Sx Load/Overload Control Handling

- Feature Summary and Revision History, on page 1
- Feature Description, on page 2
- How it Works, on page 2
- Handling Sx Messages during Peer Overload Scenario, on page 3
- Throttling and Exclusions of Sx Request Messages in Self-Overload State, on page 6
- Sx Load/Overload Control OAM Support, on page 7

Feature Summary and Revision History

Summary Data

Table 1: Summary Data

Applicable Product(s) or Functional Area	cnSGW-C
Applicable Platform(s)	SMI
Feature Default Setting	Disabled – Configuration required to enable
Related Documentation	Not Applicable

Revision History

Table 2: Revision History

Revision Details	Release
First introduced.	2021.01.0

Feature Description

This feature handles the load and overload control of messages over Sx interface. There are two scenarios of load and overload control for Sx messages:

- **Peer Overloaded:** When the peer is in overload state, Load control enables the user-plane function to send its load information to the control plane function. This load information is to balance the PFCP session load across the user-plane functions according to their effective loads.

  Overload controls the information for throttling of new session requests towards specific user-plane. UP selection takes place when the user-plane reports LCI (Load control information) and OCI (Overload Control Information).

- **Self-Overload State:** During self-protection state, upon receiving an incoming message, cnSGWc verifies the corresponding DNN, ARP, QCI, Message Priority values. Based on this, cnSGWc throttles the messages or excludes them from throttling as per the overload exclude profile configuration.

How it Works

The load and overload control over Sx interface consists of two parts:

- **Peer Overload Handling:** Handling the messages when UPF is overloaded.
- **Self Overload Handling:** Handling the messages when cnSGWc is overloaded.

Node Feature Support

As per 3GPP standard:

- CP informs load and overload feature to the user-plane.
- User-plane decides to send load or overload information towards the CP peer or not.

Configure load and overload feature at CP as a part of PFCP Sxa endpoint node feature. This configuration in turn communicates to UP during Sx Association Response message or Sx Association Update Request message when change in configuration occurs.

The CP Function Feature IE indicates the supported CP function features. This IE contains features which have (system-wide) UP function behavior impact.

Note If CP does not support load or overload feature through CLI then it ignores the user-plane reported load or overload information for the UP selection process.

UP Selection

UP selection occurs as per LCI value only whereas throttling occurs as per OCI value only (Specified in 3GPP standards).

Per Peer Level LCI and OCI display:

```
show peers | tab | exclude rest
                                                            POD
ENDPOINT  LOCAL ADDRESS  PEER ADDRESS  DIRECTION  INSTANCE  TYPE  CONNECTED TIME  RPC
ADDITIONAL DETAILS
-----------------------------------------------------------------------------------------
S5/S8  <nil>:2123  209.165.202.143:2123  Inbound  nodemgr-0  Udp  6 minutes   SGW  Recovery:
 10
SXA  209.165.200.226:8805  209.165.202.143:8805  Inbound  nodemgr-0  Udp  About a minute
SGW-U  Capacity: 65535,
LoadMetric: 20,LoadSeqNo: 1,OverloadMetric: 0,OverloadSeqNo: 0,Priority: 10
SXA  209.165.200.226:8805  209.165.202.147:8805  Inbound  nodemgr-0  Udp  2 minutes  SGW-U
  Capacity: 10,
LoadMetric: 40,LoadSeqNo: 1,OverloadMetric: 100,OverloadSeqNo: 1,Priority: 20
SXA  209.165.200.226:8805  209.165.202.159:8805  Inbound  nodemgr-0  Udp  2 minutes  SGW-U
  Capacity: 10,
LoadMetric: 100,LoadSeqNo: 1,OverloadMetric: 77,OverloadSeqNo: 1,Priority: 1
```

Handling Sx Messages during Peer Overload Scenario

This section discusses the mechanism of handling Sx messages when the peer node is in overload state.

Throttling Support for Sx Establishment

When user-plane is in overload situation, cnSGW-C establishes throttling the Sx Establishment request message toward user-plane. This throttling avoids new calls (Low priority or non-emergency) towards the overloaded user-plane.

Throttling takes place as per the reported OCI values in percentage. Following actions takes place when throttling happens:

- Random drop of percentage in reported Sx Establishment Request messages towards that user-plane.
- Call drop occurs at cnSGW-C with `sx_no_resource_available` disconnect reason.
- Respective statistics get incremented.

Session Termination Trigger From User-Plane in Self-Protection

User-plane triggers the session termination request towards cnSGW-C in pacing manner through Sx Report Request message. User-plane triggers session termination request when it is in self-protection mode and there is no improvement in load. This trigger happens with setting of SPTER (Self Protection Termination Request) bit.

cnSGW-C initiates Sx Termination Request for those PDNs and releases the PDN session with disconnect reason as `userplane_requested_termination`.

Failure-handling Profile Support for Congestion Cause

When the user-pane is in self-protection mode and rejects the new sessions with the cause `PFCP_ENTITY_IN_CONGESTION (74)`, cnSGW-C selects different user-plane as per the failure template profile configuration.

Failure-handling profile is associated with UPF-Group.

Reselection of UPF follows the UPF selection process and considers the retries count to different UPF from profile configuration.

Note Currently, only `PFCP_ENTITY_IN_CONGESTION(74)` is supported as cause code for retry and reselection of user-plane as part of this feature.

Configuring the Sx Load/Overload Feature

This section describes how to configure Sx Load/Overload.

Use the following commands to configure Sx Load/Overload configuration.

```
config
 instance instance-id instance_id
   endpoint endpoint_name
    interface interface_name
     supported-features [ load-control | overload-control ]
    exit
   exit
```

NOTES:

- **endpoint** *endpoint_name* - Specify the endpoint name.
- **interface** *interface_name* - Specify the interface name.
- **supported-features [load-control | overload-control]** - Enable load/overload control.

Sample Configuration

Following is a sample configuration.

```
configure
 instance instance-id 1
  endpoint pfcp
   interface sxa
    supported-features load-control overload-control
   exit
```

Verifying Sx Load/Overload Configuration

Use the following `show` command to view the Sx load/overload configuration.

```
show running-config instance instance-id 1 endpoint
instance instance-id 1
endpoint pfcp
interface sxa
supported-features load-control overload-control
exit
exit
```

Configuring Failure Handling Profile

This section describes how to configure failure handling profile.

Use the following commands to configure failure handling profile.

```
config
 profile failure-handling failure-handling_profile_name
   interface interface_name
    message message_type
      cause-code cause_code
        action action_type
          max-retry max_retry_count
      exit
    exit
   exit
 profile upf-group upf-group_profile_name
  failure-profile profile_name
 exit
```

NOTES:

- **profile failure-handling** *failure-handling_profile_name* - Specify the failure-handling profile name.
- **interface** *interface_name* - Specify the interface name.
- **message** *message_type* - Specify the message type.
- **cause-code** *cause_code* - Specify the cause ID (range of 2-255) or range of cause IDs (range of 2-255) separated by either '-' or ',' or both.

  -Or-

  Must be one of the following:

  - no-resource-available
  - no-response-received
  - pfcp-entity-in-congestion
  - reject
  - service-not-supported
  - system-failure

- **action** *action_type* - Specify the action type for the cause. Must be one of the following:
  - retry-terminate
  - terminate
- **max-retry** *max_retry_count* - Specify the maximum retry count for the retry-terminate action. Must be an integer in the range of 0-5. Default value is 1.
- **profile upf-group** *upf-group_profile_name* - Specify the UPF group profile name.
- **failure-profile** *profile_name* - Specify the UPF failure profile name.

Sample Configuration

Following is the sample configuration:

```
profile failure-handling fh1
 interface sxa
  message SessionEstablishmentReq
   cause-code pfcp-entity-in-congestion action terminate
  exit
 exit
exit
profile failure-handling fh2
 interface sxa
  message SessionEstablishmentReq
   cause-code 74 action retry-terminate max-retry 3
  exit
 exit
exit
profile upf-group g1
 failure-profile fh1
exit
profile upf-group g2
 failure-profile fh2
exit
```

Throttling and Exclusions of Sx Request Messages in Self-Overload State

Table 3: Feature History

Feature Name	Release Information	Description
Handling the Incoming Sx Messages at Self-overload State	2024.04.1	The load and overload control capability of cnSGWc is enhanced to handle the incoming Sx message during the self-overload state. This feature allows the cnSGWc to throttle the incoming DLDR session report request messages in the self-protection mode. **Default Setting:** Disabled- Configuration required to enable.

Throttling and Exclusion of Incoming Sx Request Messages

cnSGWc receives DDLR session report request messages from UPF whenever UPF receives any downlink for an idle session. When the cnSGWc is in the self-protection mode and if the overload exclude profile is configured, cnSGWc verifies the incoming DDLR session report messages for DNN, ARP, QCI, and message priority values.

To configure the overload exclude profile for the Sxa interface, see the Configure the Overload Exclude Profile section.

In case of a match or the session is identified as a WPS or an emergency session, cnSGWc processes the incoming DLDR session report request message, otherwise rejects it with **Cause 74 (PFCP Entity in Congestion)** and initiates an Internal DDN Self-protection Timer.

The Internal DDN Self-protection Timer works in the following way:

- If before Internal DDN Self-protection Timer expires, the cnSGWc moves out of the self-protection state, cnSGW sends the Downlink Data Notification message toward MME.
- If after Internal DDN Self-protection Timer expiry, the cnSGWc remains in the self-protection state, cnSGW sends the Sx Modification Request toward the UPFs with DROBU flag and Downlink FAR apply action as BUFFER.
- If the UE moves out of the idle state (MBReq received) before the DDN Self-protection Timer expires, then cnSGW stops the DDN Self Protection Timer and starts processing MBReq.

Note cnSGWc processes DLDR Session Report Request for emergency, WPS sessions, and Session Report Requests other than DLDR as usual in the self-protection mode.

Throttling and Exclusion of Outgoing Sx Request Messages

In the self-overload state, cnSGWc throttles the outgoing request messages on the Sxa interface from cnSGWc indirectly, as the throttling is applied on incoming GTPC interfaces. cnSGWc processes the messages that are excluded from throttling over the GTPC interface, over the Sxa interface as well.

Sx Load/Overload Control OAM Support

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

Bulk Statistics

UE Disconnect Statistics

```
sgw_ue_disconnect_stats{app_name="smf",cluster="cn",data_center="cn",instance_id=
"0",reason="sx_no_resource_available",service_name="sgw-service"} 1
```

```
sgw_ue_disconnect_stats{app_name="smf",cluster="cn",data_center="cn",instance_id=
"0",reason="userplane_requested_termination",service_name="sgw-service"} 1
```

PDN Disconnect Statistics

```
sgw_pdn_disconnect_stats{app_name="smf",cluster="cn",data_center="cn",instance_id=
"0",pdn_type="ipv4",rat_type="EUTRAN",reason="sx_no_resource_available",service_name="sgw-service"}
 1
```

```
sgw_pdn_disconnect_stats{app_name="smf",cluster="cn",data_center="cn",instance_id=
"0",pdn_type="ipv4v6",rat_type="EUTRAN",reason="userplane_requested_termination",service_name="sgw-service"}
 1
```

SGW Service Statistics

```
sgw_service_stats{app_name="smf",cluster="cn",data_center="cn",fail_reason="sx_oci_throttling_reject",
instance_id="0",interface="interface_sgw_ingress",reject_cause="no_resources_available",service_name=
"sgw-service",sgw_procedure_type="initial_attach",status="rejected",sub_fail_reason=""}
 1
```

```
sgw_service_stats{app_name="smf",cluster="cn",data_center="cn",fail_reason="",instance_id="0",
interface="interface_sgw_egress",reject_cause="",service_name="sgwservice",sgw_procedure_type=
"upf_initiated_deletion",status="attempted",sub_fail_reason=""} 1
```

```
sgw_service_stats{fail_reason="sx_cause_fail",interface="interface_sgw_ingress",reject_cause=
"service_denied",sub_fail_reason="pfcp_entity_in_congestion",sgw_procedure_type="initial_attach",
status="rejected"}
```

Session Report Request Throttling Statistics

A new status string **validation_failurePFCP_Entity_In_Congestion** is added in the existing statistics **sgw_sx_session_report_stats**. cnSGWc populates the session report statistics with this status value in case DLDR session report request is rejected in self-protection mode.

```
sgw_sx_session_report_stats{app_name="smf",cluster="Local",data_center="DC",gr_instance_id="1",
instance_id="0",reason="",service_name="sgw-service",status="validation_failurePFCP_Entity_In_Congestion",
sx_session_report_type="DLDR_NO_ARP"} 1
```