



Peer NF Failure Handling Support

- [Feature Summary and Revision History, on page 1](#)
- [Feature Description, on page 2](#)
- [Offline Failover Support for Charging, on page 2](#)
- [SMF Failover to Secondary PCF, on page 8](#)
- [Unified Data Management Failure Handling, on page 12](#)
- [UPF Failure Handling, on page 16](#)

Feature Summary and Revision History

Summary Data

Table 1: Summary Data

Applicable Products or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Disabled - Configuration Required
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 2: Revision History

Revision Details	Release
First introduced.	Pre-2020.02.0

Feature Description

The SMF uses the NRF Client profile configuration and the NRF failure profile configuration to achieve the NF failover support functionality. The SMF utilizes the failover support for all the NFs such as Charging Function (CHF), Policy Control Function (PCF), Unified Data Management (UDM), and User Plane Function (UPF).

The failure handling support provides the flexibility for the operator to take an action upon a failure, based on the message type and failure status code received.

This chapter describes how the SMF implements the failure handling functionality for CHF, PCF, UDM, and UPF.

Offline Failover Support for Charging

Feature Description

The SMF supports offline failover for charging when a CHF server fails. When the SMF continues after the CHF server failure, the SMF relays the offline charging services to the offline CHF server.

Failure Handling Profile contains the configurations that are invoked when a failure occurs. The Failure Handling feature supports the N11 and GTPC interfaces. With the dynamic configuration, you can change the dynamic attributes associated with the Failure Handling Profile while the SMF is running.

How it Works

The offline failover support for the charging feature works as follows.

Selecting a CHF Server

The CHF server selection involves the following steps:

1. The smf-service sends packets to rest-ep. The NF library of rest-ep attempts to search a CHF server through NRF discovery. This library receives a CHF server IP address or the list along with the priority as a search result.
2. The NF library selects the CHF server based on the priority from the list that is received through NRF discovery. If no CHF server is selected, NF library falls back to the static configuration that exists in the CHF network profile.

After selecting a CHF server or a list, NF library relays the message to the first CHF server according to the priority.

Handling a CHF Server Failure

The CHF server failure occurs when the selected CHF sends failure response or sends no response. For a CHF server failure, the NF library sends status code that is based on the failure template. This template is associated with the CHF network profile. The smf-service sends the profile information to smf-rest-ep while sending the IPC message.

The failure template is configured with the list of HTTP error codes and the associated failure actions and retry count, as required. Following are the failure actions as available in the feature template for this feature:

- **Retry and Continue**—For this failure action, NF library attempts until the configured number of times before fallback. After the configured number of times completes, the NF library falls back to the lower priority CHF server IP address. If the failure or no response is received from CHF server, the "continue" action is returned to the smf-service.
- **Terminate**—For this failure action, NF library does not attempt to send message to other CHF servers. The library sends a reply to smf-service with the action as "terminate". For the "terminate" failure action, the smf-service deletes the session.
- **Continue**—For this failure action, the smf-service continues the session and sends the charging message to the offline CHF server. This server is configured as part of the local static CHF profile that is meant for the offline purpose. In addition, the failure handling profile for offline CHF is configured.



Note For the "continue" failure action, you must configure the offline CHF server at SMF in a separate profile. SMF will use this profile after the CHF server failure. If the offline CHF server is not configured, the session is continued without imposing any charging.

Relaying to an Offline CHF Server

After CHF server failure, when the SMF continues, it converts the ongoing charging services as follows:

- Converts the services with both online and offline charging method to the offline charging method.
- Converts the services with online charging method to the offline charging method.
- Makes no change for the services with the offline charging method.

Failure Handling Profile

The Failure Handling Profile defines the various parameters for failure handling.

The following table lists the configurations that allow dynamic update.

Table 3: Failure Handling Profile Parameters

Configuration Parameters	Configuration	Dynamic Change	Impact on Existing Sessions
profile failure-handling	<p>profile failure-handling <i>name</i> interface <i>gtpc/n11</i> message <i>message</i> cause-code <i>cause_code</i> action <i>action</i> timeout <i>timeout</i> max-retry <i>retry_count</i></p> <p>Supported values:</p> <ul style="list-style-type: none"> • interface: gtpc or n11 • message: <ul style="list-style-type: none"> • gtpc-message: <ul style="list-style-type: none"> • S5S8CreateBearerReq • S5S8CreateBearerReq • S5S8CreateBearerReq • N11-message: n1n2transfer • cause-code: <ul style="list-style-type: none"> • gtpc-cause-code: temp-fail • N11-cause-code: temp-reject-handover/ temp-reject-register • action: retry/clear/terminate • timeout: Range: [1000-5000] (default: 1000) • max-retry: Range: [0-5] (default: 1) <p>Note</p> <ul style="list-style-type: none"> • The timeout and max-retry parameters are applicable only if the action is set to 'retry'. • The CLI supports only the 'retry' action. 	Allowed	Sessions that use the old value in a call flow and procedure continues to use the old value.

HTTP Cause Code Mapping with Failure Actions

Following table lists the mapping of failure actions with the associated HTTP cause code. Based on the network requirements, you can change the mapping.

Table 4: HTTP Cause Code Mapping with Failure Actions

Http-2 Cause Codes and Description		Converged CHF Failure Action			Offline CHF Failure Actions		
Code	Description	CDR-I	CDR-U	CDR-T	CDR-I	CDR-U	CDR-T
400	Bad Request	Terminate	No config	No config	Terminate	No config	No config
403	Forbidden	Terminate	No config	No config	Terminate	No config	No config
404	Not found	Terminate	No config	No config	Terminate	No config	No config
405	Method Not allowed	Retry and Continue	Retry and Continue	Retry and Continue	Terminate	No config	No config
408	Request Timeout	Retry and Continue	Retry and Continue	Retry and Continue	Terminate	Retry and Continue	Retry and Continue
500	Internal Server Error	Retry and Continue	Retry and Continue	Retry and Continue	Terminate	Retry and Continue	Retry and Continue
503	Service Unavailable	Retry and Continue	Retry and Continue	Retry and Continue	Terminate	Retry and Continue	Retry and Continue
508	Gateway Timeout	Retry and Continue	Retry and Continue	Retry and Continue	Terminate	Retry and Continue	Retry and Continue
0	No reply from server	Retry and Continue	Retry and Continue	Retry and Continue	Terminate	Retry and Continue	Retry and Continue

SMF Behaviour for Failure Actions

The following table describes the SMF behaviour on receiving different failures (Continue, Ignore, and Terminate) in CDR-(I/U/T).

CHF Failure Actions	Converged CHF			Offline CHF		
	CDR-I	CDR-U	CDR-T	CDR-I	CDR-U	CDR-T
Continue	Send CDR to offline CHF. If offline CHF is not configured, continue the session without charging.	Send CDR to offline CHF. If offline CHF is not configured, continue the session without charging.	Send CDR to offline CHF if offline CHF is configured	Continue the session without charging	Continue the session without charging	Continue the session deletion
Terminate	Delete the session	Delete the session	Continue the session deletion	Delete the session	Delete the session	Continue the session deletion

CHF Failure Actions	Converged CHF			Offline CHF		
	CDR-I	CDR-U	CDR-T	CDR-I	CDR-U	CDR-T
Ignore	Delete the session	No action taken. Record(s) will be reattempted in the next CDR request.	Continue the session deletion	Delete the session	No action taken. Record(s) will be reattempted in the next CDR request.	Continue the session deletion

Standards Compliance

The offline failover support for charging feature complies with the following standards:

- 3GPP TS 32.255
- 3GPP TS 32.290
- 3GPP TS 32.291

Limitations

The offline failover support for charging feature has the following limitations:

- Session Level Limits are mandatory from CHF or you must configure them locally. As per the 3GPP specification, the last linked URR cannot be removed when online URR needs to be delinked from the offline URR.

Configuring the Offline Failover Support for Charging

This section describes how to configure the offline failover support for charging feature.

Configuring the offline failover support for charging feature involves the following steps:

1. Configure failure handling profile in an NF library
2. Configuring an offline server client and an offline failure handling profile

Configuring Failure Handling Profile in an NF Library

This section describes how to configure the failure handling profile in an NF library.

Use this CLI configuration to configure the failure handling profile. You can configure HTTP status code with the corresponding action for the CHF create, update, or release messages. Based on the configuration of the failure handling profile, NF library takes an action when the CHF server failure occurs.

configure

```

profile nf-client-failure nf-type chf_name
  profile failure-handling profile_failure_handling_name
  service name type service_name_type
  message type message_type_value

```

```

status-code status_code_value
action failure_action_value
exit

```

NOTES:

- **profile nf-client-failure nf-type** *chf_name*—Enter the name of the network function that is required after the NF client failure.
- **profile failure-handling** *profile_failure_handling_name*—Enter the name of the profile for failure handling.
- **service name type** *service_name_type*—Enter the name of the service type.
service_name_type : nchf-convergedcharging
- **message type** *message_type_value*—Enter the value for type of message.*message_type_value* can be one of the following values:
 - ChfConvergedchargingCreate
 - ChfConvergedchargingUpdate
 - ChfConvergedchargingDelete
- **status-code** *status_code_value*—Enter the status code as per the configured failure template.
status_code_value can be one of the following values:
 - 500
 - 400
 - 404
- **action** *failure_action_value*—Enter the value for the failure action as per the configured failure template.
failure_action_value can be one of the following values:
 - continue
 - terminate
 - retry-and-continue
 - retry-and-terminate
 - retry-and-ignore

Configuring an Offline Server Client and an Offline Failure Handling Profile

This section describes how to configure the offline server client and offline failure handling profile.

Use this CLI to configure the offline client profile and offline failure handling profile for the selected CHF server.

configure

```

profile network-element chf chf_name
nf-client-profile nf_client_profile_name
failure-handling-profile failure_handling_profile_name

```

```

query-params [ dnn ]
nf-client-profile-offline nf_client_profile_offline_IP_port_number
failure-handling-profile-offline failure_handling_profile_offline_name
exit

```

NOTES:

- profile network-element chf – Enter the name of the CHF server.
- nf-client-profile – Enter the name of the client profile.
- failure-handling-profile – Enter the name of the failure handling profile.
- query-params – Enter the query parameter value, which is the data network name.
- nf-client-profile-offline – Enter the name of the offline client profile.
- failure-handling-profile-offline – Enter the name of the offline failure handling profile.

SMF Failover to Secondary PCF

Feature Description

The NF failover support is available in the SMF using the NRF Client profile configuration and the NRF failure profile configuration. The following functionality is supported:

- Configure multiple endpoints for a service as primary and secondary endpoints.
- Specify the failure behavior based on:
 - Message Type
 - HTTP Status Codes in the response messages

SMF Functionality

The SMF utilizes the NF Failover to achieve the PCF failover support functionality. This section covers working of SMF for message-level failures handling and the corresponding HTTP Status Code-based failure.

The SMF PCF failover supports the following messages that are initiated from the SMF.

- PcfSmpolicycontrolCreate
- PcfSmpolicycontrolUpdate
- PcfSmpolicycontrolDelete

During the PDU session lifecycle, the SMF exchanges the preceding messages at various stages with the PCF. Depending on the HTTP Status code configured in the NRF failure profile, the SMF receives one of the following actions:

- Ignore
- Continue

- Terminate

Table 5: Relationship between SMF PCF Failover Messages and Actions

	PcfSmpolicy controlCreate	PcfSmpolicy controlUpdate	PcfSmpolicy controlDelete
Ignore	Continue with locally configured/UDM-provided policy parameters. Note Do not contact PCF for subsequent messages. PCF-Interaction Status: OFF	Continue with ‘currently available snapshot’ of policy parameters. Contact PCF for subsequent messages. PCF-Interaction Status: ON	Current failure ignored. Session is deleted. PCF-Interaction Status: Session deleted
Continue	Continue with locally configured/UDM-provided policy parameters. Note Do not contact PCF for subsequent messages. PCF-Interaction Status: OFF	Continue with ‘currently available snapshot’ of policy parameters. Note Do not contact PCF for subsequent messages. PCF-Interaction Status: OFF	Current failure ignored. Session is deleted. PCF-Interaction Status: Session deleted
Terminate	Terminate the session.	Terminate the session.	Terminate the session.



Note The messages in [Table 5: Relationship between SMF PCF Failover Messages and Actions, on page 9](#) are SMF-initiated messages.

SMF PCF Failure Handling

• PCF-Interaction Status: ON

SMF-initiated messages: The SMF continues to initiate the messages towards the PCF whenever the criteria is met.

PCF-initiated messages: The SMF continues to accept all the messages initiated from the PCF towards the SMF.

• PCF-Interaction Status: OFF

SMF-initiated messages: The SMF does not initiate or send the messages towards the PCF whenever the criteria is met. The SMF treats the PCF as if it is not available and continues further actions.

PCF-initiated messages: There are two messages initiated by the PCF.

- SmPolicyUpdateNotifyReq: On receiving this message, the SMF sends a 404 error code in response and cleans up the session and does not send the Delete Request to the PCF.



Note The SMF also sends FIVEGSM_CAUSE value as **REACTIVATION REQUESTED** in the FIVEG_PDU_SESSION_RELEASE_COMMAND to UE for 5G. In case of 4G, the SMF sends cause **REACTIVATION REQUESTED** in DELETE BEARER REQUEST message to the S-GW.

- SmPolicyAssociationTerminationReq: On receiving this message, the SMF sends a success response and cleans up the session. As part of this interaction, the SMF sends a Delete Request to the PCF.



Note This is an exception when the PCF-Interaction Status is set to OFF.

Configuring SMF Failover to Secondary PCF Support

Use the following configuration to configure the PCF failure handling profile with action config:

```
profile nf-client-failure nf-type pcf
profile failure-handling FH1
service name type npcfsmpolicycontrol
message type PcfSmpolicycontrolCreate
status-code httpv2 0
action continue
```

Use the following configuration to configure the association of FH profile in the respective network element:

```
profile network-element pcf pcf1
nf-client-profile PP1
failure-handling-profile FH1
query-params [ dnn ]
rulebase-prefix cbn#
predefined-rule-prefix crn#
exit
```

Use the following configuration to configure secondary and tertiary IP addresses:

```
profile nf-client nf-type pcf
pcf-profile PP1
locality LOC1
priority 30
service name type npcfsmpolicycontrol
endpoint-profile EP1
capacity 30
uri-scheme http
endpoint-name EP1
priority 56
primary ip-address ipv4 primaryipaddress
primary ip-address port 8098
secondary ip-address ipv4 secondaryipaddress
```

```
secondary ip-address port 9098
end
```

Statistics

The following statistics are added in support of SMF Failover to Secondary PCF feature.

- PcfSmpolicyControlCreate
 - Number of ignore responses
 - Number of continue responses
 - Number of terminate responses
- PcfSmPolicyControlUpdate
 - Number of ignore responses
 - Number of continue responses
 - Number of terminate responses
- PcfSmpolicyControlDelete
 - Number of ignore responses
 - Number of continue responses
 - Number of terminate responses
- PolicyUpdateNotifyReq
 - Number of accepted requests
 - Number of rejected requests
 - Number of skipped requests
- PolicyDeleteReq
 - Number of accepted requests
 - Number of rejected requests
 - Number of skipped requests
- PolicyUpdateRequest
 - Number of accepted requests
 - Number of rejected requests
 - Number of skipped requests
- Gauge counter for number of subscribers with policy type local/pcf.

Unified Data Management Failure Handling

Feature Description

The Unified Data Management (UDM) is responsible for primarily storing the subscriber data, which SMF accesses for managing the user sessions on the network.

The UDM failure handling support on SMF introduces a new failure handling template (FHT) profile. This profile is associated with the UDM profile in SMF.

The FHT template provides flexibility for SMF to fine tune its interactions with UDM over N10 for the sessions. It supports the SMF to handle the HTTP status codes in response from UDM for both new and existing sessions.

The NF failover support is available in the SMF using the NRF Client profile configuration and the NRF failure profile configuration. The following functionality is supported:

- Configure multiple endpoints for a service as primary and secondary endpoints.
- Specify the failure handling behavior based on:
 - Message Type
 - HTTP Status Codes in the response messages

How it Works

The SMF utilizes the NF Failover to achieve the UDM failover support functionality. This section provides information on how the SMF handles message-level failures and the corresponding HTTP status code-based failures.

The UDM failover supports the following messages that are initiated from the SMF.

- UE-Connection-Management (UE-CM)
 - Nudm_UECM_Registration
 - Nudm_UECM_DeRegistration
- UE-Subscription-Management (UE-SDM)
 - Nudm_SDM_Get
 - Nudm_SDM_Subscribe
 - Nudm_SDM_Unsubscribe

During the PDU session lifecycle, the SMF exchanges the preceding messages at various stages with the UDM. Depending on the HTTP status code configured in the NRF failure profile, the SMF performs one of the following actions:

- Ignore
- Continue

- Terminate

The SMF provides the following actions to attempt the same request to other available UDM servers.

- retry-and-terminate
- retry-and-ignore
- retry-and-continue

When all the retry attempts fail, the SMF takes the appropriate failure handling action. For example, if the FH action is retry-and-terminate, the SMF terminates the call after all the attempts fail.



Note The SMF allows dynamic changes to the failure handling template configuration. Any changes to the configuration apply only to the new calls.

Table 6: Relationship between N10 Messages and Failover Actions

Scenario	Service	Message	Condition	Action	Success Response	Handling of Failure Response		
						Terminate	Continue	Ignore
PDU Session Creation procedures in 5G, 4G, WiFi Inter-RAT Handover procedures	UECM	Nudm_UECM_Registration	If the Nudm UECM Registration is not done and the access type is not 4G	Send the message	Mark the Registration is successful	Terminate call	Continue call	Continue call
		Nudm_UECM_DeRegistration	If the Nudm UECM Registration is done	Send the message	No action	Terminate call	Terminate call	Terminate call
PDU Session Creation procedures in 5G, 4G, WiFi	SDM	Nudm_SDM_Get	If skipping the subscription fetch config is not enabled	Send the message	Mark the subscription fetch is successful	Terminate call	Continue call	Continue call
		Nudm_SDM_Subscribe	If the subscription fetch is successful	Send the message	No action	Terminate call	Continue call if the subscription is not done	Continue call if the subscription is not done

Scenario	Service	Message	Condition	Action	Success Response	Handling of Failure Response		
						Terminate	Continue	Ignore
PDU Session Release procedures in 5G, 4G, WiFi	SDM	Nudm_SDM _Unsubscribe	If the subscription fetch is successful and the registration isns	Send the message	No action	Terminate call	Continue call	Continue call

**Note**

- **Terminate:** The SMF terminates the call in any message type.
- **Continue:** The SMF ignores the current failure and skips the subsequent interaction for the other messages in the same service group.
- **Ignore:** The SMF ignores failure only for the current interaction and proceeds with the call. The SMF processes the subsequent message interaction.
- Perform UDM subscription fetch only during the session establishment in EPS and NR network.
If the UDM subscription fetch fails and the FH action is 'Ignore' or the configuration to skip subscribe-to-notification is enabled, then the SMF skips the subscribe-to-notification interaction.
- When the UDM failure handling template is not configured, the default failure handling action is 'Terminate'.

Configuring UDM Failure Handling Support

Use the following configuration to configure the UDM failure handling profile with action config:

```

config
  profile nf-client-failure nf-type udm
  profile failure-handling fh_profile_name
    service name type { nudm-ee | nudm-pp | nudm-sdm | nudm-ueau
    | nudm-uecm }
    message type { UdmRegistrationReq | UdmSdmGetUESMSSubscriptionData
    | UdmSdmSubscribeToNotification | UdmSubscriptionReq
    | UdmUecmRegisterSMF | UdmUecmUnregisterSMF |
    UdmSdmUnsubscribeToNotification }
    status-code httpv2 0
    action { continue | retry-and-continue | retry-and-ignore
    | retry-and-terminate | terminate }
  end

```

Use the following configuration to configure the association of FH profile in the respective network element:

```

config

```

```

profile network-element udm udmprofile_name
  nf-client-profile profile_name
  failure-handling-profile fh_profile_name
  query-params [ dnn ]
  rulebase-prefix cbn#
  predefined-rule-prefix crn#
  exit

```

Use the following configuration to configure secondary and tertiary IP addresses:

```

config
  profile nf-client nf-type udm
    udm-profile udmprofile_name
    locality LOC
    priority priority_value
    service name type { nudm-ee | nudm-pp | nudm-sdm |
      nudm-ueau | nudm-uecm }
    endpoint-profile epprofile_name
    capacity capacity_value
    uri-scheme http
    endpoint-name endpoint_name
    priority priority_value
    primary ip-address ipv4 primary_ipaddress
    primary ip-address port port_num
    secondary ip-address ipv4 secondary_ipaddress
    secondary ip-address port port_num
  end

```

OAM Support

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

Statistics Support

The SMF maintains the following statistics in support of the UDM Failure Handling feature.

- Nudm_UECM_Registration
 - Number of ignore responses
 - Number of continue responses
 - Number of terminate responses
- Nudm_UECM_DeRegistration
 - Number of ignore responses
 - Number of continue responses
 - Number of terminate responses
- Nudm_SDM_Get
 - Number of ignore responses

- Number of continue responses
- Number of terminate responses
- Nudm_SDM_Subscribe
 - Number of ignore responses
 - Number of continue responses
 - Number of terminate responses
- Nudm_SDM_Unsubscribe
 - Number of ignore responses
 - Number of continue responses
 - Number of terminate responses

UPF Failure Handling

Feature Description

During a session, if the User Plane function (UPF) is in congested state, it rejects the Packet Forwarding Control Protocol (PFCP) establishment messages from SMF with a cause code in the response message. To reduce the call loss, SMF retries to send PFCP establishment messages to a different UPF. Then, SMF selects a UPF based on priority (configuration) and capacity (load information from UPF).

The UPF failure handling support on N4 interface feature in SMF introduces a new failure handling template (FHT) profile for PFCP. This profile is associated with the UPF profile in SMF (in network elements).

The FHT template provides flexibility for SMF to fine tune its interactions with UPFs for sessions. It supports SMF to handle the error cause codes in response from UPF for both new and existing sessions. Based on the error cause codes in response from UPF, this feature provides the following configurable actions:

- terminate
- retry-terminate

Configuring the UPF Failure Handling on N4 Interface

This section describes how to configure the UPF failure handling on N4 interface feature.

```
configure
  profile failure-handling pcfp_name
    interface pfcpc message N4SessionEstablishmentReq
      cause-code pfcpc-entity-in-congestion
      action retry-terminate max-retry value
    end
```

NOTES:

- **profile failure-handling**: Specifies the UPF profile that is associated with FHT.
- **interface pfc message {N4SessionEstablishmentReq | N4SessionModificationReq}**: Specifies the failure handling for N4SessionEstablishmentReq (for new sessions) and N4SessionModificationReq messages (for existing sessions).



Note UPF reselection is not applicable for message type N4SessionModificationReq because the session is already active on a UPF.

- **cause-code {pfc-entity-in-congestion | mandatory-ie-incorrect | mandatory-ie-missing | session-ctx-not-found | system-failure | service-not-supported | no-resource-available | no-response-received | reject}**: Specifies the error codes that SMF receives in the failure response message from UPF.



Note

- The **no-response-received** cause code is introduced in this feature to identify the scenarios where SMF does not receive any response from UPF.
- FHT does not support the following cause codes, which are configured with their default behaviour:
request-reject-undefined, cond-ie-missing, invalid-length, invalid-fw-policy, invalid-ftaid-alloc-opt, no-established-pfc-assoc, rule-creation-mod-failure.

- **pfc-entity-in-congestion**: Specifies the cause code when UPF is congested.
- **reject**: Specifies the option to handle the cause codes in the failure response message from UPF, which are not configured by using the CLI commands available for this feature.
- **action {retry-terminate | terminate}**: Specifies the action to perform based on the error cause code received in the failure response message from UPF.
 - **retry-terminate**: Specifies a retry attempt to an alternate UPF. If the retry attempt fails, the session is terminated.



Note If all UPFs are in congested state, call fails even if the action is set to **continue**.

- **max-retry**: Specifies the number of retry attempts to reselect an alternate UPF.
 - **Default value**: 2
 - **Maximum value**: 5

Configuring the Failure Profile Association

This section describes how to configure the failure profile association in this feature.

```

configure
  profile upf-group upf upf_group_name
    failure-profile pfcpl pfcpl_name
  end

```

NOTES:

- **profile upf-group upf**: Specifies the UPF group.
- **failure-profile**: Specifies the FHT profile for PFCP.

Configuration Matrix

This section describes the configuration options available for N4 Session Establishment Request and N4 Session Modification Request messages in this feature.

Message Type	Applicable Action	Applicable Cause Code	Default Behaviour
N4SessionEstablishmentReq	retry-terminate	<ul style="list-style-type: none"> • pfcpl-entity-in-congestion • system-failure • service-not-supported • no-resource-available • no-response-received 	terminate
N4SessionModificationReq	terminate	<ul style="list-style-type: none"> • mandatory-ie-incorrect • session-ctx-not-found • no-response-received 	continue

Monitoring and Troubleshooting

This section describes the show command that is supported by the UPF failure handling on N4 interface feature.

show running-config

Use the show **running-config** command to view the configuration.

The following configuration is a sample output of the show running-config command:

```

profile network-element upf upf1
  pfcpl pfcpl-failure-profile pfcpl
node-id      n4-peer-upf1
n4-peer-address ipv4 1.1.1.1
n4-peer-port 0000
keepalive    60
  dnn-list   [ uncarrier.5g ]
capacity     10
priority     1
exit
profile failure-handling pfcpl
  interface pfcpl message N4SessionEstablishmentReq

```

```
cause-code pfcpc-entity-in-congestion
  action retry-terminate max-retry 2
exit
interface pfcpc message N4SessionModificationReq
  cause-code mandatory-ie-incorrect
  action terminate
exit
exit
exit
```

