Ultra Packet Core CUPS Sx Interface Administration and Reference Guide, Release 21.26

First Published: 2021-12-24

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

About this Guide

Note Control and User Plane Separation (CUPS) represents a significant architectural change in the way StarOS-based products are deployed in the 3G, 4G, and 5G networks. This document provides information on the features and functionality specifically supported by this 3G/4G CUPS product deployed in a 3G/4G network. It should not be assumed that features and functionality that have been previously supported in legacy or non-CUPS products are supported by this product. References to any legacy or non-CUPS products or features are for informational purposes only. Furthermore, it should not be assumed that any constructs (including, but not limited to, commands, statistics, attributes, MIB objects, alarms, logs, services) referenced in this document imply functional parity with legacy or non-CUPS products. Please contact your Cisco Account or Support representative for any questions about parity between this product and any legacy or non-CUPS products.

Note The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

This guide describes the Sx interface in Control and User Plane Separation (CUPS). This document also contains feature descriptions, configuration procedures, and monitoring and troubleshooting information.

• Conventions Used, on page vii

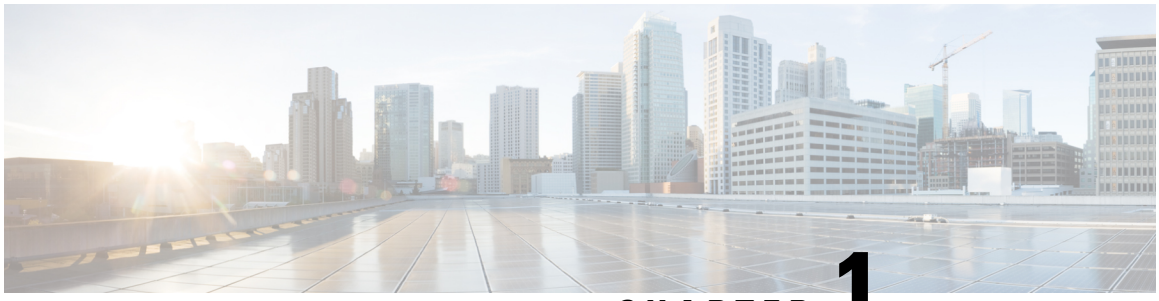
Conventions Used

The following tables describe the conventions used throughout this documentation.

Notice Type	Description
Information Note	Provides information about important features or instructions.
Caution	Alerts you of potential damage to a program, device, or system.

Notice Type	Description
Warning	Alerts you of potential personal injury or fatality. May also alert you of potential electrical hazards.

Typeface Conventions	Description
Text represented as a `screen display`	This typeface represents displays that appear on your terminal screen, for example: `Login:`
Text represented as **commands**	This typeface represents commands that you enter, for example: **show ip access-list** This document always gives the full form of a command in lowercase letters. Commands are not case sensitive.
Text represented as a **command** *variable*	This typeface represents a variable that is part of a command, for example: **show card** *slot_number* *slot_number* is a variable representing the desired chassis slot number.
Text represented as menu or sub-menu names	This typeface represents menus and sub-menus that you access within a software application, for example: Click the **File** menu, then click **New**



CHAPTER 1

Overview

The Evolved Packet Core (EPC) network is evolving and moving toward Control User Plane Separation (CUPS) based architecture where User-Plane and Control-Plane are separate node for P-GW, S-GW, and TDF products. The User Plane and Control Plane combined together provide functionality of a node for other elements in the EPC network. However, keeping them separate has numerous advantages from the network point of view – support different scaling for Control-Plane and User-Plane, support more capacity on per session level in User-Plane, and so on.

This chapter highlights high-level details, call flows, and configurations related to the Sx Interface implementation for P-GW, S-GW, and SAEGW products.

Product Description

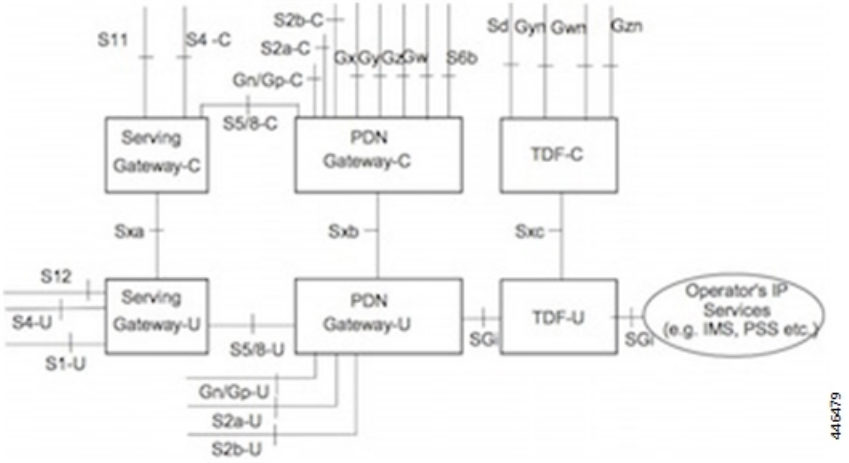
Sx is the interface between the Control-Plane and User-Plane in a split P-GW, S-GW, and TDF architecture in an Evolved Packet Core (EPC) that provides Packet Forwarding Control Protocol (PFCP) service. One of the main tasks of the Sx interface is to enable the Control-Plane function to instruct the User-Plane function about how to forward user data traffic.

How It Works

The following section provides a brief overview of the Sx service works.

Architecture

The following illustration provides a reference model in the case of separation between Control-Plane and User-Plane.



Note

- The -C or -U suffix appended to S2a, S2b, S5 and S8 existing reference points only indicate the Control-Plane and User-Plane components of those interfaces.
- The architecture only depicts the case when the Control-Plane and User-Plane functions of all S-GW, P-GW and TDF nodes are split. It also supports scenarios where the Control-Plane and User-Plane function of only one of these nodes is split while the Control-Plane and User-Plane function of the other interfacing node is not split. For example, it supports a scenario where the Control-Plane and User-Plane of the P-GW is split while that of the S-GW is not split. This split architecture of a node does not put any architectural requirements on the peer nodes with which it interfaces.
- TDF is an optional functional entity.

The following sections describe the services supported on the Sx Interface.

Sx Service

The Sx Service provides an interface mentioned as the following reference points:

- **Sxa:** Reference point between SGW-C and SGW-U.
- **Sxb:** Reference point between PGW-C and PGW-U.
- **Sxc:** Reference point between Traffic Detection Function-C (TDF-C) and TDF-U.

The Sx service is agnostic of the interface it supports. A single Sx service instance is capable of running on Sxa, Sxb, and Sxb interfaces. The Sx service runs in two different modes:

- Sx-Control instance
- Sx-Data instance

The Sx service is associated with the SAEGW service at the Control-Plane and User-Plane service at the User-Plane. There is one-to-one mapping of the Sx service with the Control-Plane and Data Plane.

The association of the SAEGW service occurs as follows:

```
saegw-service saegw-service
      associate sgw-service sgw-service
      associate pgw-service pgw-service
      associate gtpu-service control_gtpu up-tunnel
      associate sx-service sxc
```

The association of the User-Plane service occurs as follows:

```
user-plane-service user-plane-service
      associate gtpu-service sx-gtpu-service pgw-ingress
      associate gtpu-service sx-sgw_ingress_gtpu sgw-ingress
      associate gtpu-service sx-sgw_egress_gtpu sgw-egress
      associate gtpu-service control_gtpu cp-tunnel
      associate sx-service sxu
```

At the Control-Plane for SAEGW service (legacy SAEGW Service), CUPS-enabled flag in EGTPC service determines whether SAEGW is CUPS enabled or not. If SAEGW service is CUPS enabled, then Sx service is a mandatory parameter for SAEGW service to start. Only having association at the SAEGW service does not make Sx a mandatory parameter for SAEGW service.

If Sx service is a mandatory parameter (because of CUPS-enabled flag), then Sx service stop and Sx IP address brings down the SAEGW service.

For information about configuring the Sx Service, see the “Configuring Sx Service” section.

Sx-u Interface

This section explains the interaction between the Sx-u Interface, User-Plane-service, and SAEGW-service.

Sx-u is the User-Plane interface over the Sxa and Sxb reference points. The protocol used on the Sx-u Interface is GTP-U. Both IPv4 and IPv6 transport is supported.

At the User-Plane, Sx-u service is a mandatory parameter for User-Plane service to start. Being a mandatory parameter, Sx-u Interface stops and Sx-u IP address brings down the User-Plane service.

The Control-Plane establishes one Sx-u tunnel per function or session as described in the section below.

Sx-u Tunnel per PDN session

Control-Plane establishes one Sx-u tunnel per PDN session for router advertisement and router solicitation messages.

In this scenario, Control-Plane uses the existing Sx tunnel per PDN (created during GTP-C initial attach procedure) for installing Packet Detection Rule (PDR) or Forwarding Action Rule (FAR) related to data forwarding between the Control-Plane and User-Plane functions on the User-Plane.

For information about configuring the Sx-u Interface, see the *Configuring Sx-u Interface* section.

Sx Demux

The Sx Demux provides session de-multiplexing functionality on the Data plane. One instance of Sx Demux is started per context. When implemented, the Sx Demux supports the following behavior:

1. Works as Sx Control-Plane Demux when implemented on the Control-Plane and supports handling of Node level messages such as Prime PDF Management Messages.
2. Works as Sx Data Plane Demux when implemented on the Data Plane and supports:
    - Handling of Session level messages such as Session Establish Request.
    - Handling of Session level messages such as Session Establish Request.

3. Works as Sx Data Pane Demux performing load balancing of Session Establish Request between all Session Managers.
4. Supports default PFCP packet receiver port 8805.

The Sx service is associated with SAEGW service at Control-Plane and is associated with User-Plane Service at User-Plane. Sx Demux is initiated when the first Sx service is created with the minimum mandatory parameter in the context.

The Sx Demux functions as follows:

- **When working as Sx Data Demux**

  The Session Manager (Data Plane) sends the add session response indicating addition of new session and delete session request on deletion of session on Session Manager. Sx Data Demux maintains session count per session manager.

- **When working as Sx Control Demux**

  The Sx Control Demux uses Prime PDF Management Messages (proprietary messages) to communicate static and dynamic rule configuration from Control-Plane to associated Data plane.

Proprietary Sx Messages Information

Proprietary Prime PFD message format

	Bits							
Octets	8	7	6	5	4	3	2	1
1	Version			Spare	Spare	Spare	MP=0	S=0
2	Message Type							
	47 Prime PFD Management Request							
	48 Prime PFD Management Response							
3	Message Length (1st Octet)							
4	Message Length (2nd Octet)							
5	Sequence Number (1st Octet)							
6	Sequence Number (2nd Octet)							
7	Sequence Number (3rd Octet)							
8	Spare							

Cisco PFD Management Request

Information elements	**P**	**Condition / Comment**	**IE Length**	**IE ID**

Config Action	M	1 – Add configuration 2 – Delete Configuration	1 Byte	202
Co-Relation id	M	unique number which will represent transaction id. During Split buffer message, correlation id will be same so that receiver can combine buffer.	2 Byte	203
Number of Sub Part	O	N – Indicates Total number of sub parts	1 Byte	204
Sub Part index	O	Indicates the part number going into this message.	1 Byte	205
Content TLV	M	Type – Indicates Rule-Def, Charging Action or Action priority line - 1 Byte Length – Length of Content - 2 Byte Value – Actual Buffer conent - Max size 3000 Bytes	3003 byte	 206

Cisco PFD Management Response

Information elements	P	Condition / Comment	IE Length	IE ID
PFCP Cause	M	1 Success 0 Failure	1 byte	19
CoRelation id	M	Unique number – same as request message. Indicates to sender that this correlation has been received.	2 byte	203

Sub Part Index	O	Indicates the part number received into this message. This will be only present when Split mode is used.	1 byte	205

Header information

Proprietary Sx Stats Query Req/Rsp/Ack

Table 1: PFCP Header format for Node level Query Message

Octets	8	7	6	5	4	3	2	1
1	Version			Spare	Spare	Spare	MP=0	S=0
2	Message Type 44 Sx Stats Query Request 45 Sx Stats Query Response 46 Sx Stats Query Ack/NAck							
3	Message Length (1st Octet)							
4	Message Length (2nd Octet)							
5	Sequence Number (1st Octet)							
6	Sequence Number (2nd Octet)							
7	Sequence Number (3rd Octet)							
8	Spare							

PFCP Header format for Subscriber/Session level Query Message

Octets	8	7	6	5	4	3	2	1
1	Version			Spare	Spare	Spare	MP=0	S=1
2	Message Type 44 Sx Stats Query Request 45 Sx Stats Query Response							
3	Message Length (1st Octet)							
4	Message Length (2nd Octet)							
5	Session Endpoint Identifier (1st Octet)							
6	Session Endpoint Identifier (2nd Octet)							
7	Session Endpoint Identifier (3rd Octet)							
8	Session Endpoint Identifier (4th Octet)							

9	Session Endpoint Identifier (5th Octet)
10	Session Endpoint Identifier (6th Octet)
11	Session Endpoint Identifier (7th Octet)
12	Session Endpoint Identifier (8th Octet)
13	Sequence Number (1st Octet)
14	Sequence Number (2nd Octet)
15	Sequence Number (3rd Octet)
16	Spare

IEs and Message Formats

Stats reporting framework shall use the messages and IE types as outlined below.

Table 2: Information Elements in Sx Stats Query Request Message

Information elements	P	Condition / Comment	IE Type	IE ID
Correlation ID	M	Unique number, which will represent transaction ID	Correlation ID	203
Stats Request	C	This IE shall be present if the Node Report Type indicates a statistics report request.	Stats request	209

Table 3: Information Elements in Sx Stats Query Response Message

Information elements	P	Condition / Comment	IE Type	IE ID
PFCP Cause	M	1 Success , 0 Failure	PFCP Cause	
Correlation ID	M	Unique number, which will represent transaction ID. During Split buffer message, Correlation ID will be same for all the messages so that receiver can identify uniquely the request to which the responses correspond.	Correlation ID	203

Stats response	C	This IE shall be present if the Node Report Type indicates a statistics report response.	Stats response	212

Table 4: Information Elements in Sx Stats Query Ack/NAck

Information elements	P	Condition / Comment	IE Type	IE ID
Correlation ID	M	Unique number, which will represent transaction ID.	Correlation ID	203
Stats Ack/NAck	M	This IE shall be present to inform Ack/NAck to peer.	Stats response ACK/NACK	213

Sx Interface Private Information Element (IE) List

IE Type: 201

IE Name: PFCP_IE_UPDATE_ADDNL_FORW_PARAMS

IE Format and Encoding Information

Octet 1 and 2	Update Additional Forwarding Parameters IE Type = x (decimal)					
Octets 3 and 4	Length = n					
Information elements	P	Condition / Comment	Appl.			IE Type
			Sxa	Sxb	Sxc	
Destination Interface	C	This IE shall only be provided if it is changed. When present, it shall indicate the destination interface of the outgoing packet.	X	X	X	Destination Interface
Outer header removal	C	This IE shall only be provided if it is changed.	X	X	-	

Outer Header Creation	C	This IE shall only be provided if it is changed.	X	X	-	Outer Header Creation
Outer header marking	C	This IE shall only be provided if it is changed.			-	
Forwarding Policy	C	This IE shall only be provided if it is changed.	-	X	X	Forwarding Policy

Sx Message(s) Using the IE: Update FAR IE within Sx Session Modification Request.

IE Type: 202

IE Name: PFCP_IE_CONFIG_ACTION

IE Format and Encoding Information

Octet 1 and 2	Sub Part Number IE Type = 202 (decimal)			
Octets 3 and 4	Length = 1 byte			
Information elements	**P**	**Condition / Comment**	**IE Length**	**IE ID**
Config Action	O	Add or Delete the config	1 Byte	202

IE Type: 203

IE Name: PFCP_IE_CORRELATION_ID

IE Format and Encoding Information

Octet 1 and 2	Correlation ID IE Type = 203 (decimal)			
Octets 3 and 4	Length = 2 bytes			
Information elements	**P**	**Condition / Comment**	**IE Length**	**IE ID**

Co-Relation ID	M	Unique number which will represent transaction ID. During Split buffer message, correlation ID will be same so that receiver can combine buffer.	2 Byte	203

Sx Message(s) Using the IE: Sx Prime PFD MGMT Request for configuring the UP with various configurations.

Sx Prime PFD MGMT Response

IE Type: 204

IE Name: PFCP_IE_SUB_PART_NUMBER

IE Format and Encoding Information

Octet 1 and 2	Sub Part Number IE Type = 204 (decimal)			
Octets 3 and 4	Length = 1 byte			
Information elements	**P**	**Condition / Comment**	**IE Length**	**IE ID**
Number of Sub Parts	O	N – Indicates Total number of sub parts for this config	1 Byte	204

Sx Message(s) Using the IE: Sx Prime PFD MGMT Request for configuring the UP with various configurations.

IE Type: 205

IE Name: PFCP_IE_SUB_PART_INDEX

IE Format and Encoding Information

Octet 1 and 2	Sub Part Index IE Type = 205 (decimal)			
Octets 3 and 4	Length = 1 byte			
Information elements	**P**	**Condition / Comment**	**IE Length**	**IE ID**
Sub Part index	O	Indicates the sub part number going into this config message.	1 Byte	205

Sx Message(s) Using the IE: Sx Prime PFD MGMT Request for configuring the UP with various configurations.

Sx Prime PFD MGMT Response.

IE Type: 206

IE Name: PFCP_IE_CONTENT_TLV

IE Format and Encoding Information

Octet 1 and 2	Content TLV IE Type = 206 (decimal)			
Octets 3 and 4	Length = 3003 bytes			
Information elements	**P**	**Condition / Comment**	**IE Length**	**IE ID**
Content TLV	M	Type – Indicates Rule-Def, Charging Action ,Action priority line , Rule and Route config,Group of Ruledef,	3003 bytes	206
		Rule in GoR - 1 Byte		
		Length – Length of Content - 2 Byte		
		Value – Actual Buffer content - Max size 3000 Bytes		

Sx Message(s) Using the IE: Sx Prime PFD MGMT Request for configuring the UP with various configurations.

IE Type: 207

IE Name: PFCP_IE_RBASE_NAME

IE Format and Encoding Information

	Bits							
Octets	8	7	6	5	4	3	2	1
1 to 2	Type = 202 (decimal)							
3 to 4	Length = n							
5 to n	Rulebase Name							

Note

- Octets 1-2—Indicates Rulebase IE. Type 202 Reserved
- Octets 3-4—Indicates the length of rulebase name
- Octets 5-n—Rulebase name

This IE contains the active Rulebase Name for a subscriber to be communicated to User Plane.

IE Type: 208

IE Name: NSH-INFO

IE Format and Encoding Information

	Bits							
Octets	8	7	6	5	4	3	2	1
1 to 2	Type = 208 (decimal)							
3 to 4	Length = n							
5 to 5	BitOctet							
6 to 6	MSISDN Len							
7 to 22	MSISDN							
23 to 23	IMSI Len							
24 to 40	IMSI							

IE Type: 209

IE Name: Stats request IE

IE Format and Encoding Information

Information Elements	P	Condition / Comment	IE Type	IE ID
Query Params	M	Query Params shall describe the type of the query and optionally the name of the entity being queried.	Query Params	210

Classifier Params	O	These shall be used along with query params for narrowing down the search.	Classifier Params	211

This IE are be of grouped type and consist of two IEs: Query Params IE and the Classifier Params IE. Multiple instances of Classifier Params IE can be present.

IE Type: 210

IE Name: Query Params IE

IE Format and Encoding Information

Octets	8	7	6	5	4	3	2	1
1 to 2	Type = 210 (decimal)							
3 to 4	Length = n							
7	ENTITY TYPE							
8	Spare						QUERY TYPE	QUERY ALL
9 to 10	Entity Name Length							
10 to n	Entity Name							

Query Params is encoded as follows:

Octet 7: ENTITY TYPE – Numeric Identifier. Indicates the type of entity being queried:

1: Network Instance (APN name) – [PFCP IE ID: 22] 2: Rulebase etc. (Future use) – [PFCP IE ID: 207]

Octet 8 encodes following flags:

- QUERY ALL—Indicates whether we are querying one instance of the specified entity or all of them.
- QUERY TYPE—Indicates whether we are querying individual ENTITY of the given type or we are expecting aggregated node level statistics. It takes values as follows:
  - 0: Bit when unset, indicates individual statistics.
  - 1: Bit when set indicates aggregated statistics.

Valid combinations of above flags are used to realize the use cases.

IE Type: 211

IE Name: Classifier Params IE

IE Format and Encoding Information

Bits

Octets	8	7	6	5	4	3	2	1
1 to 2	Type = 211 (decimal)							
3 to 4	Length = n							
5	Classifier Type							
6	Classifier Length							
7 to n	Classifier							

Classifier Params IE is encoded as follows:

Octet 5: Encodes the type of the classifier. It is defined by the context set by entity type.

So, same numeric identifiers may mean different for two different entity types.

Octet 6 encodes the length of classifier. The maximum of 256 byte long classifier is accommodated.

Octet 7 onwards is used to encode the classifier content. This content is encoded as an octet string. In case of numeric classifiers, the numbers are appropriately converted into string format and are delivered as is to the application. This process removes the length limitation on type of encoded numeric identifiers.

IE Type: 212

IE Name: Stats response IE

IE Format and Encoding Information

	Bits							
Octets	8	7	6	5	4	3	2	1
1 to 2	Type = 212 (decimal)							
3 to 4	Length = n							
5	ENTITY TYPE							
6	Part Number							
7	Total Number of Parts							
8 to n	Blob of data							

ENTITY TYPE is same as the one that is received in request. Else, Control Plane rejects the response from the User Plane.

The response from User plane can span across multiple messages depending upon the amount of data that needs to be sent to Control Plane.

- Message ID identifies one subpart of the response.
- Total number of messages this response consists of.

Blob of data consists of compressed context specific data. Contents of the same are uncompressed at Control Plane and interpreted as per the identifiers received (ENTITY TYPE).

IE Type: 213

IE Name: Stats response ACK/NACK

IE Format and Encoding Information

	Bits							
Octets	8	7	6	5	4	3	2	1
1 to 2	Type = 213 (decimal)							
3 to 4	Length = n							
5	RESPONSE TYPE							
6 to n	Missing message parts							

RESPONSE TYPE is: 0: ACK (success) if all parts of the response are correctly received at CP 1: NACK (failure) - CP responds with the message parts that were not received within the specified time.

Octets 6 and onwards specifies missing part numbers at CP in case CP sends out a NAck.

Use of NAck mechanism is not envisaged as of now. These will be incorporated in call flows, if required in future.

IE Type: 214

IE Name: PFCP_IE_PACKET_MEASUREMENT

IE Format and Encoding Information

The Packet Measurement IE contains the measured traffic volume in packets. This IE is encoded as shown below:

	Bits							
Octets	8	7	6	5	4	3	2	1
1 to 2	Type = 214 (decimal)							
3 to 4	Length = n							
5	Spare					DLVOL	ULVOL	TOVOL
m to (m+7)	Total Packets							
p to (p+7)	Uplink Packets							
q to (q+7)	Downlink Packets							
s to (n+4)	These octet(s) is/are present only if explicitly specified							

The following flags are coded within Octet 5:

- Bit 1 – TOVOL— If this bit is set to "1", then the Total Packets field appears. Else, the Total Packets field is does not appear.
- Bit 2 – ULVOL—If this bit is set to "1", then the Uplink Packets field appears. Else, the Uplink Packets field does not appear.
- Bit 3 – DLVOL—If this bit is set to "1", then the Downlink Packets field appears. Else, the Downlink Packets field does not appear.
- Bit 4 to bit 8—These are spare bits for future use, and are set to 0.

At least one bit is set to 1. However, you can set many bits to 1.

The Total Packets, Uplink Packets, and Downlink Packets fields are encoded as an Unsigned64 binary integer value. They contain the total, uplink, or downlink number of packets respectively.

This is not a mandatory IE for any Message.

This IE is available in the following Messages between Control Plane and User Plane.

- Sx Session Modification over SxA, SxB, SxC, SxAB
- Sx Usage Report Session Deletion Response over SxA, SxB, SxC, SxAB
- Sx Usage Report Session Report Request over SxA, SxB, SxC, SxAB

IE Type: 215

IE Name: PFCP_IE_EXTENDED_MEASUREMENT_METHOD

IE Format and Encoding Information

A new IE (215 - Extended Measurement Method) is encoded as shown below. This IE indicates the method for measuring the usage of network resources.

	Bits							
Octets	8	7	6	5	4	3	2	1
1 to 2	Type = 215 (decimal)							
3 to 4	Length = n							
5	Spare	Spare	Spare	Spare	Spare	Spare	Spare	Pkt
6 to (n+4)	These octet(s) is/are present only if explicitly specified							

Figure Extended Measurement Method

Octet 5 is encoded as follows:

- Bit 1 – Pkt (Packet)—When set to 1, this bit indicates a request for measuring the usage of the traffic in packets.
- Bit 2 to 8—These are spare bits for future use, and are set to 0.

Note Only one bit is set to 1.

This is not a mandatory IE for any Message.

This IE can be available in the following message between Control Plane and User Plane.

- Sx Session Establishment over SxA, SxB, SxC, SxAB

Similarly, Usage Report from User Plane is enhanced to support the packet information.

IE Type: 216

IE Name: PFCP_IE_RECALCULATE_MEASUREMENT

IE Format and Encoding Information

This private IE has been added to support "Max number of change conditions" trigger for offline charging records, such as Gz and Rf.

	Bits							
Octets	8	7	6	5	4	3	2	1
1 to 2	Type = 62 (decimal)							
3 to 4	Length = n							
5	Spare	Spare	Spare	Spare	Spare	Spare	RCVOL	RCDUR
6 to (n+4)	These octet(s) is/are present only if explicitly specified							

The following flags are coded within Octet 5:

- Bit 1 – RCDUR (Re-calculate Duration Measurement)—When set to 1, this flag indicates a request for resetting the Duration Measurement to ‘0’ by the UP function.
- Bit 2 – RCVOL (Re-calculate Volume Measurement)—When set to 1, this flag indicates a request for resetting the Volume Measurement to ‘0’ by the UP function. Then, the UP function proceeds to repopulate the Volume Measurement. The repopulation is done by aggregating the Volume Measurement of all the URRs that contain Linked URR ID as the URR ID sent in Update URR IE.
- Bit 3 to 8—Spare bits for future use, and are set to 0.

1. PFCP Session Modification Request
2. PFCP Session Report Response

IE Type: 217

IE Name: PFCP_IE_SUB_INFO

IE Format and Encoding Information

	Bits							
Octets	8	7	6	5	4	3	2	1
1 to 2	Type = 217 (decimal)							
3 to 4	Length = n							
5 to 5	BitOctet							
6 to 6	MSISDN Len							
7 to 22	MSISDN							
23 to 23	IMSI Len							
24 to 40	IMSI							
41 to 41	IMEI Len							
42 to 57	IMEI							
58 to 61	Call ID							

Octets 5-5: BitOctet. Indicates the available fields.

- Bit 1—IMSI
- Bit 2—MSISDN
- Bit 3—IMEI
- Bit 4—Call ID

IE Type: 218

IE Name: PFCP_IE_INTR_INFO

IE Format and Encoding Information

The IE is part of Create Dupl Params and Update Duplicate Params IE.

Create Duplicate Params IE can be part of SX Establishment Req and SX Session Modify Request.

Update Duplicate Params IE can be part of SX Session Modify Request.

	Bits

Octets	8	7	6	5	4	3	2	1
1 to 2	Type = 218 (decimal)							
3 to 4	Length = n							
5 to 5	BitOctet							
6 to 9	Intercept ID							
10 to 13	Charging ID							
14 to 17	Bearer ID							
18 to 18	Context name Len							
19 to 22	Context name							

Octets 5-5: BitOctet. Indicates the available fields.

- Bit 1—Intercept ID
- Bit 2—Charging ID
- Bit 3—Bearer ID
- Bit 4—Context name

IE Type: 219

IE Name: PFCP_IE_NODE_CAPABILITY

IE Format and Encoding Information

	Bits							
Octets	8	7	6	5	4	3	2	1
1 to 2	Type = 219 (decimal)							
3 to 4	Length = n							
5 to 8	Max Sessions Supported							
9 to (n+4)	These octet(s) is/are present only if explicitly specified							

The Max Sessions Supported value are encoded as an Unsigned32 binary integer value.

Max Sessions supported value is the maximum number of sessions that are supported by User Plane for this association with Control Plane.

IE Type: 220

IE Name: INNER PACKET MARKING

IE Format and Encoding Information

The Inner Packet Marking IE type shall be encoded as shown below. It indicates the DSCP to be used for UL/DL Inner packet marking.

	Bits							
Octets	8	7	6	5	4	3	2	1
1 to 2	Type = 220 (decimal)							
3 to 4	Length = n							
5 to 6	ToS/Traffic Class							

The ToS/Traffic Class shall be encoded on two octets as an OctetString. The first octet shall contain the DSCP value in the IPv4 Type-of-Service or the IPv6 Traffic-Class field and the second octet shall contain the ToS/Traffic Class mask field, which shall be set to "0xFC".

IE Type: 221

IE Name: TRANSPORT LEVEL MARKING OPTIONS

IE Format and Encoding Information

TRANSPORT LEVEL MARKING OPTIONS shall be encoded as shown below. It indicates the copy-inner/outer flags for encaps-header marking.

	Bits							
Octets	8	7	6	5	4	3	2	1
1 to 2	Type = 221 (decimal)							
3 to 4	Length = n							
5 to 5	Copy-Inner/Outer Flag							

Copy-Inner/Outer flags shall be encoded on 1 Octet.

IE Type: 223

PFCP_IE_CHARGING_PARAMS

IE Format and Encoding Information

	Bits

Octets	8	7	6	5	4	3	2	1
1 to 2	Type = 223 (decimal)							
3 to 4	Length = n							
5 to 6	Charging Chars							
7	GTPP Group Name length							
8	GTPP Group							
9 to 12	GTPP ContextID							
13	Accounting Policy Name length							
14	Accounting Policy Name							
15 to 18	Accounting Policy Service type							
19 to 22	Diameter Interim Interval							
23	AAA Group Name Length							
24	AAA Group Name							
25 to 28	AAA Group ContextId							
29 to 32	Radius Interim Interval							
33	GY Offline charging							
34	gtpp_dict							

IE Type: 224

IE Name: PFCP_IE_GY_OFFLINE_CHARGE

IE Format and Encoding Information

	Bits							
Octets	8	7	6	5	4	3	2	1
1 to 2	Type = 224 (decimal)							
3 to 4	Length = n							
5 to 5	Gy Offline Charging Status							

IE Type: 226

PFCP_IE_SUB_PARAMS

IE Format and Encoding Information

	Bits

Octets	8	7	6	5	4	3	2	1
1 to 2	Type = 226 (decimal)							
3 to 4	Length = n							
5 to 8	BitOctet							
9 to 10	Charging Characters							
11 to 11	Rat Type							
12 to 12	MCC MNC Length							
Variable Length	MCC MNC Value							
4 bytes/16 bytes	SGSN Address IPv4/IPV6							
1 byte	ULI Length							
Variable Length	ULI Value							
4 bytes	Congestion Level Value							
1 byte	Customer ID Length							
Variable Length	Customer ID value							
4 bytes/16 bytes	GGSN Address IPv4/IPV6							
1 byte	UserName Length							
Variable Length	UserName Value							
1 byte	Radius String Length							
Variable Length	Radius String Value							
1 byte	Session ID Length							
Variable Length	Session ID Value							
1 byte	MS Timezone Length							
Variable Length	MS Timezone Value							
1 byte	User Agent Length							
Variable Length	User Agent Value							
1 byte	Hash Value Length							

Variable Length	Hash Value
1 byte	Called Station Id Length
Variable Length	Called Station Id Value
1 byte	Calling Station Id Length
Variable Length	Calling Station Id Value
4 bytes	Content Filtering Policy ID
1 byte	Traffic Optimization Policy ID

IE Type: 227

IE Name: PFCP_IE_RULE_NAME

IE Format and Encoding Information

	Bits							
Octets	8	7	6	5	4	3	2	1
1 to 2	Type = 227 (decimal)							
3 to 4	Length = n							
5 to 68	Rule Name							

IE Type: 228

IE Name: LAYER2 MARKING

IE Format and Encoding Information

To pass the L2 Marking information to the UP for the bearer, a new custom-IE is defined and the FAR is modified to include it as follows. It identifies the Layer 2 Marking to be applied for the packets matching this FAR.

The length of the IE could be either 0 or 1.

	Bits

Octets	8	7	6	5	4	3	2	1
1 to 2	Type = 228 (decimal)							
3 to 4	Length = n							
5 to 5	TYPE (2 Bits) PRIORITY (6 Bits) **Type :** (1-DSCP, 2-QCI, 3-None) - beginning 2 Bits **Priority-Value:** the last 6 bits • Internal-Priority in case of QCI/None type • DCSP value in case of DSCP type							

IE Type: 229

IE Name: PFCP_IE_MONITOR_SUBSCRIBER_INFO

IE Format and Encoding Information

	Bits							
Octets	8	7	6	5	4	3	2	1
1 to 2	Type = 229 (decimal)							
3 to 4	Length = n							
5	Spare		C		D		Action	
d to (d+7)	Data tracing parameters							
p to (p+15)	Protocol tracing parameters							
s to (n+4)	These octet(s) is/are present only if explicitly specified							

Action: STOP / START monitor subscriber tracing. STOP =1, START =2.

D = DATA events tracing is ON if D=1. The 8 octets (d to d+7) contain data events tracing (fastpath) information should be present only when D=1.

C = CONTROL events tracing is ON if C=1.

Data Tracing (fastpath) Information (8 octets): It will contain the data filter parameters like Packet capture, Packet capture size, and MEH header.

Octet 1:

- Bit 1 – VPP enable/disable
- Bit 2 – FCAP - Packet capture
- Bit 3 – MEH present
- Bit 4 to 6 - Priority

Octet 2 to 3: Packet size

Octet 4 – 8: Reserved for future use. Currently, all set to 0.

Protocol Tracing Information (16 octets/128 bits): The 16 octets (p to p+15) contain protocol tracing information and should be present only when either control flag (C) or data flag (D) is enable. Each bit represents a unique protocol to monitor. E.g. If 49th bit is 1, PFCP events tracing is ON. Protocol Tracing 'Rulematch Events (Option 34)', 'L3 Data (Option 19)', 'EDR (Option 77)' and 'Subscriber Summary After Call Disconnect' are controlled by control event flag.

IE Type: 230

IE Name: PFCP_IE_MON_SUB_REPORT_SESS_REP_REQ

IE Format and Encoding Information

	Bits							
Octets	8	7	6	5	4	3	2	1
1 to 2	Type = 230 (decimal)							
3 to 4	Length = n							
5	Status code							

Status code: It indicates the acceptance or the rejection of the subscriber trace at UP. Status code = 0 will mean a success. Values 1-255 will uniquely specify the specific error code or notification.

IE Type: 237

IE Name: PFCP_IE_RATING_GRP

IE Format and Encoding Information

	Bits							
Octets	8	7	6	5	4	3	2	1
1 to 2	Type = 237 (decimal)							
3 to 4	Length = 2 bytes							
5 to 8	Rating Group							

IE Type: 238

IE Name: PFCP_IE_NEXTHOP

IE Format and Encoding Information

	Bits

Octets	8	7	6	5	4	3	2	1
1 to 2	Type = 238 (decimal)							
3 to 4	Length = n							
5 to 10	PFCP_IE_NEXTHOP_ID							
11 to 14	PFCP_IE_NEXTHOP_IP							

IE Type: 239

IE Name: PFCP_IE_NEXTHOP_ID

IE Format and Encoding Information

	Bits							
Octets	8	7	6	5	4	3	2	1
1 to 2	Type = 239 (decimal)							
3 to 4	Length = 5							
5								

IE Type: 240

IE Name: PFCP_IE_NEXTHOP_IP

IE Format and Encoding Information

	Bits							
Octets	8	7	6	5	4	3	2	1
1 to 2	Type = 240 (decimal)							
3 to 4	Length = n							
5	Spare			V4			V6	
m to (m+3)	IPv4 Address							
p to (p+15)	IPv6 Address							

IE Type: 241

PFCP_IE_QGR_INFO

IE Format and Encoding Information

	Bits

Octets	8	7	6	5	4	3	2	1
1 to 2	Type = 241 (decimal)							
3 to 4	Length = n							
5 to 6	Number of QGR							
7 to 7	QGR 1 information stats - Bit Octet							
8 to 8	QGR Operation(Add/Modify/Remove)							
9 to 12	QGR Priority							
13 to 13	QGR Name Length							
14 to n	QGR Name							
n+1 to n+4	FAR ID							
n+5 to n+8	QER ID							
n+8 to n+11	URR ID							
Same as 7 to n+11	Next QGR(if any) information stats							

IE Type: 242

IE Name: PFCP_IE_UE_IP_VRF

IE Format and Encoding Information

	Bits							
Octets	8	7	6	5	4	3	2	1
1 to 2	Type = 242 (decimal)							
3 to 4	Length = n							
5	Spare		Identical VRF flag		IPv6 VRF Valid		IPv4 VRF Valid	
m to (m+1)	VRF-1 Name Length = p							
Variable Length	VRF-1 Name							
n to n+1	VRF-2 Name Length = q							
Variable Length	VRF-2 Name							

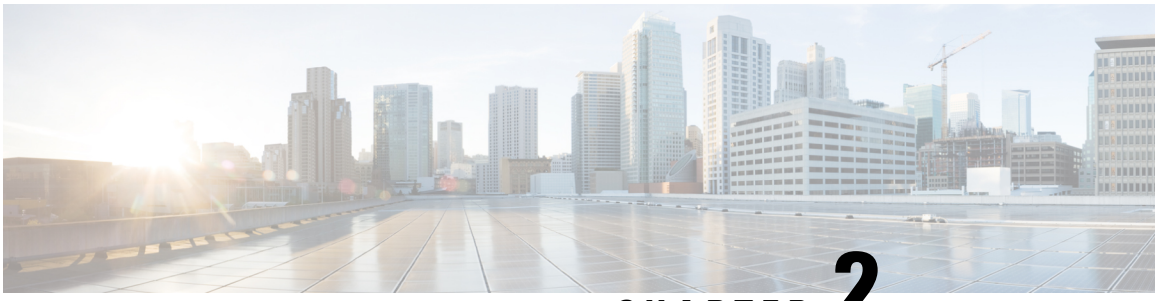
IE Type: 246

IE Name: PFCP_IE_GX_ALIAS

IE Format and Encoding Information

The IE to communicate a Gx-Alias GoR(Group-of-Ruledef) name, Start and End PDR IDs and also the operation to perform, from CP to UP during Sx Session Establishment/Modification Request message. There can be multiple instances of same IE in an Sx-message.

	Bits							
Octets	8	7	6	5	4	3	2	1
1 to 2	Type = 246 (decimal)							
3 to 4	Length n [Min=7, Max=69 {5+ACSCTRL_GRP_OF_RDEFS_NAMELEN (64)}]							
5	flags (Add/delete GoR Rules),for eg: 1 for Add, 0 Delete rules in GoR							
6 to 7	Start PDR ID							
8 to 9	End PDR ID							
10 to n+4	Gx-alias GoR name (min size=2, max size=64)							



CHAPTER 2

Configuring Sx Service for CUPS

The following section provides the configuration commands available for configuring Sx service for CUPS.

Configuring Sx Service

Use the following commands to specify a Sx service name to allow configuration of the Sx service under Context Configuration Mode.

```
configure
  context context_name
    [ no ] sx-service service_name
    end
```

NOTES:

- **no** : Disables the command.
- By default, this command is disabled.

Selectively Compress or Decompress Optimization Based on Sx Message Length

By default, certain Packet Forwarding Control Protocol (PFCP) messages are compressed. To extract certain CPU benefits, a new CLI command is introduced that compresses the messages only when the total encoded packet length exceeds the configured packet length. Although the compression is enabled by default, the compression begins only on the packets that are either above or equal to the configured length. Maximum restriction on the size of the Sx message is 5120. Packets exceeding this upper limit must be compressed. The packet length is not applicable to the **sx-update-ip-pool** keyword, which compresses the IP pool TLVs in PFCP messages. As the **packet-length** keyword is optional, the default value is configured when the packet length is not specified.

Use the following command to selectively compress or decompress optimization that is based on Sx message length.

```
configure
   context context_name
      sx-service service_name
         [ no ] sx-protocol compression [ packet-length length ]
sx-update-ip-pool
        end
```

NOTES:

- **no**: Disables command.
- **sx-update-ip-pool**: Configures SX update message to the userplane with compression.
- **packet-length**: Configures compression above or equal to the packet length of 5120.

Verifying Sx Service Configuration

Use the following commands to verify a particular attribute or all attributes associated with the Sx Service configuration:

- **show sx-service all**
- **show sx-service name**
- **show sx-service statistics all**
- **show sx-service statistics header-decoder-errors**

Binding an Sx Service

Use the following commands to bind the specified Sx service to an IP address under Sx Service Configuration Mode.

```
configure
   context context_name
      sx-service service_name
         [ no ] bind { ipv4-address ipv4_address | ipv6-address ipv6_address }
         end
```

NOTES:

- **no**: Disables the command.
- **ipv4-address**: Designates an IPv4 address of the Sx service. Enter a valid IPv4 address.
- **ipv6-address**: Designates an IPv6 address of the Sx service. Enter a valid IPv6 address.
- By default, this command is disabled.

Modifying Sxa Parameters

Use the following commands to modify the Sxa parameters for the S-GW under Sx Service Configuration Mode.

```
configure
  context context_name
    sx-service service_name
      sxa { max-retransmissions number | retransmissions-timeout-ms number
 }
       end
```

NOTES:

- **max-retransmissions**: Configures the maximum retries for Sx control packets on the S-GW. Enter an integer. The valid values range from 0 to 15. The default value is 4.
- **retransmissions-timeout-ms**: Configures the retransmission timeout for Sx control packets (on the S-GW), in milliseconds. Enter a value in multiples of 100. The valid values range from 1000 to 20000. The default value is 5000.
- By default, this command is disabled.

Modifying Sxab Parameters

Use the following commands to modify the Sxab parameters for the S-GW and P-GW under Sx Service Configuration Mode.

```
configure
  context context_name
    sx-service service_name
     sxab { max-retransmissions number | retransmissions-timeout-ms number
 }
       end
```

NOTES:

- **max-retransmissions**: Configures the maximum retries for Sx control packets on the S-GW and P-GW. Enter an integer. The valid values range from 0 to 15. The default value is 4.
- **retransmissions-timeout-ms**: Configures the retransmission timeout for Sx control packets (on the S-GW and P-GW), in milliseconds. Enter a value in multiples of 100. The valid values range from 1000 to 20000. The default value is 5000.
- By default, this command is disabled.

Modifying Sxb Parameters

Use the following commands to modify the Sxb parameters for the P-GW under Sx Service Configuration Mode.

```
configure
   context context_name
      sx-service service_name
        sxb { max-retransmissions number | retransmissions-timeout-ms number
 }
        end
```

NOTES:

- **max-retransmissions**: Configures the maximum retries for Sx control packets on the P-GW. Enter an integer. The valid values range from 0 to 15. The default value is 4.
- **retransmissions-timeout-ms**: Configures the retransmission timeout for Sx control packets (on the P-GW), in milliseconds. Enter a value in multiples of 100. The valid values range from 1000 to 20000. The default value is 5000.
- By default, this command is disabled.

Associating Sx Service to SAEGW Service

Use the following commands to associate an SAEGW service to an existing Sx service within this context.

```
configure
   context context_name
      saegw-service service_name
         [ no ] associate sx-service service_name
         end
```

NOTES:

- **no**: Removes the selected association from this service.
- **sx-service**: Configures Sx service for the SAEGW service.
- By default, this command is disabled.

Verifying SAEGW Service Configuration

Use the following commands to verify if Sx service is associated with the SAEGW Service configuration:

- **show saegw-service statistics**
- **show saegw-service name**

The output of this command displays the entire configuration for SAEGW or the one specified. The following sample output below illustrates the line to indicate the Sx service configured.

sx-service : sxc

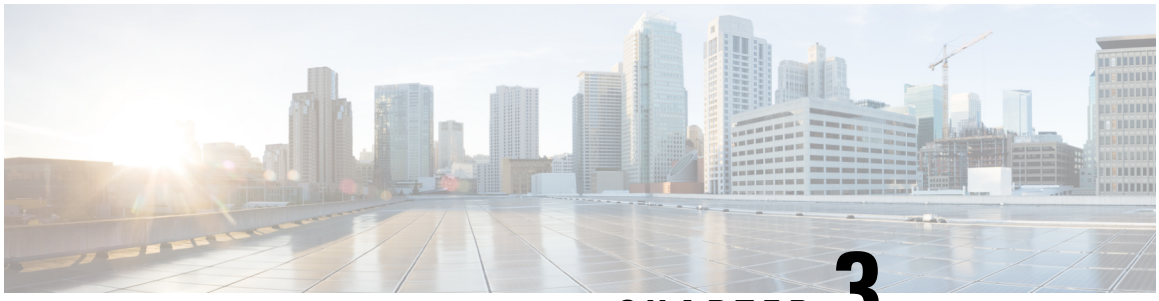
Associating Sx Service to User-Plane Service

Use the following commands to associate User-Plane service to an existing Sx service within this context.

```
configure
  context context_name
    user-plane-service service_name
      [ no ] associate sx-service sx-service-name
      end
```

NOTES:

- **no**: Removes the selected association from this service.
- **sx-service**: Configures Sx service for the User-Plane service.
- By default, this command is disabled.
- The **no associate sx-service** CLI command is recommended to be executed only during the maintenance window when there are no or minimal active sessions.



CHAPTER 3

Configuring Sx-u Interface for CUPS

The following section provides the configuration commands to enable or disable the feature.

Associating Sx-u Interface to SAEGW Service

Use the following commands to associate an existing GTP-U service to an existing Control Plane function under SAEGW Service Configuration Mode.

```
configure
  context context_name
    saegw-service service_name
      [ no ] associate gtpu-service gtpu_service_name up-tunnel
      end
```

NOTES:

- **no**: Removes the selected association from this service.
- **up-tunnel**: Configures the interface type as up-tunnel (tunnel towards User Plane function).
- By default, this command is disabled.

Associating Sx-u Interface to User Plane Service

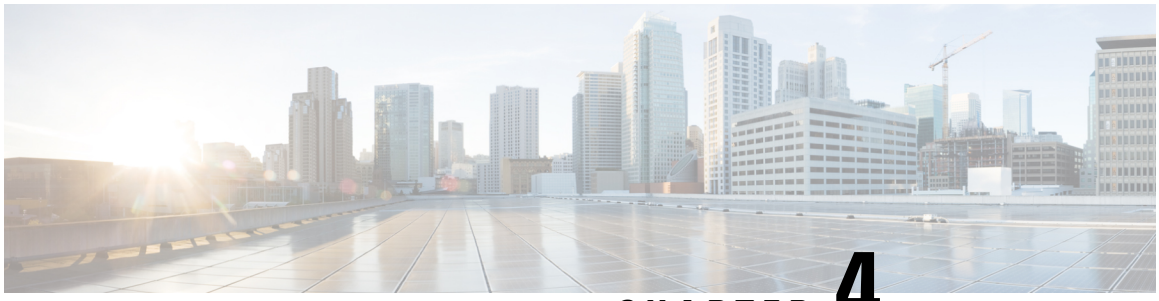
Use the following commands to associate an existing GTP-U service to an existing User Plane function under User Plane Configuration Mode.

```
configure
  context context_name
    user-plane-service service_name
      [ no ] associate gtpu-service gtpu_service_name cp-tunnel
      end
```

NOTES:

- **no**: Removes the selected association from this service.

- **cp-tunnel**: Configures the interface type as cp-tunnel (tunnel towards Control Plane function).
- By default, this command is disabled.



CHAPTER 4

Configuring Sx Demux for CUPS

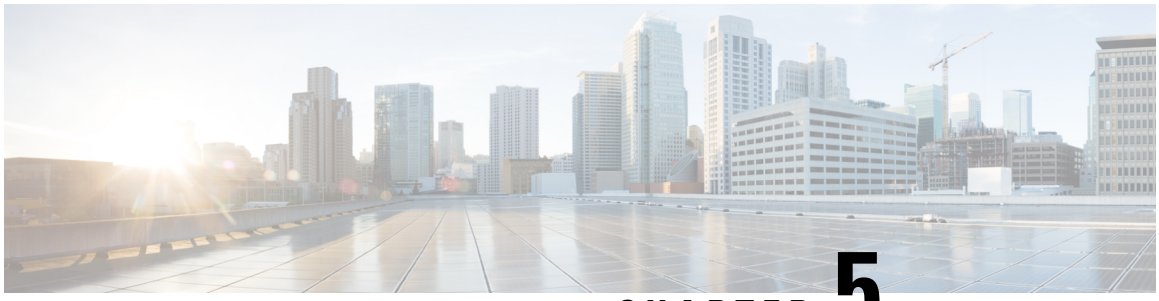
Configuring Instance Type for Sx Demux

Use the following commands to configure the instance type for which the Sx service with Sx Demux is used under Sx Service Configuration Mode.

```
configure
   context context_name
      sx-service service_name
         [ no ] instance-type { controlplane | userplane }
         end
```

NOTES:

- **no** : Disables the command.
- **controlplane**: Configures Sx service with Demux on the Control-Plane instance.
- **userplane**: Configures Sx service with Demux on the User-Plane instance.
- Only one instance type can be configured at a given time.
- By default, this command is disabled.



CHAPTER 5

Monitoring and Troubleshooting Sx Interface in CUPS

This section provides information about the CLI commands available to monitor and/or troubleshoot Sx Interface in CUPS.

Show Command(s) and/or Outputs

This section provides information regarding show commands and/or their outputs in support of this feature.

show sx-service all

The output of this command has been enhanced to include the following new fields in support of the Sx Service in CUPS.

- Service name
- Service-Id
- Context
- Status
- Instance Type
- SX Bind IPv4 Address
- SX Bind IPv6 Address
- SX Association Reattempt Timeout
- SX Recovery Time Stamp
- SXA
  - SX Retransmission Timeout
  - SX Maximum Request Retransmissions

- SXB
  - SX Retransmission Timeout
  - SX Maximum Request Retransmissions
- SXAB
  - SX Retransmission Timeout
  - SX Maximum Request Retransmissions
- SX Heartbeat
  - Interval
  - Retransmission Timeout
  - Max Retransmission
- SX path failure detection policy
  - Heartbeat Timeout
  - Heartbeat Req/Rsp Recovery timestamp change
  - Control Msg Recovery timestamp change

show sx-service name

The output of this command is similar to the **show sx-service all** CLI command and displays the field for the specified sx-service name.

show saegw-service all

The output of this command has been enhanced to include the following new field in support of the Sx Service associated with an SAEGW Service.

sx-service

show saegw-service name

The output of this command is similar to the **show saegw-service all** CLI command and displays the field for the specified saegw-service name.

show sx-service statistics all

The output of this command has been enhanced to include the following new fields and statistics in support of the Sx Service.

- Session Management Messages
- Session Establishment Request

    - Total TX
    - Total RX
    - Initial TX
    - Initial RX
    - Retrans TX
    - Retrans RX
    - Discarded
    - No Rsp RX
- Session Establishment Response
    - Total TX
    - Total RX
    - Initial TX
    - Accepted
    - Denied
    - Initial RX
    - Accepted
    - Denied
    - Retrans RX
    - Discarded
- Session Modification Request
    - Total TX
    - Total RX
    - Initial TX
    - Initial RX
    - Retrans TX
    - Retrans RX
    - Discarded
    - No Rsp RX
- Session Modification Response
    - Total TX
    - Total RX

    - Initial TX
        - Accepted
        - Denied
    - Initial RX
        - Accepted
        - Denied
    - Retrans TX
    - Discarded
- Session Deletion Request
    - Total TX
    - Total RX
    - Initial TX
    - Initial RX
    - Retrans TX
    - Retrans RX
    - Discarded
    - No Rsp RX
- Session Deletion Response
    - Total TX
    - Accepted
    - Denied
    - Total RX
    - Accepted
    - Denied
    - Discarded
- Session Report Request
    - Total TX
    - Total RX
    - Initial TX
    - Initial RX
    - Retrans TX

    - Retrans RX
    - Discarded
    - No Rsp RX
- Session Report Response
    - Total TX
    - Total RX
    - Initial TX
    - Accepted
    - Denied
    - Initial RX
    - Accepted
    - Denied
    - Retrans TX
    - Discarded
- Node Management Messages
- Prime PFD Management Request
    - Total TX
    - Total RX
    - Initial TX
    - Initial RX
    - Retrans TX
    - Retrans RX
    - No Rsp received TX
    - Discarded
- Prime PFD Management Response
    - Total TX
    - Total RX
    - Initial TX
    - Accepted
    - Denied
    - Initial RX

- Accepted
- Denied
- Retrans TX
- Discarded

- Total Signalling Bytes
  - TX
  - RX

show sx-service statistics header-decoder-error

the output of this command has been enhanced to include the following new fields in the header decoder error statistics for the Sx-service

- Message header decoder errors at SX
  - Incorrect PFCP version
  - Incorrect PFCP version discard rsp msg
  - Unsupported msg received
  - Incorrect msg length
  - Invalid msg format

show logging active

The output of this command has been enhanced to include the following new field in support of the Sx Demux in CUPS.

sxdemux

show task resources facility sxdemux

The output of this command has been enhanced to include the following new field in support of the Sx Demux in CUPS.

sxdemux

show task resources facility sxdemux all

The output of this command has been enhanced to include the following new field in support of the Sx Demux in CUPS.

sxdemux

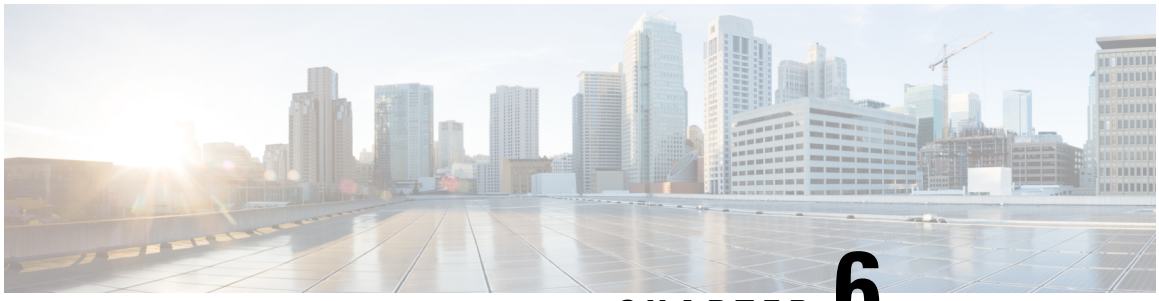
show task memory facility sxdemux all

The output of this command has been enhanced to include the following new field in support of the Sx Demux in CUPS.

sxdemux

Monitor Protocol

When using the monitor protocol command, enable option 49 to see all Sx Session Establishment Request and Sx Session Establishment Response on C-Plane.



CHAPTER 6

Heartbeat Support for Sx Interface

Revision History

Note Revision history details are not provided for features introduced before release 21.24.

Revision Details	Release
First introduced	Pre 21.24

Feature Description

In accordance with 3GPP standard, support has been added for node-level Heartbeat procedures between the Control Plane (CP) function and User Plane (UP) function over Sx Interface.

The Heartbeat procedure contains the following two messages:

1. Heartbeat Request
2. Heartbeat Response

Heartbeat Request

The CP function or the UP function sends a Heartbeat Request on a path to the peer node to find out if it is alive. The Heartbeat Request messages are sent for each peer with which a Packet Forwarding Control Protocol (PFCP) control association is established.

For each peer with which a PFCP control association is established, a CP function or UP function is prepared to receive a Heartbeat Request at any time, and replies with a Heartbeat Response.

Heartbeat Response

This message is sent as a response to a Heartbeat Request.

How It Works

CP function and UP function sends Heartbeat messages after configurable time duration. If the peer does not respond, the message is retried for configured number of times with the retry-interval and then the configured action is taken for the calls associated with the corresponding peer.

Recovery Time Stamp Information Element (IE), which contains the start time of the node, is supported by both Heartbeat Request and Heartbeat Response. Heartbeat Request contains its own Recovery Time Stamp value and sends it to the peer while Heartbeat Response contains the peers Recovery Time Stamp value.

Path Failure Detection

Path failure is detected in following conditions:

1. Heartbeat failure: This condition occurs when the peer does not respond to the Heartbeat that is sent and also retires.
2. Recovery Time stamp change in Heartbeat: This condition occurs when the Heartbeat Request or Heartbeat Response has a new larger value than the previously received value.
3. Recovery Time stamp change in Sx Association message: This condition occurs when the Sx association message is received again from the peer with a new Recovery Time Stamp.

Path Failure Handling

When the Recovery Time Stamp value received is more than the previously received value, then the peer restart is detected. If the Recovery Time Stamp value is lower than the previously received value then the value is ignored and peer restart is not detected.

When a peer restart is detected, an SNMP Trap is generated to indicate the path failure for the peer. Also, based on the path failure configuration (refer Configuring Heartbeat for Sx Interface, on page 48), all the calls connected to that peer can be cleared.

Configuring Heartbeat for Sx Interface

This section provides information about the CLI commands available in support of this feature.

Enabling Heartbeat for Sx Interface

Use the following commands under Sx Service Configuration mode to enable Heartbeat parameters for Sx Interface.

```
configure
  context context_name
    sx-service service_name
```

```
       [ default ] sx-protocol heartbeat { interval seconds |
max-retransmissions number | path-failure detection-policy {
control-recovery-timestamp-change | heartbeat-retry-failure |
heartbeat-recovery-timestamp-change } | retransmission-timeout seconds }
      no sx-protocol heartbeat { interval | path-failure detection-policy
 { control-recovery-timestamp-change | heartbeat-retry-failure |
heartbeat-recovery-timestamp-change }
       end
```

Notes:

- **default**: Sets/restores default value assigned for specified parameter.
- **no**: Disables the followed option.
- **heartbeat**: Configures Sx heartbeat parameters.
- **interval** *seconds*: Configures heartbeat interval (in seconds) for SX Service. *seconds* must be an integer in the range of 1 to 3600.

Important In releases prior to 24th July CUPS Lab Drop, *seconds* was set as 60 seconds by default.

- **max-retransmissions** *number*: Configures maximum retries for SX heartbeat request. Must be followed by integer, ranging from 0 to 15. Default is 4.
- **retransmission-timeout** *seconds*: Configures the heartbeat retransmission timeout for SX Service, in seconds, ranging from 1 to 20. Default is 5.
- **path-failure**: Specifies policy to be used when path failure happens via heartbeat request timeout.

Configuring Detection Policy for Path Failure

Use the following commands under Sx Service Configuration mode to specify detection policy to be used for path failure.

```
configure
  context context_name
    sx-service service_name
      [ default | no ] sx-protocol heartbeat path-failure detection-policy
 { control-recovery-time-stamp-change | heartbeat-retry-failure |
heartbeat-recovery-
timestamp-change }
       end
```

Notes:

- **default**: Sets/restores default value assigned for specified parameter.
- **no**: Disables the followed option.
- **detection-policy**: Specifies the policy to be used. Default action is to do cleanup upon heartbeat request timeout.

- **control-recovery-time-stamp-change**: Path failure is detected when the recovery timestamp in control request/response message changes.
- **heartbeat-retry-failure**: Path failure is detected when the retries of heartbeat messages times out.
- **heartbeat-recovery-timestamp-change**: Path failure is detected when the recovery timestamp in heartbeat request/response message changes.

Monitoring and Troubleshooting

This section provides information about CLI commands available for monitoring and troubleshooting the feature.

Show Command(s) and/or Outputs

This section provides information regarding show commands and/or their outputs in support of this feature.

show sx-service all

The output of this show command has been enhanced to include the following fields introduced in support of this feature.

- SX Heartbeat
  - Interval
  - Retransmission Timeout
  - Max Retransmission
- SX path failure detection policy
  - Heartbeat Timeout
  - Heartbeat Req/Rsp Recovery timestamp change
  - Control Msg Recovery timestamp counter change

show sx-service statistics all

The output of this show command has been enhanced to include the following fields introduced in support of this feature.

- Heartbeat Request
  - Total TX
  - Total RX
  - Initial TX
  - Initial RX
  - Retrans TX

- Heartbeat Response
  - Total TX
  - Total RX

Disconnect Reasons

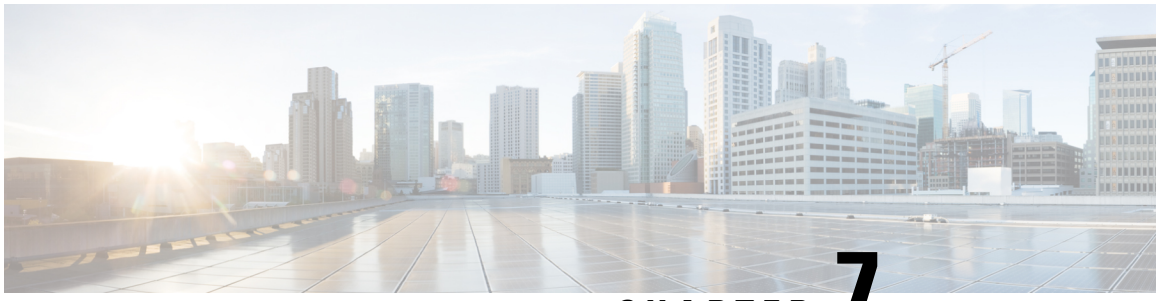
The following disconnect reason has been added in support of this feature:

- sx-path-failure - When the Recovery timestamp changes or heartbeat failure is detected, based on the configuration, calls are cleared with this disconnect reason.

SNMP Traps

The following SNMP traps have been added in support of this feature:

- SxPathFailure - This trap is generated when the peer path failure is detected.
- SxPathFailureClear - This trap is generated when the path is restored for the peer.



CHAPTER 7

N+2 UP Recovery

Revision History

Revision History

Note Revision history details are not provided for features introduced before release 21.24.

Revision Details	Release
First introduced	Pre 21.24

Feature Description

In accordance with 3GPP, the CP uses Sx-based failure detection which relies on Sx keep alive message responses from the UP.

Using this approach, when the CP does not receive responses from the UP, it retransmits the Sx message a configurable number of times before declaring the UP as down and initiating session tear downs. Depending on the number of retries and the retry interval, the failure detection period can take more than 10 seconds for a reliable determination that the UP is down. Until the Sx-path failure is detected at CP, the CP continues to select the failed-UP and place new PDN-connections from UEs on the failed-UP.

In order to reduce the time it takes for the CP to detect that a UP is down, Cisco CPs can be configured to use the Bidirectional Forwarding Detection (BFD) protocol (RFC 5883 - Bidirectional Forwarding Protocol Detection (BFD) for Multihop Paths).

BFD uses significantly smaller retry periods (in the order of 200 msec) allowing for more rapid UP down detection. It is in addition to the Sx keepalive mechanism for alternate deployment scenarios (e.g. 1:1 UP redundancy).

NOTE: This feature is not dependent on Packet Flow Description (PFD) since PFD pushes common Day-N configurations across the UPs.

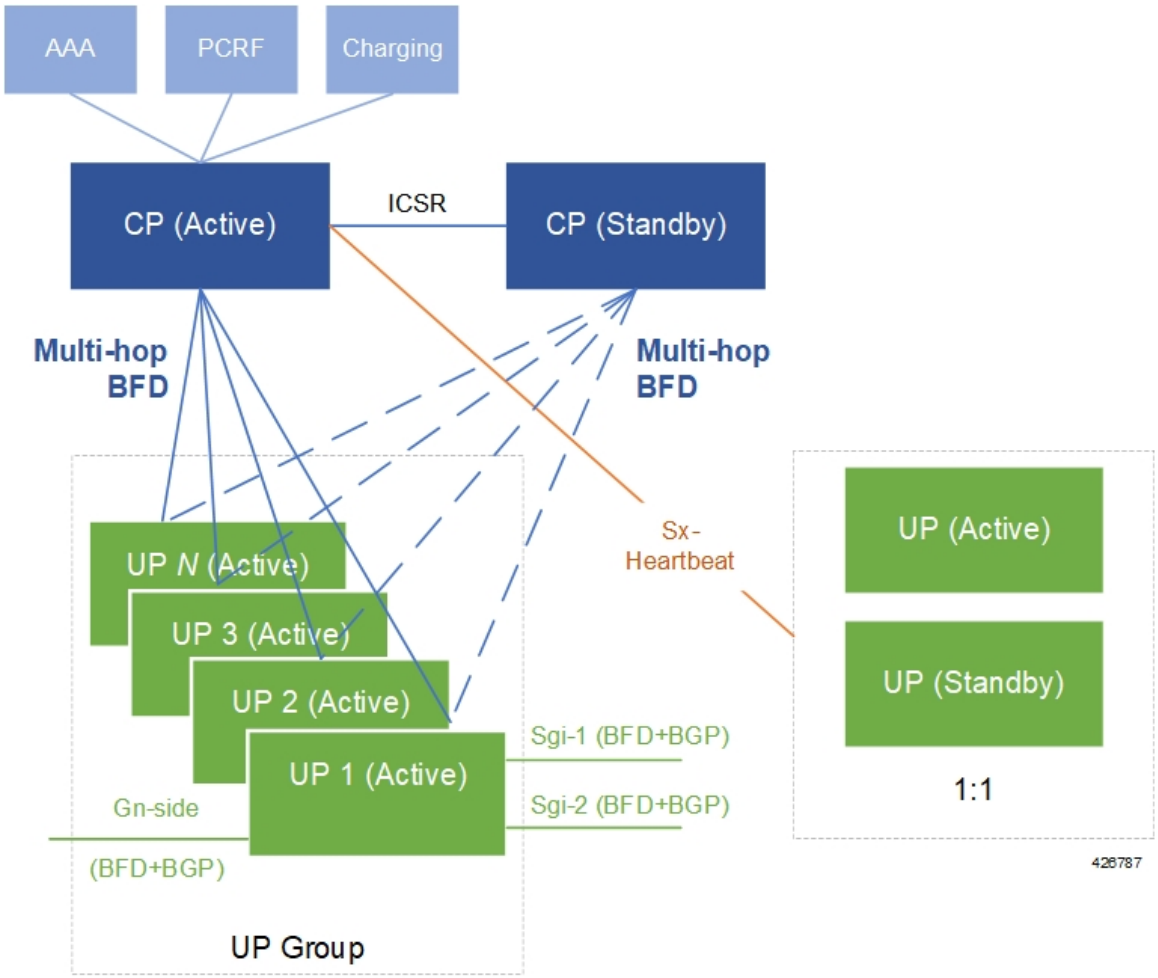
Deployment Architecture

This functionality can be enabled only in an "N+2" deployment scenario for UPs that process data sessions. In this scenario, CPs are deployed as an active-standby pair. "N" number of active UPs can be deployed to communicate with the CP. All of these UPs must be part of a specific, non-default, UP group.

NOTE: In N+2, all UPs are active. As such, this functionality only serves to improve data UP recovery times, it is not a redundancy model. It is highly recommended that UPs processing IMS traffic only be deployed in a 1:1 redundancy model.

BFD communications between the CP and UP requires the configuration of one additional loopback IP address per CP/per UP.

Figure 1: BFD Monitoring in N+2 Deployment



Limitations

- BFD-based CP failure detection is not supported in this release. CP failures can continue to be detected using the existing mechanism of Sx-path failure detection at the UP

  NOTE: It is recommended that Sx-path failure timers be configured more aggressively to more quickly prevent stale UP sessions.

- BGP monitoring on Gi/Gn interface (of UP) is not supported.
- Multi-BFD is not supported.
- BFD must be configured in the same context in which Sx is configured (Gn-side) on both the CP and UP.

How It Works

The figure and the table that follow provide a high-level description of the session detach and re-attach process when a UP is detected as down.

Figure 2: N+2 UP Recovery Flow

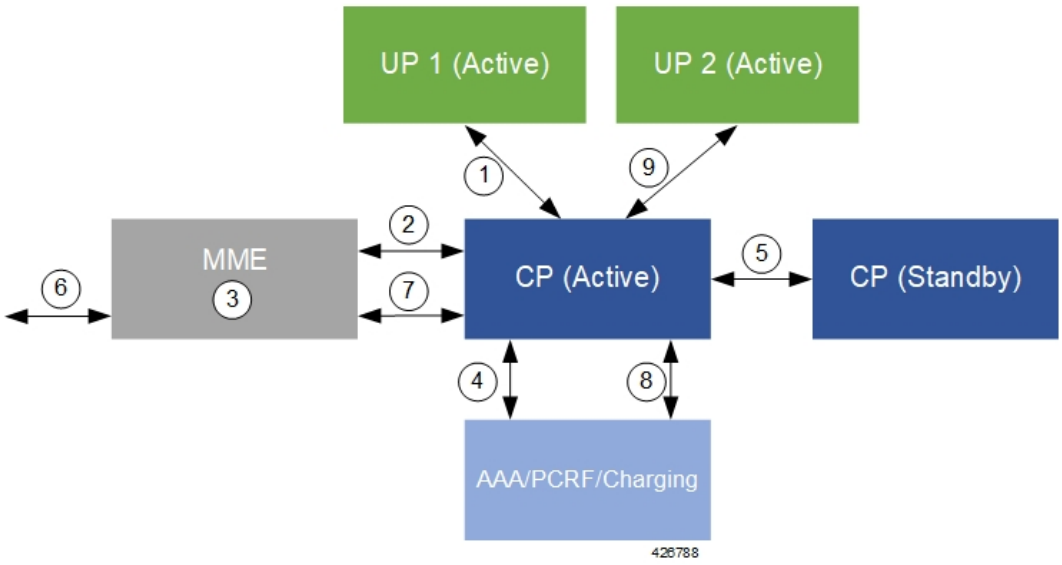


Table 5: N+2 UP Recovery Flow

Number	Description
1	The CP detects a UP failure.
2	The CP sends UP detach session messages to the MME(s) with a cause code of Local-Detach.
3	The MMEs process the request(s) and detach the sessions.
4	The CP communicates with the AAA/PCRF/Charging infrastructure to detach the sessions.
5	The CP (active) communicate with the standby CP to checkpoint the UP detach.

Number	Description
6	UEs whose sessions were previously detached, re-attach to the MME.
7	The MME communicates with the CP to re-attach UE sessions.
8	The CP communicates with the AAA/PCRF/Charging infrastructure to re-attach the sessions.
9	The CP completes the session re-attach process over the Sx interface with an alternate active UP.

Detailed detach and reattach on path failure flows for SAEGW CP/UP, P-GW CP/UP, S-GW CP/UP, and GnGp GGSN CP/UP are in the sections that follow.

Call Flows

SAEGW Detach and Reattach on Path Failure

The figure and the table that follows describe the detach and re-attach on path failure process for SAEGW CPs and UPs.

Figure 3: SAEGW CP/UP Detach and Re-attach on Path Failure Process

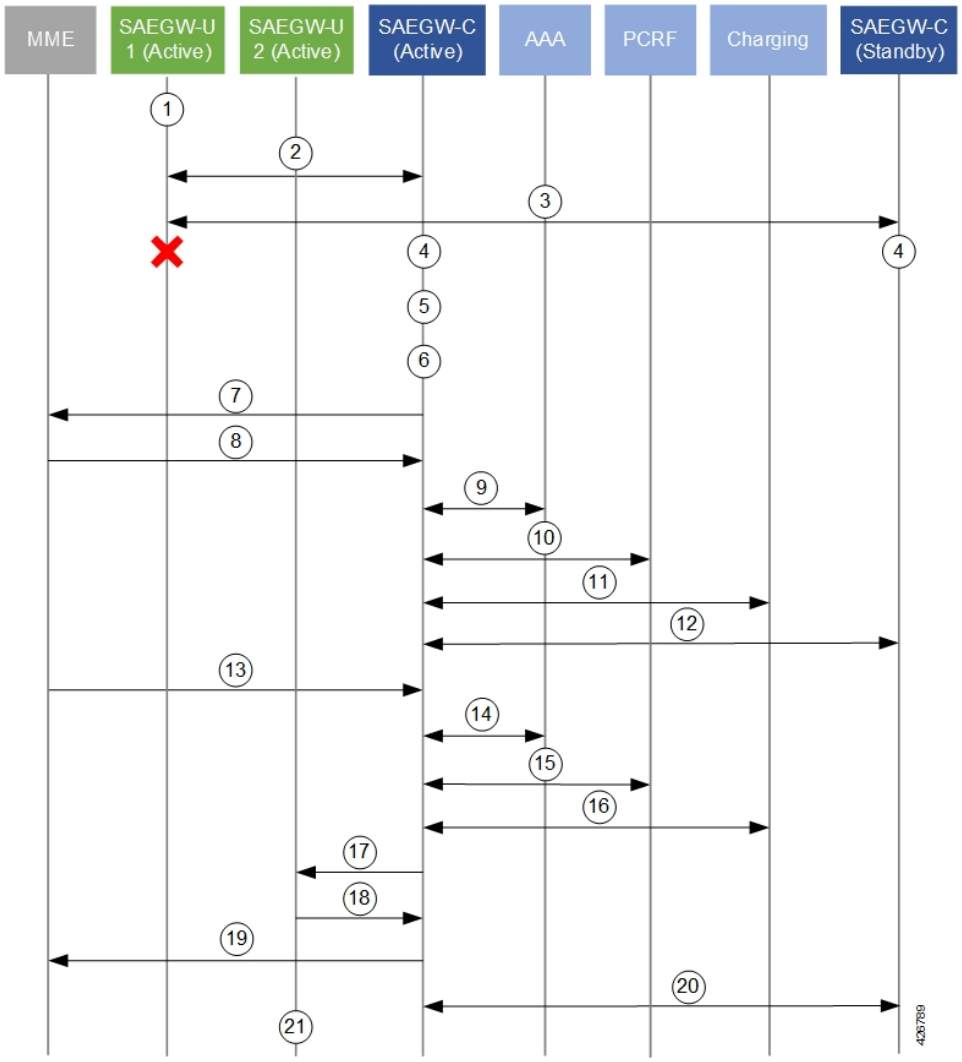


Table 6: SAEGW CP/UP Detach and Re-attach on Path Failure Process

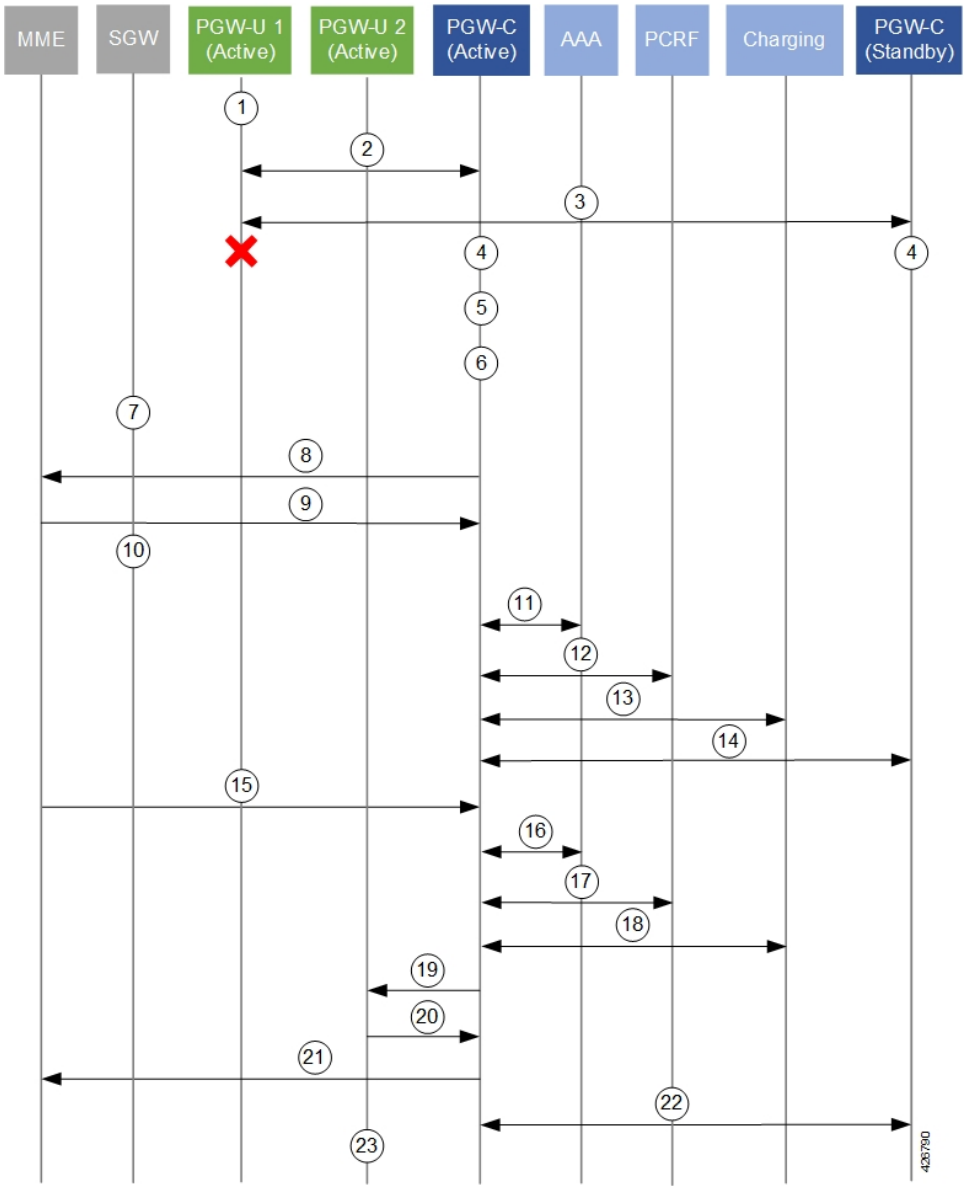
Number	Description
1	UE data sessions are processed by an active SAEGW UP.
2	The active SAEGW CP monitors SAEGW UPs via BFD and Sx-Heartbeat messages.
3	The secondary CP also monitors SAEGW UPs via BFD.
4	The active and standby CPs detect a BFD failure on a UP before eNB detection (relays on Sx timers (interval, retransmission, timeout)).
5	The BFD/VPNMGR on the active CP informs the Sx-demux process of a BFDDown event.
6	The Sx-demux process on the active CP initiates a path Failure notice to all Session Managers on the CP.

Number	Description
7	All Session Managers initiate the process of detaching sessions by sending Delete-bearer-req messages with a cause of Local-Detach to the MME. The detaches are initiated at a pre-defined rate.
8	The MME sends Delete-bearer-resp messages back to the CP. The MME does not page idle UEs with sessions being detached. The MME sends E-RAB release messages to active UEs with sessions being detached.
9	The active CP releases the session release with the AAA server(s).
10	The active CP releases the session with the PCRF.
11	The active CP releases the session with the Charging infrastructure.
12	The active CP syncs session detach information with the secondary CP.
13	For UEs re-initiating their session(s), the MME sends a Create-session-request message to the active CP. The MME selects the CP based on load algorithm (DNS, local config etc.).
14	The active CP processes the session attach request with the AAA server(s).
15	The active CP processes the session attach request with the PCRF.
16	The active CP processes the session attach request with the Charging infrastructure.
17	The active CP sends a Sx Session Establishment Request message to an alternate active UP. The CP selects the UP based on its load algorithm.
18	The UP sends a Sx Session Establishment Response message back to the CP.
19	The CP sends a Create-session-response message to the MME.
20	The active CP syncs information for the newly attached session with the secondary CP.
21	UE data sessions are now processed by the active SAEGW UP.

P-GW Detach and Reattach on Path Failure

The figure and the table that follows describe the detach and re-attach on path failure process for P-GW CPs and UPs.

Figure 4: P-GW CP/UP Detach and Re-attach on Path Failure Process



P-GW CP/UP Detach and Re-attach on Path Failure Process

Table 7: P-GW CP/UP Detach and Re-attach on Path Failure Process

Number	Description
1	UE data sessions are processed by an active P-GW UP.
2	The active P-GW CP monitors P-GW UPs via BFD and Sx-Heartbeat messages.
3	The secondary CP also monitors P-GW UPs via BFD.
4	The active and standby CPs detect a BFD failure on a UP before eNB detection (relays on Sx timers (interval, retransmission, timeout)).

Number	Description
5	The BFD/VPNMGR on the active CP informs the Sx-demux process of a BFDDown event.
6	The Sx-demux process on the active CP initiates a path Failure notice to all Session Managers on the CP.
7	The S-GW initiates a db-req to the MME.
8	All Session Managers initiate the process of detach sessions by sending Delete-bearer-req messages with a cause of Local-Detach to the MME. The detaches are initiated at a pre-defined rate.
9	The MME sends Delete-bearer-resp messages back to the CP. The MME does not page idle UEs with sessions being detached. The MME sends E-RAB release messages to active UEs with sessions being detached.
10	The S-GW forwards the db-resp to the PGW-C and removes it's PDN session.
11	The active CP releases the session release with the AAA server(s).
12	The active CP releases the session with the PCRF.
13	The active CP releases the session with the Charging infrastructure.
14	The active CP syncs session detach information with the secondary CP.
15	For UEs re-initiating their session(s), the MME sends a Create-session-request message to the active CP. The MME selects the CP based on load algorithm (DNS, local config etc.).
16	The active CP processes the session attach request with the AAA server(s).
17	The active CP processes the session attach request with the PCRF.
18	The active CP processes the session attach request with the Charging infrastructure.
19	The active CP sends a Sx Session Establishment Request message to an alternate active UP. The CP selects the UP based on its load algorithm.
20	The UP sends a Sx Session Establishment Response message back to the CP.
21	The CP sends a Create-session-response message to the MME.
22	The active CP syncs information for the newly attached session with the secondary CP.
23	UE data sessions are now processed by the active SAEGW UP.

S-GW Detach and Reattach on Path Failure

The figure and the table that follows describe the detach and re-attach on path failure process flow for S-GW CPs and UPs.

Figure 5: S-GW CP/UP Detach and Re-attach on Path Failure Process

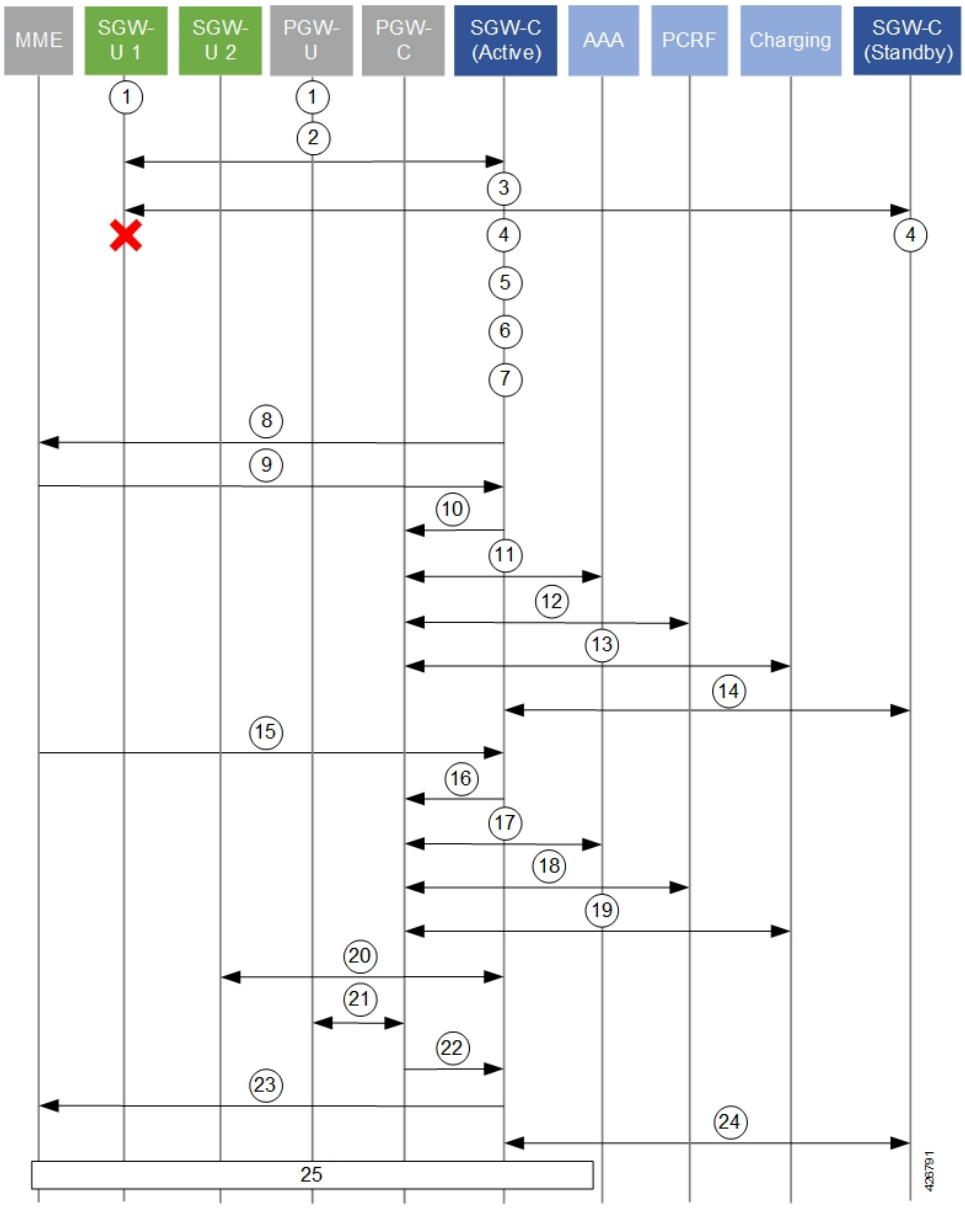


Table 8: S-GW CP/UP Detach and Re-attach on Path Failure Process

Number	Description
1	UE data sessions are processed by an active S-GW UP and an active PGW UP.
2	The active S-GW CP monitors S-GW UPs via BFD and Sx-Heartbeat messages.
3	The secondary S-GW CP also monitors S-GW UPs via BFD.
4	The active and standby S-GW CPs detect a BFD failure on the S-GW UP before eNB detection (relays on Sx timers (interval, retransmission, timeout)).

Number	Description
5	The BFD/VPNMGR on the active S-GW CP informs the Sx-demux process of a BFDDown event.
6	The Sx-demux process on the active CP initiates a path Failure notice to all Session Managers on the CP.
7	The S-GW CP initiates a db-req to the MME.
8	All Session Managers initiate the process of detach sessions by sending Delete-bearer-req messages with a cause of Local-Detach to the MME. The detaches are initiated at a pre-defined rate.
9	The MME sends Delete-bearer-resp messages back to the S-GW CP. The MME does not page idle UEs with sessions being detached. The MME sends E-RAB release messages to active UEs with sessions being detached.
10	The active S-GW CP releases the session release with the PGW UP.
11	The PGW CP releases the session with the AAA server(s).
12	The PGW CP releases the session with the PCRF.
13	The PGW CP releases the session with the Charging infrastructure.
14	The active S-GW CP syncs session detach information with the secondary S-GW CP.
15	For UEs re-initiating their session(s), the MME sends a Create-session-request message to the active S-GW CP. The MME selects the CP based on load algorithm (DNS, local config etc.).
16	The active S-GW CP relays the Create-session-request message to the PGW CP
17	The PGW CP processes the session attach request with the AAA server(s).
18	The PGW CP processes the session attach request with the PCRF.
19	The PGW CP processes the session attach request with the Charging infrastructure.
20	The active S-GW CP exchanges Sx Session Establishment Request and Response messages with an alternate active S-GW UP.
21	The active PGW CP exchanges Sx Session Establishment Request and Response messages with an active PGW UP.
22	The PGW CP sends a Create-session-response message to the S-GW CP.
23	The S-GW CP sends a Create-session-response message to the MME.
24	The active S-GW CP syncs information for the newly attached session with the secondary S-GW CP.
25	The S-GW CP and the complete the Modify Bearer Request procedure with the MME before UE data can flow through the active UPs.

GnGp GGSN Detach and Reattach on Path Failure

The figure and the table that follows describe the detach and re-attach on path failure process flow for GnGp GGSN CPs and UPs.

Figure 6: GnGp GGSN CP/UP Detach and Re-attach on Path Failure Process

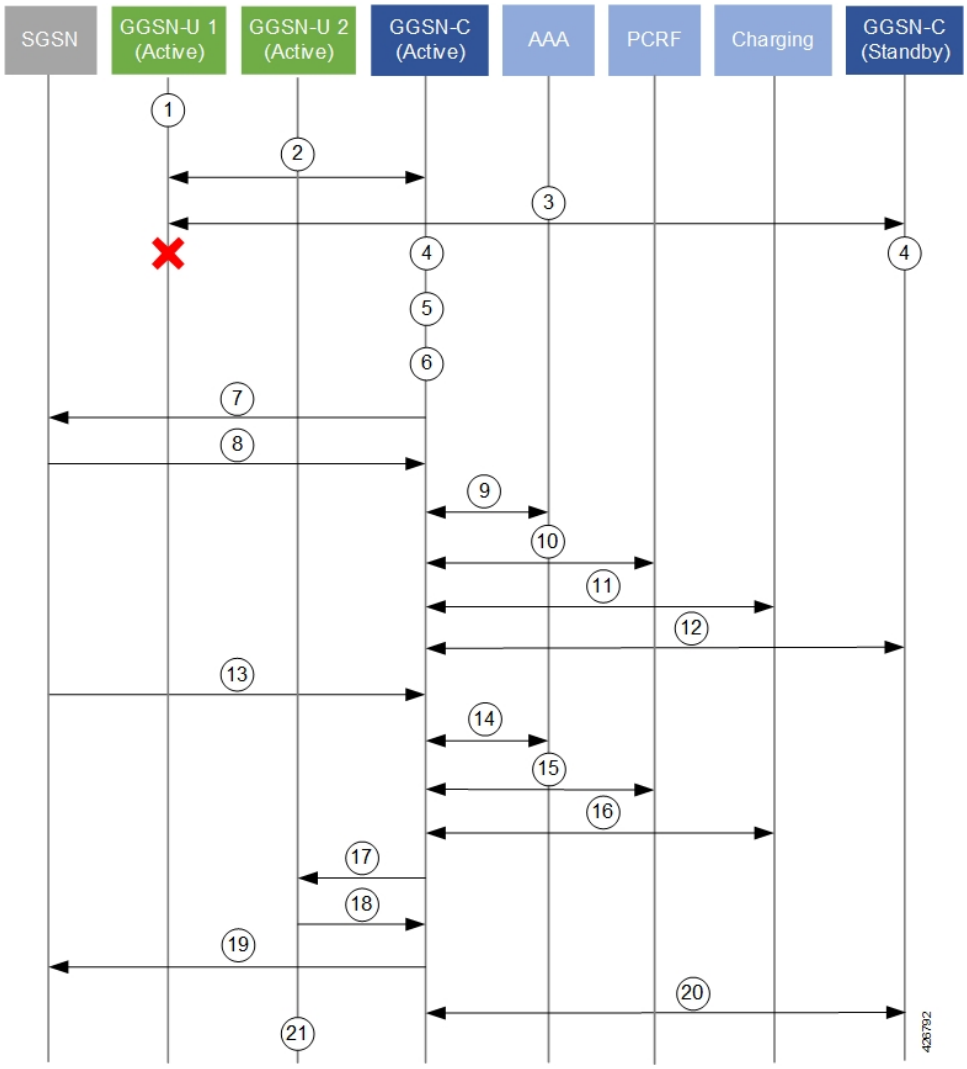


Table 9: GnGp GGSN CP/UP Detach and Re-attach on Path Failure Process

Number	Description
1	UE data sessions are processed by an active GGSN UP.
2	The active GGSN CP monitors GGSN UPs via BFD and Sx-Heartbeat messages.
3	The secondary CP also monitors GGSN UPs via BFD.
4	The active and standby CPs detect a BFD failure on a UP before eNB detection (relays on Sx timers (interval, retransmission, timeout)).
5	The BFD/VPNMGR on the active CP informs the Sx-demux process of a BFDDown event.
6	The Sx-demux process on the active CP initiates a path Failure notice to all Session Managers on the CP.

Number	Description
7	All Session Managers initiate the process of detaching sessions by sending Delete-pdp-context-req messages with no cause code to the SGSN. The detaches are initiated at a pre-defined rate.
8	The SGSN sends Delete-pdp-context-resp messages back to the CP. The SGSN does not page idle UEs with sessions being detached. The SGSN sends E-RAB release messages to active UEs with sessions being detached.
9	The active CP releases the session release with the AAA server(s).
10	The active CP releases the session with the PCRF.
11	The active CP releases the session with the Charging infrastructure.
12	The active CP syncs session detach information with the secondary CP.
13	For UEs re-initiating their session(s), the SGSN sends a Create-pdp-request message to the active CP. The SGSN selects the CP based on load algorithm (DNS, local config etc.).
14	The active CP processes the session attach request with the AAA server(s).
15	The active CP processes the session attach request with the PCRF.
16	The active CP processes the session attach request with the Charging infrastructure.
17	The active CP sends a Sx Session Establishment Request message to an alternate active UP. The CP selects the UP based on its load algorithm.
18	The UP sends a Sx Session Establishment Response message back to the CP.
19	The CP sends a Create-pdp-context response message to the SGSN.
20	The active CP syncs information for the newly attached session with the secondary CP.
21	UE data sessions are now processed by the active GGSN UP.

Additional N+2 Handling Scenarios

Beyond the flows described in the previous sections, the following table provides a description of network function (NF)/system behavior under various conditions with N+2 configured.

Table 10: N+2 Handling Scenarios

ID	Scenario	Handling	Notes
1	Active UP crash	Active CP detects BFD-failure with UP and detaches sessions belonging to that UP. Active CP propagates the disconnects to standby CP through SRP. When UP returns to active, it will re-associate with the active CP.	Detection occurs within the BFD timeout interval. CP Sx monitors BFD.
2	Active CP crash	Active CP switches over to standby CP. Active UP monitors Sx-heartbeat session for both active and standby CPs. Active UP does not purge sessions until ICSR failover time is reached.	Standby CP starts sending Sx-heartbeat upon failover – no sessions are purged by active UP.
3	Standby CP crash	Standby CP comes up and performs checkpoint with active CP to recover sessions	Sessions remain intact on active CP and active UP.
4	Network flaps between active CP and active UP; network between standby CP and active UP remains alive	Active CP detects BFD-Down for UP and initiates session detach processes and disassociates UP. Active CP propagates the disconnects to standby CP through SRP. Active UP monitors Sx-heartbeat with active CP. Active UP waits until configured Sx-heartbeat /path failure detection timeout occurs (>SRP switchover time) before clearing sessions.	

ID	Scenario	Handling	Notes
5	Network flaps between standby CP and active UP; active CP and active UP Sx-heartbeat also down	Active UP detects Sx-path failure. Active UP waits until configured Sx-heartbeat /path failure detection timeout occurs (>SRP switchover time) before clearing sessions. Active CP detects BFD-Down for UP and initiates session detach processes and disassociates UP.	UPs delete the sessions due to Sx-heartbeat timeout.
6	Network flaps between standby CP and active UP; Network between active CP and active UP is alive	Standby CP operates normally. Active CP-active is alive and responds to heartbeat. Active UP operates normally.	
7	Sx is not reachable, however BFD is reachable.	Active UP detects Sx-path failure. Active UP waits until configured Sx-heartbeat/path failure detection timeout occurs (>SRP switchover time) before clearing sessions. Active CP detects Sx-path failure for UP and initiates session detach processes and disassociates UP.	Corner case that is treated as Sx-path failure per current behavior (before N+2).
8	ICSR link between active and standby CPs goes down and standby CP also becomes active (Dual-Active case)	Upon becoming dual-Active, standby CP sends message to active UP with higher metric.	All service IPs advertised by dual-Active standby CP are with higher metric.
9	BGP failure Gn side of active UP	No action is taken in relation to N+2.	
10	BGP failure SGI side of active UP	No action is taken in relation to N+2.	
11	SessMgr crashes on active UP	Session recovery process occurs on active UP.	

ID	Scenario	Handling	Notes
12	Sx-demux crashes on active UP	Sx-demux recovery process occurs on active UP.	
13	VPP crashes on active UP	NPUMgr restarts the UP resulting in BFD loss triggering UP failure detection. Refer to Handling information for IDs 1 and 5 in this table.	
14	VPNMgr crashes on active UP	VPNMgr recovery process occurs on active UP.	
15	BFD crashes on active UP	BFD recovery process occurs on active UP.	
16	Sx-demux crashes on active CP	Sx-demux recovery process occurs on active CP. Sx-demux re-registers for BFD between CP and all UPs as part of recovery and rediscovers the state of each UP. Sx-demux recovers the restart-timestamp from the SessMgr.	It is possible for a UP state change to occur during the Sx-demux recovery on active CP (e.g. UP restarts but still shows as active to CP post recovery). Condition detected as follows: • Sx-demux recovers and CP detects either UP restart timestamp from Sx-heartbeat or UP-failure. • Based on this information, active CP initiates session purging.
17	VPNMgr crashes on active CP	VPNMgr recovery process occurs on active CP. BFDregistration information from recovered from SCT on active CP. Active CP restarts BFD with UP.	

ID	Scenario	Handling	Notes
18	BFD crashes on active CP	BFD recovery process occurs on active CP.	
19	SessMgr crashes on active CP	SessMgr recovery process occurs on active CP.	

Double Failure Handling Scenarios

N+2 double failure scenarios occur when there is a BFD failure followed by another event/failure. The handling of such scenarios is described in the following table.

Table 11: N+2 Double Failure Scenario Handling

ID	Scenario	Handling	Notes
1	Active CP fails while session detaches are in progress	ICSR switchover occurs between CPs. Standby CP becomes active CP. Active CP detects UP failure via BFD. Active CP detects UP restart vis Sx-heartbeat.	Impact: If UP restarts on double failure, it will have no sessions even though the standby CP will have recovered the sessions. These sessions are then cleaned as part of session replacement or session disconnects from UEs. If UP does not restart then the CP-new-active clears the sessions of the failed UP.
2	Standby CP fails while session detaches are in progress	Standby CP checkpoints state information with the Active CP. Information pertaining to deleted sessions is invalidated from active CP.	
3	Active CP determines UP failure due to router flap; Active CP receives UP BFD after initiating session detaching	Once UP BFD down is initially detected, all sessions are detached.	

BFD Flapping and VPC

N+2 uses BFD to monitor the existence/viability of a network path between the session endpoints. By using multihop BFD with loopback endpoints, the BFD session state functions as a proxy for the state of the system to which it connects.

However, a BFD session can go down, or bounce/flap, for reasons other than far-side system failure (e.g. due to ARP storms or router misconfiguration). If the disruption is sufficiently severe and long lasting, it can cause systems on both sides to detect BFD session failure even though both systems are functional.

Configuration adjustments can be made to help offset the occurrence of such events.

The following recommendations are offered based on the platform on which your NFs are deployed:

- VPC-SI: Adjust the BFD multihop-peer settings to increase the BFD detection time to 2-3 sec and the number of retries correspondingly.
- VPC-DI: CF switchover and SF migration can interrupt BFD packet generation and processing for multiple seconds. To prevent BFD session flaps when these events occur, BFD detection time for sessions involving VPC-DI systems must be set to 7 seconds or longer.

Sx-association Scenarios

The following table provides information on associating and disassociating CPs and UPs when using N+2.

Table 12: N+2 Sx-association Scenarios

Scenario	Mechanism(s)
Sx-disassociation from UP to CP	• Sx-demux to disable BFD monitoring with VPNMgr • SAEGW-service is removed • Sx-disassociation from UP
Adding UPs	As part of Day-0: • Add BFD loopback address for UP. • Configurate BFD on CPs. • Add UP Group and configure it for selection on CPs.
Removing UPs	On CP, execute the CLI command to clear subscribers with IP address of UP and keyword to block new sessions being placed on that UP. • Verify that all the subscribers are torn down on UP. • On the UP, execute the CLI command to disassociate from CP. This will disassociate the UP from CP and CP will not choose this UP for further sessions. Verify that all the sessions have been torn down. • On CP, remove the UP from the UP Group. • On CP, execute the CLI command to remove the UP from the UP Group (this will also deregister the BFD monitoring of the UP). • Disable the BFD configurations for monitoring at UP and at CP: no monitor-group CLI command.
UP-initiated Sx-association	Sx-demux on CP starts processing the BFDUp and BFDDown notifications from VPNMGr.

UP-released Sx-association	Sx-demux on CP ignores the BFDUp and BFDDown notifications from VPNMgr.

N+2 and IP Addressing

Loopback IP Addresses

The following is true of BFD loopback addresses in relation to N+2:

- BFD loopback-IP-Address on the active CP and standby CP must be configured on Day-0.
- BFD operates between the active CP and active UP as well as between the standby CP and active UP. As such, all three components must use unique BFD loopback-IP-addresses
- For each CP and UP, configured BFD loopback-IP-addresses must be different from the addresses used for the Sx interfaces, and, in the case of the CPs must also be different from the addresses used for the SRP interface.

IP Address Availability

With the N+2 deployment scenario, UEs may re-attach at a high rate (comparable to the detach rate). To facilitate this process, UPs must have sufficient IP addresses available.

CUPS IP Pool Management includes the capability to provision UPs with "chunks" of addresses. The chunk size and number of pools configured on the CP need to be increased proportionately so as to accommodate the high rate of re-attachments from the CP to UP such that sessions do not get rejected by the UP due to unavailability of IP addresses.

The potential re-attach rate can be roughly estimated by multiplying the number of Session Manager tasks processing UP sessions by 1000 sessions/second.

Address capacity is determined by multiplying the size of the chunk (between 16 and 8192) and the number of IP pools. Both configured on the CP.

Configuring N+2 UP Recovery

To configure N+2 UP Recovery:

1. Configure BFD on the CP and UP.

```
configure
   context bfd_context_name
      ip route static multihop bfd mhbfd_session_name local_endpoint_ip_address
 remote_endpoint_ip_address
      bfd-protocol
         bfd multihop-peer dst_ip_address interval tx_interval min_rx
rx_interval multiplier value
         #exit
      #exit
```

NOTES:

- *bfd_ctx_name* is the name of the context in which BFD is to be configured. This must be the same context in which Sx is configured.
- *mhbfd_session_name* is a name for the BFD session route. Multiple session routes can be created, one for each peer connection.
- *local_endpoint_ip_address* is the IPv4 or IPv6 address corresponding to the local interface in the current context.
- *remote_endpoint_ip_address* is the IPv4 or IPv6 address corresponding to the remote BFD peer.
  - If this route is being configured on the CP, then the remote address is that of the peer UP.
  - If this route is being configured on the UP, then the remote address is that of the peer CP.
- *dst_ip_address* is the IPv4 or IPv6 address corresponding to the remote BFD peer. This must be the same as the *remote_endpoint_ip_address* interface configured for the static multihop BFD route. Multiple peers can be configured, one for each remote peer.
- **interval** *tx_interval* is the transmit interval (in milliseconds) between BFD packets.
- **min_rx** *rx_interval* is the minimum receive interval capability (in milliseconds) between BFD packets.
- **multiplier** *value* the multiplier value used to compute holddown.
- To determine the Detect Time (X), you can use the following calculation:

  Detect Time (X) = **interval** *tx_interval* * **multiplier** *value*

  The recommended value of Detect time (X) is 3 seconds for VPC-SI, and 7 seconds for VPC-DI.

2. Configure the BFD-loopback per context on the CP and UP.

```
configure
   context monitor_ctx_name
      monitor-protocols
         monitor-group monitor_group_name protocol bfd
           session-ctx session_ctx_name local-addr { ipv4_address | ipv6_address
 } remote-address { ipv4_address | ipv6_address }
             #exit
```

NOTES:

- *Monitor_ctx_name* is the name of the context in which BFD monitoring is to be configured. This must be the same context in which Sx is configured.
- *Monitor_group_name* is the name of the group specifying the BFD monitoring parameters. Multiple monitor-groups can be configured.
- *Session_ctx_name* is the name of the context containing the local interfaces over which BFD monitoring will occur. This must be the same context in which Sx is configured.
- **local-addr {** *ipv4_address* **|** *ipv6_address* **}** is the IPv4 or IPv6 address corresponding to the local interface in the specified context.
- **remote-addr {** *ipv4_address* **|** *ipv6_address* **}** is the IPv4 or IPv6 address corresponding to the remote peer with which BFD monitoring will occur.

- If this monitor group is being configured on the CP, then the remote address is that of the UP group.
- If this monitor group is being configured on the UP, then the remote address is that of the CP.

3. Configure the BFD-loopback (remote-IP) within a specific UP-group on the CP:

```
configure
   user-plane-group up_group_name
      peer-node-id { ipv4_address | ipv6_address } monitor-group-name
monitor_group_name
      #exit
```

NOTES:

- *up_group_name* is the name of the UP group containing the data UPs for N+2 UP Recovery will be supported.
  - This cannot be the default group.
  - This group should not contain UPs intended to support IMS/VoLTE.
- **{** *ipv4_address* **|** *ipv6_address* **}** is the IPv4 or IPv6 address of the Sx interface on an active UP that will be part of the UP group. Multiple peer-nodes can be configured within the group. Note that the Sx interface is a different interface from the one that will be used to monitor BFD.
- *monitor_group_name* is the name of the monitoring group the UP will be associated with.

Monitoring and Troubleshooting

Show Commands

show sx peers { full address *peer_ip_address* **| wide }**

show sx peers full address *peer_ip_address*

Displays the Monitor-related information for the specified peer (e.g. VPN context name, group name, and state).

show sx peers wide

Displays "Monitor State" with the default state being "U" for UP, "D" for Down, and "N" for Not Applicable.

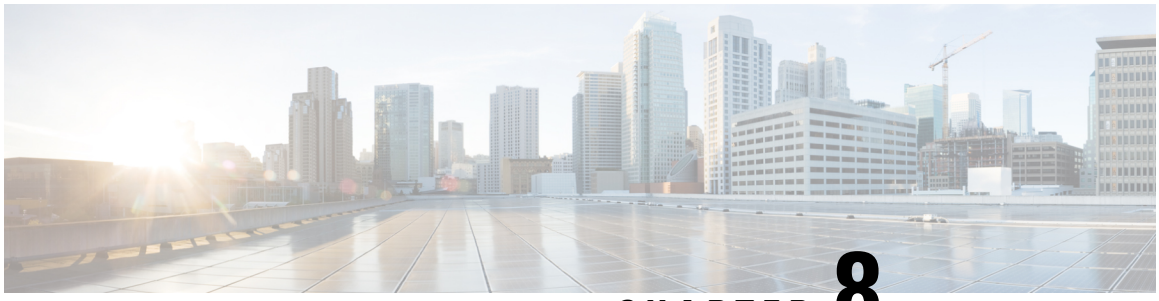
show sx-service statistics all

SNMP

The following SNMP traps can be used to monitor N+2 UP Recovery health:

- starBFDSessUp (starentTraps 1276)
- starBFDSessDown (starentTraps 1277)

- starSxPathFailure (starentTraps 1382) – This trap has been updated to include a new cause code: bfd-failure(8)
- starSxPathFailureClear (starentTraps 1383)



CHAPTER 8

PDI Optimization

Feature Summary and Revision History

Revision History

Note Revision history details are not provided for features introduced before release 21.24.

Revision Details	Release
First introduced	Pre 21.24

Feature Description

The Packet Detection Information (PDI) Optimization feature allows the optimization of PFCP signaling, through Sx Establishment and Sx Modification messages, between the Control Plane and the User Plane function. Without PDI Optimization, the following common parameters are repeated in the PDI of all Packet Detection Rules (PDRs), for a given bearer, resulting in an unwanted increase in signaling between Control Plane and User Plane:

- Local F-TEID
- Network Instance
- UE IP address

- The PDI Optimization is achieved by consolidating the common parameters, in the PDI of the PDRs, into a single container that is called the Traffic Endpoint (Traffic Endpoint ID). The consolidated parameters from multiple PDRs are then referred to the Traffic Endpoint.
- The PDI Optimization is a CLI-controlled feature, and supported over the Sxa, Sxb, Sxc, Sxab, and N4 interfaces.

Relationships

The PDI Optimization feature is a prerequisite for the following features:

- GTP-U Error Indication Support on User Plane.
- Sx Bulkstats
- CUPS Bulkstats Support

How It Works

The Traffic Endpoint ID is unique within a PFCP session. When a PDI refers to a Traffic Endpoint, the parameters that are in the Traffic Endpoint is not provided in the PDI once again. The Control Plane function updates the Traffic Endpoint whenever applicable.

If a Traffic Endpoint is updated, all the PDRs that refer to this Traffic Endpoint in the User Plane function uses the updated information.

If the F-TEID allocation is performed in the User Plane function, the User Plane function allocates and stores the F-TEID associated to the Traffic Endpoint. When the User Plane function provides the allocated F-TEID to the Control Plane function in the PFCP Session Establishment response or PFCP Session Modification response message, the Control Plane function updates the Traffic Endpoint information that is stored in the Control Plane function with the received F-TEID.

The Control Plane function uses the Traffic Endpoint ID created in a different PFCP message only after getting the confirmation from the User Plane function of the Traffic Endpoint ID creation.

If the Control Plane function deletes a Traffic Endpoint, the User Plane function deletes all the PDRs that refer to the Traffic Endpoint that was deleted by Control Plane function. For Evolved Packet Core (EPC), the Remove Traffic Endpoint IE is used to delete a bearer for which multiple PDRs exist (with the same Traffic Endpoint ID).

The Traffic Endpoints is used as a mechanism to identify the bearers uniquely for a given Sx session on the User Plane. This is achieved with the help of Traffic Endpoint IDs that are associated with the PDRs of a bearer.

PDI Optimization Changes on Control Plane

A new container, called Traffic Endpoint, is supported to carry the repeated PDI information of a given bearer. Each Traffic Endpoint is associated with a Traffic Endpoint ID. This ID is unique for a given Sx Session.

A new IE, Create Traffic Endpoint IE, is supported as part of Sx Establishment Request.

Following are the new IEs supported as part of Sx Modification Request:

- Create Traffic Endpoint IE
- Update Traffic Endpoint IE
- Remove Traffic Endpoint IE

Create PDR supports a new IE, Traffic Endpoint ID, that identifies either the ingress or the egress Traffic Endpoint of a bearer to which this PDR is associated.

A new IE, Created Traffic Endpoint IE, is supported as part of Sx Establishment Response and Sx Modification Response message.

Create Traffic Endpoint IE

Following are the IEs in a Create Traffic Endpoint IE that are supported for a Pure-P call:

- Traffic Endpoint ID
- Local F-TEID
- Network instance
- UE IP address

Following are the IEs in a Create Traffic Endpoint IE that are supported for a Pure-S call:

- Traffic Endpoint ID
- Local F-TEID

NOTE: The Network instance and UE IP address IEs are currently not supported for a Pure-S call.

For a Collapsed call, Sxa Traffic Endpoints has IEs that are relevant to S-GW and Sxb Traffic Endpoints has IEs that are relevant to P-GW.

In addition to the 3GPP standards defined IEs, a private IE called "Bearer Info IE", is added to the Create Traffic Endpoint which includes:

- QCI of the bearer being created.
- ARP of the bearer being created.
- Charging ID of the bearer being created.

For a Pure-S call, there are two Traffic Endpoints that are created for each bearer of that PDN:

1. Create Traffic Endpoint for Ingress Traffic Endpoint, that is sent for the ingress F-TEID and referred by ingress S-GW PDR of the bearer.
2. Create Traffic Endpoint for Egress Traffic Endpoint, that is sent for the egress F-TEID and referred by egress S-GW PDR of the bearer.

For a Pure-S call, a bearer is uniquely identified on the User Plane that is based on Ingress and Egress Traffic Endpoint IDs of the bearer. The Traffic Endpoints also store the QCI, ARP, and Charging ID of the bearer.

For a Pure-P call, only one Traffic Endpoint is created for each bearer of that PDN. Create Traffic Endpoint for Ingress Traffic Endpoint, that is sent for ingress F-TEID and referred by ingress PDRs of the bearer. There is no separate egress Traffic Endpoint that is created for a Pure-P call as no Tunnel Endpoint ID is allocated on the P-GW egress. The same Traffic Endpoint is referred by both ingress and egress PDRs of a bearer. A

bearer is uniquely identified on the User Plane that is based on the Traffic Endpoint ID of the bearer. The Traffic Endpoint also stores the QCI, ARP, and Charging ID of the bearer.

For a Collapsed call, there are two Traffic Endpoints that are created for the S-GW leg of the call for each bearer. So, two Create Traffic Endpoints are sent for Ingress and Egress. The Sxa PDRs refer to these traffic endpoints based on the direction (ingress or egress). Only one Traffic Endpoint is created for the P-GW leg of the call for each bearer. The same Traffic Endpoint ID is referred by all Sxb PDRs of the bearer. For P-GW, Create Traffic Endpoint is sent for the ingress. The Traffic Endpoint IDs of Sxa and Sxb PDRs identify the bearer.

Created Traffic Endpoint IE

This IE is present in Sx Establishment/Sx Modification Response to inform Control Plane about the F-TEIDs that were locally allocated by the User Planes for the various Traffic Endpoints that were created.

Following are the IEs in a Created Traffic Endpoint IE:

- Traffic Endpoint ID
- Local FTEID

The information that is received in Created Traffic Endpoint IE is processed by the Control Plane, and the F-TEIDs that are allocated by the User Plane are stored in the Control Plane for ingress and egress accordingly.

Update Traffic Endpoint IE

This IE is present in Sx Modification Request to update the Traffic Endpoint information on the User Plane.

Following are the IEs in an Update Traffic Endpoint IE:

- Traffic Endpoint ID
- Local FTEID
- Network Instance
- UE IP address
- In addition to the 3GPP standards defined IEs, a private IE called "Bearer Info IE", is added to the Create Traffic Endpoint which includes:
- QCI of the bearer
- ARP of the bearer
- Charging ID of the bearer

NOTE: Currently, the Update Traffic Endpoint IE supports only the update of Private IE extensions, such as the Bearer Info IE. There are no use-cases wherein update of other information, such as Local FTEID, Network Instance, UE IP address, is required.

When the QCI/ARP of a particular bearer EPS-Bearer Identity (EBI) is modified, then the modified QCI/ARP along with the Charging ID is communicated to the User Plane with the help of Update Traffic Endpoint ID. A given Traffic Endpoint ID can be updated only if it was successfully created on the User Plane.

Remove Traffic Endpoint IE

This IE is present in Sx Modification Request to remove a traffic endpoint. Traffic Endpoint ID is included in the Remove Traffic Endpoint IE. A given Traffic Endpoint ID can be removed only if it is successfully created on the User Plane.

For Pure-S, Pure-P, and Collapsed call, when a bearer is deleted on the Control Plane, the Traffic Endpoints that are associated with the bearer are removed with Remove Traffic Endpoints. There is no explicit requirement to send Remove PDRs and Remove FARs on that bearer.

On the User Plane, for a Pure-S call, Remove Traffic Endpoints deletes all the PDRs, FARs, and URRs of that bearer. For Pure-P and Collapsed call, Remove Traffic Endpoints deletes all the PDRs, FARs, QERs, and URRs of that bearer.

PDI Changes in Create PDR

When PDI Optimization is enabled for the PDN, then the Traffic Endpoint ID is set in the PDI field of all PDRs of the bearers of the PDN. The PDI fields, such as F-TEID, PDN Instance, UE IP address, and so on, are not supposed to be filled and so, these fields are validated in the User Plane and error messages are posted in case of any validation failures. This is applicable for all interfaces, such as Sxa, Sxb, Sxab, N4, and Sxc.

PDI Optimization Changes on User Plane

Handling of Create Traffic Endpoint

When a Create Traffic Endpoint is received, the contents of the IE are validated for correctness. If validation fails, then an error message is sent back to the Control Plane.

Validations fail in the following cases:

- Basic IE validation failures.
- Traffic Endpoint exists with this Traffic Endpoint ID.
- CH-bit not set in the F-TEID IE inside Traffic Endpoint.
- PDN Instance is not valid.
- UE IP address is not valid.

When a Create Traffic Endpoint is successfully processed, then a local F-TEID is allocated by the User Plane and it is associated with the Traffic Endpoint. The Created Traffic Endpoint is sent back to Control Plane for this Traffic Endpoint with the F-TEID information and Traffic Endpoint ID.

When a Create Traffic Endpoint list is processed on the User Plane in Sx Establishment Request, PDI optimization is enabled for the lifetime of the Sx Session which cannot be changed midway.

Handling of Update Traffic Endpoint

When an Update Traffic Endpoint is received, the contents of the IE are validated for correctness. If validation fails, then an error message is sent back to the Control Plane.

Validations fail in the following cases:

- Basic IE validation failures.

- Traffic Endpoint with its Traffic Endpoint ID does not exist.

NOTE: Currently, Update Traffic Endpoint updates only bearer information, such as QCI, ARP, and Charging ID on the User Plane. Update is not supported for any other Traffic Endpoint parameters.

Handling of Remove Traffic Endpoint

When a Remove Traffic Endpoint is received, the contents of the IE are validated for correctness. If validation fails, then an error message is sent back to the Control Plane.

Validations fail in the following cases:

- Basic IE validation failures.
- Traffic Endpoint with its Traffic Endpoint ID does not exist.

When a Remove Traffic Endpoint is received, the PDRs associated with the Traffic Endpoint, FARs associated with the PDR, QERs associated with the PDR, and URRs associated with PDR are also removed.

To remove a bearer, the Control Plane sends Remove Traffic Endpoints for the Traffic Endpoints that are associated with the bearer resulting in the cleanup of the bearer-associated data on the User Plane.

The Control Plane does not explicitly send any Remove PDRs, Remove FARS, Remove QERS, or Remove URRs for a bearer removal. However, if the Control Plane does send Remove PDRs, Remove FARS, Remove QERS, or Remove URRs with Remove Traffic Endpoints, the message is accepted and successfully processed.

Handling of Create PDR

When Sx Session has the PDI Optimization enabled, the Traffic Endpoint ID is set for Create PDR. If not, an error response is sent back to the Control Plane. The Create PDR validation fails in the following cases:

- Basic IE validation failures.
- Create PDR does not have Traffic Endpoint ID set in the PDI IE.
- Create PDR has valid F-TEID IE in PDI IE.
- Create PDR has valid PDN Instance IE in PDI IE.
- Create PDR has valid UE IP address IE in PDI IE.

For a Sx Session with PDI optimization disabled, the Create PDR is validated for various other fields. If Traffic Endpoint ID is valid in PDI, then an error response is sent back to the Control Plane as Traffic Endpoint ID should not be present for a Sx Session with the PDI optimization being disabled.

Session Recovery and ICSR

Control Plane

Session Recovery and ICSR are supported for the Traffic Endpoint IDs of all bearers of a PDN. The Traffic Endpoint IDs are recovered for all bearers of a given PDN. This support is provided for Pure-S, Pure-P, and Collapsed call. With this, PDI optimization enabled status for a PDN is also recovered. Full Checkpoint is used for check-pointing and recovery of the Traffic Endpoints IDs of bearers.

User Plane

Session Recovery and ICSR are supported for the Traffic Endpoints on the User Plane for all bearers. All the Traffic Endpoints, that are associated with a given Sx Session, are recovered. For a given Traffic Endpoint, the associated PDR list is also recovered. For a given PDR, the associated Traffic Endpoint ID is recovered.

Standards Compliance

The PDI Optimization feature complies with the following standard: 3GPP TS 29.244 V15.5.0 (Interface between the Control Plane and the User Plane Nodes).

Limitations

The PDI Optimization feature has the following limitations:

- The Network instance and UE IP address IEs are currently not supported for a Pure-S call.
- The Update Traffic Endpoint IE supports only the update of Private IE extensions, such as the Bearer Info IE. Update of other information, such as Local F-TEID, Network Instance, UE IP address, are not supported.
- The Update Traffic Endpoint updates only bearer information, such as QCI, ARP, and Charging ID on the User Plane. Update is not supported for any other Traffic Endpoint parameters.

Configuring the PDI Optimization Feature

This section describes how to configure the PDI Optimization feature.

Enabling PDI Optimization

Use the following CLI commands to enable the feature.

```
configure
  context context_name
    sx-service service_name
      [ no ] sx-protocol pdi-optimization
      end
```

NOTES:

- **no**: Disables PDI optimization.
- By default, the CLI command is disabled.
- PDI Optimization is enabled or disabled at PDN level. PDI Optimization is enabled for each PDN based on the configuration in sx-service. The PDN is PDI Optimization-enabled if the configuration is enabled while processing Sx Establishment Request on the Control Plane.
- Configuration changes will not have any effect on the PDN. The configuration that is applied while processing Sx Establishment Request will be maintained throughout the lifetime of the PDN. In a multi-PDN call, each PDN has the configuration applied while PDN is set up.

- On the User Plane, there is no separate configuration to determine whether the PDN has PDI Optimization-enabled. When Create Traffic Endpoint IE is received in Sx Establishment Request for a Sx session, then the Sx session is considered to have PDI Optimization-enabled throughout the lifetime of the session. This will not change dynamically midway, and validations are done accordingly. In case of any validation failures, Error Response is sent back to the Control Plane.
- When there are multiple Create Traffic Endpoint IEs with the same Traffic Endpoint ID, the first Create Traffic Endpoint IE is processed, and rest are ignored. The same behavior is applicable for Created Traffic Endpoint IE, Update Traffic Endpoint IE, and Remove Traffic Endpoint IE.

Verifying the PDI Optimization Feature Configuration

To verify if the PDI Optimization feature is enabled or disabled, use the **show sx-service all** CLI command. The output of this show command has been enhanced to display the following:

- SX PDI Optimisation: [Enabled/Disabled]

PDI Optimization OAM Support

This section describes operations, administration, and maintenance information for this feature.

Show Command Support

The following show CLI commands are available in support of PDI Optimization feature.

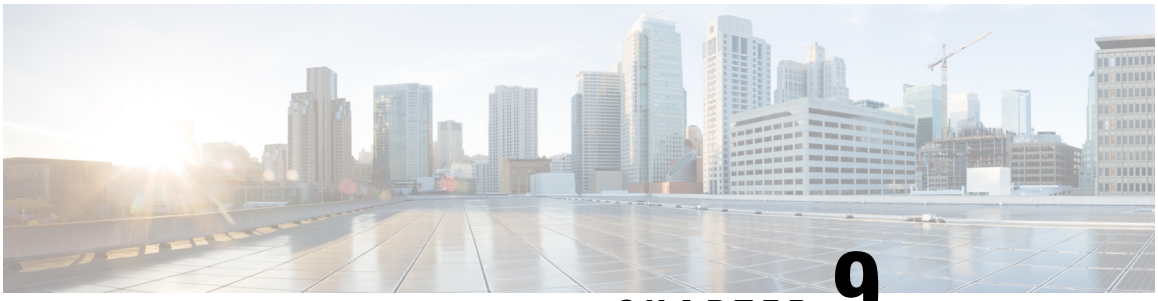
show subscribers user-plane-only callid <call_id> pdr all

The output of this CLI command has been enhanced to display the following field: Associated Create Traffic Endpoint-ID(s)

show subscribers user-plane-only callid <call_id> pdr full all

The output of this CLI command has been enhanced to display the following field:

- Create Traffic Endpoint-ID
  - Bearer QOS
    - QCI
    - ARP
    - Charging Id



CHAPTER 9

Sx Over IPSec

Revision History

Note Revision history details are not provided for features introduced before release 21.24.

Revision Details	Release
First introduced	Pre 21.24

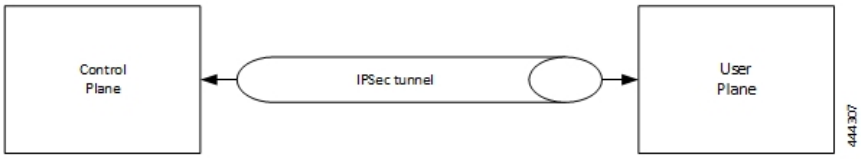
Feature Description

IPSec is a suite of protocols that interact with one another to provide secure private communications across IP networks. These protocols allow the system to establish and maintain secure tunnels with peer security gateways. IPSec provides confidentiality, data integrity, access control, and data source authentication to IP datagrams.

In CUPS, the functionality is available with IPSec in Tunnel mode both on Control Plane (CP) and User Plane (UP) nodes. The IPSec crypto-maps are associated under the appropriate interface on respective nodes. The IPSec tunnel is created between each CP or UP pair explicitly. There is no change that is required on Sx service configuration.

IPSec Tunnel Mode encapsulates the entire IP packet to provide a virtual secure hop between two gateways. It forms more familiar VPN kind of functionality, where entire IP packets are encapsulated inside another and delivered to the destination. It encapsulates the full IP header as well as the payload.

Figure 7: Sx Over IPSec tunnel



When Sx over IPSec is enabled on UP node running VPP, then following parameter must be used under "UPP Param" for Sx over IPSec feature to work.

VPP_DPDK_DATA_SIZE=5120

The UPP Param is stored in staros_para.cfg file on a CD-ROM and this configuration is read and applied to VPP by UP during its boot.

Note This parameter introduces a memory overhead of about 800 MB. The user must consider this condition before using the feature. If the UP has less RAM, then VM must be allocated with extra 1 GB of RAM memory for the feature to work properly.

For more information on IPSec support, refer StarOS *IPSec Reference*.

IKEv2 Keep-Alive Messages (Dead Peer Detection)

IPSec for Sx interface supports IKEv2 keep-alive messages, also known as Dead Peer Detection (DPD), originating from both ends of an IPSec tunnel. Per RFC 3706, DPD is used to simplify the messaging required to verify communication between peers and tunnel availability.

IPSec DPD is an optional configuration. If its disabled, the IPSec node doesn't initiate DPD request. However, the node always responds to DPD availability messages initiated by peer node regardless of its DPD configuration.

The following method/formula can be used to calculate the keep-alive interval value when Sx over IPSec feature is configured:

```
((max-retransmissions + 1) * retransmission-timeout-ms) * 2
```

The keep-alive interval value specifies the time that the IPSec tunnel will remain up till DPD is triggered.

Example:

The following is a sample output for **show configuration context** *context_name* **verbose** CLI command under Sx service:

```
sx-service sx
   instance-type userplane
   bind ipv4-address 192.168.1.1 ipv6-address bbbb:abcd::11
   sxa max-retransmissions 4
   sxa retransmission-timeout-ms 5000
```

Here, the value of **max-retransmissions** is 4 and **retransmission-timeout-ms** is 5000. Therefore, the keep-alive interval value will be 50:

((max-retransmissions + 1) * retransmission-timeout-ms) * 2 = Keep-alive interval

((4+1) * 5000) * 2 = 50

IKESA Rekey

CUPS supports both IKESA Rekey and IPSec Rekey.

For IKESA Rekey, the **lifetime** *interval* CLI must be configured under **ikev2-ikesa transform-set** *transform_set*. You must also configure **ikev2-ikesa rekey** under **crypto map** configuration. Following is a configuration example:

```
ikev2-ikesa transform-set ikesa-foo
   encryption aes-cbc-256
   group 14
   hmac sha2-256-128
   lifetime 28800
   prf sha2-256
...
...
...
crypto map foo0 ikev2-ipv4
   match address foo0
   authentication local pre-shared-key encrypted key secret_key
   authentication remote pre-shared-key encrypted key secret_key
   ikev2-ikesa max-retransmission 3
   ikev2-ikesa retransmission-timeout 15000
   ikev2-ikesa transform-set list ikesa-foo
   ikev2-ikesa rekey
   keepalive interval 50
   control-dont-fragment clear-bit
   payload foo-sa0 match ipv4
      ipsec transform-set list A-foo
      lifetime 600
      rekey keepalive
   #exit
   peer 172.19.222.2
   ikev2-ikesa policy error-notification
```

Limitations

The following is the known limitation of Sx Over IPSec feature:

- The feature is supported only in IPv4-IPv4 tunneling mode.

Recommended Timers

The following table provides the recommended timer values for CLI commands related to IPSec, Sx, and SRP.

IPSEC	**CP**	**UP**
ikev2-ikesa max-retransmission	*3*	*3*
ikev2-ikesa retransmission-timeout	*1000*	*1000*
keepalive	**interval** *4* **timeout** *1* **num-retry** *4*	**interval** *5* **timeout** *2* **num-retry** *4*
Sx	**CP**	**UP**

IPSEC	CP	UP
sx-protocol heartbeat interval	*10*	*10*
sx-protocol heartbeat retransmission-timeout	*5*	*5*
sx-protocol heartbeat max-retransmissions	*4*	*4*
sxa max-retransmissions	*4*	*4*
sxa retransmission-timeout-ms	*5000*	*5000*
sxb max-retransmissions	*4*	*4*
sxb retransmission-timeout-ms	*5000*	*5000*
sxab max-retransmissions	*4*	*4*
sxab retransmission-timeout-ms	*5000*	*5000*
sx-protocol association reattempt-timeout	*60*	*60*
SRP	**CP**	**UP**
hello-interval	*3*	*3*
dead-interval	*15*	*15*

Recommended Configurations

Following are the recommended configurations and restrictions related to Sx and SRP over IPSec:

- The multihop BFD timer between CP and UP must be seven seconds (for Data UPs).
- The singlehop BFD must be enabled on all the contexts (CP GW/Billing and UP Gn/Gi).
- Inter-chassis multihop BFD must be enabled for CP-CP ICSR and UP-UP ICSR (IMS UP).
- The SRP-IPSec ACL must be configured for TCP protocol instead of IP protocol.
- The Sx-IPSec ACL must be configured for UDP protocol instead of IP protocol.

Example Configurations in CP

Multihop BFD Configuration VPC DI

The following is an example of multihop BFD configuration with seven seconds timer.

```
bfd-protocol
      bfd multihop-peer 192.1.1.1 interval 350 min_rx 350 multiplier 20
      bfd multihop-peer 192.1.2.1 interval 350 min_rx 350 multiplier 20
      bfd multihop-peer 192.1.0.1 interval 350 min_rx 350 multiplier 20
      bfd multihop-peer 192.1.6.1 interval 350 min_rx 350 multiplier 20
      bfd multihop-peer 192.1.3.1 interval 350 min_rx 350 multiplier 20
      bfd multihop-peer 192.1.4.1 interval 350 min_rx 350 multiplier 20
    #exit
```

Multihop BFD Configuration VPC SI

The following is an example of multihop BFD configuration with three seconds timer.

```
bfd-protocol
      bfd multihop-peer 192.1.1.1 interval 150 min_rx 150 multiplier 20
      bfd multihop-peer 192.1.2.1 interval 150 min_rx 150 multiplier 20
      bfd multihop-peer 192.1.0.1 interval 150 min_rx 150 multiplier 20
      bfd multihop-peer 192.1.6.1 interval 150 min_rx 150 multiplier 20
      bfd multihop-peer 192.1.3.1 interval 150 min_rx 150 multiplier 20
      bfd multihop-peer 192.1.4.1 interval 150 min_rx 150 multiplier 20
    #exit
```

BGP Configuration

The following is an example of BGP configuration with recommended timers.

```
router bgp 1111
      router-id 192.0.0.1
      maximum-paths ebgp 15
      neighbor 192.0.0.101 remote-as 1000
      neighbor 192.0.0.101 ebgp-multihop
      neighbor 192.0.0.101 update-source 192.0.0.1
      neighbor 1111:2222::101 remote-as 1000
      neighbor 1111:2222::101 ebgp-multihop
      neighbor 1111:2222::101 update-source 1111:2222::1
      bgp graceful-restart restart-time 120
      bgp graceful-restart stalepath-time 300
      timers bgp keepalive-interval 30 holdtime-interval 90 min-peer-holdtime-interval 0
server-sock-open-delay-period 10
      address-family ipv4
        redistribute connected
      #exit
      address-family ipv6
        neighbor 1111:2222::101 activate
        redistribute connected
      #exit
    #exit
```

Singlehop BFD Configuration

The following is an example of singlehop BFD configuration with three seconds timer.

```
interface bgp-sw1-2161-10
      ip address 192.0.1.9 255.111.222.0
      ipv6 address 1111:222::9/112 secondary
      bfd interval 999 min_rx 999 multiplier 3
    #exit
    interface bgp-sw1-2161-11
      ip address 192.0.1.10 255.111.222.0
      ipv6 address 1111:222::10/112 secondary
      bfd interval 999 min_rx 999 multiplier 3
    #exit
    interface bgp-sw1-2161-12
      ip address 192.0.1.11 255.111.222.0
      ipv6 address 1111:222::11/112 secondary
      bfd interval 999 min_rx 999 multiplier 3
    #exit
    interface bgp-sw1-2161-3
      ip address 192.0.1.2 255.111.222.0
      ipv6 address 1111:222::2/112 secondary
      bfd interval 999 min_rx 999 multiplier 3
    #exit
    interface bgp-sw1-2161-4
      ip address 192.0.1.3 255.111.222.0
```

```
    ipv6 address 1111:222::3/112 secondary
    bfd interval 999 min_rx 999 multiplier 3
  #exit
  interface bgp-sw1-2161-5
    ip address 192.0.1.4 255.111.222.0
    ipv6 address 1111:222::4/112 secondary
    bfd interval 999 min_rx 999 multiplier 3
  #exit
  interface bgp-sw1-2161-6
    ip address 192.0.1.5 255.111.222.0
    ipv6 address 1111:222::5/112 secondary
    bfd interval 999 min_rx 999 multiplier 3
  #exit
  interface bgp-sw1-2161-7
    ip address 192.0.1.6 255.111.222.0
    ipv6 address 1111:222::6/112 secondary
    bfd interval 999 min_rx 999 multiplier 3
  #exit
  interface bgp-sw1-2161-8
    ip address 192.0.1.7 255.111.222.0
    ipv6 address 1111:222::7/112 secondary
    bfd interval 999 min_rx 999 multiplier 3
  #exit
  interface bgp-sw1-2161-9
    ip address 192.0.1.8 255.111.222.0
    ipv6 address 1111:222::8/112 secondary
    bfd interval 999 min_rx 999 multiplier 3
  #exit
```

-

Static Route for Multihop BFD Configuration

The following is an example of static route multihop BFD configuration.

```
ip route static multihop bfd UP-5 192.111.1.10 192.111.11.10
    ip route static multihop bfd UP-6 192.111.1.10 192.111.12.10
    ip route static multihop bfd UP-9 192.111.1.10 192.111.10.10
    ip route static multihop bfd UP-10 192.111.1.10 192.111.16.10
    ip route static multihop bfd UP-7 192.111.1.10 192.111.13.10
    ip route static multihop bfd UP-8 192.111.1.10 192.111.14.10
```

Static Route for Singlehop BFD Configuration

The following is an example of static route singlehop BFD configuration.

```
ip route static bfd bgp-sw1-2161-3 192.0.1.1
    ip route static bfd bgp-sw1-2161-4 192.0.1.1
    ip route static bfd bgp-sw1-2161-5 192.0.1.1
    ip route static bfd bgp-sw1-2161-6 192.0.1.1
    ip route static bfd bgp-sw1-2161-7 192.0.1.1
    ip route static bfd bgp-sw1-2161-8 192.0.1.1
    ip route static bfd bgp-sw1-2161-9 192.0.1.1
    ip route static bfd bgp-sw1-2161-10 192.0.1.1
    ip route static bfd bgp-sw1-2161-11 192.0.1.1
    ip route static bfd bgp-sw1-2161-12 192.0.1.1
```

IPSec ACL Configuration

The following is an example IPSec ACL configuration in CP.

```
ip access-list UP-1
      permit udp host 192.0.1.1 host 192.0.1.2
    #exit
```

IPSec Transform Set Configuration

The following is an example of IPSec Transform Set configuration in CP.

```
ikev2-ikesa transform-set ikesa-UP-1
      encryption aes-cbc-256
      group 14
      hmac sha2-256-128
      lifetime 28800
      prf sha2-256

    ipsec transform-set A-UP-1
      encryption aes-cbc-256
      hmac sha2-256-128
      group 14
```

IPSec Crypto Map Configuration

The following is an example of IPSec Crypto Map configuration in CP.

```
crypto map UP-1 ikev2-ipv4
      match address UP-1
      authentication local pre-shared-key encrypted key secretkey
      authentication remote pre-shared-key encrypted key secretkey
      ikev2-ikesa max-retransmission 3
      ikev2-ikesa retransmission-timeout 1000
      ikev2-ikesa transform-set list ikesa-UP-1
      ikev2-ikesa rekey
      keepalive interval 4 timeout 1 num-retry 4
      control-dont-fragment clear-bit
      payload foo-sa0 match ipv4
        ipsec transform-set list A-UP-1
        lifetime 300
        rekey keepalive
      #exit
      peer 192.1.1.1
      ikev2-ikesa policy error-notification
    #exit
```

Sx Configuration

The following is an example of Sx configuration in CP.

```
sx-service SX-1
      instance-type controlplane
      sxa max-retransmissions 4
      sxa retransmission-timeout-ms 5000
      sxb max-retransmissions 4
      sxb retransmission-timeout-ms 5000
      sxab max-retransmissions 4
      sxab retransmission-timeout-ms 5000
      n4 max-retransmissions 4
      n4 retransmission-timeout-ms 5000
      sx-protocol heartbeat interval 10
      sx-protocol heartbeat retransmission-timeout 5
      sx-protocol heartbeat max-retransmissions 4
      sx-protocol compression
      sx-protocol supported-features load-control
      sx-protocol supported-features overload-control
    exit
end
```

Example Router Configurations

Static Routes for Interface

The following is an example configuration of static route for interface.

```
ip route 192.1.1.1/32 Vlan1111 192.1.1.2
ip route 192.1.1.1/32 Vlan1111 192.1.1.3
ip route 192.1.1.1/32 Vlan1111 192.1.1.4
ip route 192.1.1.1/32 Vlan1111 192.1.1.5
ip route 192.1.1.1/32 Vlan1111 192.1.1.6
ip route 192.1.1.1/32 Vlan1111 192.1.1.7
ip route 192.1.1.1/32 Vlan1111 192.1.1.8
ip route 192.1.1.1/32 Vlan1111 192.1.1.9
ip route 192.1.1.1/32 Vlan1111 192.1.1.10
ip route 192.1.1.1/32 Vlan1111 192.1.1.11
```

Static Routes for Singlehop BFD

The following is an example configuration of static route for singlehop BFD.

```
ip route static bfd Vlan1111 192.1.1.2
ip route static bfd Vlan1111 192.1.1.3
ip route static bfd Vlan1111 192.1.1.4
ip route static bfd Vlan1111 192.1.1.5
ip route static bfd Vlan1111 192.1.1.6
ip route static bfd Vlan1111 192.1.1.7
ip route static bfd Vlan1111 192.1.1.8
ip route static bfd Vlan1111 192.1.1.9
ip route static bfd Vlan1111 192.1.1.10
ip route static bfd Vlan1111 192.1.1.11
```

Interface for Singlehop BFD

The following is an example configuration of interface for singlehop BFD.

```
interface Vlan1111
  no shutdown
  bandwidth 10000000
  bfd interval 999 min_rx 999 multiplier 3
  no bfd echo
  ip address 192.1.1.1/24
  ipv6 address 1111:222::1/112
```

BGP Configuration

The following is an example of BGP configuration with recommended timers.

```
router bgp 1000
  router-id 192.1.1.1
  timers bgp 30 90
  timers bestpath-limit 300
  timers prefix-peer-timeout 30
  timers prefix-peer-wait 90
  graceful-restart
  graceful-restart restart-time 120
  graceful-restart stalepath-time 300
```

Example Configurations in UP

IPSec ACL Configuration

The following is an example of IPSec ACL configuration in UP.

```
ip access-list CP-1
      permit udp host 192.0.1.1 host 192.0.1.2
    #exit
```

IPSec Transform Set Configuration

The following is an example of IPSec Transform Set configuration in UP.

```
ipsec transform-set A-CP-1
      encryption aes-cbc-256
      hmac sha2-256-128
      group 14

    ikev2-ikesa transform-set ikesa-CP-1
      encryption aes-cbc-256
      group 14
      hmac sha2-256-128
      lifetime 28800
      prf sha2-256
```

IPSec Crypto Map Configuration

The following is an example of IPSec Crypto Map configuration in UP.

```
crypto map CP-1 ikev2-ipv4
      match address CP-1
      authentication local pre-shared-key encrypted key secretkey
      authentication remote pre-shared-key encrypted key secretkey
      ikev2-ikesa max-retransmission 3
      ikev2-ikesa retransmission-timeout 1000
      ikev2-ikesa transform-set list ikesa-CP-1
      ikev2-ikesa rekey
      keepalive interval 5 timeout 2 num-retry 4
      control-dont-fragment clear-bit
      payload foo-sa0 match ipv4
        ipsec transform-set list A-CP-1
      #exit
      peer 192.1.1.2
      ikev2-ikesa policy error-notification
    #exit
```

Sx Configuration

The following is an example of Sx configuration in UP.

```
sx-service SX-1
      instance-type userplane
      sxa max-retransmissions 4
      sxa retransmission-timeout-ms 5000
      sxb max-retransmissions 4
      sxb retransmission-timeout-ms 5000
      sxab max-retransmissions 4
      sxab retransmission-timeout-ms 5000
      n4 max-retransmissions 4
      n4 retransmission-timeout-ms 5000
      sx-protocol heartbeat interval 10
      sx-protocol heartbeat retransmission-timeout 5
      sx-protocol heartbeat max-retransmissions 4
```

```
      sx-protocol compression
    exit
```

Example SRP Configurations

IPSec ACL Configuration

The following is an example of IPSec ACL configuration for SRP.

```
ip access-list SRP
      permit tcp host 192.1.1.1 host 192.1.1.2
    #exit
```

SRP Configuration

The following is an example of SRP configuration.

```
configure
  context srp
    bfd-protocol
      bfd multihop-peer 192.1.1.1 interval 999 min_rx 999 multiplier 3
    #exit
configure
  context srp
    service-redundancy-protocol
      chassis-mode primary
      hello-interval 3
      dead-interval 15
      monitor bfd context srp 192.1.1.6 chassis-to-chassis
      monitor bgp context gi-pgw 192.1.1.7
      monitor bgp context gi-pgw 3333:888::1
      monitor bgp context saegw 192.1.1.7
      monitor bgp context saegw 3333:888::2
      peer-ip-address 192.1.1.6
      bind address 192.0.1.6
    #exit
    ip route static multihop bfd srp 192.0.1.7 192.1.1.7
    ip route 192.2.2.2 255.0.0.1 192.2.2.3 SRP-Physical-2102
    ip route 192.2.2.4 255.0.0.2 192.2.2.5 SRP-Physical-2102
    ip route 192.2.2.6 255.0.0.3 192.2.2.7 SRP-Physical-2102
    ip igmp profile default
    #exit
  #exit
end
```

Sample Configurations

In following sample configuration, the Sx and IPSec interface IP Addresses are defined as:

```
CP Sx - 20.0.0.101
UP Sx - 20.0.0.106
CP IPSec - 192.168.4.1
UP IPSec - 192.168.4.2
```

Note

- For this release, following are the recommended timer values on UP:

```
sx-protocol heartbeat retransmission-timeout 20
sx-protocol heartbeat max-retransmissions 3
```

- For this release, following are the recommended timer values on CP:

```
sx-protocol heartbeat retransmission-timeout 20
sx-protocol heartbeat max-retransmissions 5
```

On Control Plane

IPSec Configuration

```
config
  context EPC-CP
    ip access-list foo0
      permit ip host 20.0.0.101 host 20.0.0.106
    #exit
    ipsec transform-set A-foo
    #exit
    ikev2-ikesa transform-set ikesa-foo
    #exit
    crypto map foo0 ikev2-ipv4
      match address foo0
      authentication local pre-shared-key key secret
      authentication remote pre-shared-key key secret
      ikev2-ikesa max-retransmission 3
      ikev2-ikesa retransmission-timeout 15000
      ikev2-ikesa notify-msg-error no-apn-subscription backoff-timer 0
      ikev2-ikesa notify-msg-error network-failure backoff-timer 0
      ikev2-ikesa transform-set list ikesa-foo
      ikev2-ikesa configuration-attribute p-cscf-v6 private length 0
      ikev2-ikesa configuration-attribute p-cscf-v6 iana length 0
      keepalive interval 50
      payload foo-sa0 match ipv4
        ipsec transform-set list A-foo
        lifetime 300
        rekey keepalive
      #exit
      peer 192.168.4.2
      ikev2-ikesa policy error-notification
      notify-payload error-message-type ue base 0
      notify-payload error-message-type network-transient-minor base 0
      notify-payload error-message-type network-transient-major base 0
      notify-payload error-message-type network-permanent base 0
    #exit
    interface CP_IPSEC loopback
      ip address 192.168.4.1 255.255.255.255
   crypto-map foo0
    #exit
end
```

Sx Configuration

```
   sx-service SX-1
      instance-type controlplane
      bind ipv4-address 20.0.0.101
      sx-protocol heartbeat retransmission-timeout 20
      sx-protocol heartbeat max-retransmissions 5
   exit
```

On User Plane

IPSec Configuration

```
config
  context EPC-UP
    ip access-list foo0
      permit ip host 20.0.0.106 host 20.0.0.101
    #exit
    ipsec transform-set A-foo
    #exit
    ikev2-ikesa transform-set ikesa-foo
    #exit
    crypto map foo0 ikev2-ipv4
      match address foo0
      authentication local pre-shared-key key secret
      authentication remote pre-shared-key key secret
      ikev2-ikesa max-retransmission 3
      ikev2-ikesa retransmission-timeout 15000
      ikev2-ikesa notify-msg-error no-apn-subscription backoff-timer 0
      ikev2-ikesa notify-msg-error network-failure backoff-timer 0
      ikev2-ikesa transform-set list ikesa-foo
      ikev2-ikesa configuration-attribute p-cscf-v6 private length 0
      ikev2-ikesa configuration-attribute p-cscf-v6 iana length 0
      keepalive interval 50
      payload foo-sa0 match ipv4
        ipsec transform-set list A-foo
      #exit
      peer 192.168.4.1
      ikev2-ikesa policy error-notification
      notify-payload error-message-type ue base 0
      notify-payload error-message-type network-transient-minor base 0
      notify-payload error-message-type network-transient-major base 0
      notify-payload error-message-type network-permanent base 0
    #exit
    interface UP_IPSEC  loopback
      ip address 192.168.4.2 255.255.255.255
   crypto-map foo0
    #exit
end
```

Sx Configuration

```
   sx-service SX-1
      instance-type userplane
      bind ipv4-address 20.0.0.106 ipv6-address dddd:51:31:1:209::
      sxa max-retransmissions 12
      sxb max-retransmissions 12
      sxab max-retransmissions 12
      sx-protocol heartbeat interval 30
      sx-protocol heartbeat retransmission-timeout 20
      sx-protocol heartbeat max-retransmissions 3
    exit
```

Monitoring and Troubleshooting

This section contains sample CLI command output of show commands available for the Sx over IPSec feature in both CP and UP.

show crypto ikev2-ikesa security-associations summary

```
I - Initiator
  R - Responder
Mgr                                                                    Lifetime
ID  VPN Local IPSec GW:Port   Remote IPSec GW:Port  State             /Remaining
=== === ==================== ==================== ================ ===========
54  2   192.168.170.55 :500   192.168.196.55 :500   AUTH_COMPLETE(I) 86400/16448

1 IKEv2 Security Association found in this context.
```

show crypto ipsec security-associations summary

```
+------ SA state:           (E) - Established
      |                          (P) - Partially Established
      |                          (N) - No SAs
      |
      |+----- Rekey/Keepalive:    (D) - Rekey Disabled
      ||                          (E) - Rekey Enabled/No Keepalive
      ||                          (K) - Rekey Enabled/Keepalive
      ||
      ||+---- Crypto Type:        (D) - Dynamic Map
      |||                         (I) - IKEv1 Map
      |||                         (J) - IKEv2 Map
      |||                         (M) - Manual Map
      |||                         (C) - CSCF Map
      |||
      |||
      VVV           Map Name                                                 Rekeys En Pkts
    De Pkts
===== === ============================================================== ====== ==========
 ==========
1     EDJ foo0                                                              0      3496
     3496

1 Crypto Map Found.
1 Crypto Map Established.
```