Session Timers

Feature Summary and Revision History

Summary Data

Table 1: Summary Data

Applicable Product(s) 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
Added support for session setup timer and back-off timer.	2021.02.0
First introduced.	2020.02.0

Feature Description

This chapter provides detailed information about the function, operation, and configuration of the timers.

The SMF supports configurable timers that are either session timers or non 3GPP session imers.

- Non 3GPP session timers
  - Absolute timer
  - Control Plane Inactive timer
  - User Plane Inactive timer
  - Session Setup timer
- 3GPP session timers
  - GTP timer
  - N11 timer
  - Back-off timer
  - Default Flow Only timer
  - EPS Fallback Guard timer
  - Indirect Data Forwarding Tunnel timer
  - Dedicated Bearer Delay and Retry timer
  - Dedicated Bearer Procedure Failure Handling timer
  - Procedure SLA timer
  - Dynamic Configuration Change Support timer
  - IPAM Quarantine timer
  - Provisioning of Policy Revalidation timer
  - Router Advertisement Parameters timer

For details on timers other than GTP and N11, see the following sections:

- Configuring Default Flow Only Timer in DNN Profile
- EPS Fallback Guard Timer Support
- Indirect Data Forwarding Tunnel (IDFT) Timer Support
- Create Dedicated Bearer Delay and Retry Support
- Handling Dedicated Bearer Procedure Failures Caused by Timer Expiry
- Dynamic Configuration Change Support
- IPAM Quarantine Timer

3GPP-Compliant Timers

GTP and N11 Timers

Feature Description

The SMF supports retransmission through the GTP and N11 timers. With this provision, when the peer does not respond with the timer value, the SMF retransmits the GTP and N11 requests. You can configure the maximum number of retransmissions through SMF.

How it Works

The SMF supports the following 3GPP timers:

GTP Retransmission Timer

The SMF or PGW-C starts the timer denoted in the T3-RESPONSE. The timer is invoked when a signalling message, for which a reply is expected, is sent. A signalling message or the triggered message may be lost if a response is not received before the T3-RESPONSE timer expires.

After the T3-RESPONSE timer expires, the message corresponding to the T3-RESPONSE timer is then retransmitted if the total number of retry attempts is less than N3REQUESTS.

5G N1N2 Reattempt Timer

If AMF rejects the N1N2 MessageTransfer with cause code as "Temporary reject registration ongoing" or "Temporary reject handover ongoing", then the SMF starts the timer for reattempting N1N2 MessageTransfer.

After the timer expires, the message corresponding to N1N2 MessageTransfer is reattempted based on the configured retry attempts.

Standards Compliance

The 3GPP timers support feature complies with the following standards:

• *3GPP TS 29.510 V15.2.0 (2018-12)—5G; 5G System; Network function repository services; Stage 3*

Configuring the N11 and GTP Timers

This section describes how to configure the 3GPP-compliant timers—N11 and GTP timers.

Configuring the N11 Timers

The N11 timer configuration is invoked when AMF rejects the N1N2 message transfer with the "Temporary reject registration ongoing" or "Temporary reject handover ongoing" cause code. Then, SMF considers the timer and reattempts the message transfer. When the timer expires, the transfer is reattempted based on the configured retry count.

To configure an N11 timer, use the following sample configuration:

```
config
  profile failure-handling failure_handling_name
    interface [ gtpc | N11 ] message message_type
      cause-code [ temp-reject-register | temp-reject-handover ]
        action [ retry { timeout timeout_duration |
        max-retry retry_count } | clear | terminate ]
        end
```

NOTES:

- **profile failure-handling** *failure_handling_name*—Enter the name of the profile for failure handling.
- **interface [gtpc | N11]** —Configure the interface over which the message transfer must happen.
- **message** *message_type*—Configure the message type to be transferred over the interface. The N11 interface supports the message type as N1N2Transfer.
- **cause-code [temp-reject-register | temp-reject-handover]** —Configure the HTTP cause code. You can configure multiple cause code values for a message.
- **action [retry | clear | terminate]**—Configure the action to perform when the message transfer is not successful.
- **action [retry { max-retry** *retry_count* **| timeout** *timeout_duration* **}** —Specify the number of times the message transfer must be reattempted and the time interval between the consecutive attempts.

Example Configuration

Following is an example of N11 timer configuration.

```
show running-config
profile failure-handling n11-fht
  interface n11 message n1n2transfer
    cause-code temp-reject-register
     action retry
       timeout 1000
         max-retry 2
```

Configuring the GTP Timers

The GTP timer configuration is implemented when a signaling message or triggered message, for which a reply is expected, is lost as it did not get a response before the T3-RESPONSE timer expired. After the T3-RESPONSE timer expires, the message corresponding to the T3-RESPONSE timer is retransmitted if the total number of retry attempts is less than the N3-REQUESTS times.

To configure a GTP timer, use the following sample configuration:

```
config
   instance instance-id gr_instance_id
      endpoint gtp
         retransmission { max-retry retry_count | timeout timeout_duration }
         end
```

NOTES:

- **endpoint gtp**—Enter the GTP retransmission configuration.

- **max-retry** *retry_count*—Specify the number of times the signalling message request to SMF must be reattempted. The accepted range is 0–5. Default range is 3. When the *retry_count* is set to "0", the retransmission feature is disabled.
- **timeout** *timeout_duration*—Configure the interval of time (in milliseconds) after which the GTP retransmission request is reattempted. The accepted range is 0–10. Default range is 2. When the *timeout_duration* is set to "0", the retransmission feature is disabled.

Example Configuration

Following is an example of GTP timer configuration.

```
show running-config
instance instance-id 1
  endpoint gtp
   retransmission max-retry 2 timeout 5
```

Back-off Timer Support

Feature Description

The SMF supports configurable back-off timer to inform the UE to wait with a re-registration and new connection attempt after a network-initiated release. This timer helps to recover the system from failure.

The SMF sends the configured back-off timer value to AMF in the following scenarios:

- N4 path failure during a UPF switchover
- IP address exhaustion

Important These scenarios are currently supported only in home-routed roaming and non-roaming sessions.

The SMF sends the back-off timer value to S-GW only during the exhaustion of IP address.

Note The back-off timer support is applicable only for the 4G non-roaming sessions and 5G roaming and non-roaming sessions.

If the SMF detects that the UPF is inactive, it includes a back-off timer and cause value in PDU Session Release Command message sent over N1. Then, SMF clears the PDU session.

When the IP addresses get exhausted while initiating the 4G attach, the PGW-C includes the back-off timer IE and cause value in Create Session Response message.

In case of IP address exhaustion during 5G attach, the SMF includes the back-off timer IE and cause value in PDU Session Establishment Reject message sent over N1.

How it Works

The SMF provides an option to configure back-off timer value with failure condition and Cause value. For configuration details, see the Configuring Back-off Timer, on page 12 section in this guide.

The SMF detects if the UPF is down due to N4 path failure. If the UPF is down, SMF includes the configured back-off timer value and cause value in the N1 PDU Session Release Command while clearing PDU session.

In home-routed roaming scenario, vSMF includes the back-off timer and cause value in PDU Session Release Command message sent over N1 when any of the following conditions are met:

- hSMF detects that the hUPF is inactive due to path failure.
- vSMF detects that the vUPF is inactive due to path failure.

If the SMF or PGW-C detects that the IP addresses are exhausted, SMF includes the back-off timer and cause value in the N1 PDU Session Establishment Reject message or Create Session Response depending on the RAT type.

In the roaming scenario, if the hSMF detects that the IP addresses are exhausted, it sends PDU Session Create Error to vSMF with the back-off timer and cause values. Based on this value, vSMF includes the back-off timer and Cause value in N1 PDU Session Establishment Reject message.

Note Encoding of back-off timer in PDU Release Command and PDU Establishment Reject is as defined in *3GPP TS 24.008—Mobile radio interface Layer 3 specification; Core network protocols; Stage 3*.

Encoding of back-off timer in Create Session Response is as defined in *3GPP TS 29.274—3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service (GPRS) Tunnelling Protocol for Control plane (GTPv2-C); Stage 3*.

Call Flows

This section provides the call flows for this feature.

N4 Path Failure Handling Call Flow

This section describes how the SMF handles the N4 path failures observed in non-roaming and roaming scenarios.

Handling of N4 Path Failures in Non-roaming Session

The following figure illustrates the N4 path failure handling call flow for a non-roaming session.

Figure 1: N4 Path Failure Handling Call Flow for Non-roaming Session

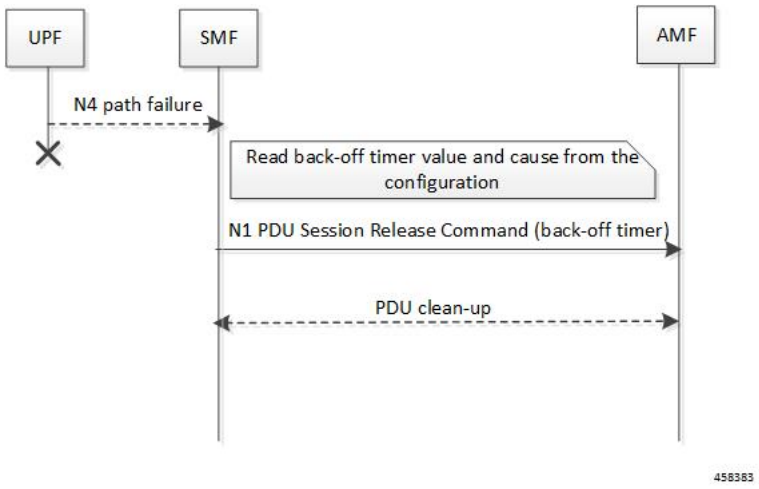

Table 3: N4 Path Failure Handling Call Flow Description for Non-roaming Session

Step	Description
1	The SMF checks if the UPF is inactive due to N4 path failure.
2	If the SMF detects that the UPF is inactive, it fetches the back-off timer and cause value from the DNN profile configuration. The SMF sends the timer and cause value in the N1 PDU Session Release Command to AMF. Then, the SMF performs the PDU clean up.

Handling of N4 Path Failures in vUPF During Roaming Session

The following figure illustrates the call flow of handling N4 path failures in vUPF during the roaming session.

Figure 2: vUPF Path Failure Handling Call Flow for Roaming Session

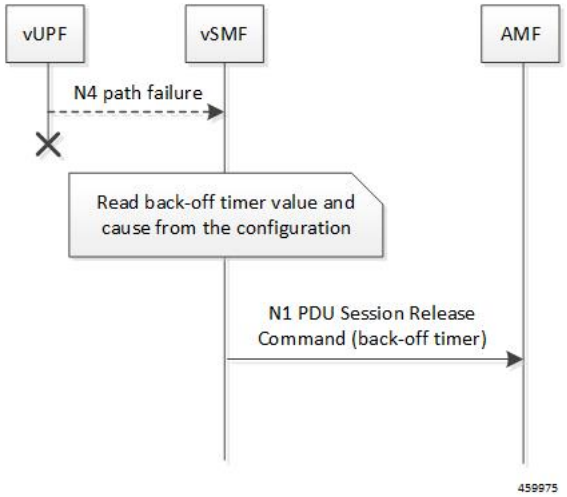

Table 4: vUPF Path Failure Handling Call Flow Description for Roaming Session

Step	Description
1	The vSMF checks if the vUPF is inactive due to N4 path failure.
2	If the vSMF detects that the vUPF is inactive, it fetches the back-off timer value and cause from the DNN profile configuration. The vSMF sends the timer and cause value in the N1 PDU Session Release Command to AMF. Then, the vSMF performs the PDU clean up.

Handling of N4 Path Failures in hUPF During Roaming Session

The following figure illustrates the call flow of handling N4 path failures in hUPF during the roaming session.

Figure 3: hUPF Path Failure Handling Call Flow for Roaming Session

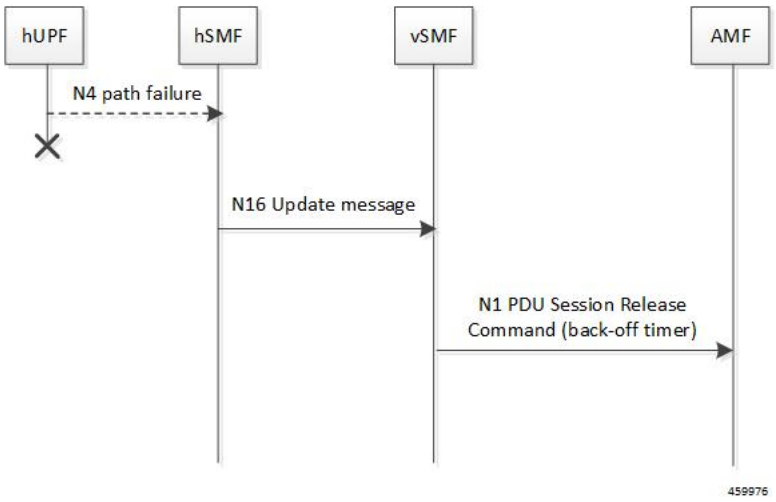

Table 5: hUPF Path Failure Handling Call Flow Description for Roaming Session

Step	Description
1	The hSMF checks if the hUPF is inactive due to N4 path failure.
2	If the hUPF is inactive, hSMF sends the back-off timer and cause to vSMF through the N16 update request.
3	The vSMF includes the back-off timer and cause value in N1 PDU Session Release Command message.

IP Address Exhaustion Handling Call Flow for 5G Sessions

This section describes how the SMF handles the IP address exhaustion condition in 5G sessions.

Handling of IP Address Exhaustion in 5G Non-roaming Sessions

The following figure illustrates the IP address exhaustion handling call flow for 5G non-roaming sessions.

Figure 4: IP Address Exhaustion Handling Call Flow for 5G Non-roaming Sessions

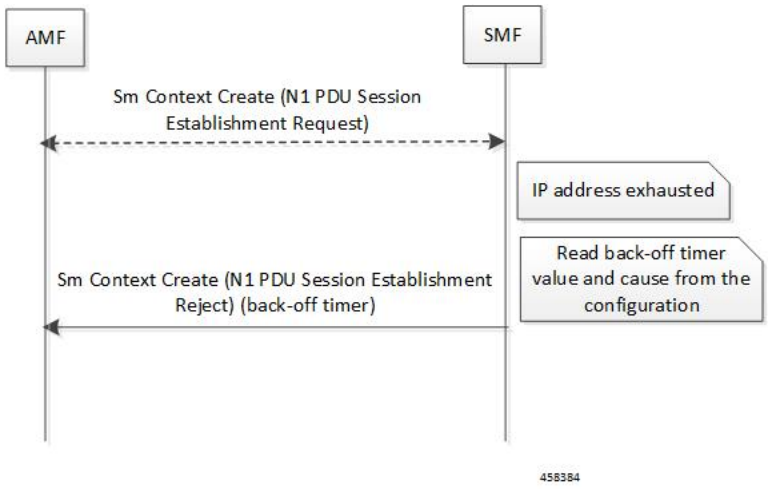

Table 6: IP Address Exhaustion Handling Call Flow Description for 5G Non-roaming Sessions

Step	Description
1	AMF sends the SM Context Create message for the N1 PDU Session Establishment Request to SMF.
2	Upon detecting the exhaustion of IP address in a 5G non-roaming call, the SMF reads the configured back-off timer and cause value. Then, SMF sends this timer and cause value in the N1 PDU Session Establishment Reject message to AMF.

Handling of IP Address Exhaustion in 5G Roaming Sessions

The following figure illustrates the IP address exhaustion handling call flow for 5G roaming sessions.

Figure 5: IP Address Exhaustion Handling Call Flow for 5G Roaming Sessions

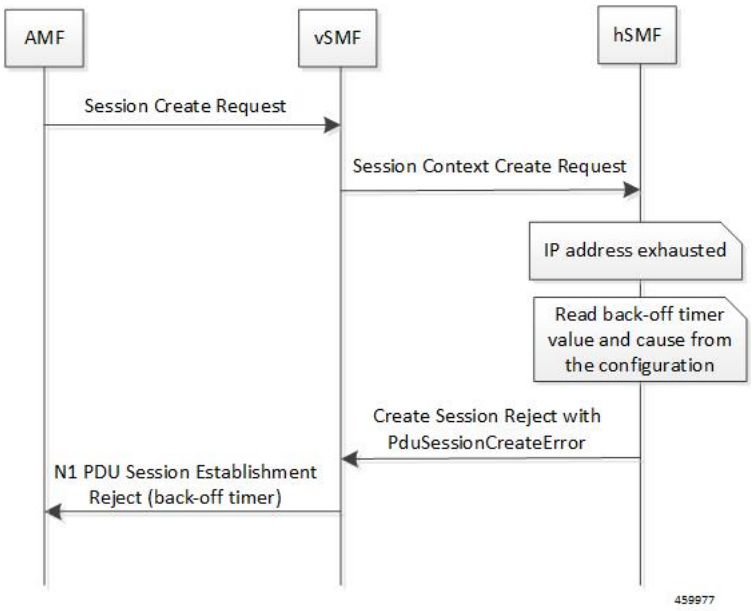

Table 7: IP Address Exhaustion Handling Call Flow Description for 5G Roaming Sessions

Step	Description
1	The AMF sends the SM Context Create message for the N1 PDU Session Establishment Request to vSMF.
2	The vSMF sends Session Context Create Request message to the hSMF.
3	If hSMF detects that the IP addresses are exhausted, it sends PduSessionCreateError to the vSMF with back-off timer and cause value based on configuration on hSMF. Based on this value, the vSMF includes the back-off timer and cause value in N1 PDU Session Establishment Reject message.

IP Address Exhaustion Handling Call Flow for 4G Sessions

This section describes how the SMF handles the IP address exhaustion condition in a 4G session.

The following figure illustrates the IP address exhaustion handling call flow for 4G sessions.

Figure 6: IP Address Exhaustion Handling Call Flow for 4G Sessions

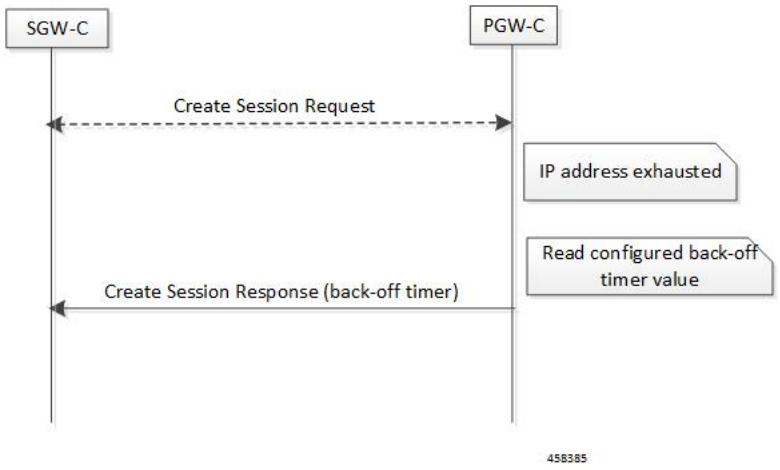

Table 8: IP Address Exhaustion Handling Call Flow Description for 4G Sessions

Step	Description
1	SGW-C sends the Create Session Request to PGW-C.
2	Upon detecting the exhaustion of IP address in a 4G call, the PGW-C reads the configured back-off timer value and cause. Then, PGW-C sends this timer value and cause in the Create Session Response message to SGW-C.

Limitations

This feature has the following limitation:

- Back-off timer triggering is not supported while clearing 4G PDN sessions as the 3GPP 29.274 specification does not support back-off timer IE in Delete Bearer Request message.

Note The preceding limitation is applicable only to the non-roaming scenarios.

Standards Compliance

The Back-off Timer Support feature complies with the following standards:

- *3GPP 29.274, version 15.9.0, Release 15—Universal Mobile Telecommunications System (UMTS); LTE; 3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service (GPRS) Tunnelling Protocol for Control plane (GTPv2-C); Stage 3*
- *3GPP 24.008, version 15.9.0, Release 15—Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; 5G; Mobile radio interface Layer 3 specification; Core network protocols; Stage 3*
- *3GPP 24.501, version 15.6.0, Release 15—5G; Non-Access Stratum (NAS) protocol for 5G System (5GS); Stage 3*

- *3GPP TS 29.502, version 15.6.0, Release 15—5G; Session Management Services; Stage 3*

Configuring Back-off Timer

This section describes how to configure the back-off timer.

Configuring the back-off timer involves the following steps:

- Configuring Back-off and Jitter Timers in DNN Profile, on page 12
- Enabling Message-level Back-off Timer, on page 12

Note This feature works only when both the back-off timer and cause are configured. The back-off timer configuration remains the same for both the non-roaming and roaming calls.

Configuring Back-off and Jitter Timers in DNN Profile

To define values for the back-off and jitter timers in DNN profile, use the following sample configuration:

```
config
   profile dnn dnn_profile_name
      timeout backoff backoff_timer_value
      timeout jitter jitter_timer_value
      end
```

NOTES:

- **timeout backoff** *backoff_timer_value*: Specify the back-off timer value, in seconds. *backoff_timer_value* must be an integer in the range of 0-576000.

  The back-off timer is the maximum allowed duration used during IP exhaustion and N4 path failure cases.

- **timeout jitter** *jitter_timer_value*: Specify a jitter value to introduce randomness in the back-off timer value. *jitter_timer_value* must be an integer in the range of 0-1000.

  The jitter allows spreading the different backoff timers to the UE devices so that they all wait at different times before the next reconnection attempt.

  This configuration helps to prevent a session storm after the back-off timer expiry.

The following is an example configuration used during N4 path failure scenarios.

```
config
   profile dnn test
      timeout backoff 200 jitter 50
      end
```

Enabling Message-level Back-off Timer

Use the following sample configuration to enable the back-off timer at the GTP-C and N1 message levels.

```
config
   profile access access_profile_name
      gtpc message-handling create-session-response condition ip-exhaust
```

```
 action backoff cause cause_code_value
     n1 message-handling pdu-session-release condition n4-pathfail action
 backoff cause cause_code_value
      n1 message-handling pdu-session-establishment condition ip-exhaust
 action backoff cause cause_code_value
      end
```

NOTES:

- **gtpc message-handling create-session-response condition ip-exhaust action backoff cause** *cause_code_value*: Use this command to enable back-off timer at the GTP-C interface level for the Create Session Response (CSR) message. That is, the CSR message includes the Back-off Timer IE and its cause code during the exhaustion of IP address.
- **n1 message-handling pdu-session-release condition n4-pathfail action backoff cause** *cause_code_value*: Use this command to enable back-off timer at the N1 interface level for the PDU Session Release message. That is, the PDU Session Release message includes the Back-off Timer IE and its cause code when the N4 path failure occurs.
- **n1 message-handling pdu-session-establishment condition ip-exhaust action backoff cause** *cause_code_value*: Use this command to enable back-off timer at the N1 interface level for the PDU Session Establishment message. That is, the PDU Session Establishment message includes the Back-off Timer IE and its cause code during the exhaustion of IP address.

The following is an example configuration used during the 4G attach and the exhaustion of IP addresses.

```
config
   profile access access1
      gtpc message-handling create-session-response condition ip-exhaust
 action backoff cause 73
      end
```

In this scenario, the attach fails and the CSR is sent with Back-off Timer IE and cause 73.

The following is an example configuration used during the 5G attach and the exhaustion of IP addresses.

```
config
   profile access access1
      n1 message-handling pdu-establishment condition ip-exhaust action
backoff cause 26
      end
```

In this scenario, the attach fails and the PDU Session Establishment is sent with Back-off Timer and cause code value set to 26.

The following is an example configuration used during the 5G attach and the N4 path failure scenario.

```
config
   profile access access1
     n1 message-handling pdu-session-release condition n4-pathfail action
 backoff cause 26
      end
```

In this scenario, clear subscriber is triggered internally and PDU Session Release command is sent with Back-off Timer IE and cause 26.

Verifying the Back-off Timer Configuration

This section describes how to verify the back-off timer configuration.

Use the **show running-config** command to verify the feature configuration.

The following is an example output of the **show running-config profile access access1** command.

```
[unknown] smf# show running-config profile access access1
profile access access1
n1 message-handling pdu-establishment condition ip-exhaust action backoff cause 26
n1 message-handling pdu-release condition n4-pathfail action backoff cause 26
n26 idft enable timeout 15
n2 idft enable timeout 15
gtpc gtpc-failure-profile gtp1
gtpc message-handling create-session-response condition ip-exhaust action backoff cause 76
exit
```

The following is an example output of the **show running-config profile dnn intershat** command.

```
[unknown] smf# show running-config profile dnn intershat
profile dnn intershat
network-element-profiles chf chf1
network-element-profiles amf amf1
network-element-profiles pcf pcf1
network-element-profiles udm udm1
timeout backoff 500 jitter 100
charging-profile chgprf1
virtual-mac b6:6d:47:47:47:47
ssc-mode 2 allowed [ 3 ]
session type IPV4 allowed [ IPV6 IPV4V6 ]
upf apn intershat
dcnr true
exit
```

Non-3GPP Compliant Timers

Feature Description

The SMF supports non-3GPP session timers for each PDU session. This section provides detailed information about the function, operation, and configuration of the following timers:

- Absolute Timer
- Control Plane and User Plane Inactive Timer
- Session Setup Timer

Configuring Non-3GPP Session Timers

To configure non-3GPP session timers in the DNN profile, use the following sample configuration:

```
config
  profile dnn dnnprofile_name
    timeout absolute absolutetimer_value
    timeout { cp-idle timer_value | up-idle timer_value }
```

```
timeout setup timeout_value
end
```

NOTES:

- **timeout absolute** *absolutetimer_value*: Specifies the maximum duration of the session (in seconds), before the system automatically terminates the session. The default value is 0, which indicates that the function is disabled.

  The absolute session timer triggered during the session creation. You cannot modify the timer value during interim handling of any access and mobility procedures for that session. Once the timer expires, the SMF performs SMF-initiated release by informing all SBI interfaces and N4 Interfaces, that is, toward UE, UDM, PCF, CHF, and UPF interfaces.

  absolutetimer_value must be an integer in the range of 0-2147483647.

- **timeout cp-idle** *timer_value*: Specifies the maximum duration of the 5G session after the migration to CP idle state and before the automatic termination. The default value is 0, which indicates the function is disabled. *timer_value* must be an integer in the range of 0-2147483647.

- **timeout up-idle** *timer_value*: Specifies the maximum duration of the 5G session after the migration to UP idle state and before the automatic termination. The default value is 0, which indicates the function is disabled. *timer_value* must be an integer in the range of 0-2147483647.

  The up-idle timer starts when an AN-initiated or Network-initiated 5G session enters the idle mode. This timer stops when the session exits the idle mode. On expiry of the timer, the SMF clears the 5G sessions.

  The cp-idle timer starts when any 4G or 5G procedure ends, and stops when any new procedure starts. If the timer expires, the SMF clears the session.

- **timeout setup** *timeout_value*: Specify the session setup timeout value in milliseconds. *timeout_value* must be an integer in the range of 5000-60000. The default value is 10000 milliseconds.

- SMF aborts the create procedure if the call isn't complete within the configured time, and sends PDU Session Establishment Reject or Create Session Reject. This timer is applicable to 4G, 5G, and Wi-Fi sessions.

  In the 4G Create procedure, if CSR receives Maximum Wait Time, then the procedure SLA timer sets the Maximum Wait Time. Either the guard timer or the SLA timer expires first, depending on the timeout values.

The following is a sample configuration.

```
smf(config)# profile dnn intershat timeout absolute 900
```