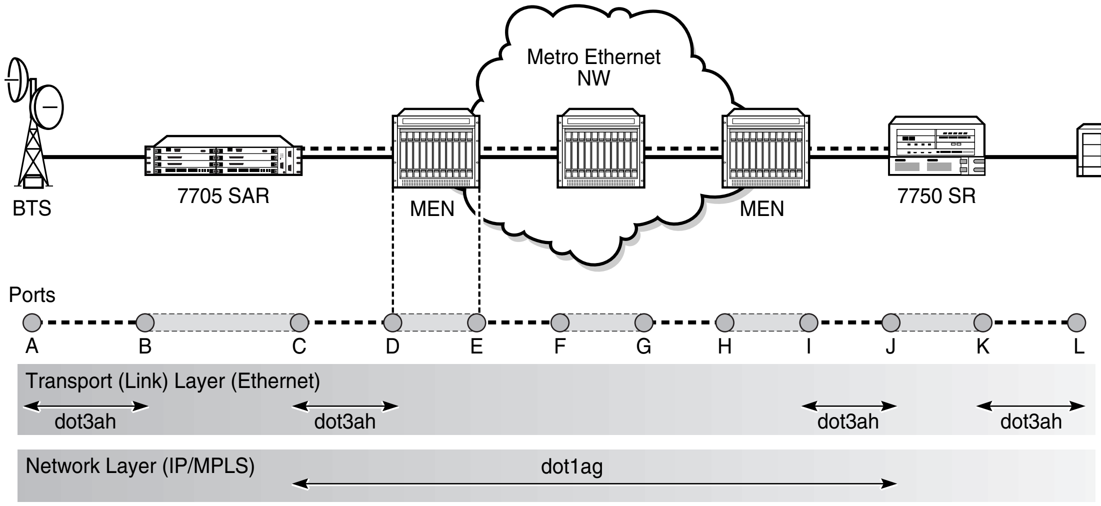
- IEEE 802.1ag (dot1ag) to provide Ethernet Connectivity Fault Management (ETH-CFM) OAM capabilities for the network layer ("network layer" in this instance refers to an end-to-end context across a network, not as a reference to the OSI model)
- IEEE 802.3ah (dot3ah) to provide Ethernet First Mile (EFM) OAM capabilities for the transport layer ("transport layer" in this instance refers to a point-to-point link context or transport hop, not as a reference to the OSI model)

Ethernet OAM capabilities on the 7705 SAR are similar to the OAM capabilities offered in SONET/SDH networks and include loopback tests to verify end-to-end connectivity, test pattern generation (and response) to verify error-free operation, and alarm message generation in case of fault conditions to ensure that the far end is notified of the failure.

Ethernet OAM configurations are maintained across Control and Switching module (CSM) switchovers.

Figure 34 illustrates the complementary use of dot3ah and dot1ag to locate points of failure along a route from BTS to BSC. From the IP/MPLS (network) layer perspective, the 7705 SAR looks as though it is connected directly to the 7750 SR. From the Ethernet (transport) layer perspective, the route passes through many ports and nodes, where each port or node is a potential point of failure. These failure points cannot be detected using IP/MPLS OAM capabilities (that is, ETH-CFM, also referred to as dot1ag). However, they can be detected using EFM OAM (dot3ah) capabilities.

Figure 34: 7705 SAR Ethernet OAM Endpoints



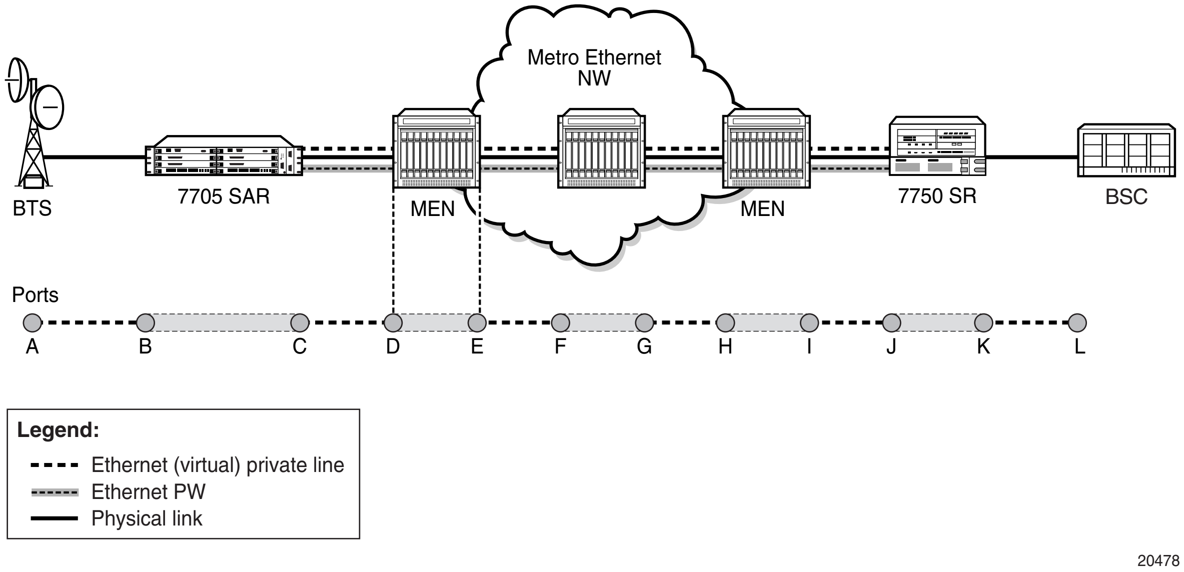
Dot3ah uses port-level loopbacks to check and verify last-mile Ethernet frame integrity, connectivity verification between ports and nodes, and so on. As shown in Figure 34, dot3ah provides transport (link) layer OAM between the BTS and the 7705 SAR access port facing the BTS (ports A and B), or between the 7705 SAR network port and the MEN switch (ports C and D). Ethernet first mile (EFM) OAM allows users to test frame integrity and detect Ethernet layer failures faster than using associated heart-beat messages.

Dot1ag checks end-to-end connectivity across an Ethernet PW (across a network). Since end-to-end connectivity differs depending on the service provided and the span of the network, dot1ag can operate at several MD levels (as defined in the IEEE 802.1ag standard). For example, in Figure 34, ETH-CFM (dot1ag) could be used by a MEN provider to ensure connectivity between ports D and I (or possibly all the way to their customer's Ethernet ports, C and J). Similarly, a Mobile Backhaul Service Provider (MBSP) can use dot1ag to ensure connectivity between ports B and K (and possibly between ports A and L).

Figure 35 and Figure 36 illustrate the use of ETH-CFM to verify connectivity across an Ethernet PW and EFM OAM to verify transport layer connectivity between two directly connected nodes.

For example, in Figure 35, a mobile backhaul service provider (MBSP) can use dot1ag between the two Ethernet spoke SDP endpoints (ports C and J, which define the Ethernet PW) to ensure connectivity. Similarly, a MEP can use dot1ag between ports D and I to ensure the health status of the Ethernet (virtual) private line.

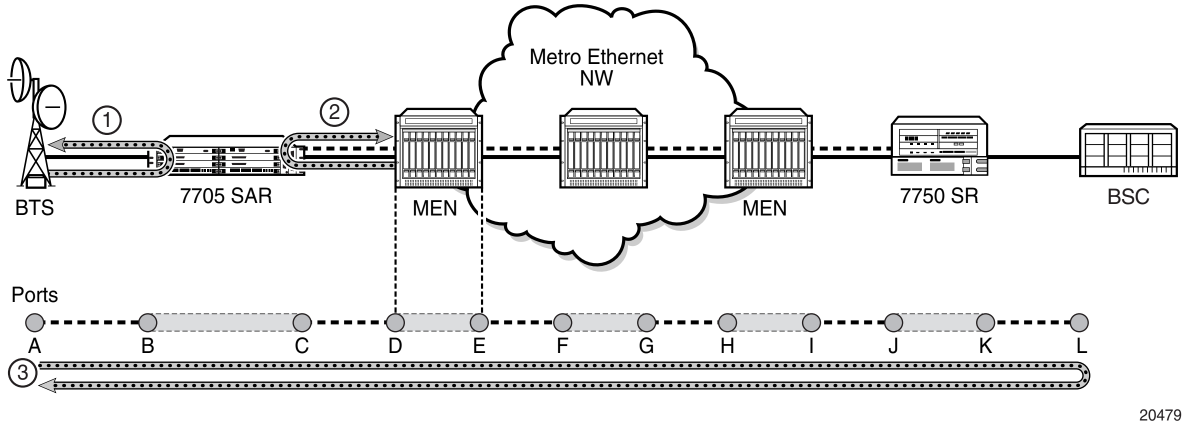
Figure 35: Dot1ag Capabilities on the 7705 SAR



In Figure 36, EFM OAM ensures transport layer connectivity between two directly connected nodes. Figure 36 illustrates three scenarios in which EFM can be used by the MEN provider to ensure error-free connectivity to the 7705 SAR (the cell site) via loopback tests, including:

- scenario 1: EFM termination at the Ethernet access port, which includes loopback tests, heart-beat messages at the Ethernet layer with dying gasp and termination of customer device-initiated EFM packets at the access port
- scenario 2: EFM termination at the Ethernet network port, which includes network side loopbacks
- scenario 3: EFM tunneling through an Epipe service

Figure 36: EFM OAM (Dot3ah) Capabilities on the 7705 SAR



ETH-CFM (802.1ag)

Ethernet Connectivity Fault Management (ETH-CFM) is defined in the IEEE 802.1ag standard. It specifies protocols, procedures, and managed objects to support fault management (including discovery and verification of the path), detection, and isolation of a connectivity fault for each Ethernet service instance.

IEEE 802.1ag can detect:

- loss of connectivity
- unidirectional loss
- loops
- merging of services

CFM uses Ethernet frames and can be distinguished by its Ethertype and special Ethernet multicast addresses. CFM frames are only processed by IEEE MAC bridges. With ETH-CFM, interoperability can be achieved between different vendor equipment in the service provider network, up to and including customer premises bridges.

ETH-CFM is configured at the global level and the Ethernet service level. The following attributes and their configuration levels are listed below:

- global level
  - → MA
  - → MD
  - → MD level
- Ethernet service level
  - → MEP

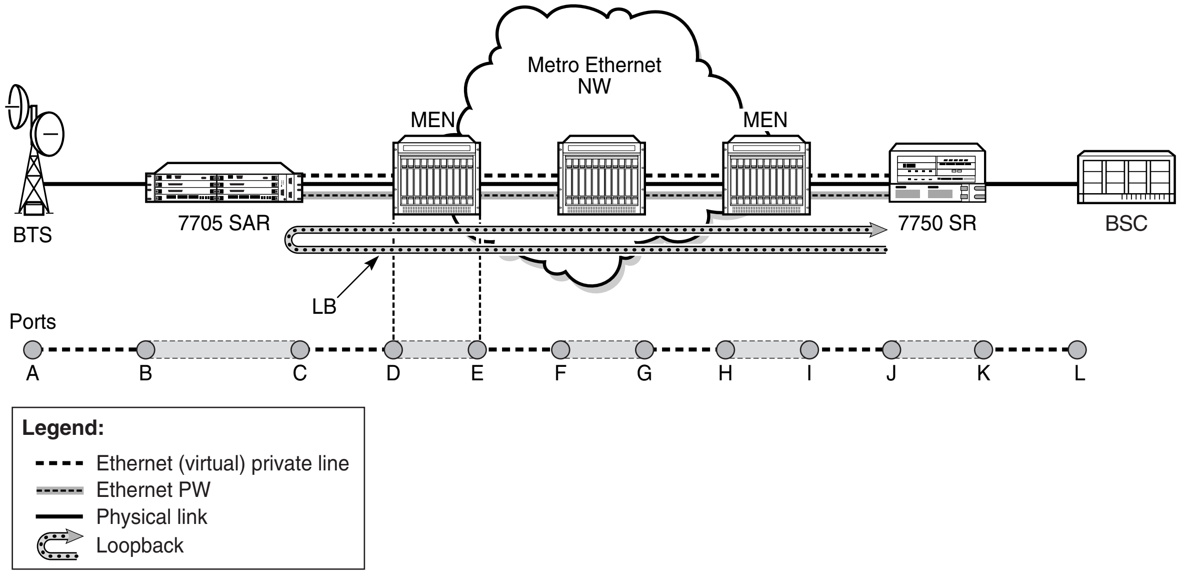
For more information on ETH-CFM, see ETH-CFM (802.1ag) on page 68 (global level) and ETH-CFM (802.1ag) on page 138 (VLL service level).

Loopback (LB)

A Loopback Message (LBM) is generated by a MEP to its peer MEP. Both dot1ag and dot3ah loopbacks are supported. Its function is similar to IP or MPLS ping in that it verifies Ethernet connectivity between the nodes on a per-request basis. That is, it is non-periodic and is only initiated by a user request.

In Figure 37, the line labeled LB represents the dot1ag loopback message between the 7750 SR (source) and 7705 SAR (target) over an Epipe. The 7750 SR-generated LBM is switched to the 7705 SAR, where the LBM message is processed. Once the 7705 SAR generates the Loopback Reply message (LBR), the LBR is switched over the Ethernet PW to the 7750 SR.

Figure 37: Dot1ag Loopback Test



Linktrace (LT)

A Linktrace Message (LTM) is originated by a MEP and targeted to a peer MEP in the same MA and within the same MD level. Its function is similar to IP traceroute. The peer MEP responds with a Linktrace Reply (LTR) message after successful inspection of the LTM.

Continuity Check (CC)

A Continuity Check Message (CCM) is a multicast frame that is generated by a MEP and sent to its remote MEPs in the same MA. The CCM does not require a reply message. To identify faults, the receiving MEP maintains a MEP database with the MAC addresses of the remote MEPs with which it expects to maintain connectivity checking. The MEP database can be provisioned manually. If there is no CCM from a monitored remote MEP in a preconfigured period, the local MEP raises an alarm.

The following CC capabilities are supported:

- enable and disable CC for a MEP
- automatically put local MEPs into the database when they are created
- manually configure and delete the MEP entries in the CC MEP monitoring database. Note that the only local provisioning required to identify a remote MEP is the remote MEP identifier (using the `remote-mepid` *`mep-id`* command).
- CCM transmit interval: 10ms, 100ms, 1s, 10s, 1m, 10m (default: 10s)
- CCM declares a fault, when it:
  - → stops hearing from one of the remote MEPs for a period of 3.5 times the CC interval
  - → hears from a MEP with a lower MD level
  - → hears from a MEP that is not in the same MA
  - → hears from a MEP that is in the same MA but is not in the configured MEP list
  - → hears from a MEP that is in the same MA with the same MEP id as the receiving MEP
  - → recognizes that the CC interval of the remote MEP does not match the local configured CC interval
  - → recognizes that the remote MEP declares a fault

    An alarm is raised and a trap is sent if the defect is greater than or equal to the configured low-priority-defect value.

EFM OAM (802.3ah)

802.3ah clause 57 defines the Ethernet First Mile (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 that 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.

EFM is configured at the Ethernet port level. For more information, see the 7705 SAR OS Interface Configuration Guide.

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 by enabling the OAM remote loopback command. After receiving the loopback control OAMPDU, the remote OAM client puts the remote port into local loopback mode.

OAMPDUs are slow protocol frames that contain appropriate control and status information used to monitor, test, and troubleshoot OAM-enabled links.

To exit a remote loopback, the local EFM OAM client sends a loopback control OAMPDU by disabling the OAM remote loopback command. After receiving the loopback control OAMPDU, the remote OAM client puts the port back into normal forwarding mode.

When a port is in local loopback mode (the far end requested an Ethernet OAM loopback), any packets received on the port will be looped back, except for EFM OAMPDUs. No data will be transmitted from the node; only data that is received on the node will be sent back out.

When the node is in remote loopback mode, local data from the CSM is transmitted, but any data received on the node is dropped, except for EFM OAMPDUs.

When a port is in loopback mode, service mirroring is not operational if the port is a mirror-source or mirror-destination SAP.

Remote loopbacks should be used with caution; if dynamic signaling and routing protocols are used, all services go down when a remote loopback is initiated. If only static signaling and routing is used, the services stay up. On the 7705 SAR, the Ethernet port can be configured to accept or reject the remote-loopback command.

802.3ah OAMPDU Tunneling and Termination for Epipe Services

Customers who subscribe to Epipe service might have customer equipment running 802.3ah at both ends. The 7705 SAR can be configured to tunnel EFM OAMPDUs received from a customer device to the other end through the existing network using MPLS or GRE, or to terminate received OAMPDUs at a network or an access Ethernet port.

Note: This feature applies only to port-based Epipe SAPs because 802.3ah runs at port level, not at VLAN level.

While tunneling offers the ability to terminate and process the OAM messages at the head-end, termination on the first access port at the cell site can be used to detect immediate failures or can be used to detect port failures in a timelier manner.

The user can choose either tunneling or termination, but not both at the same time.

In Figure 36, scenario 1 shows the termination of received EFM OAMPDUs from a customer device on an access port, while scenario 2 shows the same thing except for a network port. Scenario 3 shows tunneling of EFM OAMPDUs through the associated Ethernet PW. To configure termination (scenario 1), use the `config>port>ethernet> efm-oam>no shutdown` command.

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 343). 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* × 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 (SAA) 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 for parameters such as latency, jitter, 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.

For SAA ICMP ping, one-way timestamping can be enabled at the system level for all outbound SAA ICMP ping packets.

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 because 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 which hop is being measured.

SAA Jitter

Mobile operators require millisecond-level granularity when it comes to delay and jitter measurements. This is especially true for synchronization-over-packet based applications.

Two-way jitter tests measure the jitter in each direction separately. For the most accurate two-way SAA jitter test results, the ingress timestamp function should occur on the network process (NP) of the 7705 SAR adapter card (that is, the timestamp for traffic received from a port should occur on an adapter card). The 7705 SAR provides two-way jitter tests with millisecond granularity for all network deployment applications.

Configuring SAA Test Parameters

Use the following CLI syntax to create an SAA test and set 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 4
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 4
            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
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
```

OAM and SAA Command Reference

Command Hierarchies

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*]
  - **vccv-trace** *sdp-id:vc-id* [**size** *octets*] [**min-ttl** *min-vc-label-ttl*] [**max-ttl** *max-vc-label-ttl*] [**max-fail** *no-response-count*] [**probe-count** *probe-count*] [**reply-mode ip-routed** | **control-channel**] [**timeout** *timeout-value*] [**interval** *interval-value*] [**fc** *fc-name* [**profile {in** | **out}**]] [**detail**]

Ethernet in the First Mile (EFM) Commands

global
- **oam**
  - **efm** *port-id*
    - **local-loopback** {**start** | **stop**}
    - **remote-loopback** {**start** | **stop**}

ETH-CFM Commands

global
- **oam**
  - **eth-cfm**
    - **linktrace** *mac-address* **mep** *mep-id* **domain** *md-index* **association** *ma-index* [**ttl** *ttl-value*]
    - **loopback** *mac-address* **mep** *mep-id* **domain** *md-index* **association** *ma-index* [**send-count** *send-count*] [**size** *data-size*] [**priority** *priority*]

SAA Configuration Commands

```
config
    — saa
        — [no] test test-name [owner test-owner]
            — description description-string
            — no description
            — jitter-event rising-threshold threshold [falling-threshold threshold] [direction]
            — no jitter-event
            — [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] [fc fc-name [profile {in | out}]]
                — icmp-trace [ip-address | dns-name] [ttl time-to-live] [wait milli-
                  seconds] [tos type-of-service] [source ip-address] [tos type-of-service]
                  [router router-instance]
                — 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]
                — vccv-trace sdp-id:vc-id [size octets] [min-ttl min-vc-label-ttl] [max-ttl
                  max-vc-label-ttl] [max-fail no-response-count] [probe-count probe-
                  count] [reply-mode {ip-routed | control-channel}] [timeout timeout-
                  value] [interval interval-value] [fc fc-name [profile {in |out}]] [detail]

config
    — system
        — enable-icmp-vse
        — no enable-icmp-vse
```

SAA Diagnostics

global
— **oam**
— **saa** *test-name* [**owner** *test-owner*] {**start** | **stop**}

Show Commands

show
- — **eth-cfm**
  - — **association** [*ma-index*] [**detail**]
  - — **cfm-stack-table**
  - — **cfm-stack-table** [**port** [*port-id* [**vlan** *vlan-id*] | **sdp** *sdp-id*[**:***vc-id*]] [**level** *0..7*] [**direction down**]
  - — **domain** [*md-index*] [**association** *ma-index* | **all-associations**] [**detail**]
  - — **mep** *mep-id* **domain** *md-index* **association** *ma-index* [**loopback**] [**linktrace**]
- — **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**

Command Descriptions

OAM and SAA Commands

Operational Commands

ping

Syntax	**ping** [*ip-address* **|** *dns-name*] [**rapid | detail**] [**ttl** *time-to-live*] [**tos** *type-of-service*] [**size** *bytes*] [**pattern** *pattern*] [**source** *ip-address*] [**interval** *interval*] [**{next-hop** *ip-address***} | {interface** *interface-name***} | bypass-routing**] [**count** *requests*] [**do-not-fragment**] [**router** *router-instance*] [**timeout** *timeout*]
Context	<GLOBAL>
Description	This command verifies the reachability of a remote host.

Parameters

ip-address — identifies the far-end IP address to which to send the **svc-ping** request message in dotted decimal notation

Values ipv4-address: a.b.c.d
dns-name

dns-name — identifies the DNS name of the far-end device to which to send the **svc-ping** request message, expressed as a character string

rapid — specifies that packets will be generated as fast as possible instead of the default 1 per second

detail — displays detailed information

time-to-live **—** specifies the TTL value for the MPLS label, expressed as a decimal integer

Values 1 to 128

type-of-service **—** specifies the service type

Values 0 to 255

bytes **—** specifies the request packet size in bytes, expressed as a decimal integer

Values 0 to 16384

pattern **—** 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

Values 0 to 65535

source *ip-address* **—** specifies the IP address to be used

Values ipv4-address: a.b.c.d

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.

Values 1 to 10

Default 1

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-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

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-instance — specifies the router name or service ID

Values	router-name:	Base, management
	service-id:	1 to 2147483647

Default Base

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.

Values 1 to 10

Default 5

shutdown

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

Context config>saa>test

Description 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.

When a test is created, it remains in shutdown mode until a **no shutdown** command is executed.

In order to modify an existing test, it must first be shut down.

The **no** form of this command sets the state of the test to operational.

traceroute

Syntax **traceroute** [*ip-address* | *dns-name*] [**ttl** *ttl*] [**wait** *milli-seconds*] [**no-dns**] [**source** *ip-address*] [**tos** *type-of-service*] [**router** *router-instance*]

Context <GLOBAL>

Description This command determines the route to a destination address.

Parameters *ip-address* — specifies the far-end IP address to which to send the traceroute request message in dotted decimal notation

Values ipv4-address : a.b.c.d

dns-name — specifies the DNS name of the far-end device to which to send the traceroute request message, expressed as a character string

ttl — specifies the maximum Time-To-Live (TTL) value to include in the traceroute request, expressed as a decimal integer

Values 1 to 255

milli-seconds — specifies the time in milliseconds to wait for a response to a probe, expressed as a decimal integer

Values 10 to 60000

Default 5000

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

Default DNS lookups of the responding hosts are performed

source *ip-address* — 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.

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-instance — specifies a router name or service ID

Values	router-name	Base, management
	service-id	1 to 2147483647

Default Base

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

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 **—** 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.

Values 1 to 100

Default 1

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.

Values 1 to 10

Default 5

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.

Values	1 to 10
Default	1

Service Diagnostics

sdp-mtu

Syntax **sdp-mtu** *orig-sdp-id* **size-inc** *start-octets end-octets* [**step** *step-size*] [**timeout** *timeout*] [**interval** *interval*]

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 *orig-sdp-id* — 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 *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

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-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.

Values 1 to 512

Default 32

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.

Values 1 to 10

Default 5

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.

Values 1 to 10

Default 1

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.

Table 39 describes the SVC ping report fields.

Table 39: 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 *service-id* does not exist locally, N/A is displayed.	Epipe, Apipe TLS IES Mirror-Dest N/A
Local Service Admin State	The local administrative state of *service-id*. 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 *service-id*. 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 *service-id* does not exist remotely, N/A is displayed.	Epipe, Apipe TLS IES Mirror-Dest N/A

Table 39: SVC Ping Report Fields (Continued)

Field	Description	Values
Remote Service Admin State	The remote administrative state of *service-id*. 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 *service-id*. If the service does not exist, N/A is displayed.	service-mtu N/A
Remote Service MTU	The remote **service-mtu** for *service-id*. If the service does not exist remotely, N/A is displayed.	remote-service-mtu N/A
Local Customer ID	The local *customer-id* associated with *service-id*. If the service does not exist locally, N/A is displayed.	customer-id N/A
Remote Customer ID	The remote *customer-id* associated with *service-id*. 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 39: 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 *service-id* 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 *service-id*. 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 *service-id*. If an SDP-ID is not bound to the service, N/A is displayed.	Oper-Up Oper-Down N/A

Table 39: 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 *service-id*, 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 *service-id*. 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 *service-id*. 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 *service-id*. 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 *service-id*. 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 *service-id*. If the SDP-ID signaling is off, *originator-vc-id* is 0. If the *originator-vc-id* does not exist, N/A is displayed.	originator-vc-id N/A

Table 39: SVC Ping Report Fields (Continued)

Field	Description	Values
Responding VC-ID	The responder's VC-ID associated with the SDP-ID to *originator-id* that is bound to *service-id*. If the SDP-ID signaling is off or the service binding to SDP-ID does not exist, *responder-vc-id* 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 *service-id* for the originating SDP-ID. If *service-id* does not exist locally, N/A is displayed. If *service-id* 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 *service-id* 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 *service-id* 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 *service-id* to the originating 7705 SAR. If *service-id* does not exist in the remote 7705 SAR, N/A is displayed. If *service-id* 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 *service-id* 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 *service-id* does not exist or the responder's egress service label is non-existent, N/A is displayed.	Up Down N/A

Table 39: 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 *service-id* when sending to the originating 7705 SAR. If *service-id* does not exist locally, N/A is displayed. If *service-id* 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 *service-id* 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 *service-id* 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 *service-id* when sending to the originating 7705 SAR. If *service-id* does not exist in the remote 7705 SAR, N/A is displayed. If *service-id* 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 *service-id* 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 *service-id* 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-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 40 indicates whether a message is sent and how the message is encapsulated based on the state of the service ID.

Table 40: 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 41 indicates how the message response is encapsulated based on the state of the remote Service ID.

Table 41: 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** *port-id*

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

ETH-CFM Commands

linktrace

Syntax **linktrace** *mac-address* **mep** *mep-id* **domain** *md-index* **association** *ma-index* [**ttl** *ttl-value*]

Context oam>eth-cfm

Description This command specifies to initiate a linktrace test.

Parameters *mac-address* — specifies a unicast destination MAC address

mep-id — specifies the target MAC address

Values 1 to 8191

md-index — specifies the MD index

Values 1 to 4294967295

ma-index — specifies the MA index

Values 1 to 4294967295

ttl-value — specifies the TTL for a returned linktrace

Values 0 to 255

loopback

Syntax **loopback** *mac-address* **mep** *mep-id* **domain** *md-index* **association** *ma-index* [**send-count** *send-count*] [**size** *data-size*] [**priority** *priority*]

Context oam>eth-cfm

Description This command specifies to initiate a loopback test.

Parameters *mac-address* — specifies a unicast MAC address

mep-id — specifies the target MAC address

Values 1 to 8191

md-index — specifies the MD index

Values 1 to 4294967295

ma-index — specifies the MA index

Values 1 to 4294967295

send-count — specifies the number of messages to send, expressed as a decimal integer. Dot1ag loopback messages are sent back-to-back, with no delay between the transmissions.

Values 1 to 5

Default 1

data-size — specifies the packet size in bytes, expressed as a decimal integer

Values 0 to 1500

priority — specifies a 3-bit value to be used in the VLAN tag, if present, in the transmitted frame

Values 0 to 7

Service Assurance Agent (SAA) Commands

saa

Syntax **saa**

Context config

Description This command creates the context to configure the SAA tests.

test

Syntax **test** *test-name* [**owner** *test-owner*]
[**no**] **test** *test-name* [**owner** *test-owner*]

Context config>saa

Description 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.

A test must be shut down before it can be modified or removed from the configuration.

The **no** form of this command removes the test from the configuration.

Parameters *test-name* — identifies the saa test name to be created or edited

test-owner **—** specifies the owner of an SAA operation, up to 32 characters in length

Values if a *test-owner* value is not specified, tests created by the CLI have a default owner "TiMOS CLI"

description

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

Context config>saa>test

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 configuration.

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.

jitter-event

Syntax **jitter-event rising-threshold** *threshold* [**falling-threshold** *threshold*] [*direction*]
no jitter-event

Context config>saa>test

Description This command specifies that at the termination of an SAA test probe, the calculated jitter value is evaluated against the configured rising and falling jitter thresholds. SAA threshold events are generated as required.

Once the threshold (rising/falling) is crossed, it is disabled from generating additional events until the opposite threshold is crossed. If a falling-threshold is not supplied, the rising threshold will be re-enabled when it falls below the threshold after the initial crossing that generated the event.

The configuration of jitter event thresholds is optional.

Parameters **rising-threshold** *threshold* — specifies a rising threshold jitter value. When the test run is completed, the calculated jitter value is compared to the configured jitter rising threshold. If the test run jitter 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.

Values 0 to 2147483 milliseconds

Default 0

falling-threshold *threshold* — specifies a falling threshold jitter value. When the test run is completed, the calculated jitter value is compared to the configured jitter falling threshold. If the test run jitter 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.

Values 0 to 2147483 milliseconds

Default 0

direction — specifies the direction for OAM ping responses received for an OAM ping test run

Values **inbound** — monitor the value of jitter calculated for the inbound, one-way, OAM ping responses received for an OAM ping test run

outbound — monitor the value of jitter calculated for the outbound, one-way, OAM ping requests sent for an OAM ping test run

roundtrip — monitor the value of jitter calculated for the round trip, two-way, OAM ping requests and replies for an OAM ping test run

Default roundtrip

latency-event

Syntax [**no**] **latency-event rising-threshold** *threshold* [**falling-threshold** *threshold*] [*direction*]

Context config>saa>test

Description 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.

The configuration of latency event thresholds is optional.

Parameters **rising-threshold** *threshold* **—** 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.

Values 0 to 2147483647 ms

Default 0

falling-threshold *threshold* **—** 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.

Values 0 to 2147483647 ms

Default 0

direction — specifies the direction for OAM ping responses received for an OAM ping test run

Values **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

Default roundtrip

loss-event

Syntax [**no**] **loss-event rising-threshold** *threshold* [**falling-threshold** *threshold*] [*direction*]

Context config>saa>test

Description 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.

The configuration of loss event thresholds is optional.

Parameters **rising-threshold** *threshold* **—** 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.

Values 0 to 2147483647 packets

Default 0

falling-threshold *threshold* **—** 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.

Values 0 to 2147483647 packets

Default 0

direction — specifies the direction for OAM ping responses received for an OAM ping test run

Values **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

Default roundtrip

type

Syntax [**no**] **type**

Context config>saa>test

Description This command creates the context to provide the test type for the named test. Only a single test type can be configured.

A test can only be modified while the test is in shutdown mode.

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.

To change the test type, the old command must be removed using the **config>saa>test>no type** command.

icmp-ping

Syntax **icmp-ping** [*ip-address* **|** *dns-name*] [**rapid | detail**] [**ttl** t*ime-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*] [**fc** *fc-name* [**profile** {**in | out**}]]

Context config>saa>test>type

Description This command configures an ICMP ping 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

time-to-live **—** specifies the TTL value for the MPLS label, expressed as a decimal integer

Values 1 to 128

Default 64

type-of-service **—** specifies the service type

Values 0 to 255

Default 0

bytes — specifies the request packet size in bytes, expressed as a decimal integer

Values	0 to 16384
Default	56

pattern — 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.

Values	0 to 65535

source *ip-address* — specifies the IP address to be used

Values	ipv4-address:	a.b.c.d

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.

Values	1 to 10000
Default	1

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-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

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-instance — specifies the router name or service ID

Values	router-name:	Base, management
	service-id:	1 to 2147483647
Default	Base	

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.

Values 1 to 10

Default 5

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 SAR.

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

Default nc

profile {**in** | **out**} — specifies the profile state of the MPLS echo request encapsulation

Default in

icmp-trace

Syntax **icmp-trace** [*ip-address* **|** *dns-name*] [**ttl** *time-to-live*] [**wait** *milli-seconds*] [**tos** *type-of-service*] [**source** *ip-address*] [**tos** *type-of-service*] [**router** *router-instance*]

Context config>saa>test>type

Description This command configures an ICMP traceroute test.

Parameters *ip-address* — the far-end IP address to which to send the svc-ping request message in dotted decimal notation

Values ipv4-address: a.b.c.d

dns-name — the DNS name of the far-end device to which to send the svc-ping request message, expressed as a character string to 63 characters maximum

time-to-live — the TTL value for the MPLS label, expressed as a decimal integer

Values 1 to 255

milli-seconds — the time, in milliseconds, to wait for a response to a probe, expressed as a decimal integer

Default 5000

Values 1 to 60000

type-of-service — specifies the service type

Values 0 to 255

source *ip-address* — specifies the IP address to be used

Values ipv4-address: a.b.c.d

router *router-instance* — specifies the router name or service ID

Values	router-name:	Base, management
	service-id:	1 to 2147483647
Default	Base	

lsp-ping

Syntax **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**]

Context oam
config>saa>test>type

Description This command performs in-band LSP connectivity tests using the protocol and data structures defined in RFC 4379, *Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures*.

The LSP ping operation is modeled after the IP ping utility, which uses ICMP echo request and reply packets to determine IP connectivity.

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.

The `detail` parameter is available only from the `oam` context.

Parameters *ip-prefix/mask* — specifies the address prefix and subnet mask of the destination node

Values	ipv4-address:	a.b.c.d
	mask:	value must be 32

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.

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

profile {**in** | **out**} — specifies the profile state of the MPLS echo request encapsulation

Default out

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.

Values 80, and 85 to 1500 — Prefix-specified ping
92, and 97 to 1500 — LSP name-specified ping

Default 80 — Prefix-specified ping
92 — LSP name-specified ping
The system sends the minimum packet size, depending on the type of LSP. No padding is added.

label-ttl — specifies the TTL value for the MPLS label, expressed as a decimal integer

Values 1 to 255

Default 255

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.

Values 1 to 100

Default 1

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.

Values 1 to 10

Default 5

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.

Values 1 to 10

Default 1

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 *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

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

Values 1 to 255

Default 5

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.

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

Default be

profile {**in** | **out**} — specifies the profile state of the MPLS echo request encapsulation

Values out

probes-per-hop — specifies the number of OAM requests sent for a particular TTL value, expressed as a decimal integer

Values 1 to 10

Default 1

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.

Values 104 to 1500

Default 104 — The system sends the minimum packet size, depending on the type of LSP. No padding is added.

min-label-ttl — specifies the minimum TTL value in the MPLS label for the LSP trace test, expressed as a decimal integer

Values 1 to 255

Default 1

max-label-ttl — specifies the maximum TTL value in the MPLS label for the LDP trace test, expressed as a decimal integer

Values 1 to 255

Default 30

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.

Values 1 to 60

Default 3

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.

Values 1 to 10

Default 1

detail — displays detailed information

sdp-ping

Syntax **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*]

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. Table 42 displays the response messages sorted by precedence.

Table 42: 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 *orig-sdp-id*	Orig-SDP Non-Existent	2
Request not sent due to administratively down *orig-sdp-id*	Orig-SDP Admin-Down	3
Request not sent due to operationally down *orig-sdp-id*	Orig-SDP Oper-Down	4
Request terminated by user before reply or timeout	Request Terminated	5
Reply received, invalid *origination-id*	Far End: Originator-ID Invalid	6
Reply received, invalid *responder-id*	Far End: Responder-ID Error	7
Reply received, non-existent *resp-sdp-id*	Far End: Resp-SDP Non-Existent	8
Reply received, invalid *resp-sdp-id*	Far End: Resp-SDP Invalid	9

Table 42: SDP Ping Response Messages (Continued)

Result of Request	Displayed Response Message	Precedence
Reply received, *resp-sdp-id* 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-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 encapsulaton. 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.

Values 1 to 17407

Default null – use the non-SDP return path for message reply

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.

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

Default be

profile {**in** | **out**} — specifies the profile state of the SDP encapsulation

Default out

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.

Values 1 to 10

Default 5

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.

Values 1 to 10

Default 1

octets — the size of the packet 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.

Values 72 to 1500

Default 40

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.

Values 1 to 100

Default 1

Special Cases

Single Response Connectivity Tests — A single response sdp-ping test provides detailed test results (see Table 43).

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 43: 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 *orig-sdp-id* 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 *orig-sdp-id* does not exist, N/A will be displayed.	Oper-Up Oper-Down N/A
Originating SDP-ID Path MTU	The local **path-mtu** for *orig-sdp-id*. If *orig-sdp-id* 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 *resp-sdp-id* 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 43: Single Response Connectivity (Continued)

Field	Description	Values
Responding SDP-ID Administrative State	The administrative state of the responding SDP-ID. When *resp-sdp-id* is administratively down, Admin-Down will be displayed. When *resp-sdp-id* is administratively up, Admin-Up will be displayed. When *resp-sdp-id* exists on the far-end 7705 SAR but is not valid for the originating 7705 SAR, Invalid is displayed. When *resp-sdp-id* 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 *service-id*. 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 *resp-sdp-id*. If *resp-sdp-id* 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 *orig-sdp-id*.	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
```

vccv-ping

Syntax **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*]

Context oam
config>saa>test>type

Description 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.

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 **—** 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-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 SAR.

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

Default be

profile {**in** | **out**} — specifies the profile state of the MPLS echo request encapsulation

Default out

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.

Values 1 to 10

Default 5

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.

Values 1 to 10

Default 1

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.

Values 88 to 9198

Default 88

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.

Values 1 to 100

Default 1

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
```

vccv-trace

Syntax **vccv-trace** *sdp-id:vc-id* [**size** *octets*] [**min-ttl** *min-vc-label-ttl*] [**max-ttl** *max-vc-label-ttl*] [**max-fail** *no-response-count*] [**probe-count** *probe-count*] [**reply-mode ip-routed | control-channel**] [**timeout** *timeout-value*] [**interval** *interval-value*] [**fc** *fc-name* [**profile** {**in** |**out**}]] [**detail**]

Context oam

Description This command configures a Virtual Circuit Connectivity Verification (VCCV) automated trace test. The automated VCCV trace can trace the entire path of a PW with a single command issued at the terminating PE (T-PE) 7705 SAR. VCCV-trace is equivalent to LSP-trace and is an iterative process by which the source T-PE or S-PE node sends successive VCCV-ping messages with incrementing the TTL value, starting from TTL=1.

In each iteration, the T-PE builds the MPLS echo request message in a way similar to VCCV-ping. The first message (with TTL=1) includes the next-hop S-PE targeted LDP session source address in the Remote PE Address field of the PW FEC TLV. Each S-PE that terminates and processes the message will include the FEC 128 TLV corresponding the PW segment to its downstream node in the MPLS echo reply message.The source T-PE node can then build the next echo reply message with TTL=2 to test the next-next hop for the MS-PW. It will copy the FEC TLV it received in the echo reply message into the new echo request message. The process is terminated when the reply is from the egress T-PE or when a timeout occurs.

The user can specify to display the result of the VCCV trace for a fewer number of PW segments of the end-to-end MS-PW path. In this case, the `min-ttl` and `max-ttl` parameters should be configured accordingly. However, the T-PE or S-PE node will still probe all hops up to `min-ttl` in order to correctly build the FEC of the desired subset of segments.

Parameters *sdp-id:vc-id* — specifies the VC ID of the pseudowire being tested must be indicated with this parameter. The VC ID needs to exist on the local 7705 SAR and the far-end peer needs to indicate that it supports VCCV to allow the user to send VCCV-ping message.

Values sdp-id : 1 to 17407

vc-id: 1 to 4294967295

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.

Values 88 to 9198

Default 88

min-vc-label-ttl — specifies the TTL value for the VC label of the echo request message for the first hop of the MS-PW for which the results are to be displayed. This is expressed as a decimal integer. Note that the outer label TTL is still set to the default of 255 regardless of the value of the VC label.

Values 1 to 255

Default 1

max-vc-label-tt — specifies the TTL value for the VC label of the echo request message for the last hop of the MS-PW for which the results are to be displayed. This is expressed as a decimal integer. Note that the outer label TTL is still set to the default of 255 regardless of the value of the VC label.

Values 1 to 255

Default 8

no-response-count — specifies the maximum number of consecutive VCCV-trace echo requests, expressed as a decimal integer, that do not receive a reply before the trace operation fails for a given TTL value.

Values 1 to 255

Default 5

probe-count — specifies the number of VCCV-trace echo request messages to send per TTL value.

Values 1 to 10

Default 1

reply-mode {**ip-routed** | **control-channel**} — the **reply-mode** parameter indicates to the far end how to send the reply message. The **control-channel** option indicates a reply mode in-band using vccv control channel. The **ip-routed** option indicates a reply mode out-of-band using UDP IPv4.

Default control-channel

timeout-value — specifies the **timeout** parameter, in seconds, expressed as a decimal integer. This value is used to override the default timeout value and is the amount of time that the 7705 SAR will wait for a message reply after sending the message request. Upon the expiration of message timeout, the requesting 7705 SAR 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.

Values 1 to 60

Default 3

interval-value — specifies the **interval** parameter, in seconds, expressed as a decimal integer. This parameter is used to override the default request message send interval and 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.

Values 1 to 255

Default 1

fc-name — specifies the forwarding class of the VCCV-trace echo request encapsulation. The **fc** and **profile** parameters are used to indicate the forwarding class of the VCCV-trace 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 controls the mapping back to the internal forwarding class used by the far-end router that receives the message request. The egress mappings of the egress network interface on the far-end router controls the forwarding class markings on the return reply message. The LSP-EXP mappings on the receive network interface controls the mapping of the message reply back at the originating router.

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

Default be

profile {**in** | **out**} — specifies the profile state of the VCCV-trace echo request encapsulation.

Default out

detail — displays detailed information

Sample Output

```
*A:138.120.214.60# oam vccv-trace 1:33
VCCV-TRACE 1:33 with 88 bytes of MPLS payload
1 1.1.63.63 rtt<10ms rc=8(DSRtrMatchLabel)
2 1.1.62.62 rtt<10ms rc=8(DSRtrMatchLabel)
3 1.1.61.61 rtt<10ms rc=3(EgressRtr)
```

Trace with detail:

```
*A:ALU2>oam vccv-trace 1:33 detail
VCCV-TRACE 1:33 with 88 bytes of MPLS payload
1 1.1.63.63 rtt<10ms rc=8(DSRtrMatchLabel)
Next segment: VcId=34 VcType=AAL5SDU Source=1.1.63.63 Remote=1.1.62.62
2 1.1.62.62 rtt<10ms rc=8(DSRtrMatchLabel)
Next segment: VcId=35 VcType=AAL5SDU Source=1.1.62.62 Remote=1.1.61.61
3 1.1.61.61 rtt<10ms rc=3(EgressRtr)
----------------------------------------------
*A:ALU2>oam vccv-trace#
```

enable-icmp-vse

Syntax **enable-icmp-vse**
no enable-icmp-vse

Context config>system

Description This command is a global command that enables and disables one-way timestamping of outbound SAA ICMP ping packets. When disabled, one-way timestamping is not performed on outbound SAA ICMP ping packets. The current status can be seen on the **show>system>information** CLI display.

The **no** form of this command disables one-way timestamping.

Default **no enable-icmp-vse**

OAM SAA Commands

saa

Syntax **saa** *test-name* [**owner** *test-owner*] {**start** | **stop**}

Context oam

Description This command starts or stops an SAA test.

Parameters *test-name* — specifies the name of the SAA test to be run. The test name must already be configured in the **config>saa>test** context.

test-owner — specifies the owner of an SAA operation, up to 32 characters in length

Values If a *test-owner* value is not specified, tests created by the CLI have a default owner "TiMOS CLI"

start — starts the test. A test cannot be started if the same test is still running.

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.

stop — stops a test in progress. A log message will be generated to indicate that an SAA test run has been aborted.

Show Commands

eth-cfm

Syntax **eth-cfm**

Context show

Description This command enables the context to display CFM information.

association

Syntax **association** [*ma-index*] [**detail**]

Context show>eth-cfm

Description This command displays dot1ag association information.

Parameters *ma-index* — specifies the MA index

Values 1 to 4294967295

detail — displays detailed information for the dot1ag association

Output The following output is an example of eth-cfm association information, and Table 44 describes the fields.

Sample Output

```
*A:ALU-1>show>eth-cfm# association
======================================================================
Dot1ag CFM Association Table
======================================================================
Md-index   Ma-index   Name                     CCM-interval Bridge-id
----------------------------------------------------------------------
1          1          kanata_MA                10           2
1          2          2                        10           20
======================================================================
*A:ALU-1>show>eth-cfm#

*A:ALU-1>show>eth-cfm# association detail
-------------------------------------------------------------------------------
Domain 1 Associations:
-------------------------------------------------------------------------------
Md-index          : 1                         Ma-index          : 1
Name Format       : charString                CCM-interval      : 10
Name              : kanata_MA
Bridge-id         : 2                         MHF Creation      : defMHFnone
PrimaryVlan       : 2                         Num Vids          : 0
-------------------------------------------------------------------------------
*A:ALU-1>show>eth-cfm#
```

Table 44: ETH-CFM Association Field Descriptions

Label	Description
`Md-index`	Displays the MD index
`Ma-index`	Displays the MA index
`Name`	Displays the name of the MA
`CCM-interval`	Displays the CCM interval (in seconds)
`Bridge-id`	Displays the bridge ID for the MA. The bridge ID is the same value as the service ID of the service to which the MEP belongs.
`Name Format`	Displays the format for the MA name
`MHF Creation`	Not applicable
`PrimaryVlan`	Displays the VLAN ID
`Num Vids`	Displays the number of VLAN IDs
`Remote Mep Id`	Displays the MEP identifier for the remote MEP

cfm-stack-table

Syntax **cfm-stack-table**
cfm-stack-table [**port** [*port-id* [**vlan** *vlan-id*]] **| sdp** *sdp-id*[**:***vc-id*]] [**level** *0..7*] [**direction down**]

Context show>eth-cfm

Description This command displays stack-table information.

Parameters *port-id* — displays the bridge port or aggregated port on which MEPs or MHFs are configured

Values *port-id*: *slot*/*mda*/*port*[.*channel*]

vlan-id — displays the associated VLAN ID

Values *vlan-id*: 0 to 4094

sdp-id[:*vc-id*] — displays the SDP binding for the bridge

Values *sdp-id*[:*vc-id*]: *sdp-id* 1 to 17407
vc-id 1 to 4294967295

0...7 — display the MD level of the maintenance point

Values 0 to 7

direction down — displays the direction in which the MEP faces on the bridge port

Output The following output is an example of eth-cfm stack table information, and Table 45 describes the fields.

Sample Output

```
*A:ALU-1>show>eth-cfm# cfm-stack-table
=======================================================================
Dot1ag CFM SAP Stack Table
=======================================================================
Sap            Level Dir  Md-index   Ma-index   Mep-id Mac-address
-----------------------------------------------------------------------
1/5/1          5     Down 1          1          1
=======================================================================

=======================================================================
Dot1ag CFM SDP Stack Table
=======================================================================
Sdp            Level Dir  Md-index   Ma-index   Mep-id Mac-address
-----------------------------------------------------------------------
1:11           5     Down 1          1          2      a4:58:ff:00:00:00

=======================================================================
*A:ALU-1>show>eth-cfm#
```

Table 45: ETH-CFM Stack Table Field Descriptions

Label	Description
`Sap`	Displays the SAP identifier
`Sdp`	Displays the spoke SDP identifier
`Level`	Displays the MD level of the domain
`Dir(direction)`	Displays the direction of OAMPDU transmission. In Release 2.1, only down MEP direction is supported.
`Md-index`	Displays the MD index of the domain
`Mep-id`	Displays the MEP identifier
`Mac-address`	Displays the MAC address of the MEP

domain

Syntax **domain** [*md-index*] [**association** *ma-index* **| all-associations**] [**detail**]

Context show>eth-cfm

Description This command displays domain information.

Parameters *md-index* — displays the index of the MD to which the MEP is associated, or 0, if none

Values 1 to 4294967295

ma-index — displays the index to which the MA is associated, or 0, if none

Values 1 to 4294967295

all-associations — displays all associations to the MD

detail — displays detailed domain information

Output The following output is an example of eth-cfm domain information, and Table 46 describes the fields.

Sample Output

```
*A:ALU-1>show>eth-cfm# domain
==============================================================================
Dot1ag CFM Domain Table
==============================================================================
Md-index   Level Name                                        Format
------------------------------------------------------------------------------
1          5     kanata_MD                                   charString
==============================================================================

*A:ALU-1>show>eth-cfm# domain detail
===============================================================================
Domain 1
Md-index          : 1                         Level             : 5
Permission        : sendIdNone                MHF Creation      : defMHFnone
Name Format       : charString                Next Ma Index     : 2
Name              : kanata_MD
===============================================================================

*A:ALU-1>show>eth-cfm# domain all-associations
======================================================================
Dot1ag CFM Association Table
======================================================================
Md-index   Ma-index   Name                      CCM-interval Bridge-id
----------------------------------------------------------------------
1          1          kanata_MA                 10           2
======================================================================
```

```
*A:ALU-1>show>eth-cfm# domain all-associations detail
===============================================================================
Domain 1
Md-index           : 1                          Level             : 5
Permission         : sendIdNone                 MHF Creation      : defMHFnone
Name Format        : charString                 Next Ma Index     : 2
Name               : kanata_MD
-------------------------------------------------------------------------------
Domain 1 Associations:

Md-index           : 1                          Ma-index          : 1
Name Format        : charString                 CCM-interval      : 10
Name               : kanata_MA
Bridge-id          : 2                          MHF Creation      : defMHFnone
PrimaryVlan        : 2                          Num Vids          : 0

===============================================================================
*A:ALU-1>show>eth-cfm#
```

Table 46: ETH-CFM Domain Field Descriptions

Label	Description
`Md-index`	Displays the MD index of the domain
`Ma-index`	Displays the MA index of the association
`Level`	Displays the MD level of the domain
`Name`	Displays the name of the MD when the `domain` command is used, or the name of the MA when the `association` command is used
`Format`	Displays the format for the name
`CCM-interval`	Displays the CCM interval (in seconds)
`Bridge-id`	Displays the bridge ID for the MA. The bridge ID is the same value as the service ID of the service to which the MEP belongs.
`Domain`	Displays the MD index
`Permission`	Indicates what is included in the sender ID TLV transmitted by MHFs
`MHF Creation`	Not applicable
`Name Format`	Displays the format for the MD name
`Next Ma Index`	Displays the value of the next MA index

mep

Syntax **mep** *mep-id* **domain** *md-index* **association** *ma-index* [**loopback**] [**linktrace**]

Context show>eth-cfm

Description This command displays MEP, MEP loopback, and MEP linktrace information.

Parameters *mep-id* — specifies the MEP

Values 1 to 8191

md-index — displays the index of the MD to which the MEP is associated, or 0, if none

Values 1 to 4294967295

ma-index — displays the index to which the MEP is associated, or 0, if none

Values 1 to 4294967295

loopback — displays loopback information for the specified MEP

linktrace — displays linktrace information for the specified MEP

Output The following output is an example of eth-cfm MEP information, and Table 47 describes the fields.

Sample Output

```
*A:ALU-1>show>eth-cfm# mep 2 domain 1 association 1 loopback linktrace
-------------------------------------------------------------------------------
Mep Information
-------------------------------------------------------------------------------
Md-index           : 1                          Direction         : Down
Ma-index           : 1                          Admin             : Disabled
MepId              : 2                          CCM-Enable        : Disabled
IfIndex            : 0                          PrimaryVid        : 0
FngState           : fngReset
LowestDefectPri    : macRemErrXcon              HighestDefect     : none
Defect Flags       : None
Mac Address        : a4:58:ff:00:00:00          CcmLtmPriority    : 7
CcmTx              : 0                          CcmSequenceErr    : 0
CcmLastFailure Frame:
    None
XconCcmFailure Frame:
    None
-------------------------------------------------------------------------------
Mep Loopback Information
-------------------------------------------------------------------------------
LbRxReply          : 0                          LbRxBadOrder      : 0
LbRxBadMsdu        : 0                          LbTxReply         : 0
LbSequence         : 1                          LbNextSequence    : 1
LbStatus           : False                      LbResultOk        : False
DestIsMepId        : False                      DestMepId         : 0
DestMac            : 00:00:00:00:00:00          SendCount         : 0
VlanDropEnable     : True                       VlanPriority      : 7
Data TLV:
    None
-------------------------------------------------------------------------------
```

```
Mep Linktrace Message Information
-------------------------------------------------------------------------------
LtRxUnexplained    : 0                        LtNextSequence    : 1
LtStatus           : False                    LtResult          : False
TargIsMepId        : False                    TargMepId         : 0
TargMac            : 00:00:00:00:00:00        TTL               : 64
EgressId           : 00:00:a4:58:ff:00:00:00  SequenceNum       : 1
LtFlags            : useFDBonly
-------------------------------------------------------------------------------
Mep Linktrace Replies
-------------------------------------------------------------------------------
SequenceNum        : 1                        ReceiveOrder      : 1
Ttl                : 63                       Forwarded         : False
LastEgressId       : 00:00:00:21:05:6e:5a:f1  TerminalMep       : True
NextEgressId       : 00:00:00:21:05:4d:a8:b2  Relay             : rlyHit
ChassisIdSubType   : unknown value (0)
ChassisId:
    None
ManAddressDomain:
    None
ManAddress:
    None
IngressMac         : 00:21:05:4d:a8:b2        Ingress Action    : ingOk
IngrPortIdSubType  : unknown value (0)
IngressPortId:
    None
EgressMac          : 00:00:00:00:00:00        Egress Action     : egrNoTlv
EgrPortIdSubType   : unknown value (0)
EgressPortId:
    None
Org Specific TLV:
    None
-------------------------------------------------------------------------------

*A:ALU-1>show>eth-cfm# mep 2 domain 1 association 1 linktrace
```

Table 47: ETH-CFM MEP Field Descriptions

Label	Description
`Mep Information`	
`Md-index`	Displays the MD index of the domain
`Direction`	Displays the direction of OAMPDU transmission. In Release 2.1, only down MEP direction is supported.
`Ma-index`	Displays the MA index of the association
`Admin`	Displays the administrative status of the MEP
`MepId`	Displays the MEP identifier
`CCM-Enable`	Displays the CCM interval (in seconds)
`IfIndex`	Displays the index of the interface
`PrimaryVid`	Displays the identifier of the primary VLAN

Table 47: ETH-CFM MEP Field Descriptions (Continued)

Label	Description
`FngState`	Indicates the different states of the Fault Notification Generator
`LowestDefectPri`	Displays a configured value that defects are evaluated against
`HighestDefect`	Identifies the highest defect that is present (for example, if defRDICCM and defXconCCM are present, the highest defect is defXconCCM)
`Defect Flags`	Displays the number of defect flags
`Mac Address`	Displays the MAC address of the MEP
`CcmLtmPriority`	Displays the priority value transmitted in the linktrace messages (LTM)s and CCMs for this MEP. The MEP must be configured on a VLAN.
`CcmTx`	Displays the number of Continuity Check Messages (CCM) sent The count is taken from the last polling interval (every 10 s)
`CcmSequenceErr`	Displays the number of CCM errors
`CcmLast Failure Frame`	Displays the frame that caused the last CCM failure
`XconCcmFailure Frame`	Displays the frame that caused the XconCCMFailure
`Mep Loopback Information`	
`LbRxReply`	Displays the number of received loopback (LB) replies
`LbRxBadOrder`	Displays the number of received loopback messages that are in a bad order
`LbRxBadMsdu`	Displays the number of loopback replies that have been received with the wrong destination MAC address (MSDU = MAC Service Data Unit)
`LbTxReply`	Displays the number of loopback replies transmitted out this MEP
`LbSequence`	Displays the sequence number in the loopback message
`LbNextSequence`	Displays the next loopback sequence
`LbStatus`	Displays the loopback status as True or False: `True` — loopback is in progress `False` — no loopback is in progress
`LbResultOk`	Displays the result of the loopback test

Table 47: ETH-CFM MEP Field Descriptions (Continued)

Label	Description
`DestIsMepId`	Identifies whether the destination interface has a MEP-ID (true or false)
`DestMepId`	Displays the MEP-ID of the destination interface
`DestMac`	Displays the MAC address of the destination interface
`SendCount`	Indicates the number of loopback messages sent
`VlanDropEnable`	Identifies whether the VLAN drop is enabled (true or false)
`VlanPriority`	Displays the VLAN priority
`Data TLV`	Displays the data TLV information
`Mep Linktrace Message Information`	
`LtRxUnexplained`	Displays the number of unexplained linktrace messages (LTM) that have been received
`LtNextSequence`	Displays the sequence number of the next linktrace message
`LtStatus`	Displays the status of the linktrace
`LtResult`	Displays the result of the linktrace
`TargIsMepId`	Identifies whether the target interface has a MEP-ID (true or false)
`TargMepId`	Displays the MEP-ID of the target interface
`TargMac`	Displays the MAC address of the target interface
`TTL`	Displays the TTL value
`EgressId`	Displays the egress ID of the linktrace message
`SequenceNum`	Displays the sequence number of the linktrace message
`LtFlags`	Displays the linktrace flags
`Mep Linktrace Replies`	
`SequenceNum`	Displays the sequence number returned by a previous transmit linktrace message, indicating which linktrace message response will be returned
`ReceiveOrder`	Displays the order in which the linktrace initiator received the linktrace replies
`Ttl`	Displays the TTL field value for a returned linktrace reply

Table 47: ETH-CFM MEP Field Descriptions (Continued)

Label	Description
`Forwarded`	Indicates whether the linktrace message was forwarded by the responding MEP
`LastEgressId`	Displays the last egress identifier returned in the linktrace reply egress identifier TLV of the linktrace reply The last egress identifier identifies the MEP linktrace initiator that initiated, or the linktrace responder that forwarded, the linktrace message for which this linktrace reply is the response This is the same value as the egress identifier TLV of that linktrace message
`TerminalMep`	Indicates whether the forwarded linktrace message reached a MEP enclosing its MA
`NextEgressId`	Displays the next egress identifier returned in the linktrace reply egress identifier TLV of the linktrace reply The next egress identifier identifies the linktrace responder that transmitted this linktrace reply and can forward the linktrace message to the next hop This is the same value as the egress identifier TLV of the forwarded linktrace message, if any
`Relay`	Displays the value returned in the Relay Action field
`ChassisIdSubType`	Displays the format of the chassis ID returned in the Sender ID TLV of the linktrace reply, if any This value is meaningless if the chassis ID has a length of 0
`ChassisId`	Displays the chassis ID returned in the Sender ID TLV of the linktrace reply, if any The format is determined by the value of the ChassisIdSubType
`ManAddressDomain`	Displays the TDomain that identifies the type and format of the related ManAddress, used to access the SNMP agent of the system transmitting the linktrace reply Received in the linktrace reply Sender ID TLV from that system
`ManAddress`	Displays the TAddress that can be used to access the SNMP agent of the system transmitting the CCM Received in the CCM Sender ID TLV from that system

Table 47: ETH-CFM MEP Field Descriptions (Continued)

Label	Description
`IngressMac`	Displays the MAC address returned in the ingress MAC address field
`Ingress Action`	Displays the value returned in the Ingress Action field of the linktrace message
`IngressPortIdSubType`	Displays the format of the ingress port ID
`IngressPortId`	Displays the ingress port ID; the format is determined by the value of the IngressPortIdSubType
`EgressMac`	Displays the MAC address returned in the egress MAC address field
`Egress Action`	Displays the value returned in the Egress Action field of the linktrace message
`EgressPortIdSubType`	Displays the format of the egress port ID
`EgressPortId`	Displays the egress port ID; the format is determined by the value of the EgressPortIDSubType
`Org Specific TLV`	Displays all organization-specific TLVs returned in the linktrace reply, if any Includes all octets including and following the TLV length field of each TLV, concatenated

saa

Syntax **saa** [*test-name*] [**owner** *test-owner*]

Context show>saa

Description This command displays information about the SAA test.

If no specific test is specified, a summary of all configured tests is displayed.

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.

Parameters *test-name* — specifies the SAA test to display. The test name must already be configured in the **config>saa>test** context. This is an optional parameter.

test-owner — specifies the owner of an SAA operation, up to 32 characters in length

Default If a *test-owner* value is not specified, tests created by the CLI have a default owner “TiMOS CLI”

Output The following output is an example of SAA test result information, and Table 48 describes the fields.

Sample Output

The following displays an SAA test result:

```
*A:ALU-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:ALU-3>config>saa>test$
```

Table 48: 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

Table 48: SAA Field Descriptions (Continued)

Label	Description
`Number of failed tests run`	Specifies the total number of tests that failed
`Last test result`	Indicates the last time a test was run

Clear Commands

saa

Syntax **saa-test** [*test-name*] [**owner** *test-owner*]

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 *test-name* — specifies the SAA test to clear. The test name must already be configured in the **config>saa>test** context.

test-owner — specifies the owner of an SAA operation, up to 32 characters in length

Default If a *test-owner* 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 Tx and Rx

raw | detail **—** displays output for the debug mode

Tools

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
                    — ospf
                            — abr [detail]
                            — asbr [detail]
                            — bad-packet [interface-name]
                            — leaked-routes [summary | detail]
                            — memory-usage [detail]
                            — request-list [neighbor ip-address] [detail]
                            — request-list [virtual-neighbor ip-address area-id area-id] [detail]
                            — retransmission-list [neighbor ip-address] [detail]
                            — retransmission-list [virtual-neighbor ip-address area-id area-id]
                              [detail]
                            — route-summary
                            — route-table [type] [detail]
                    — rsvp
                            — psb [endpoint endpoint-address] [sender sender-address] [tunnelid
                              tunnel-id] [lspid lsp-id]
                            — rsb [endpoint endpoint-address] [sender sender-address] [tunnelid
                              tunnel-id] [lspid lsp-id]
            — 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
            — isis
                — ldp-sync-exit
                — run-manual-spf [externals-only]
            — mpls
                — cspf to ip-addr [from ip-addr] [bandwidth bandwidth] [include-bitmap bitmap] [exclude-bitmap bitmap] [hop-limit limit] [exclude-address excl-addr...(up to 8 max)] [use-te-metric] [strict-srlg] [srlg-group grp-id...(up to 8 max)]
                — resignal {lsp lsp-name path path-name | delay minutes}
                — trap-suppress number-of-traps time-interval
            — ospf
                — ldp-sync-exit
                — refresh-lsas [lsa-type] [area-id]
                — run-manual-spf [externals-only]
        — 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]
        — service
            — id service-id
                — endpoint endpoint-name
                    — force-switchover sdp-id:vc-id
                    — no force-switchover
```

Command Descriptions

Tools Dump Commands

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** *port-id*

Context tools>dump

Description This command displays PPP information for a port.

Default **none**

Parameters *port-id* — specifies the port ID

Syntax: *port-id* *slot/mda/port*[.*channel*]
bundle bundle-*type-slot/mda.bundle-num*
bundle keyword
type ima, ppp
bundle-num1 to 10

system-resources

Syntax **system-resources** *slot-number*

Context tools>dump

Description This command displays system resource information.

Default **none**

Parameters *slot-number* — specifies a specific slot to view system resources information

Dump Router Commands

router

Syntax **router** *router-instance*

Context tools>dump

Description This command enables tools for the router instance.

Default **none**

Parameters *router-instance* — specifies the router name and service ID

Values		
	router-name:	Base, management
	service-id:	1 to 2147483647

Default Base

ldp

Syntax **ldp**

Context tools>dump>router

Description This command enables dump tools for LDP.

Default **none**

fec

Syntax **fec prefix** *ip-prefix/mask*
fec vc-type {**ethernet** | **vlan**} **vc-id** *vc-id*

Context tools>dump>router>ldp

Description This command displays information for an LDP FEC.

Default **none**

Parameters *ip-prefix/mask* — specifies the IP prefix and host bits

Values		
	host bits:	must be 0
	mask:	0 to 32

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.

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

- Ethernet — the VC type value for Ethernet is 0x0005
- VLAN — the VC type value for an Ethernet VLAN is 0x0004

vc-id — specifies the virtual circuit identifier

Values 1 to 4294967295

instance

Syntax **instance**

Context tools>dump>router>ldp

Description This command displays information for an LDP instance.

interface

Syntax **interface** [*ip-int-name* | *ip-address*]

Context tools>dump>router>ldp

Description This command displays information for an LDP interface.

Default **none**

Parameters *ip-int-name* — specifies the interface name

ip-address — specifies the IP address

memory-usage

Syntax **memory-usage**

Context tools>dump>router>ldp

Description This command displays memory usage information for LDP.

Default **none**

peer

Syntax	**peer** *ip-address*
Context	tools>dump>router>ldp
Description	This command displays information for an LDP peer.
Default	**none**
Parameters	*ip-address* — specifies the IP address

session

Syntax	**session** [*ip-address* **|***:label space*] [**connection | peer | adjacency**]
Context	tools>dump>router>ldp
Description	This command displays information for an LDP session.
Default	**none**
Parameters	*ip-address* — specifies the IP address of the LDP peer *label-space* — 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**

mpls

Syntax **mpls**

Context tools>dump>router

Description This command enables the context to display MPLS information.

Default **none**

ftn

Syntax **ftn** [**endpoint** *endpoint* | **sender** *sender* | **nexthop** *nexthop* | **lsp-id** *lsp-id* | **tunnel-id** *tunnel-id* | **label** *start-label end-label*]

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 *endpoint* — specifies the IP address of the last hop

Values a.b.c.d

sender — specifies the IP address of the sender

Values a.b.c.d

nexthop — specifies the IP address of the next hop

Values a.b.c.d

lsp-id — specifies the label switched path that is signaled for this entry

Values 0 to 65535

tunnel-id — specifies the SDP ID

Values 0 to 65535

start-label end-label — specifies the label range for the information dump

Values start-label — 32 to 131071

end-label — 32 to 131071

ilm

Syntax **ilm** [**endpoint** *endpoint* | **sender** *sender* | **nexthop** *nexthop* | **lsp-id** *lsp-id* | **tunnel-id** *tunnel-id* | **label** *start-label end-label*]

Context tools>dump>router>mpls

Description This command displays incoming label map (ILM) information for MPLS.

Default **none**

Parameters *endpoint* — specifies the IP address of the last hop

Values a.b.c.d

sender — specifies the IP address of the sender

Values a.b.c.d

nexthop — specifies the IP address of the next hop

Values a.b.c.d

lsp-id — specifies the label switched path that is signaled for this entry

Values 0 to 65535

tunnel-id — specifies the SDP ID

Values 0 to 65535

start-label end-label — specifies the label range for the information dump

Values start-label — 32 to 131071

end-label — 32 to 131071

lspinfo

Syntax **lspinfo** [**detail**]

Context tools>dump>router>mpls

Description This command displays LSP information for MPLS.

Default **none**

Parameters **detail** — displays detailed LSP information

memory-usage

Syntax **memory-usage**

Context tools>dump>router>mpls

Description This command displays memory usage information for MPLS.

Default **none**

ospf

Syntax **ospf**

Context tools>dump>router

Description This command enables the context to display tools information for OSPF.

Default **none**

abr

Syntax **abr** [**detail**]

Context tools>dump>router>ospf

Descriptiont This command displays area border router (ABR) information for OSPF.

Default **none**

Parameters **detail** — displays detailed information about the ABR

asbr

Syntax **asbr** [**detail**]

Context tools>dump>router>ospf

Description This command displays autonomous system boundary router (ASBR) information for OSPF.

Default **none**

Parameters **detail** — displays detailed information about the ASBR

bad-packet

Syntax **bad-packet** [*interface-name*]

Context tools>dump>router>ospf

Descriptiont This command displays information about bad packets for OSPF.

Default **none**

Parameters *interface-name* — displays only the bad packets identified by this interface name

leaked-routes

Syntax **leaked-routes** [**summary** | **detail**]

Context tools>dump>router>ospf

Description This command displays information about leaked routes for OSPF.

Default **summary**

Parameters **summary —** displays a summary of information about leaked routes for OSPF

detail — displays detailed information about leaked routes for OSPF

memory-usage

Syntax **memory-usage** [**detail**]

Context tools>dump>router>ospf

Description This command displays memory usage information for OSPF.

Default **none**

Parameters **detail —** displays detailed information about memory usage for OSPF

request-list

Syntax **request-list** [**neighbor** *ip-address*] [**detail**]
request-list [**virtual-neighbor** *ip-address* **area-id** *area-id*] [**detail**]

Context tools>dump>router>ospf

Description This command displays request list information for OSPF.

Default **none**

Parameters

neighbor *ip-address* — displays neighbor information only for the neighbor identified by the IP address

detail — displays detailed information about the neighbor or virtual neighbor

virtual-neighbor *ip-address* — displays information about the virtual neighbor identified by the IP address

area-id — the OSPF area ID expressed in dotted-decimal notation or as a 32-bit decimal integer

retransmission-list

Syntax

retransmission-list [**neighbor** *ip-address*] [**detail**]
retransmission-list [**virtual-neighbor** *ip-address* **area-id** *area-id*] [**detail**]

Context

tools>dump>router>ospf

Description

This command displays dump retransmission list information for OSPF.

Default

none

Parameters

neighbor *ip-address* — displays neighbor information only for the neighbor identified by the IP address

detail — displays detailed information about the neighbor or virtual neighbor

virtual-neighbor *ip-address* — displays information about the virtual neighbor identified by the IP address

area-id — the OSPF area ID expressed in dotted-decimal notation or as a 32-bit decimal integer

route-summary

Syntax

route-summary

Context

tools>dump>router>ospf

Description

This command displays dump route summary information for OSPF.

Default

none

route-table

Syntax	**route-table** [**type**] [**detail**]
Context	tools>dump>router>ospf
Description	This command displays dump information about routes learned through OSPF.
Default	**none**
Parameters	**type** — the type of route table to display information about **Values** intra-area, inter-area, external-1, external-2, nssa-1, nssa-2 **detail** — displays detailed information about learned routes

rsvp

Syntax	**rsvp**
Context	tools>dump>router
Description	This command enables the context to display tools information for RSVP.
Default	**none**

psb

Syntax	**psb** [**endpoint** *endpoint-address*] [**sender** *sender-address*] [**tunnelid** *tunnel-id*] [**lspid** *lsp-id*]
Context	tools>dump>router>rsvp
Description	This command displays path state block (PSB) information for RSVP. When a PATH message arrives at an LSR, the LSR stores the label request in the local PSB for the LSP. If a label range is specified, the label allocation process must assign a label from that range. The PSB contains the IP address of the previous hop, the session, the sender, and the TSPEC. This information is used to route the corresponding RESV message back to LSR 1.
Default	**none**
Parameters	*endpoint-address* — specifies the IP address of the last hop *sender-address* — specifies the IP address of the sender *tunnel-id* — specifies the SDP ID **Values** 0 to 4294967295

lsp-id — specifies the label switched path that is signaled for this entry

Values	1 to 65535

rsb

Syntax **rsb** [**endpoint** *endpoint-address*] [**sender** *sender-address*] [**tunnelid** *tunnel-id*] [**lspid** *lsp-id*]

Context tools>dump>router>rsvp

Description This command displays RSVP Reservation State Block (RSB) information.

Default **none**

Parameters *endpoint-address* — specifies the IP address of the last hop

sender-address — specifies the IP address of the sender

tunnel-id — specifies the SDP ID

Values	0 to 4294967295

lsp-id — specifies the label switched path that is signaled for this entry

Values	1 to 65535

Tools Perform Commands

Perform Commands

perform

Syntax	perform
Context	tools
Description	This command enables the context to specify tools to perform specific tasks.
Default	**none**

cron

Syntax	**cron**
Context	tools>perform
Description	This command enables the context to perform CRON (scheduling) control operations.
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.

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 *action-name* — specifies the action name

Values maximum 32 characters

action-owner — specifies the owner name

Default TiMOS CLI

all — specifies to stop all CRON scripts

ima

Syntax **ima**

Context tools>perform

Description This command enables the context to perform IMA operations.

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-ima-*slot/mda.bundle-num*

bundle-ima	keyword
bundle-num	1 to 10

log

Syntax **log**

Context tools>perform

Description This command enables event logging tools.

test-event

Syntax **test-event**

Context tools>perform>log

Description This command generates a test event.

security

Syntax **security**

Context tools>perform

Description This command provides tools for testing security.

authentication-server-check

Syntax **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*]

Context tools>perform>security

Description This command checks connection to the RADIUS server.

Parameters **server-address** *ip-address* — specifies the server ID

Values a.b.c.d

port — specifies the port ID

Values 1 to 65535

dhcp-client-user-name — specifies the DHCP client

Values 256 characters maximum

password — specifies the CLI access password

Values 10 characters maximum

key — specifies the authenication key

Values 20 characters maximum

source-address *ip-address* — specifies the source IP address of the DHCP relay messages

Values a.b.c.d

seconds — specifies the timeout in seconds

Values 1 to 90

router-instance — specifies the router name or service ID

Values	*router-name*:	Base, management
	service-id:	1 to 2147483647

Default Base

service

Syntax **service**

Context tools>perform

Description This command enables the context to configure tools for services.

id

Syntax **id** *service-id*

Context tools>perform>service

Description This command enables the context to configure tools for a specific service.

Parameters *service-id* — specifies an existing service ID

Values 1 to 2147483647

endpoint

Syntax **endpoint** *endpoint-name*

Context tools>perform>service>id

Description This command enables the context to configure tools for a specific VLL service endpoint.

Parameters *endpoint-name* — specifies an existing VLL service endpoint name

force-switchover

Syntax	**force-switchover** *sdp-id:vc-id* **no force-switchover**
Context	tools>perform>service>id
Description	This command forces a switch of the active spoke SDP for the specified service.
Parameters	*sdp-id:vc-id* — specifies an existing spoke SDP for the service

Values	*sdp-id*:	1 to 17407
	vc-id:	1 to 4294967295

Perform Router Commands

router

Syntax **router** *router-instance*

Context tools>perform

Description This command enables tools for the router instance.

Default **none**

Parameters *router-instance* — specifies the router name and service ID

Values	*router-name*:	Base, management
	service-id:	1 to 2147483647

Default Base

isis

Syntax **isis**

Context tools>perform>router

Description This command enables the context to perform specific IS-IS tasks.

mpls

Syntax **mpls**

Context tools>perform>router

Description This command enables the context to perform specific MPLS tasks.

Default **none**

cspf

Syntax **cspf to** *ip-addr* [**from** *ip-addr*] [**bandwidth** *bandwidth*] [**include-bitmap** *bitmap*] [**exclude-bitmap** *bitmap*] [**hop-limit** *limit*] [**exclude-address** *excl-addr*...(up to 8 max)] [**use-te-metric**] [**strict-srlg**] [**srlg-group** *grp-id*...(up to 8 max)]

Context tools>perform>router>mpls

Description This command computes a CSPF path with specified user constraints.

Default **none**

Parameters **to** *ip-addr* — specifies the destination IP address

from *ip-addr* — specifies the originating IP address

bandwidth — specifies the amount of bandwidth in megabits per second (Mb/s) to be reserved

include-bitmap *bitmap* — specifies to include a bitmap that lists the admin groups that should be included during setup

exclude-bitmap *bitmap* — specifies to exclude a bitmap that lists the admin groups that should be included during setup

limit — specifies the total number of hops an FRR bypass LSP can take before merging back onto the main LSP path

excl-addr — specifies an IP address to exclude from the operation (up to a maximum of eight addresses in one command)

use-te-metric — specifies to use the traffic engineering metric used on the interface

strict-srlg — specifies to use strict **frr-srlg** to compute a new CSPF path

grp-id — specifies to use up to eight SRLGs to compute a new CSPF path

resignal

Syntax **resignal** {**lsp** *lsp-name* **path** *path-name* | **delay** *minutes*}

Context tools>perform>router>mpls

Description This command resignals specified LSP paths. The *minutes* parameter is used to configure the global timer to resignal all LSPs. The resignal timer is the time before resignaling occurs after the resignal condition occurs. If only *lsp-name* and *path-name* are provided, the specified LSP is resignaled immediately. For the delay option to work, the resignal time in the **configure>router>mpls** context must be set.

Default **none**

Parameters *lsp-name* — specifies a unique LSP name, up to 32 characters in length

path-name — specifies the name for the LSP path, up to 32 characters in length

minutes — specifies the delay interval, in minutes, before all LSPs are resignaled. If the value 0 is entered, all LSPs are resignaled immediately.

Values 0 to 30

trap-suppress

Syntax **trap-suppress** *number-of-traps time-interval*

Context tools>perform>router>mpls

Description This command modifies thresholds for trap suppression. The *time-interval* parameter is used to suppress traps after a certain number of traps have been raised within a period of time. By executing this command, there will be no more than the specified number of traps within the specified interval.

Default **none**

Parameters *number-of-traps* — specifies the number of traps in multiples of 100. An error message is generated if an invalid value is entered.

Values 100 to 1000

time-interval — specifies the timer interval in seconds

Values 1 to 300

ospf

Syntax **ospf**

Context tools>perform>router

Description This command enables the context to perform specific OSPF tasks.

ldp-sync-exit

Syntax **ldp-sync-exit**

Context tools>perform>router>ospf
tools>perform>router>isis

Description This command terminates IGP-LDP synchronization. OSPF or IS-IS then advertises the actual cost value of the link for all interfaces that have IGP-LDP synchronization enabled, if the currently advertised cost is different.

refresh-lsas

Syntax **refresh-lsas** [*lsa-type*] [*area-id*]

Context tools>perform>router>ospf

Description This command refreshes LSAs for OSPF.

Parameters *lsa-type* — the specified LSA type

Values router, network, summary, asbr, extern, nssa, opaque

area-id — the OSPF area ID expressed in dotted-decimal notation or as a 32-bit integer

Values 0.0.0.0 to 255.255.255.255 (dotted-decimal), 0 to 4294967295 (decimal integer)

run-manual-spf

Syntax **run-manual-spf** [**externals-only**]

Context tools>perform>router>ospf
tools>perform>router>isis

Description This command runs the shortest path first (SPF) algorithm for OSPF or IS-IS.

The **externals-only** parameter applies only to OSPF.

Parameters **externals-only — specifies the route preference for OSPF external routes —**

Standards and Protocol Support

Standards Compliance

IEEE 802.1ag	Service Layer OAM
IEEE 802.1p/q	VLAN Tagging
IEEE 802.3	10BaseT
IEEE 802.3ah	Ethernet OAM
IEEE 802.3u	100BaseTX
IEEE 802.3x	Flow Control
IEEE 802.3z	1000BaseSX/LX
IEEE 802.3-2008	Revised base standard

Protocol Support

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

GR-253-CORE - SONET Transport Systems: Common Generic Criteria. Issue 3, September 2000

AF-PHY-0086.001 Inverse Multiplexing for ATM (IMA)

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

DIGITAL DATA NETWORK MANAGEMENT

V.35

RS-232 (also known as EIA/TIA-232)

LDP

RFC 5036 LDP Specification

IS-IS

RFC 1142 OSI IS-IS Intra-domain Routing Protocol (ISO 10589)

RFC 1195 Use of OSI IS-IS for routing in TCP/IP & dual environments

RFC 2763 Dynamic Hostname Exchange for IS-IS

RFC 2966 Domain-wide Prefix Distribution with Two-Level IS-IS

RFC 2973 IS-IS Mesh Groups

RFC 3373 Three-Way Handshake for Intermediate System to Intermediate System (IS-IS) Point-to-Point Adjacencies

RFC 3567 Intermediate System to Intermediate System (IS-IS) Cryptographic Authentication

RFC 3719 Recommendations for Interoperable Networks using IS-IS

RFC 3784 Intermediate System to Intermediate System (IS-IS) Extensions for Traffic Engineering (TE)

RFC 3787 Recommendations for Interoperable IP Networks

RFC 5309 Point-to-Point Operation over LAN in Link State Routing Protocols

MPLS

RFC 3031 MPLS Architecture
RFC 3032 MPLS Label Stack Encoding
RFC 3815 Definitions of Managed Objects for the Multiprotocol Label Switching (MPLS), Label Distribution Protocol (LDP)
RFC 4379 Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures

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 1850 OSPF-MIB
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 2096 IP-FORWARD-MIB
RFC 2138 RADIUS
RFC 2206 RSVP-MIB
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 2588 SONET-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
draft-ietf-ospf-mib-update-04.txt
draft-ietf-mpls-lsr-mib-06.txt
draft-ietf-mpls-te-mib-04.txt
IANA-IFType-MIB

OSPF

RFC 1765 OSPF Database Overflow
RFC 2328 OSPF Version 2
RFC 2370 Opaque LSA Support
RFC 3101 OSPF NSSA Option
RFC 3630 Traffic Engineering (TE) Extensions to OSPF

PPP

RFC 1332 PPP IPCP
RFC 1570 PPP LCP Extensions
RFC 1619 PPP over SONET/SDH
RFC 1661 PPP
RFC 1662 PPP in HDLC-like Framing
RFC 1989 PPP Link Quality Monitoring
RFC 1990 The PPP Multilink Protocol (MP)
RFC 2686 The Multi-Class Extension to Multi-Link PPP

PSEUDOWIRES

RFC 3550 RTP: A Transport Protocol for Real-Time Applications
RFC 3985 Pseudo Wire Emulation Edge-to-Edge (PWE3) Architecture
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

draft-ietf-pwe3-redundancy-01 Pseudowire (PW) Redundancy

RADIUS

RFC 2865 Remote Authentication Dial In User Service

RFC 2866 RADIUS Accounting

RSVP-TE and FRR

RFC 2430 A Provider Architecture for DiffServ & TE

RFC 2961 RSVP Refresh Overhead Reduction Extensions

RFC 3209 Extensions to RSVP for LSP Tunnels

RFC 3210 Applicability Statement for Extensions to RSVP for LSP Tunnels

RFC 4090 Fast Reroute Extensions to RSVP-TE for LSP Tunnels

SONET/SDH

GR-253-CORE SONET Transport Systems: Common Generic Criteria. Issue 3, September 2000

ITU-G.841 Telecommunication Standardization Section of ITU, Types and Characteristics of SDH Networks Protection Architecture, issued in October 1998 and as augmented by Corrigendum1 issued in July 2002

GR-253-CORE - SONET Transport Systems: Common Generic Criteria. Issue 3, September 2000

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

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

IEEE 1588v2 1588 PTP 2008

TACACS+

draft-grant-tacacs-02.txt The TACACS+ Protocol

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

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-RSVP-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/myaccess

Product manuals and documentation updates are available at 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

Documentation feedback

documentation.feedback@alcatel-lucent.com

3HE 04959 AAAA TQZZA Edition 01