Configuring SAToP Pseudowires

SYSTEM ADMINISTRATOR GUIDE

96/1543-CRA 119 1170/1 Uen B

Contents

1 Overview

Circuit Emulation Service (CES) transparently carries time-division multiplexing (TDM) circuits over a packet-switched network (PSN). At the source endpoint, TDM frames are converted to packets, which are then transported across the PSN core. At the destination endpoint, the packets are converted back to TDM frames.

Structure-agnostic TDM over Packet (SAToP, as defined in RFC 4553) encapsulates TDM bitstreams as pseudowires over a PSN, disregarding any TDM framing structure.

SAToP is supported on Channelized 8-port OC-3/STM-1 and Channelized 2-port OC-12/STM-4 line cards and as well as Cross-Connect Route Processor Version 4 (XCRP4) or SMRP2 Controller cards on all chassis. Packet Processing ASIC first generation (PPA1) cards are not supported.

SAToP requires an all-ports license and a ces license. For information about all-ports and ces licenses, see *Configuring Channelized Ports, 8/10948-CRA 119 1170/1*.

This document applies to both the Ericsson SmartEdge® and SM family routers. However, the software that applies to the SM family of systems is a subset of the SmartEdge OS; some of the functionality described in this document may not apply to SM family routers.

For information specific to the SM family chassis, including line cards, refer to the SM family chassis documentation.

For specific information about the differences between the SmartEdge and SM family routers, refer to the Technical Product Description *SM Family of Systems* (part number 5/221 02-CRA 119 1170/1) in the `Product Overview` folder of this Customer Product Information library.

1.1 Components in the SAToP Model

an SAToP pseudowire consists of the following components.

Attachment circuit (AC)

On SAToP, the AC is an unframed T1 or E1 trunk. Each T1 trunk is 1.544 Mbps of bandwidth. Each E1 trunk is 2.048 Mbps of bandwidth.

Interworking function (IWF)

In the ingress direction, an SAToP IWF packetizes the unframed AC data onto a pseudowire.

In the egress direction, the IWF places out the payload from the pseudowire onto the AC.

Cross connect (XC)

The XC joins the AC to the PSN, either User Datagram Protocol (UDP/IP) or Multiprotocol Label Switching (MPLS).

Pseudowire (PW)

The PW carries the framed AC data between SAToP IWFs.

SAToP circuits are created and managed using command-line interface (CLI) commands. SNMP support is limited to get, getnext, and walk functions. Simple Network Management Protocol (SNMP) set functions are not supported.

SAToP requires an all-ports license. For information about all-ports licenses, see *Configuring Channelized Ports*, *8/10948-CRA 119 1170/1*.

2 Creating an SAToP Circuit

To create an SAToP circuit, perform the following on each end of the circuit:

1. Configure the AC.
2. Configure the XC to form the PW.
3. (Optional) Configure the clock source.
4. Bind the AC to the XC.

2.1 Configuring the AC

Configuring the AC involves configuring the AC port for CES use and configuring the corresponding IWF.

When a T1 or E1 trunk is configured on a port, and the port has been configured for CES, the trunk is automatically attached to the port's IWF. To configure an IWF, configure SAToP parameters on the trunk.

An IWF can be bound to only one digital signal level 1 (DS-1) channel. The following syntax is used to specify which channel the IWF is attached to:

- For E1: `slot/port:[ds3-channel:]e1-subchannel`
- For DS-1: `slot/port:[ds3-channel:]ds1-subchannel`

To configure an AC, perform the tasks described in Table 1.

Table 1 Configure the Attachment Circuit

Task	Root Command	Notes
Configure the E-1 or DS-1 channel group of the AC.	*port [e1 / ds1]*	Enter this command in global configuration mode or in DS-3 or DS-1 configuration mode.
Create a new Layer 2 Virtual Private Network (L2VPN) profile or select an existing L2VPN profile and enter L2VPN profile configuration mode.	*l2vpn local*	Enter this command in global configuration mode.
Enable SAToP configuration mode on an attachment circuit.	*satop*	Enter this command in DS0 channel configuration mode.
Configure the end-to-end delay settings of an SAToP IWF.	*end-to-end-delay*	Enter this command in SAToP configuration mode.
Display SAToP channel attributes.	*show ces*	Enter this command in any mode.
Displays the medium access control (MAC) address and other lower-layer settings of a single port, all ports on a card, or all ports in the system.	*show port detail*	Enter this command in any mode.

For guidelines on configuring the AC, see *AC Guidelines*and *IWFGuidelines*.

See *Configuration Examples* and *Monitoring and Diagnostic Examples* for CLI examples.

2.2 Configuring the XC to Form the Pseudowire

For information on configuring a pseudowire, see *Pseudowire Guidelines*.

To configure the XC, perform the tasks described in Table 2.

Table 2   Configure the Cross Connect to Form the Pseudowire

Task	Root Command	Notes
Configure the global pseudowire settings for SAToP connections.	*pseudowire router-id*	Enter this command in global configuration mode.
Create a new L2VPN profile or select an existing L2VPN profile and enter L2VPN profile configuration mode.	*l2vpn profile*	Enter this command in global configuration mode.
Configure the remote endpoint of the PW. The remote ip address can be an IPv4 address.	*peer ip-address*	Enter this command in L2VPN profile peer configuration mode.
Specify the EXP bits configuration in an L2VPN profile.	*exp-bits*	Enter this command in L2VPN profile peer configuration mode.
Specify a particular Resource Reservation Protocol (RSVP) or Label Distributionj Protocol (LDP) tunnel for carrying traffic exiting an L2VPN cross-connect (XC).	RSVP: *tunnel lsp* LDP: *tunnel ldp-path*	Enter this command in L2VPN profile peer configuration mode.
Configure the diffserver code for the CES PW.	*dscp*	Enter this command in L2VPN profile peer configuration mode.
Display the PW global configuration.	*show pseudowire*	Enter this command in any mode.

See *Configuration Examples* and *Monitoring and Diagnostic Examples* for CLI examples.

2.3 Configuring the Clock Source

SAToP supports the following methods for clock recovery for CES channels and sub-channels:

- Adaptive
- Synchronous
- Loop-timed

For more information about these methods, see *Clock Source Guidelines*.

To configure the clock source on a channel or sub-channel, perform the tasks described in Table 3.

Table 3 Configure the Clock Source

Task	Root Command	Notes
Enter configuration mode for a DS1 channel in a channelized OC-3 or OC-12 port or in a channelized DS3 channel.	*port {ds1 | channelized-ds1}*	Enter this command in global configuration mode or in OC-3, OC-12, or DS-3 configuration mode.
Enter configuration mode for a DS3 channel in a channelized STM-1, STM-4, OC-3, or OC-12 port.	*port {ds3 | channelized-ds3}*	Enter this command in global configuration mode or in OC-3, OC-12, STM-1, or STM-4 configuration mode.
Enter configuration mode for an E1 channel in a channelized STM-1 or STM-4 port, or in a channelized DS3 channel.	*port {e1 | channelized-e1}*	Enter this command in global configuration mode or in STM-1, STM-4, or DS-3 configuration mode.
Configure the clock source settings of an SAToP circuit.	*clock-source ces-domain*	Enter this Show command to display CES timing domain. in global configuration mode.
Display the CES timing domain.	*show ces domain*	Enter this command in any mode.

See *Configuration Examples* and *Monitoring and Diagnostic Examples* for CLI examples.

2.4 Binding the AC to the XC

An IWF can be bound to only one PW, using the **xc** command.

For information on binding the IWF to a pseudowire, see *Pseudowire Guidelines* and *IWFGuidelines*.

To bind the AC to the XC, perform the tasks described in Table 4.

Table 4 Bind the Attachment Channel to the Cross Connect

Task	Root Command	Notes
Enter local context configuration mode.	*context local*	Enter this command in global configuration mode.
Enter L2VPN configuration mode.	*l2vpn*	Enter this command in context configuration mode.
Create a Layer 2 Virtual Private Network (L2VPN) cross-connection group and enters L2VPN XC group configuration mode.	*xc-group*	Enter this command in L2VPN configuration mode.

Table 4 Bind the Attachment Channel to the Cross Connect

Task	Root Command	Notes
Configure the pseudowire cross connect for the SAToP circuit.	*xc ds1*	Enter this command in L2VPN XC group configuration mode. Use the **`udp`** keyword to create a CES Over UDP pseudowire. Use the **`vpn-label`** keyword to create a CES Over MPLS pseudowire.
Display L2VPN cross-connect information.	*show xc l2vpn static*	Enter this command in any mode.

See *Configuration Examples* and *Monitoring and Diagnostic Examples* for CLI examples.

3 Monitoring SAToP Circuits

On an existing SAToP circuit, you can:

- Configure excess packet loss thresholds
- Enable outage and excess packet loss traps for managing service level agreements (SLAs)
- Monitor port and circuit counters

3.1 Monitoring Excess Packet Loss Information

For information on configuring the excess packet loss rate, see *Excess Packet Loss Measurement*.

To display and monitor excess packet loss information, perform the tasks described in Table 5.

Table 5 Monitoring Excess Packet Loss Information

Task	Root Command	Notes
Configure the excessive packet loss settings of SAToP circuits.	*ces excessive-pack et-loss*	Enter this command in global configuration mode.

Table 5 Monitoring Excess Packet Loss Information

Task	Root Command	Notes
Clear all excessive packet loss counters or only the counters of a specific SAToP circuit.	*clear ces excessive -packet-loss*	Enter this command in global configuration mode.
Display CES excessive packet loss rate on SAToP circuits.	*show ces excessiv e-packet-loss-rate [detail]*	Enter this command in any mode.

See *Configuration Examples* and *Monitoring and Diagnostic Examples* for CLI examples.

3.2 Trapping Outage Information

Trapping SLA information can be enabled on a per-PW basis for the life of the PW channel.

For information on configuring SNMP traps and alarms for CES outage or excessive packet loss rate, see *Outage Monitoring*.

To trap outage information, perform the tasks described in Table 6.

Table 6 Trapping Outage Information

Task	Root Command	Notes
Enables and disables the CES outage or excessive-packet-loss-rate trap.	*trap cesmib outage | excessive-packet-l oss-rate*	Enter this command in SNMP server configuration mode.
Clears all outage counters or only the counters of a specific SAToP. circuit.	*clear ces outage*	Enter this command in SNMP server configuration mode.
Display SAToP channel attributes.	*show ces*	Enter this command in any mode. Use the **`normal`** keyword to display attributes for normal circuits. Use the **`outage`** keyword to display attributes for circuits with outages.

See *Configuration Examples* and *Monitoring and Diagnostic Examples* for CLI examples.

3.3 Monitoring Statistics

SAToP statistics are monitored using port counters and circuit counters.

To monitor statistics, perform the tasks described in Table 7.

Table 7 Monitoring Statistics

Task	Root Command	Notes
Display output for CES port counters on SAToP circuits.	*show port counters*	Enter this command in any mode.
Clears the CES port counters on all or selected SAToP circuits.	*clear port counters*	Enter this command in any mode.
Display CES circuit counters for all or specified SAToP circuits.	*show circuit counters*	Enter this command in any mode.
Clears the CES circuit counters on all or selected CESoPSN circuits.	*clear circuit counters*	Enter this command in any mode.

See *Monitoring and Diagnostic Examples* for CLI examples.

4 SAToP Configuration Guidelines

4.1 AC Guidelines

The access port is an OC3/OC12/STM1/STM4, supporting channelized SONET/SDH interfaces.

The Channelized 8-port OC-3/STM-1 or Channelized 2-port OC-12/STM-4 line card operates in two service modes on a given port: Packet over SONET/SDH (POS) mode or CES mode. The line card can never operate in mixed mode on a given port.

If a port is configured for CES mode, the system rejects attempts to change the mode to POS. To change the mode of a port, enter the **`no port`** command before switching modes, even if no channels are configured on it.

The CES DS-1 channel is represented with the syntax ***`slot/port:[ds3-channel:]ds1-channel`***.

You can configure SAToP and CESoPSN on the same port without impacting scale or Automatic Protection Switching (APS) support (see Section 4.3 on page 11 for timing-domain constraints).

If you try to create and associate a DS-0 channel as CESoPSN, but the corresponding DS-1 channel is already configured as SAToP (or vice versa), the system rejects the configuration.

4.2 IWFGuidelines

4.2.1 IWF Egress States

The SAToP IWF can be in one of two possible states: normal or packet loss. The IWF begins in normal state when it is created. You can view the state of the IWF using the `show ces` command.

4.2.1.1 Normal State

Normal state indicates that all the following are occurring:

- Packets are being received.
- The received control words are being processed.
- Adaptive clock recovery (if configured) is taking place.
- The DS-1 channel payload is being played out according to the PW packet payload.

The IWF enters the normal state when it exits the packet loss state.

The IWF transitions to the packet loss state when the entry criteria for that state are met. Outage criteria are set using the `end-to-end-delay` command.

The following occurs while in normal state:

- The IWF sets the value of **R** to 0 in its transmitted PW control word.
- The IWF sets the value of **L** in its transmitted PW control word according to the T1 or E1 trunk state in the received direction.
- Incoming packets are added to the jitter buffer, processed and counted.

4.2.1.2 Packet Loss State

The packet loss state indicates that packet loss has occurred in the PSN or the jitter buffer has an underrun. This state is entered if either of the following is true:

- The number of consecutive missing packets is greater than or equal to the *`enter`* value configured with the `end-to-end-delay` command.
- The jitter buffer has underrun.

The IWF transitions to the normal state when both of the following have occurred:

- If a jitter buffer underrun occurred, the jitter buffer has filled to half of its depth.
- The number of consecutive packets received is greater than or equal to the ***exit*** value configured with the **end-to-end-delay** command.

While in the packet loss state:

- The IWF sets the value of **R** to 1 in its transmitted PW control word.
- The IWF sets the value of **L** in its transmitted control word according to the T1 or E1 trunk state in the received direction.
- The configured IDLE pattern is played out on every DS-1 or E1 channel of the IWF.
- Incoming packets are added to the jitter buffer, but are not processed or counted.

Note: Underrun can occur due to lost packets on the PW or if the DS-1 or E1 channel's TDM trunk has a transmit clock frequency that is too high relative to the sustained packet arrival rate on the PW.

4.2.2 IWF Egress Behavior

Table 8 illustrates the IWF behavior on egress, based on the E1 or T1 trunk state or the IWF state.

Table 8 Egress (PSN to TDM) IWF Behavior

Control Event (Received CW Bits)		Egress T1 or E1 Trunk Control (If Configured)	Counter	Effect on Egress AC Data
L	R			
0	0			Data played out as received.
1	0	AIS	Far-end AC down	Packet is discarded and an unframed "all 1s" is transmitted on the AC.
1	1	AIS	Far-end AC down	Packet is discarded and an unframed "all 1s" is transmitted on the AC.

4.2.3 IWF Ingress Behavior

Table 9 illustrates the IWF behavior on ingress, based on the E1/T1 trunk state or IWF state.

Table 9 Ingress (TDM to PSN) CES IWF Behavior

Control Event (T1 or E1 Trunk State / IWF State)	**Transmitted CW**		**Effect on TDM Data in PW Payload**
	L	**R**	
OK	0	0	None. This is the normal error-free case.
T1 or E1 Trunk LOS T1 or E1 Trunk AIS	1	0	TDM data present in the packet is considered invalid. *Note:* Because of the software latency on setting the L bit in the CW for the affected PWs, if a large number of PWs needs to be updated, some packets sent in the PSN might have an invalid payload and the L bit cleared.
IWF Loss of Packet State or Underrun	0	1	None

4.3 Clock Source Guidelines

4.3.1 Adaptive Clock Recovery

CES timing domains are created automatically for the Channelized 8-port OC-3/STM-1 or Channelized 2-port OC-12/STM-4 line card and are not configurable.

SAToP supports 16 timing domains per card (8 timing domains per port group) for CES adaptive clock recovery. All trunks in a timing domain are in the same 4-port group on the card.

You assign a DS-1 or E1 trunk to a timing domain for that trunk's port group.

Timing domains for SAToP and CESoPSN are independent of each other. If an existing timing domain for CESoPSN is changed to SAToP (or vice versa), the change is rejected.

Software on the Channelized 8-port OC-3/STM-1 or Channelized 2-port OC-12/STM-4 line card automatically selects a master IWF for each timing domain on the associated DS-1 or E1 trunk. The master IWF provides the timing domain with its reference clock based on packet arrival times.

If the source IWF experiences an error (loss-of-packet, underrun, or overrun state), the timing domain enters the holdover state. If the master IWF goes into loss-of-packet state or is deleted, the software on the card changes to a new master IWF (one that is not in loss-of-packet, underrun, or overrun state) within the same timing clock recovery domain group. If the master IWF is in underrun state, no change occurs.

If all IWFs within a domain are in loss-of-packet state, the master is not changed, and it remains in holdover state.

When in holdover state, the configured card reference clock is used. This results in 20ppm accuracy if the card reference clock is derived from the card's local clock.

A CES timing domain that is not in holdover is active.

4.3.2 Synchronous Clock Recovery

The clock source is the local clock source on the Channelized 8-port OC-3/STM-1 or Channelized 2-port OC-12/STM-4 line card or is global, referenced from the XCRP card.

4.3.3 Loop-Timed Clock Recovery

The transmit clock source for the DS-1 or E1 trunk is derived from that trunk's recovered receive clock.

4.4 Pseudowire Guidelines

4.4.1 Pseudowire Payload

The order of the payload octets corresponds to their order on the TDM trunk. Payload for E1 is 256 bytes. Payload for T1 is 192 bytes.

For the DS-1, the packet latency is .9948 milliseconds. For E1, 1–8 milliseconds is supported.

Consecutive bits coming from the TDM trunk fill each payload octet, starting from the most significant bit to the least significant bit.

All SAToP packets *must* carry the same amount of valid TDM data in both directions of the PW. The time that is required to fill an SAToP packet with the TDM data is constant.

The egress SAToP IWF reorders misordered packets. Misordered packets that cannot be reordered are discarded and treated as lost.

The egress IWF discards stray packets. Their detection does not affect mechanisms for detection of packet loss.

Loss-of-packet state is declared immediately on underrun. Use of a timer to declare the loss-of-packet state after an underrun is not supported.

After the PW is set up, TDM data is packetized using the configured number of payload bytes per packet.

The egress SAToP IWF includes a jitter buffer in which the payload of the received SAToP packets is stored prior to play-out to the local TDM AC.

4.4.1.1 CES Control Word

The CES control word format, as described in RFC 4553, is supported.

L bit

- The L bit flag in a normal packet set to zero.
- L (local failure): If the L bit flag is set, it indicates some abnormal condition on the far-end T1 or E1 trunk. The behavior of the L bit is as described in Table 8 and Table 9.
- On egress, if the payload is omitted (such as under an error condition to save bandwidth), the length is 4 (equal to the control word). In such a case, the system plays the packet as received over the TDM channel.

M bit

The M bit flag is not supported by SAToP.

R bit

The behavior of the R bit flag is as described in Table 8 and Table 9.

FRG

The FRG bits are not supported.

- On the PW ingress, the FRG bits are always set to 00b.
- On the PW egress, if the FRG bits are greater than 00b, the system ignores the FRG bits and processes the packet. A remote configuration that generates FRG bits greater than 00b is considered as invalid.

LEN

The LEN field is set to zero if the packet length (SAToP header + the payload size) is greater than or equal to 64 bytes; otherwise, it is set to the packet length.

SN

The control word sequence number (SN) provides the common PW sequencing function, as well as detection of lost packets.

- Its space is a 16-bit unsigned circular space.
- Its initial value is random (unpredictable).
- It is incremented with each SAToP data packet sent over a given PW.

4.4.2 Pseudowire Initialization and Shutdown

Before a PW has been set up and after a PW has been torn down, the IWF must play out the “all 1s” pattern to its TDM AC.

After the PW has been set up, the egress IWF begins to receive SAToP packets and to store their payload in the jitter buffer but continues to play out the “all 1s” pattern to its TDM AC. This intermediate state persists until a preconfigured amount of TDM data (usually half of the jitter buffer) has been received in consecutive SAToP packets. This amount is set with the `end-to-end-delay` command.

When the preconfigured amount of TDM data has been received, the PW enters its normal operation state in which it receives SAToP packets and stores their payload in the jitter buffer while playing out the contents of the jitter buffer in accordance with the required clock.

There is no intermediate timer involved. When the jitter buffer is half full, in the egress direction, the IWF starts transmitting data. The intermediate state depends *only* on the jitter buffer size and packetization latency.

SAToP PW monitoring is performed after the egress IWF has exited its intermediate state.

4.4.3 Pseudowire State

The PW is operationally UP when both of the following conditions are met:

- The destination peer is reachable.
- The PW state meets any of the UP conditions in Table 10.

Otherwise, the PW state is DOWN.

Table 10 CES AC and Pseudowire States

Local Physical Port Events	AC Admin Status	Port Link Status	AC Oper ational Status	CES PW State
LOS	UP	DOWN	UP	UP
AIS	UP	DOWN	UP	UP
Loopback	UP	UP	UP	UP
Administrative Shutdown	DOWN	DOWN	DOWN	DOWN

Port link status is the final stable port state at the end of the link-dampening process.

AC operational status represents the final state on AC operational status.

4.4.4 CES Over MPLS Pseudowire

- To provision CES over an MPLS pseudowire, use Layer 2 Virtual Private Network (L2VPN) MPLS static labels.
- Exp Bits support is per MPLS pseudowire.
- MPLS pseudowire using LDP signaling is not supported.
- Virtual circuit connectivity verification (VCCV) ping is not supported.
- If all the following conditions are met, the PW state is operationally UP; otherwise, the PW state is DOWN.
  - The destination peer is reachable through LSP.
  - The PW state UP conditions are as listed in Table 10.

4.4.5 CES over UDP Pseudowire

4.4.5.1 Endpoints

In a CES over UDP pseudowire connection, the PW destination endpoints are determined by the destination UDP and destination IP address. The source endpoints are determined by the source IP address, which is the loopback IP address in the local context.

4.4.5.2 UDP Ports

The port range for a UDP pseudowire is 1024–65535 for the source UDP port, and 1–65535 for the destination UDP port.

UDP ports 1–1024 are reserved ports on the system. The PW source UDP port should not overlap the system's reserved ports.

The UDP port of the source endpoint is the destination port at the peer, and vice versa.

4.4.5.3 Other UDP Considerations

Pseudowire UDP header checksum verification and generation are not supported. The UDP header checksum is always zero.

Differentiated Services Code Point (DSCP) marking is per PW. IP traffic marking is toward the ingress. If there is IP Security (IPSec) traffic, the PW DSCP present at the inner IP header is copied to the outer IP header.

A Layer 2 transport of the PW endpoints is either Ethernet or multilink Point-to-Point Protocol (MLPPP). MLPPP fragmentation is independent of CES PW traffic.

A Layer 3 PSN to the PW endpoint is either IP or IPSec.

- IPv4 datagrams are marked as “Don’t Fragment”.
- The cross-connect of the UDP PW is on the local context, and the destination peer address is routed through the local context.
- Intercontext routing of the destination peer address for unmapped UDP PW is supported.

IPSec services are provided by the Advanced Services Engine (ASE) card using tunnel mode.

- PW over manual (static) IPSec tunnel is supported.
- The PW IP address is the inner IP address of the IPSec tunnel.
- The outer IP address is the tunnel IP address.
- The source IP address configured for CES UDP PW is theh loopback IP address on the local context.

The PW state is operationally UP if all the following conditions are met; otherwise, the PW state is DOWN.

- The destination peer is reachable through IP or IPSec, depending on the user configuration.
- The source IP address is a loopback IP address in the local context.
- The PW state UP conditions are as listed in Table 10.

4.4.6 Pseudowire and Equal-Cost Multipath

The CES PW endpoint is reachable through the equal-cost multipath (ECMP) next hops. The SE implements different hashing techniques for MPLS and UDP PWs. Selection of the next hop is based on the configured hashing scheme: either two tuple or five tuple

The hashing scheme makes sure that the flows are uniquely distributed for different PWs.

UDP PW hashing is based on the source IP address, destination IP address, UDP source port, and UDP destination port.

The SAToP implementation does not negate existing ECMP capability.

4.4.7 CES with APS

An APS configuration for CES is always provided on an APS working port. The system rejects any CES configuration on the APS port.

The ingress and egress CES functions are supported on APS-enabled ports.

After APS switchover recovery, the CES function has additional predictable packet loss, because the new switched-over CES IWF must meet the loss of packet state exit criteria.

4.5 Monitoring Guidelines

4.5.1 Excess Packet Loss Monitoring

Packet loss rate can be measured on a per PW basis.

Packet loss rate (PLR) is defined as the ratio of lost packets / transmitted packets, where lost packets = dummy packet count – error packet count, and transmitted packets = valid packet count – lost packets.

The average packet loss rate (APLR) is the PLR over a given amount of time (T), equal to 2.5 seconds.

A fault declaration time (FDT) is when an excessive packet loss fault is declared if a specified number of defect samples (N) in successive periods of duration N × T) experience an excessive packet loss defect and exceed the user-configured threshold (L), that is, FDT = PLR > L.

The current snapshot entry is maintained per CES channel. The time information presented is in seconds. The snapshot entry contains the following elements:

Entry

- The time stamped on entering into excessive packet loss state.
- Total packet loss on entry is the sum of the packet loss measured at the entry point since the up time of the channel. For example, if deltaX1 and deltaX2 are the last packet loss on the entry of the current excessive packet loss, total packet loss = deltaX1 + deltaX2.

Exit

- Packet loss on exit is the loss at duration X on the channel. If the channel is already in progress of excessive packet loss, packet loss = user query timestamp − entry timestamp.
- Total packet loss on exit is the sum of the packet loss measured since the up time of the channel: total packet loss = total packet loss on entry + packet loss. If you reset the excessive packet loss statistics, total packet loss is calculated from the time the DS-1 channel stats were reset.

Total times in packet loss

Number of times the channel entered into the excessive packet loss condition.

Total circuit time

Total time elapsed since the CES channel is up, plus total packet loss time on exit. if you reset the excessive packet loss statistics, total circuit time is calculated from the time the DS-1 channel stats were reset.

Total failure rate

Total time the PW is in excessive packet loss / total circuit time. If you reset the excessive packet loss statistics, then total failure rate is calculated from the time the DS-1 channel stats were reset.

DS-1 channel ID

4.5.2 Outage Monitoring

SLA current snapshot entries are per DS-1 channel as listed in Table 11.

Table 11 SLA Current Snapshot Entries

SLA Parameter	Description
Latest Outage Time	Delta time where the IWF enters the packet-loss / underrun state and the exit time (latest outage exit timestamp – latest outage entry timestamp).
Latest Outage Exit Timestamp	Latest exit from the defective state timestamp in the format, Month/Day/Year, Hour:Min:Sec. If you query the snapshot entry and the IWF is in packet-loss / underrun state, latest outage exit timestamp is the query time. If you query the snapshot entry and the IWF is in normal state, the latest outage exit timestamp is the time when the IWF exited from the packet loss / underrun state to normal state.
Latest Outage Entry Timestamp	The latest entry to the defective state timestamp in the format, Month/Day/Year, Hour:Min:Sec.
Last Outage Time	Delta time of the outage prior to the latest outage time.
Last UP Time	Delta time when the channel was UP prior to the latest outage time (the time elapsed between the entry of the latest outage time and the exit of the last outage time).
Cumulative Outage Time	Sum of the outage since the CES channel was created.
UP Time	Total UP time since the CES channel was created, minus the cumulative outage time.
Number of Outages	Counts the number of outage times.

An outage SNMP trap is supported per card.

- The SNMP trap is raised when at least one SAToP PW is in the outage state (packet loss / underrun state).
- The SNMP trap is cleared whenever all the SAToP PWs are in normal state.

Time information in snapshot entries is in seconds.

5 Configuration Examples

5.1 IWF Binding

The following example configures the IWF on an SAToP circuit:

```
[local]Redback(config)#port e1 1/1:1:1
[local]Redback(config-e1-ces)#l2vpn local
[local]Redback(config-e1-ces)#satop
[local]Redback(config-e1-satop)#end-to-end-delay latency 4 jitter 160 outage-criteria 1 10
```

5.2 Pseudowire

The following example configures the global settings of an SAToP PW:

```
[local]Redback(config)#pseudowire router-id ipaddress xxx.xxx.xxx.xxx context local
```

The following example configures the profile settings for an SAToP PW:

```
[local]Redback(config)#l2vpn profile name1
[local]Redback(config-l2vpn-xc-profile)#peer xxx.xxx.xxx.xxx
[local]Redback(config-l2vpn-xc-profile)#exp-bits 3
[local]Redback(config-l2vpn-xc-profile)#tunnel lsp name2
[local]Redback(config-l2vpn-xc-profile)#dscp af13
```

5.3 Clock Source

The following example configures the clock source on an SAToP E1 circuit:

```
[local]Redback(config)#port 2/1:1:3
[local]Redback(config-ces-chan-el)#clock-source ces-domain 1.4
```

5.4 Cross-connect

The following example configures various types of SAToP cross-connects:

```
[local]Redback(config)#context local
[local]Redback(config-ctx)#l2vpn
[local]Redback(config-l2vpn)#xc-group name
[local]Redback(config-l2vpn-xc-group)#xc ds1 3/4:1:1 ces udp 3:4 profile name1
[local]Redback(config-l2vpn-xc-group)#xc ds1 3/4:1:1 through 8 ces udp 5:6 profile name
[local]Redback(config-l2vpn-xc-group)#xc ds1 3/4:3:1 ces vpn-label 556 profile name1
[local]Redback(config-l2vpn-xc-group)#xc ds1 3/4:3:2 through 8 ces vpn-label 556 profile name1
```

5.5 Excessive Packet Loss Settings

The following example configures settings for excessive packet loss:

```
[local]Redback(config)#ces execessive-packet-loss threshold 45 set 5 clear 20
```

The following example clears the excessive packet loss counters on a specific circuit:

```
[local]Redback(config)#clear ces execessive-packet-loss 3/2:3:1:1
```

5.6 Outage Settings

The following example enables the outage trap and disables the excessive-packet-loss-rate trap:

```
[local]Redback(config-snmp-server)#trap cesmib outage
[local]Redback(config-snmp-server)#no trap cesmib excessive-packet-loss-rate
```

The following example clears the excessive packet loss counters on a specific circuit:

```
[local]Redback(config)#clear ces outage 3/2:3:1:1
```

6 Monitoring and Diagnostic Examples

6.1 CES Operation

```
[local]Redback#show ces 3/2:1:1

Circuit     Time Slots   CES Type IWF State             L2vpn
--------------------------------------------------------------
3/2:1:1     N/A          SAToP    Normal               enabled


[local]Redback#show ces all

Circuit     Time Slots   CES Type IWF State              L2vpn
---------------------------------------------------------------
3/2:1:1     N/A          SAToP    Normal                 disabled
3/2:1:2     N/A          SAToP    Loss of Packet/under-run  enabled
3/2:1:3     N/A          SAToP    Normal                 enabled
```

6.2 Clock Source

The following example displays information about timing domain 1.3 on slot 2. There are 5 member trunks (three from port 1 and two from port 3). The current master IWF is associated with DS-0 group 4 on DS-1 2/3:1:14, indicating that the timing domain state is active.

```
[local]Redback#show ces domain 2/1.3

Slot 2 Timing Domain: 1.3
Current Master      : 2/3:1:14:4

Members:

Port/Channel Type
------------------------
2/1:1    ds1
2/1:2   ds1
2/1:1:21  ds1
2/3:1:14  ds1
2/3:1:21  ds1
```

6.3 Pseudowire

The following example displays the PW global configuration on an SAToP circuit:

```
[local]Redback#show pseudowire
    multi-path disabled
    PW MTU matching enabled
    PW Router id enabled
    ========================
    Router id              : 4.4.4.4
    Router id Context      : 0x40080001
    Router id if Grid      : 0x10000004
    Router id Nexthop Grid : 0x31d00003
    Router id State        : UP
```

6.4 Excessive Packet Loss Information

```
[local]Redback#show ces excessive-packet-loss-rate

Circuit      Time Slots CES Type Total Loss Time (dd:hh:mm:ss)
==============================================

3/2:1:1       N/A           SAToP             00:00:20:00
3/2:1:2       N/A           SAToP             00:00:20:00

Total Channels in Packet Loss : 2


[local]Redback#show ces excessive-packet-loss-rate detail


Threshold (%)                : 40
Clearing time                : 10 seconds
Declaration Time             : 2.5 seconds

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

Circuit                     : 3/2:1:1
Time Slot                   : N/A
CES Type                    : SAToP

Current Excessive packet loss snapshot

Entry

Time Stamp             : Tue Apr 20 00:00:01 2010 GMT
Total Packet Loss Time : 0 days 0 hours 1 minutes 0 seconds

Exit
Packet Loss Time       : 0 days 0 hours 0 minutes 10 seconds
Total Packet Loss Time : 0 days 0 hours 1 minutes 10 seconds
Total Failure Rate (%) : 10
Total Circuit Time     : 0 days 0 hours 10 minutes 10 seconds
Total number of times the channel in packet loss: 2


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

Circuit                     : 3/2:1:2
Time Slot                   : N/A
CES Type                    : SAToP

Current Excessive packet loss snapshot

Entry
Time Stamp             : Tue Apr 20 01:00:00 2010 GMT
Total Packet Loss Time : 0 days 0 hours 2 minutes 0 seconds

Exit
Packet Loss Time       : 0 days 0 hours 0 minutes 20 seconds
Total Packet Loss Time : 0 days 0 hours 2 minutes 20 second
Total Failure Rate (%) : 20
Total Circuit Time     : 0 days 0 hours 10 minutes 20 seconds
Total number of times the channel in packet loss: 3

Total Channels in Packet Loss: 2
```

6.5 Outage Information

```
[local]Redback#show ces outage

Circuit      CES Type      Cumulative Outage Time  (dd:hh:mm:ss)
==============================================

3/2:1:1      SAToP            00:00:12:01
3/2:1:2      SAToP            00:00:20:01


[local]Redback#show ces outage 3/2:1:1

 Circuit: 3/2:1:1 Service Type: SAToP
---------------------------------------------------------------------------------------------------------
Latest Outage Time          - 0 days 0 hours 5 minutes 0 second
(Tue Apr 20 18:25:01 2010 GMT) - (Tue Apr 20 18:20:01 2010 GMT)
Last Outage Time            - 0 days 0 hours 4 minutes 1 second
Last UP Time                - 0 days 0 hours 5 minutes 1 second
Cumulative Outage Time      - 0 days 0 hours 12 minutes 1 second
UP Time                     - 0 days 1 hours 4 minutes 1 second
Number of Outage (s)        - 3

 Circuit: 3/2:1:2 Service Type: SAToP
---------------------------------------------------------------------------------------------------------
Latest Outage Time          - 0 days 0 hours 5 minutes 0 second
(Tue Apr 20 02:25:01 2010 GMT) - (Tue Apr 20 02:10:01 2010 GMT)
Last Outage Time            - 0 days 0 hours 5 minutes 1 second
Last UP Time                - 0 days 0 hours 6 minutes 1 second
Cumulative Outage Time      - 0 days 0 hours 20 minutes 1 second
UP Time                     - 1 days 2 hours 4 minutes 1 second
Number of Outage (s)        - 2
```

6.6 Statistics

```
[local]Redback#show port counters 6/1:1:1

Port              Type
  6/1:1:1          ds1

packets sent       : 1061               bytes sent         : 27586
packets recvd      : 1061               bytes recvd        : 23342
send packet rate   : 0.10               send bit rate      : 20.80
recv packet rate   : 0.10               recv bit rate      : 17.60
rate refresh interval : 60 seconds
```

```
[local]Redback#show port counters 6/1:1:1 ces

Circuit: 6/1:1:1, Time Slot: N/A, Service Type: SAToP

Jitter Buffer      : 16 ms    Channel Size     : N/A
Packet Latency     : 2 ms     Packet Size      : 388 Bytes
Trunk State control: N/A      Idle Pattern     : N/A
Clock Recovery     : adaptive IWF State        : Normal
Loss of packet state criteria: 5, 10


CES Egress Errors:
------------------

Out of Buffer Drops                    : 0
Missing Packets                        : 0
Malformed Packet                       : 0
Jitter Buffer Over Run Dropped Packets : 0
Jitter Buffer Under Run Events         : 0
Misorder Packets                       : 0
Remote Loss of Packet packets          : 0
Window switchovers                     : 0
Remote AC Down Packets                 : 0
Duplicate Packet Drops                 : 0
Denied Packet Drops                    : 0
Error Event                            : 0
Errored Data Block                     : 0


CES Ingress Errors:
-------------------

Out of Buffer Drops                    : 0
Packet Size Violation drops            : 0
Transmit Queue Drops                   : 0


[local]Redback#show circuit counters ces
Circuit                      Packets/Bytes Sent Packets/Bytes Received
2/1:1:1                                       0                      0
                                              0                      0
2/4:1:2                                       0                      0
                                              0                      0
2/6:1:3                                  640736                  66438
                                       52488402                5548482
10/12:1:2                                     0                      0
                                              0                      0


[local]Redback#show circuit counters 2/1:1:2 ces
Circuit                         Packets/Bytes Sent Packets/Bytes Received
2/1:1:2                                          0                      0
                                                 0                      0
```