Network Slicing Support

Table 1: Feature History

Feature Name	Release Information	Description
Network Slicing Support	2023.04	Cisco AMF allows the slice selection and reallocation during the UE registration. Default Setting: Disabled – Configuration Required

Feature Summary and Revision History

Summary Data

Table 2: Summary Data

Applicable Product(s) or Functional Area	AMF
Applicable Platform(s)	SMI
Feature Default Setting	Enabled - Always-on
Related Documentation	Not Applicable

Revision History

Table 3: Revision History

Revision Details	Release
First introduced.	2023.04.0

Feature Description

Note The network slicing support is not fully qualified in this release. Contact your Cisco account representative for more information.

Slice selection is the process of choosing a specific network slice supported by the network. The AMF supports the network slice selection during the registration. The AMF selects the slice based on the requested NSSAI, subscription data from UDM, locally configured slices, and slicing information received from NSSF. Upon successful UE registration, the AMF conveys the allowed NSSAIs to both the AN (gNB) and the UE, so that UE uses the appropriate slice to access the required services.

If AMF is unable to serve any of the slices requested by the UE, the AMF initiates the re-allocation functionality. AMF supports redirection of registration request message through the direct signaling to selected target AMF (received in NSSF response) or by rerouting the NAS message to target AMF through RAN.

When the AMF receives an indication from the UDM about change in slice subscription, the AMF informs the UE with new allowed/rejected and configured slices using UE configuration update procedure.

How it Works

This section describes how this feature works.

Call Flows

This section describes about the various call flows pertaining to this feature:

Figure 1: Slice Selection

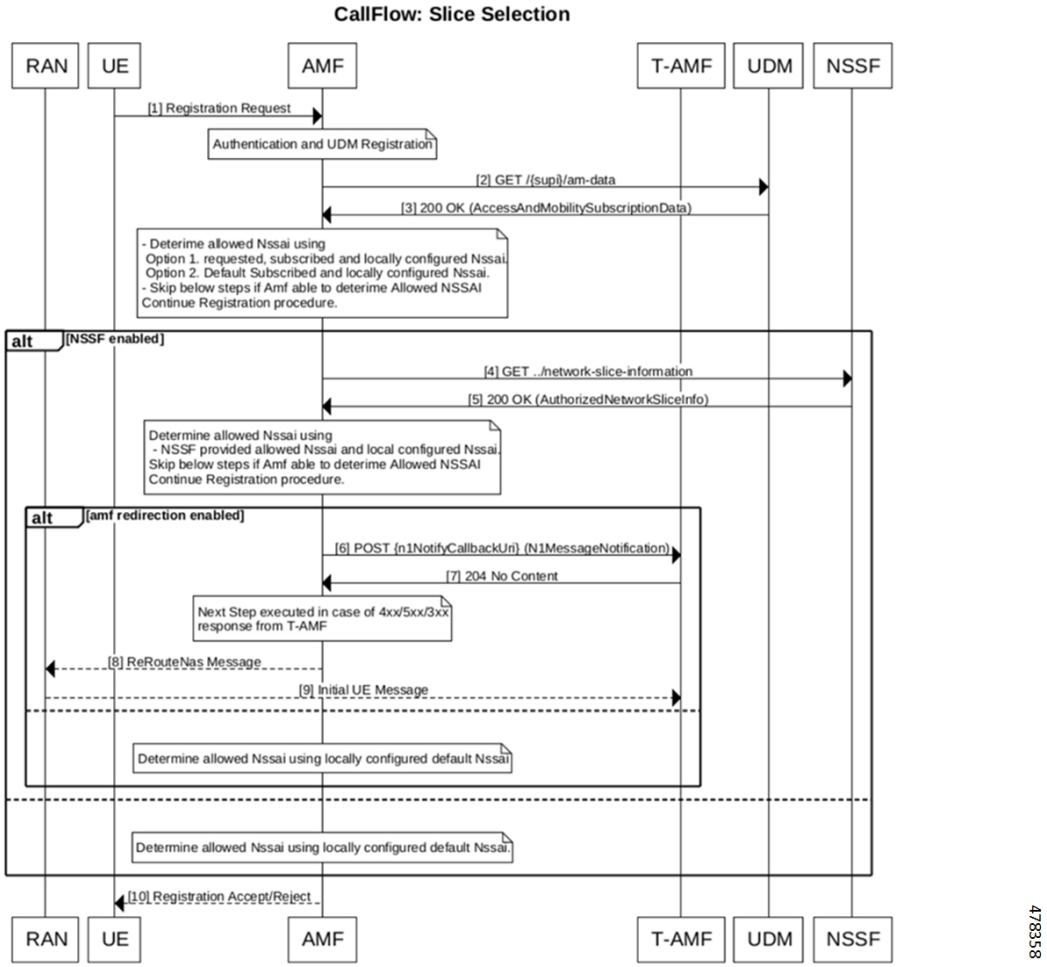


Table 4: AMF Slice Selection

Step	Description
1	UE Requested NSSAI are matched with local configuration and with the subscribed SNSSAI received from UDM. For local configuration, AMF service level NSSAI needs to be configured.
2	If there is no match, then next step is to match the default SNSSAI from UDM with local slice configuration.
3	If there is no match, and if the NSSF interaction is enabled then query NSSF and make slice selection request: • Get allowed NSSAI list and configured NSSAI from slice selection response and match with local configured slice. • If NSSF interaction is not enabled, accept the subscriber with locally configured default-NSSAI.

Step	Description
4	If there is no match, and if AMF redirection is enabled, use targetAmfSet or candidateAMF from slice selection response and proceed with AMF relocation else accept subscriber with locally configured default-NSSAI.
5	If slice matches, continue with registration procedure. **Note** The Global/PLMN level slices information are considered as local configuration. **1.** If UDM doesn't provide subscribed S-NSSAIs, it considers the default S-NSSAIs for comparison. • Allowed NSSAIs in registration accept: The matching S-NSSAIs are considered as allowed NSSAIs and are filled in registration accept message. • Rejected NSSAIs in registration accept: The AMF may include this IE to inform the UE of one or more S-NSSAIs that were included in the requested NSSAI in the REGISTRATION REQUEST message but were rejected by the network. • Configured NSSAIs in registration accept: The AMF may include a new configured NSSAI for the current PLMN in the REGISTRATION ACCEPT message if: • The REGISTRATION REQUEST message doesn't include the requested NSSAI. • The REGISTRATION REQUEST message includes the requested NSSAI containing a S-NSSAI that is not valid in the serving PLMN. • The REGISTRATION REQUEST message includes the network slicing indication IE with the default configured NSSAI indication bit set to "Requested NSSAI created from default configured NSSAI".
6	The AMF obtains the configured S-NSSAI by utilizing locally configured PLMN-level slice and subscription details. **Note** In case of registration reject due to the cause set to 62 - “No network slices available”. The AMF provides rejected NSSAI in registration accept/reject with the cause "S-NSSAI not available in the current PLMN or SNPN" unless calculated by NSSF.
7	If UDM includes “provisioningTime” (in NSSAI IE) in subscription response. The AMF provides acknowledgment (/am-data/subscribed-snssais-ack) to UDM after receiving registration complete.

AMF Reallocation

Following are the call flows for the reallocation procedure.

Figure 2: Source AMF

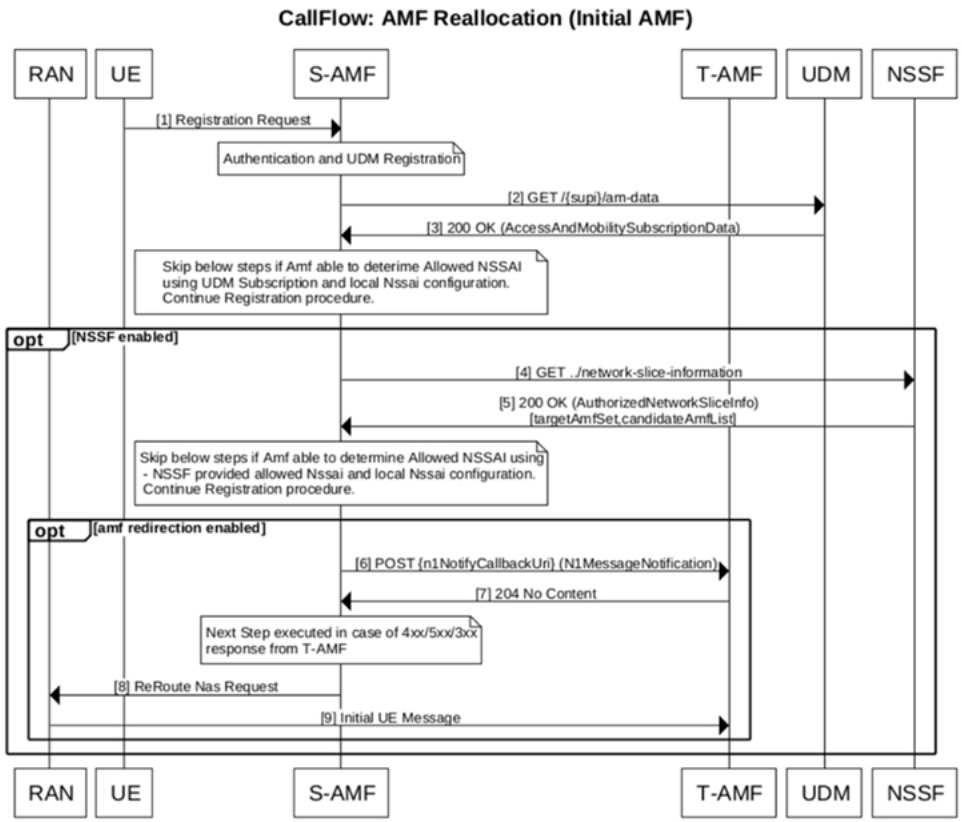


Table 5: Source AMF

Step	Description
1	The AMF redirection uses the "N1MessageNotify" message which is callback API (that means, it uses notification-subscription framework).
2	All AMFs needs to be pre-registered with NRF with “defaultNotificationSubscription”. It includes callback URL for N1MessageNotify.
3	The AMF uses the locally configured NRF (not received from NSSF) in slice selection response.
4	From the discovered AMFs, the source AMF sends N1MessageNotify message to callback URL.

Step	Description
5	If multiple instance Id's are received as part of candidate AMF List, then the S-AMF initiates a N1 message notify to T-AMF selected based on first instance id and if receives status other than 204 in N1 Message Notify Response, then it initiates the request again to target selected based on next instance id in candidate AMF List.
6	In case NRF is not available, local configuration is supported for destination AMF IOT only: • TargetAmfSet" needs to be configured as endpoint-profile name and • "CandidateAMF" needs to be configured as endpoint-name under NF-client profile.
7	The AMF reroutes the message through the RAN (REROUTE NAS REQUEST)if direct signaling to target AMF fails.

Figure 3: Destination AMF

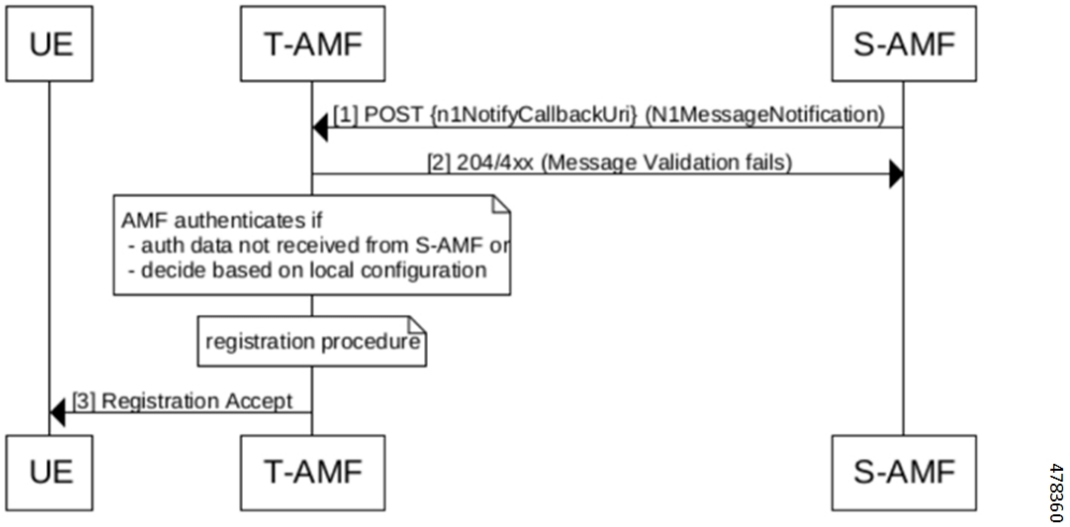


Table 6: Destination AMF

Step	Description
1	The target AMF upon receiving N1Message notify decodes the message and extracts the UEContext, location information, and gNB information
2	The AMF authenticates the subscriber based on local configuration and in case authentication data is not received from source AMF then it continues with the registration procedure with details received. **Note** If gNB is not connected to the AMF, then the registration fails.

Slice Update Notification

Following are the call flows for the slice update notification.

Figure 4: UE Configuration Update for UDM Subscription Change

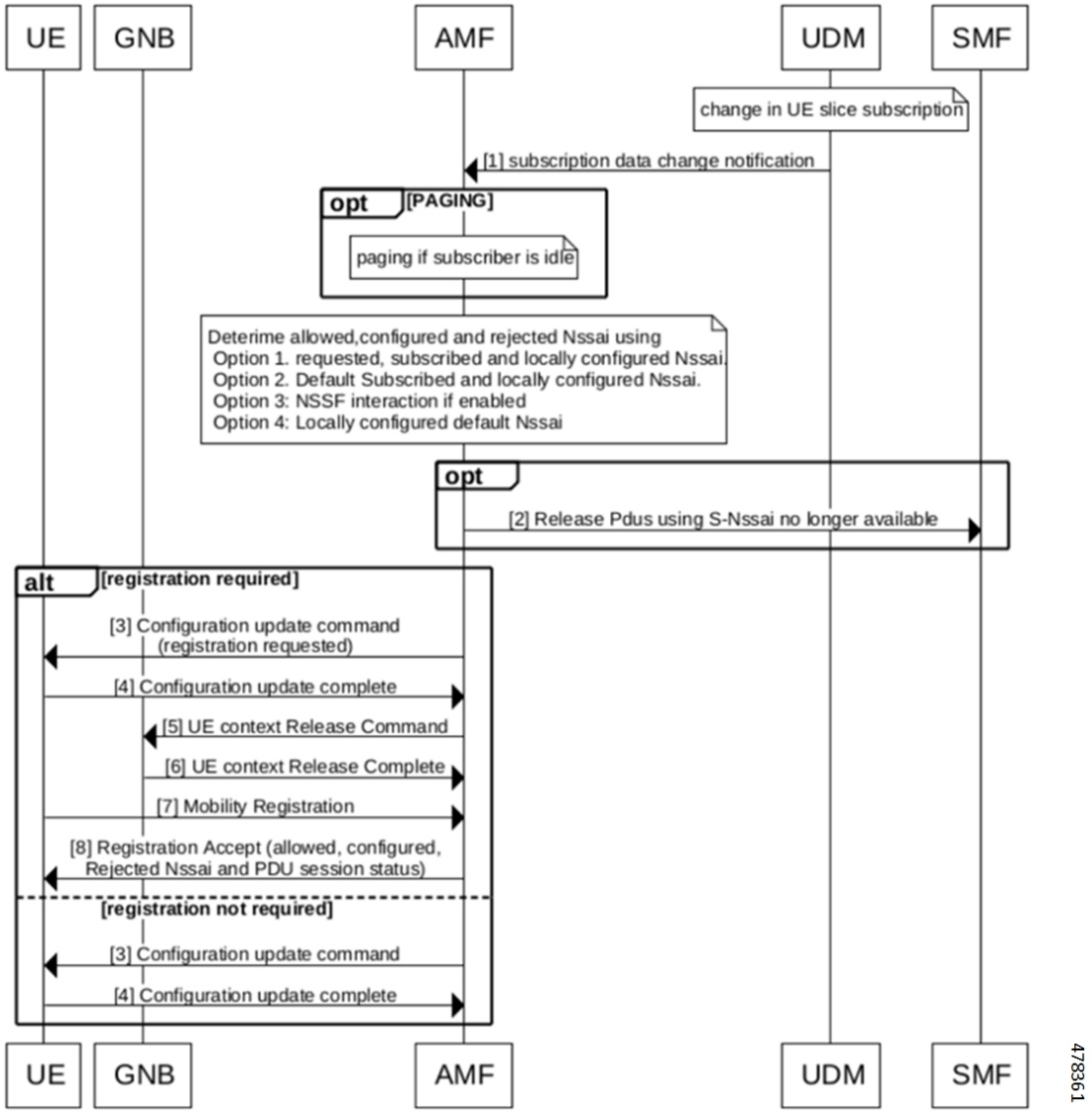


Table 7: UE Configuration Update for UDM Subscription Change

Step	Description
1	The UDM sends the notification to AMF when “subscription data for network slicing changes”.

Step	Description
2	The AMF re-calculates the slice information based on local configuration or using NSSF. If there is any change in slice (allowed-NSSAI, rejected-NSSAI, and configured NSSAI), then the amf-service sends the UE configuration update. The AMF provides UE with: • an indication that the acknowledgment from UE is required. • Allowed S-NSSAIs, configured S-NSSAIs for the Serving PLMN (if required), rejected S-NSSAI(s) (if required). • If the changes to the allowed NSSAI require the UE to perform immediate registration procedure because they affect the existing connectivity to network slices. The serving AMF indicates to the UE the need for the UE to perform a registration procedure.
3	When a network slice used for a one or multiple PDU Sessions is no longer available for a UE, the following applies: • The AMF releases a non-emergency PDU session for which network slice is no longer available and indicates SMF to release such PDUs. • The AMF modifies the PDU session status correspondingly. The PDU session(s) context is locally released in the UE after receiving the PDU session status in the registration accept message.
4	If UE is in the connected mode then UE configuration Update is sent else AMF triggers paging.
5	After receiving the acknowledgment, the AMF releases the NAS signaling connection for the UE in case of registration requested by AMF.
6	If there are established PDU session (s) associated with emergency services, then the serving AMF indicates to the UE the need for the UE to perform a registration procedure but doesn't release the NAS signaling connection to the UE. The UE performs the registration procedure only after the release of the PDU session (s) used for the emergency services.
7	The AMF rejects any NAS Message from the UE carrying PDU session establishment request for a non emergency PDU session before the required registration procedure has been successfully completed by the UE.
8	In case configuration update fails (example, subscriber not reachable): • The AMF releases a non-emergency PDU session for which network slice is no longer available and indicates SMF to release such PDUs. • The new calculated slice is provided when subscriber perform initial/mobility registration. • In case N1N2 or service request comes, the AMF sends the configuration update after handling the incoming message.

Note The configuration update doesn't happen for emergency subscriber.

Figure 5: Idle Time Expiry

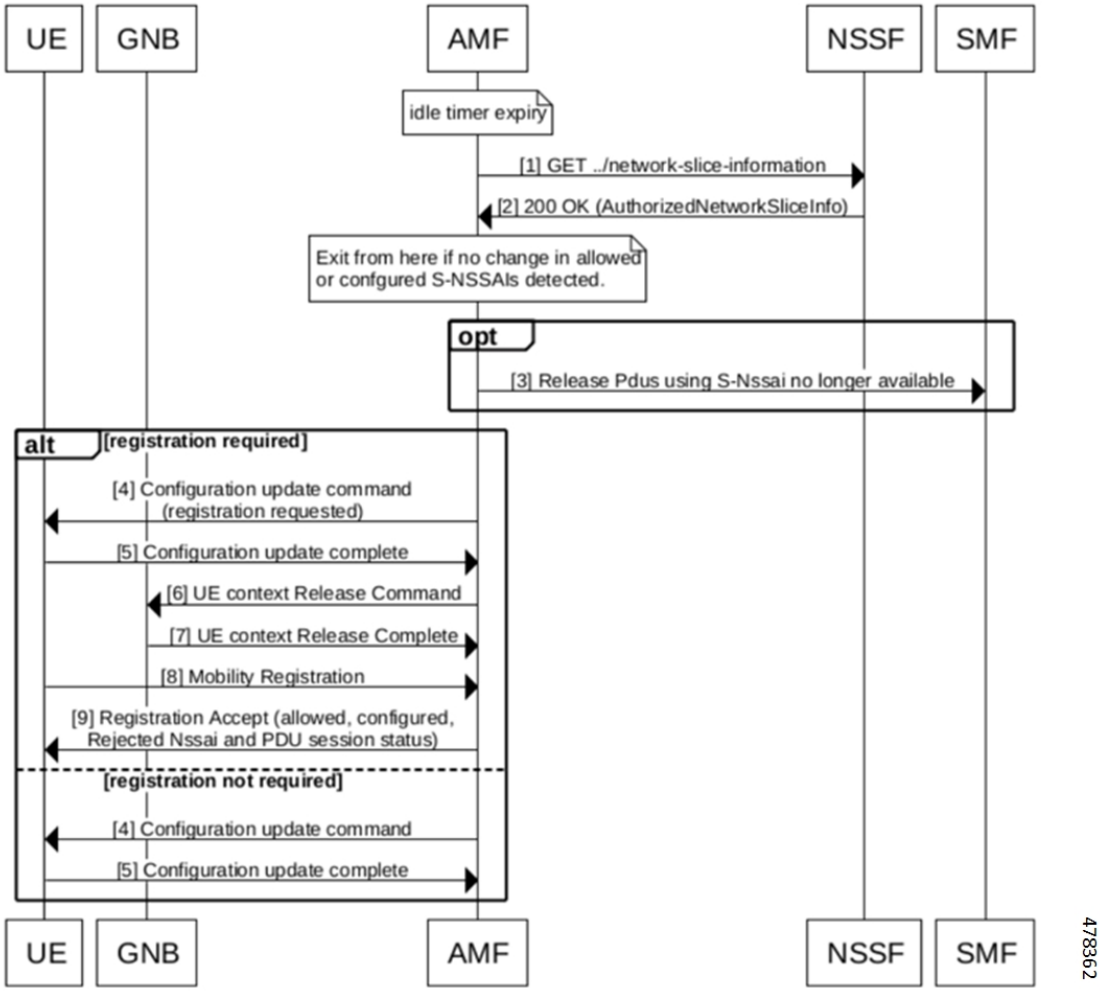
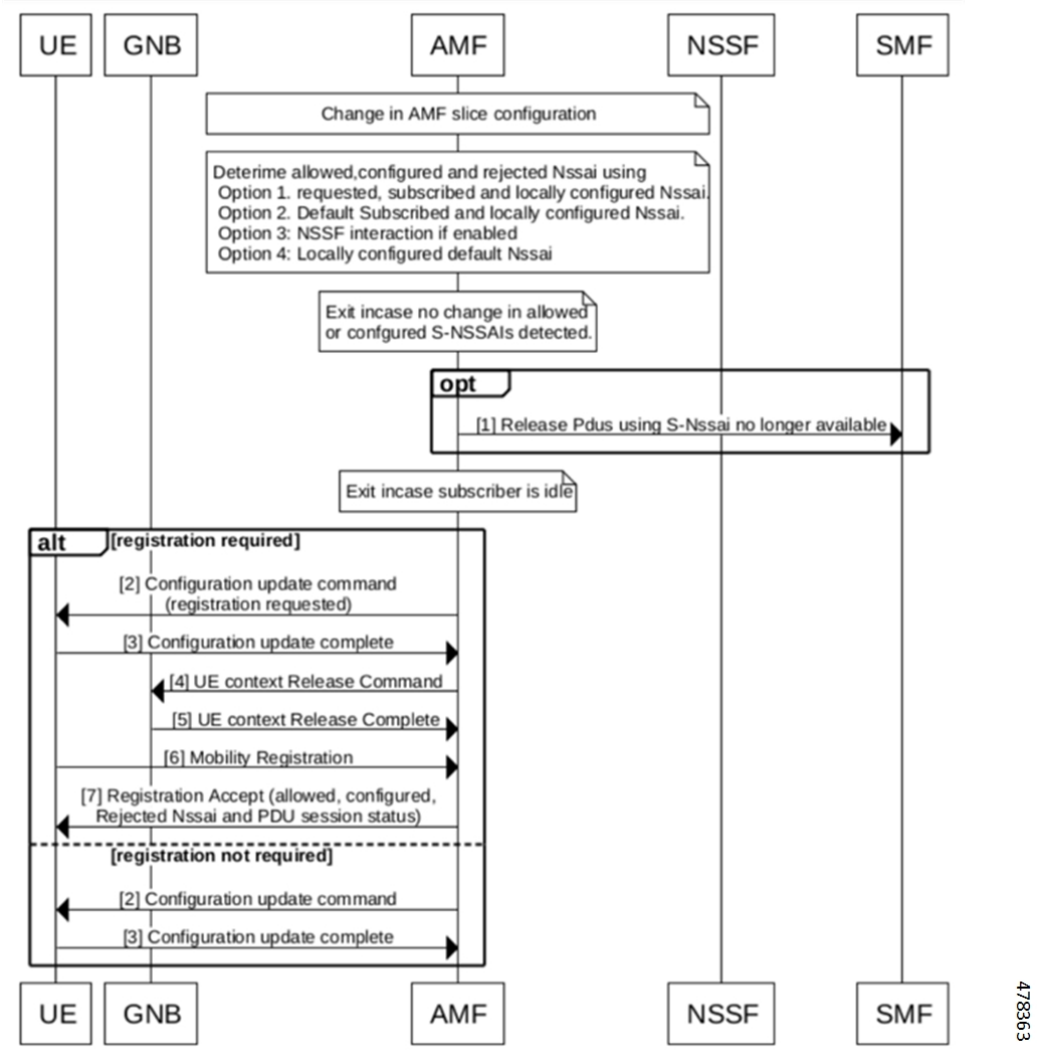


Table 8: Idle Time Expiry

Step	Description
1	On idle timer expiry, The AMF re-calculates the slice information using NSSF. **Note** prerequisite is to enable the configuration for "Enabling the UE Configuration Update".
2	The UE configuration update is sent only for those subscriber for which the NSSF was used previously for slice selection.

Figure 6: Slice Configuration Change

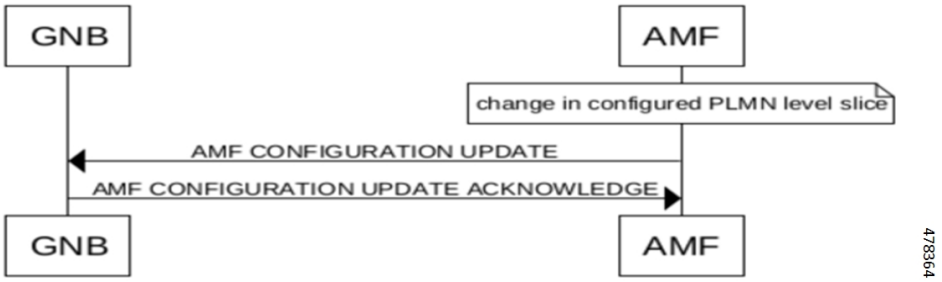


Note The AMF sends indication about the network slicing subscription change in UE configuration update, only in case of UDM subscription data changes notification.

Table 9: Slice Configuration Change

Step	Description
1	The AMF updates all non-emergency subscriber for which old slice information is no longer valid.
2	The behavior is same as the "UDM Change notification for subscriber in connected mode".
3	For idle subscriber (no paging), The AMF releases the non-emergency PDU session for which network slice is no longer available and indicates SMF to release such PDUs.

AMF Configuration Update



Changes in the slice configuration per PLMN is notified to GNBs using AMF configuration update message.

NRF Registration or Modification

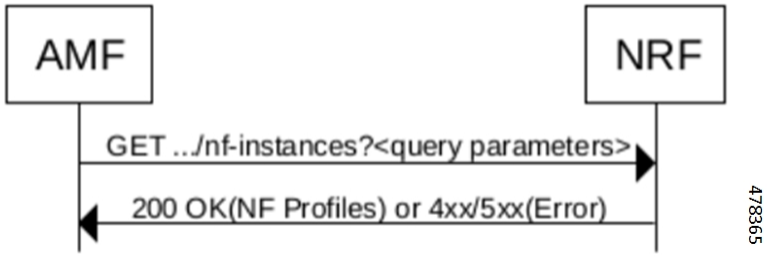
During the NRF registration/modification, the AMF sends the slice information in nfProfile which is configured at AMF.

Attribute Name	Data Type	Description
sNssais	array (Snssai)	S-NSSAIs of the network function. If not provided, the NF can serve any S-NSSAI. When present this IE represents the list of S-NSSAIs supported in all the PLMNs listed in the plmnList IE.

Note The TAI level information and NSI-list is not sent to NRF during registration or modification.

Peer NF Discovery through NRF

The AMF supports the discovery of peer NFs based on the slice data. The “SNSSAIS” is configured in the query-params CLI. The AMF, while sending the discovery request to NRF, must include the SNSSAIS for the filter criteria in the query parameters.



Attribute Name	Data type	Description
SNSSAIS	array (SNSSAIS)	If included, this IE contains the list of S-NSSAIs that are served by the NF (service) instances being discovered. The NRF returns those NF profiles/NF services of NF (service) instances that have at least one of the S-NSSAIs in this list.

Limitations

Following are the limitations for this feature:

- The AMF doesn't support the slice selection for roaming subscriber (Mapped NSSAI).
- The AMF doesn't support the network slice specific authentication and authorization (NSSAA).
- The AMF doesn't support the slice selection for handover scenario (Xn and N2).
- The AMF doesn't support the reallocation for the roaming subscribers and registration with the foreign-5g-GUTI.
- The AMF doesn't support the PDU establishment using NSSF.
- The AMF supports reallocation only for the initial registration.

Feature Configuration

Configuring this feature involves the following steps:

- Slice Selection Enable and Slice Migration—This configuration enables the slice selection. For more information, refer to Configuring the AMF Reallocation, on page 13.
- Inclusion Mode—This configuration provides the commands for Inclusion mode configuration. For more information, refer to Configuring the Inclusion Mode, on page 14.
- Enabling UE Update—This configuration enables the UE update. For more information, refer to Enabling the UE Configuration Update, on page 15.
- Query Parameters for AMF Discovery—This configuration provides the Query parameters commands for AMF discovery. For more information, refer to Configuring the Query Parameters for AMF Discovery, on page 15.
- NSSF—This configuration provides the commands for NSSF configuration. For more information, refer to Configuring the NSSF, on page 16.
- Local AMF—This configuration provides the Local AMF configuration. For more information, refer to Configuring the Local AMF, on page 19.

Configuring the AMF Reallocation

To configure the reallocation, use the following configuration:

```
config
   amf-global
      call-control-policy policy_name
         policy amf-redirection use-source-key { false | true }
         policy amf-redirection horizontal-key-derivation { false | true
 }
         policy nssf-interaction { disabled | enabled }
         end
```

NOTES:

- **call-control-policy** *policy_name*—Specify the call control policy name.
- If the NSSF interaction is disabled, and slice selection fails, in that case AMF falls back to the default slice configuration on AMF and registration accept is sent with the default slice in the allowed NSSAI. If the default slice configuration is absent (which is less likely since it is mandatory for the N26 HandIn to succeed), only then AMF sends the registration reject.
- In case amf-redirection is disabled, then S-AMF doesn't reroute to T-AMF and initiates registration reject with cause code set to 62 - "No network slices available".
- Use-source-key: If true, then T-AMF uses the key received from S-AMF.
- horizontal-key-derivation: The T-AMF uses the source provided keys or generates a new key based on CLI configuration. The S-AMF sends existing keys or generates a new key and then sends these newly generated keys in N1MsgNotify.
- The AMF-redirection is enabled by configuring use-source-key/horizontal-key-derivation or both with true/false and if none of the options are configured then AMF-redirection is considered to be in disabled state.

Configuring the AMF Slice

The following is the global level slice configuration representing system level slice configuration supported by AMF.

```
config
   amf-services amf_service_name
      nssai name slice_name
         sst sst_value
         sdt sdt_value
         end
```

NOTES:

- **nssai name** *slice_name* - Specify the slice name.
- **sst** *sst_value* - Specify the SST value.
- **sdt** *sdt_value* - Specify the SDT name.

Note The AMF supports a maximum of eight slices.

Configuring the Emergency Slice

When you configure the emergency slice, then the AMF sends this slice in the registration accept message for emergency subscriber.

```
config
   emergency-profile profile_name
      nssai
         sst sst_value
         sdt sdt_value
         end
```

NOTES:

- **emergency-profile***profile_name* - Specify the emergency profile name.
- **sst** *sst_value* - Specify the SST value.
- **sdt** *sdt_value* - Specify the SDT name.

Note You must associate an emergency profile to amf-service or operator policy to enable this configuration.

Configuring the Inclusion Mode

When you configure this CLI, the inclusion mode is sent in registration accept.

To configure the Inclusion mode, use the following CLI:

```
config
   amf-global
      call-control-policy policy_name
         policy slicing inclusion-mode policy_inclusion_mode
         end
```

NOTES:

- **call-control-policy** *policy_name*—Specify the call control policy name.
- **policy slicing inclusion-mode** *policy_inclusion_mode*—Specify the policy inclusion mode for slicing. The possible values for the inclusion mode is - A, B, C, and D.

Configuration Example

The following is an example configuration.

```
config
   amf-global
      call-control-policy local
```

```
policy slicing inclusion-mode B
end
```

Configuring Default Slice

Use the following CLI to configure the default slice in AMF:

```
config
   amf-global
      call-control-policy policy_name
        default-nssai
           sst sst_value
           sdt sdt_value
           end
```

NOTES:

- **sst** *sst_value* - Specify the SST value.
- **sdt** *sdt_value* - Specify the SDT value.

Enabling the UE Configuration Update

When you configure this CLI, the AMF sends the configuration update command to UE upon idle timer expiry if there are any changes in the slices (configured or allowed S-NSSAIs) for any subscriber.

```
config
   amf-global
      call-control-policy policy_name
         policy ue-cfg-update on-nssf-slice-change { true | false }
         end
```

NOTES:

- **call-control-policy** *policy_name*—Specify the call control policy name.
- **policy ue-cfg-update on-nssf-slice-change { true | false }**—Enable or disable the UE configuration update.

Configuration Example

The following is an example configuration.

```
config
  amf-global
     call-control-policy local
        policy ue-cfg-update on-nssf-slice-change true
        end
```

Configuring the Query Parameters for AMF Discovery

To configure the query parameters for AMF discovery, use the following configuration:

```
config
   profile network-element amf amf_name
```

```
nf-client-profile nf_client_name
failure-handling-profile profile_name
query-params { target-plmn | amf-set-id | target-nf-instance-id }
end
```

NOTES:

- **profile network-element amf** *amf_name*—Specify the name of AMF network element.
- **nf-client-profile** *nf_client_name*—Specify the name of NF client.
- **failure-handling-profile** *profile_name*—Specify the name of failure handling profile name.
- **query-params { target-plmn | amf-set-id | target-nf-instance-id }**—Specify the query parameters for AMF discovery.

Configuration Example

The following is an example configuration.

```
config
   amf-global
      profile network-element amf amf1
         nf-client-profile nf1
         failure-handling-profile FH5
         query-params [ target-plmn amf-set-id target-nf-instance-id ]
         end
```

Configuring the Query Parameter for Slice Data in NF Discovery

To configure the query parameters in NF discovery, use the following configuration:

```
config
   profile network-element { pcf | smf }
      failure-handling-profile profile_name
      query-params { snssais }
      end
```

NOTES:

- **profile network-element** *profile_name*—Specify the network profile name.
- **failure-handling-profile** *profile_name*—Specify the name of failure handling profile name.
- **query-params { snssais }**—select SNSSAIS as query parameter in network function discovery.

Configuring the NSSF

Configuring the NSSF involves the following configurations:

1. Network Element Profile List—This configuration provides the commands to configure the Network element profile list. For more information, refer to Configuring the Network Element Profile List, on page 17.
2. Profile Network Element—This configuration provides the commands to configure the profile networkeElement. For more information, refer to Configuring the Profile Network Element, on page 17.

3. Profile NF-client—This configuration provides the commands to configure the profile NF-client. For more information, refer to Configuring the Profile NF-client, on page 17.
4. Profile NF-client-failure—This configuration provides the commands to configure the Profile NF-client-failure. For more information, refer to Configuring the Profile NF-client-failure, on page 18.
5. Profile NF-pair NF-type—This configuration provides the commands to configure the Profile NF-pair NF-type. For more information, refer to Configuring the Profile NF-pair NF-type, on page 19.

Configuring the Network Element Profile List

To configure the network element profile list, use the following configuration:

```
config
   amf-global
      operator-policy policy_name
         ccp-name ccp_name
         network-element-profile-list nssf nssf_name
         end
```

NOTES:

- **operator-policy** *policy_name*—Specify the operator profile name.
- **ccp-name** *ccp_name*—Specify the Configuration Control Point (CCP) name. The CCP is used for managing and controlling configuration settings.
- **network-element-profile-list nssf** *nssf_name*—Specify the NSSF with the network element profile.

Configuring the Profile Network Element

To configure the profile network element, use the following configuration:

```
config
 profile network-element nssf nssf_name
  nf-client-profile nf_client_name
  failure-handling-profile failure_handling_profile_name
  end
```

NOTES:

- **profile network-element nssf** *nssf_name*—Specify the profile name for the network element.
- **nf-client-profile** *nf_client_name*—Specify the network function client profile name.
- **failure-handling-profile** *failure_handling_profile_name*—Specify the failure handling profile name.

Configuring the Profile NF-client

To configure the profile NF-client, use the following configuration:

```
config
   profile nf-client nf-type nf_client_name
      nssf-profile profile_name
         locality locality_name
            priority priority_value
```

```
service name type nnssf-nsselection
   endpoint-profile profile_name
      capacity capacity_value
      uri-scheme uri_scheme_name
      version
      uri-version uri_version
      exit
  exit
  endpoint-name end_point_name
     priority priority_value
        primary ip-address ipv4 ipv4_address
        primary ip-address port ipv4_port_number
        secondary ip-address ipv4 secondary_ipv4_address
        secondary ip-address port secondary_ipv4_port_number
        tertiary ip-address ipv4 tertiary_pv4_address
        tertiary ip-address port tertiary_ipv4_port_number
        end
```

NOTES:

- **profile nf-client nf-type** *nf_client_name*—Specify the profile name of the NF client.
- **nssf-profile** *profile_name*—Specify the profile name for the NSSF.
- **locality** *locality_name*—Specify the locality name within the NSSF profile.
- **priority** *priority_value*—Specify the priority value of the locality name within the NSSF profile.
- **endpoint-profile** *profile_name*—Specify the associated end point profile name.
- **capacity** *capacity_value*—Specify the capacity of the endpoint.
- **uri-scheme** *uri_scheme_name*—Specify the uri scheme associated with the endpoint.
- **uri-version** *uri_version*—Specify the uri version associated with the endpoint.

Configuring the Profile NF-client-failure

To configure the profile NF-client-failure, use the following configuration:

```
config
   profile nf-client-failure nf-type nssf nssf_name
      profile failure-handling failure_handling_profile_name
         service name type nnssf-nsselection
            responsetimeout timeout_value
               message type NssfNSSelectionReq
                  status-code httpv2 503
                  retry retry_count
                  action retry-and-ignore
                  end
```

NOTES:

- **profile nf-client-failure nf-type nssf** *nssf_name*—Specify NF (Network Function) client failure profile.
- **profile failure-handling** *failure_handling_profile_name*—Specify failure-handling profile name.

- **responsetimeout** *timeout_value*—Specify the response timeout for the specified services.
- **retry** *retry_count*—Specify the retry count for the status code.

Configuring the Profile NF-pair NF-type

To configure the profile NF-pair NF-type, use the following configuration:

```
config
   profile nf-pair nf-type nf_type_name
       locality client client_name
       locality preferred-server server_name
       locality geo-server server_name
       end
```

NOTES:

- **profile nf-pair nf-type** *nf_type_name*—Specify NF (Network Function) type name.
- **locality client** *client_name*—Specify the locality name for the client.
- **locality preferred-server** *server_name*—Specify the server name as the preferred server locality.
- **locality geo-server** *server_name*—Specify the geographical location for the geo-server.

Note The failure handling configuration leading to the session delete is not valid for NSSF.

Configuring the Local AMF

It's optional configuration when real NRF isn't available.

The following is an example configuration.

```
profile nf-client nf-type amf
 amf-profile AMF1
  locality LOC1
   priority 56
   service name type namf-comm
    endpoint-profile EP1
     capacity 30
     priority 30
     uri-scheme http
     endpoint-name EP1
      priority 30
      primary ip-address ipv4 10.81.70.232
      primary ip-address port 9052
      default-notification-subscriptions s1
       notification-type N1_MESSAGES
       callback-uri http://xx.xx.xx.xx:xxxx/namf-comm/v1/callbacks/n1-message-notify
       n1-message-class 5GMM
       end
```

Configuring Label Slice Data Filters in Metrics

you can enable or disable the slice data filters for the slices only in metrics by using the following CLIs:

Use the following CLI for disabling the slice data filter:

```
config
        amf-global
           metric-label-filter
           slice-data disabled
        end
```

Use the following CLI for enabling the slice data filter:

```
config
        amf-global
           metric-label-filter
           slice-data slices [ sst-sdt sst-sdt sst ]
        end
```

Note A maximum of eight slices can be configured and there is no validation to check the sst/sd format.

NOTES:

- **metric-label-filter**—To define and configure the metric label filters.
- **slice-data** *slices [sst-sdt sst-sdt sst]*—Specify the slices to configure the metric label filter.

Configuring Clear Subscriber with Slice Filter

By using the **clear subscriber** command, you can configure the new slice filter to clear all subscribers with specified slice in accepted slice list. This is not applicable to emergency subscribers or non-emergency subscribers with emergency PDUs.

Note

- You can specify only one slice at a time.
- There is no validation to check the sst/sd format.

Following is the example of the clear subscriber configuration:

```
clear subscriber nssai
Description: Specify slice value. Format sst-sd or sst (e.g. 4-abc12e or 123)
Possible completions: <string>

[amf] amf# clear subscriber nssai 4-123546
result
ClearSubscriber Request submitted
```

Bulk Statistics

amf_ngap_message_total

The `amf_ngap_message_total` metric tracks the total number of NGAP Next Generation Application Protocol (NGAP) messages sent by the AMF. These messages are categorized based on different attributes:

- `app_name`: Specifies the name of the application (AMF).
- `message_direction`: Indicates the direction of the message (example, "outbound").
- `message_type`: Specifies the type of NGAP message (example, "N2ReRouteNasRequest").
- `service_name`: Identifies the service name (example, "amf-protocol-ep").

Example usage:

```
amf_ngap_message_total{app_name="AMF", message_direction="outbound",
message_type="N2ReRouteNasRequest", service_name="amf-protocol-ep"}
```

n2_service_stats

The `n2_service_stats` metric provides statistics related to N2 service operations in the AMF. These statistics include:

- `app_name`: Specifies the name of the application (AMF).
- `message_type`: Indicates the type of N2 service operation (example, "N2ReRouteNasRequest").
- `service_name`: Identifies the service name (example, "amf-service").
- `status`: Indicates the status of the service operation (example, "success").

Example usage:

```
n2_service_stats{app_name="AMF", message_type="N2ReRouteNasRequest",
service_name="amf-service", status="success"}
```

n22_service_stats

The `n22_service_stats` metric provides statistics related to N22 service operations in the AMF. These statistics include:

- `app_name`: Specifies the name of the application (AMF).
- `message_type`: Indicates the type of N22 service operation (example, "NssfGetNetworkSliceInformationReq").
- `service_name`: Identifies the service name (example, "amf-service").
- `status`: Indicates the status of the service operation (example, "success/failure").

Example usage:

```
n22_service_stats{app_name="AMF", message_type="NssfGetNetworkSliceInformationReq",
service_name="amf-service", status="success"}
```

n14_service_stats

The `n14_service_stats` metric provides statistics related to N14 service operations in the AMF. These statistics include:

- `app_name`: Specifies the name of the application (AMF).
- `message_type`: Indicates the type of N14 service operation (example, "N14N1MessageNotifyClientRequest").
- `service_name`: Identifies the service name (example, "amf-service").
- `status`: Indicates the status of the service operation (example, "success/failure").
- `reason`: Provides additional information about the operation's status.

Example usage:

```
n14_service_stats{app_name="AMF", message_type="N14N1MessageNotifyClientRequest",
service_name="amf-service"}
```