

NF Discovery and Management

- Feature Description, on page 1
- NF Management, on page 1
- NF Discovery, on page 19
- Static Configuration for Peer NF Management, on page 37
- Failure Handling, on page 42

Feature Description

The Network Function (NF) Repository Function (NRF) supports the following functionality:

- Maintains the NF profile of available NF instances and their supported services.
- Allows other NF instances to subscribe to, and get notified about, the registration in NRF of new NF instances of a given type.
- Supports service discovery function. It receives NF Discovery Requests from NF instances, and provides the information of the available NF instances fulfilling certain criteria (for example, supporting a given service).

NF Management

Feature Description

This section describes the NF management procedures and their configurations that AMF supports. These procedures are NF registration, NF deregistration, NF heartbeat, and NF Update. The NF registration, update, and heartbeat are sent from only one of the rest-ep pods, which is the elected primary node. After this nodes is elected, the instance remains as primary node for the NF management activities till the pod crashes or is removed.

NF management supports dynamic configuration change. With this feature, if the configurations were modified in the middle of the transaction or procedure, the ongoing transactions are not impacted.

The dynamic configuration change feature supports the following:

- NRF transaction or procedure picks a configuration version (v1) and uses the same version until the NRF transaction or procedure completes.
- If you change the configuration during an ongoing NRF transaction, then a new configuration version (v2) is created. However, the new configuration is applied in the new transaction.

The dynamic configuration changes apply to the following data structures:

- NrfFailureProfileSt
- NrfClntProfileSt
- NrfGrpSt
- NrfPairProfileSt
- NrfMgmtGrpSt

Registration

AMF registers with NRF. During registration with NRF, AMF includes at least one of the addressing parameters, such as FQDN, IPv4 or IPv6 address in the NF profile. Including at least one of the addressing parameters in the NF profile registration is mandatory. If AMF supports "https" uri scheme, then AMF provides FQDN in the NFProfile or NFService.

Configuring NRF Endpoints Profile Parameters for NF Management

The AMF provides CLI for configuring NRF endpoints for **nnrf-nfm** (NF Management).

Note For NF management, you can configure only the **nnrf-nfm** service.

The CLI configuration allows configuring multiple endpoints under each endpoint profile. The AMF uses the priority and capacity parameters to load balance between these endpoints. Primary, secondary, and tertiary hosts [ip:port] can be configured within each endpoint. Both IPv4 and IPv6 addresses can be specified. If both are specified, then the IPv4 address is preferred.

A URI uniquely identifies a resource. In the 5GC SBI APIs, when a resource URI is an absolute URI, its structure is specified as follows:

```
{apiRoot}/{apiName}/{apiVersion}/{apiSpecificResourceUriPart}
```

Note In this release of the specification, both HTTP and HTTPS scheme URIs are allowed. See the *3GPP TS 33.501, subclause 13.1* for more information on security of service-based interfaces.

" apiRoot " is a concatenation of the following parts: scheme ("http" or "https")

- fixed string "://"
- authority (host and optional port) as defined in IETF RFC 3986
- an optional deployment-specific string (API prefix) that starts with a "/" character [api-root in CLI]

To configure the NRF endpoints for different services supported by NRF, use the following sample configuration.

```
config
  group nrf mgmt mgmt_name
    service type nrf nnrf-nfm
      endpoint-profile epprofile_name
        priority priority_value
        capacity capacity
        api-root api_string
        api-uri-prefix uri_prefix_string
        uri-scheme { http | https }
        endpoint-name ep_name { capacity capacity | primary ip-address
        { ipv4 ipv4_address | ipv6 ipv6_address | port port_num}
        | secondary ip-address { ipv4 ipv4_address | ipv6 ipv6_address
        | port port_num } | tertiary ip-address { ipv4 ipv4_address
        | ipv6ipv6_address | port port_num }
        | fqdn { name fqdn_name | port port_num } }
        version [ uri-version version_num full version version_num ]
        end
```

NOTES:

- **group nrf mgmt** *mgmt_name* : Show the NRF self-management group configurations.
- **api-root** *api_string*: Specify the deployment-specific service API prefix that is used within the { apiRoot }.
- **api-uri-prefix** *uri_prefix_string*: Specify the {apiName}. If not configured, it takes the standard API name for the service as per the specification.
- **capacity** *capacity*: Specify the profile capacity.
- **endpoint-name** *ep_name* **{ capacity** *capacity* **| primary ip-address { ipv4** *ipv4_address* **| ipv6** *ipv6_address* **| port** *port_num* **} | secondary ip-address { ipv4** *ipv4_address* **| ipv6** *ipv6_address* **| port** *port_num* **} | tertiary ip-address { ipv4** *ipv4_address* **| ipv6** *ipv6_address* **| port** *port_num* **} }**: Specify the endpoint name. You can configure the primary, secondary, and tertiary hosts (IP: Port) within each endpoint for NF server failover handling. The server failover configuration accepts both the IPv4 and IPv6 addresses. However, the AMF gives preference to the IPv4 address.
  - **capacity** *capacity*: Specify the node capacity for the endpoint. *capacity* must be an integer in the range of 0-65535.
  - The endpoint selection for sending the message is based on probabilistic load-balancing algorithm (IETF RFC 2782) using the priority and capacity parameters.
  - **primary ip-address { ipv4** *ipv4_address* **| ipv6** *ipv6_address* **| port** *port_num* **}**: Specify the primary endpoint IPv4 address, IPv6 address, or port.
  - **secondary ip-address { ipv4** *ipv4_address* **| ipv6** *ipv6_address* **| port** *port_num* **}**: Specify the secondary endpoint IPv4 address, IPv6 address, or port.
  - **tertiary ip-address { ipv4** *ipv4_address* **| ipv6** *ipv6_address* **| port** *port_num* **}**: Specify the tertiary endpoint IPv4 address, IPv6 address, or port.
  - **priority** *priority_value*: Specify the priority for the service to select the appropriate profile using the load-balancing logic. *priority* must be an integer in the range of 0-65535.

- **fqdn name** *fqdn_name*: Specify the FQDN name.
- **fqdn port** *fqdn_port*: Specify the FQDN port number. If port is not configured, uses the standard port for FQDN, that is 80 for URI scheme HTTP and 443 for URI scheme HTTPS.

- **uri-scheme { http | https }**: Specify the URI scheme as **http** or **https**.
- **version [uri-version** *version_num* **full version** *version_num* **]**: Specify the api/version. The full version format is <Major-version>.<Minor-version>.<patch-version>.[alpha-<draft-number>].

Verifying the NF Endpoint Profile Parameters for NF Management

Use the **show running-config group nrf** command to verify the NF endpoint profile parameters for NF management.

```
show running-config group nrf
group nrf mgmt mgmt_group
 service type nrf nnrf-nfm
  endpoint-profile epprof
  uri-scheme http
   endpoint-name EP1
   priority       2
   primary ip-address ipv4 209.165.200.231
   primary ip-address port 8082
   secondary ip-address ipv4 209.165.200.232
   secondary ip-address port 8082
 exit
   endpoint-name EP2
      priority 10
       primary ip-address ipv4 209.165.200.231
       primary ip-address port 8082
       secondary ip-address ipv4 209.165.200.232
       secondary ip-address port 8082
     exit
   exit
 exit
exit
```

AMF Deregistration with NRF

Feature Description

The AMF supports the deregistration of Network Function (NF) Repository Function (NRF), wherein the NF deregister service operation of the AMF removes the profile of a network function that is registered in the NRF.

The AMF starts the NF deregister service operation in the following scenarios:

- When the Service Based Interface (SBI) endpoint is not configured and all the rest endpoints stop functioning.
- When all the configured SBI endpoints VIP IP and N11 VIP IPs are offline.

Note AMF can't perform NRF deregistration when all the REST endpoints abruptly stop functioning. Only the REST endpoints can perform registration or deregistration of NRF.

How it Works

The NF deregister service operation deletes the specific resource based on its NF instance ID. The NF deregistration starts when the Uniform Resource Identifier (URI) receives a request to delete a specific NF instance.

The recommended AMF shutdown process involves the following steps:

1. All N11 and SBI VIP IPs are marked as offline. After these endpoints appear offline, the NF deregistration request is sent to the NRF. The NRF notifies the peer NFs, such as SMF, about the AMF shutdown and its unavailability for traffic.
2. Wait for a grace period to allow convergence and perform a "system mode shutdown" to stop all the pods.

When the endpoint SBI is not configured, the system deletes the rest-ep pod immediately and avoids proper convergence. Implementing the system mode shutdown without taking the SBI and N11 VIP IPs offline also avoids convergence.

Call Flows

This section describes the following call flows:

- NRF deregistration call flow
- NRF deregistration trigger events call flow

NRF Deregistration Call Flow

This section describes the NF deregistration call flow.

Figure 1: NRF Deregistration Call Flow

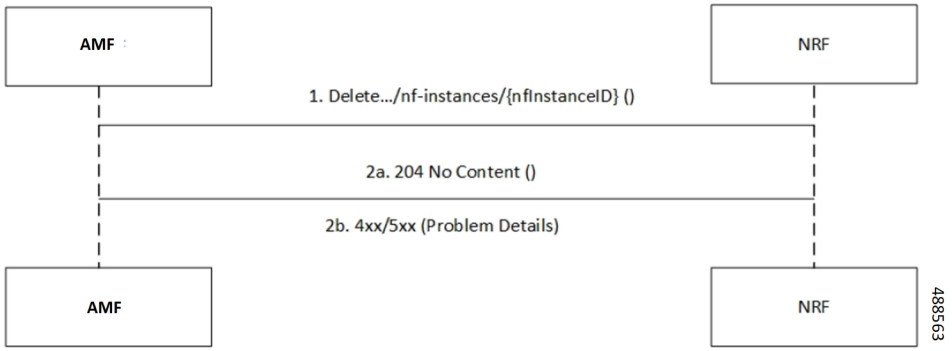


Table 1: NRF Deregistration Call Flow Description

Step	Description
1	The AMF sends a Delete request to the resource URI that indicates the NF instance. The request body is empty.
2a	If the deletion of the specified resource is successful, the "204 No Content" message appears. The response body remains empty.

Step	Description
2b	If the NF instance, which is identified with the NF instance ID, does not exist in the list of registered NF instances in the NRF database, the NRF sends the "404 Not Found" status code with the problem details.

NF Deregistration Trigger Events Call Flow

This section describes the NF deregistration trigger events call flow.

Figure 2: NF Deregistration Trigger Events Call Flow

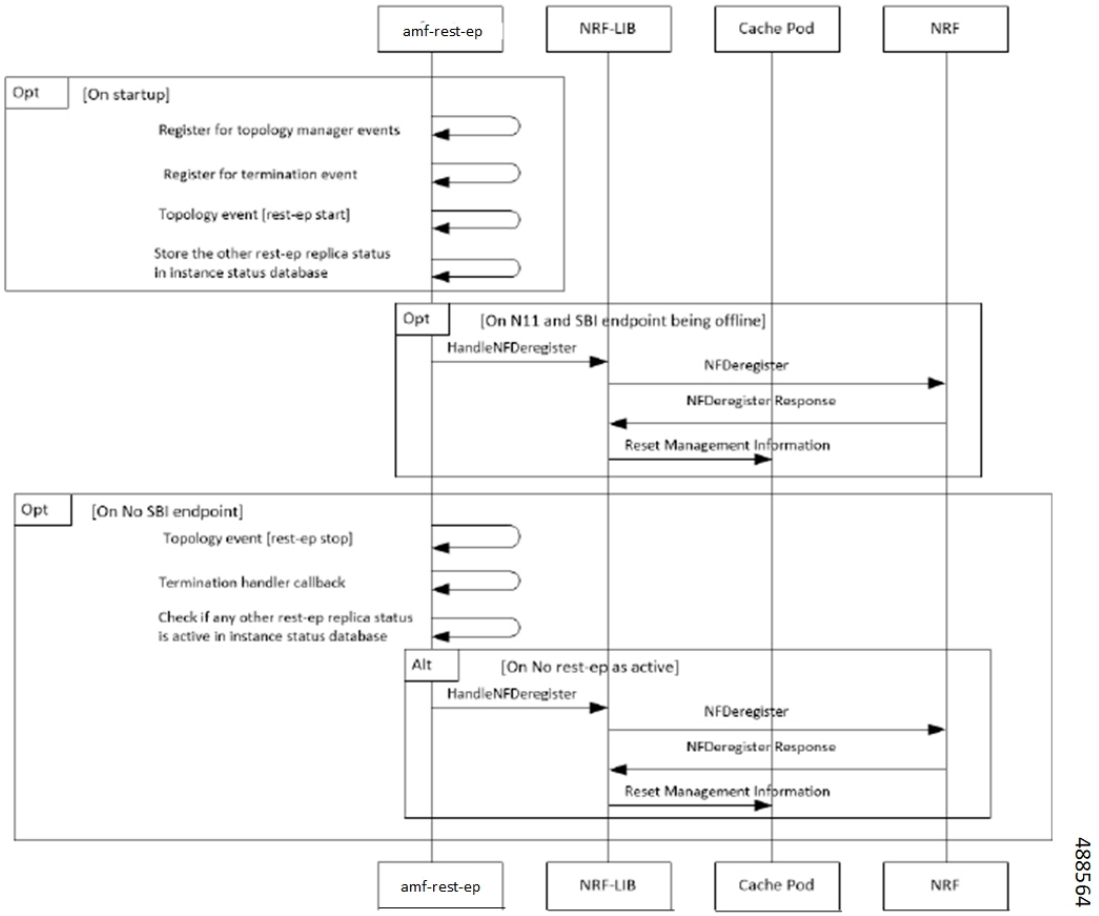


Table 2: NF Deregistration Trigger Events Call Flow Description

Step	Description
On startup	
1	The AMF rest-ep registers for topology manager events to identify the state of other rest-ep instances and keeps a track of these instances in an instance state database.
2	The AMF rest-ep registers for the termination handler with the application infrastructure for receiving notification when the application infrastructure stops functioning. As part of the termination handler, the AMF rest-ep monitors the instance state database for any other working rest-ep.

Step	Description
3	The AMF rest-ep starts the topology event.
4	The AMF rest-ep saves the status of other rest-ep replicas in the instance state database.
When the N11 and SBI endpoints are offline	
5	The AMF rest-ep sends the Handle NF deregister message to the NRF-Lib.
6	When all the SBI and N11 VIP IP endpoints are offline, the AMF rest-ep sends the deregistration request to the NRF.
7	The NRF sends the NF deregister response to the NRF-Lib.
8	The NRF-Lib resets all the management information that is configured in the cache pod.
When no SBI endpoint exists	
9	The AMF rest-ep starts the topology event to stop the other rest-ep.
10	The AMF rest-ep starts the termination handler callback.
11	The AMF rest-ep checks the instance status database for any other working rest-ep.
When no rest-ep is functional	
12	The AMF rest-ep sends the Handle NF deregister message to the NRF-Lib.
13	The AMF rest-ep sends the deregistration request to the NRF.
14	The NRF sends the NF deregistration response to the NRF-Lib.
15	The NRF-Lib resets all the management information that is configured in the cache pod.

Standards Compliance

The AMF deregistration with NRF feature complies with the following standards:

- *3GPP TS 29.510 version 15.4.0 — 5G System; Network function repository services; Stage 3*

Limitations

The AMF deregistration with NRF feature has the following limitation:

- When N11 and SBI VIP IPs are not marked offline, the NF deregistration is not sent for the system mode shutdown because no specific order for pod deletion exists. In addition, no monitoring procedure exists to check if the rest-ep pods are working.

NF Heartbeat

Feature Description

The NF Heartbeat feature enables the NFs to notify the NRF that the NF is operational. Each NF registered with the NRF contacts the NRF periodically by invoking the NF Update service operation. The time interval at which the NRF is contacted is deployment-specific and is returned by the NRF to the AMF as a result of a successful registration.

AMF sends the NF status and load parameter as part of NF heartbeat to NRF. AMF provides a CLI to configure the interval between periodic NF heartbeat. If the heartbeat value is configured in the NF registration response, the same value is used instead of another configured value.

NF Heartbeat Interval

The AMF NF Heartbeat feature notifies the NRF that the AMF is operational. The default heartbeat interval is once in 10 seconds. With the **heartbeat interval** CLI command, you can configure the interval (in seconds) between the heartbeats. If NRF returns a different heartbeat time value as part of NF registration response or heartbeat response, then the same interval is used for subsequent heartbeats. As part of the heartbeat, NRF sends the HTTP PATCH Request to the resource URI representing the NF instance. The payload body of the PATCH Request contains a "replace" operation on the "nfStatus" attribute of the NF profile of the NF instance, and configures it to the "REGISTERED" value. This release does not support parameters, such as load and capacity.

Note AMF uses the configured heartbeat. If the heartbeat is not configured, AMF uses the locally configured heartbeat.

How it Works

Call Flows

NF Heartbeat Call Flow

The following figure illustrates the NF heartbeat call flow.

Figure 3: NF Heartbeat Call Flow

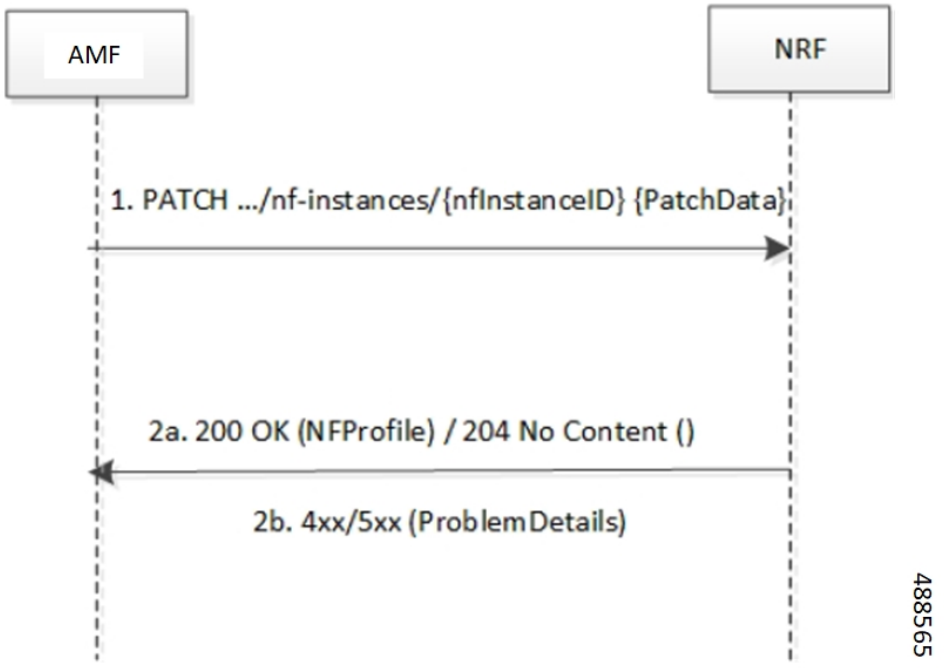


Table 3: NF Heartbeat Call Flow Description

Step	Description
1	The NF Service Consumer sends a PATCH request to the resource URI representing the NF instance. The payload body of the PATCH request contains a replace operation on the nfStatus attribute of the NF Profile of the NF instance, and set it to the value REGISTERED.
2	On success, if the NF Profile changes, the NRF returns "200 OK" along with the full NF Profile data in the response body; otherwise, "204 No Content" is returned.
3	If the NF instance, identified by the "nfInstanceID", is not found in the list of registered NF instances in the NRF's database, the NRF returns "404 Not Found" status code with the ProblemDetails IE providing details of the error. Example: **PATCH .../nf-instances/4947a69a-f61b-4bc1-b9da-47c9c5d14b64** **Content-Type: application/json-patch+json** **[** **{"op": "replace", "path": "/nfStatus", "value": "REGISTERED"}** **]** **HTTP/2 204 No Content** **Content-Location:** **.../nf-instances/4947a69a-f61b-4bc1-b9da-47c9c5d14b64**

Standards Compliance

The NF Heartbeat feature complies with the following standards:

- *3GPP TS 29.510, version 15.4.0 (2019-07) — 5G System; Network function repository services; Stage 3*

Configuring NRF Heartbeat Interval

This section describes how to configure the NRF heartbeat interval.

```
config
  group nf-mgmt nf_mgt_name
    hearbeat interval  hearbeat_interval
  end
```

NOTES:

- **group nf-mgmt** *nf_mgt_name*: Specify the group name of NF management.
- **hearbeat interval** *hearbeat_interval*: Specify the interval of hearbeat between the heartbeats. The value of heartbeat interval is in seconds.

Note If NRF returns a different heartbeat interval value as part of NF registration response or heartbeat response, the same value is used for subsequent heartbeats.

NRF Support for AMF Subscription and Notification

Feature Description

The AMF uses the NRF-provided Subscription service to subscribe to NF status changes that the NF receives as a discovery response. This feature helps in updating the cached NF discovery responses.

The AMF honors only the notification changes in load, capacity, status at the NF level, and at the service level. It ignores all other parameter changes in the notification.

After the successful subscription for notification service, the AMF receives notifications of registration and deregistration of NF Instances, or notifications of NF profile changes for a given NF Instance.

The AMF supports the "NFProfile" field and "ChangeItem" field in the "NotificationData". If the notification event type is set to "NF_PROFILE_CHANGED", the AMF receives notification about the profile-level changes or a list of individual change items for the NFProfile parameters along with nfInstanceUri.

The "ChangeItem" field includes the following parameters:

- op—Indicates the type of change that happens to the resource.
- path—Contains the JSON pointer value which indicates the target location within the resource.
- from—Indicates the path of the JSON element that is moved or copied to the location indicated by the "path" attribute. It is present if the "op" attribute is of value "MOVE".
- origValue—Indicates the original value at the target location within the resource specified in the "path" attribute.
- newValue—Indicates a new value at the target location within the resource specified in the "path" attribute.



Note The AMF currently supports only the ADD, REPLACE, and REMOVE operations as part of the "op" parameter.

The following is an example of the notification payload sent from the NRF when an NF instance has changed its profile by updating the IP address value and the TCP port for the first endpoint of the first NF service.

Example 1:

```
{
  "event": "NF_PROFILE_CHANGED",
  "nfInstanceUri": ".../nf-instances/4947a69a-f61b-4bc1-b9da-47c9c5d14b64",
  "profileChanges": [
    {
      "op": "REPLACE",
     "path": "/nfServices/0/ipEndPoints/0/ipAddress", ===> Change ipAddress to ipv4Address

      "newValue": "209.165.201.10"
    },
    {
      "op": "REPLACE",
      "path": "/nfServices/0/ipEndPoints/0/port",
      "newValue": 8080
    }
  ]
```

Example 2:

```
{
"event": "NF_PROFILE_CHANGED",
"nfInstanceUri": ".../nf-instances/4947a69a-f61b-4bc1-b9da-47c9c5d14b64",
"nfProfile": <Newly updated complete profile>
}
```

How it Works

This feature uses the NF Subscribe service to subscribe to changes on the status of NF instances that the NF receives as discovery responses. The AMF sends a subscription for the response validity period for each of the NF profiles that it receives in the discovery response. The AMF checks if an existing NF instance subscription time needs an extension or not depending on the current response time validity. If a subscription needs an extension, a subscription PATCH is sent with the extended validity time.

During subscription, the NRF may respond with a modified validity time. This validity time might differ from the AMF validity time request. In such a scenario, the AMF tracks the required subscription time and the actual subscription time returned by the NRF.

The AMF periodically (every two minutes) checks in database if there is any subscription with the actual subscription time ending soon (as in next five minutes) but has required validity time more than the actual validity time. In this scenario, the AMF sends a PATCH subscription to extend the subscription validity time.

The AMF fills the Status Notification URI based on the interface NRF configuration that is specified in the configuration. The notification VIP IP and VIP port are used to frame the status notification URI.

```
http://{nrfinterface.vip-ip}:{ nrfinterface.vip-port}/{notifResourceURI}
```

On status notification, the AMF updates the local cache and the external cache (cache pod) with the changed attributes.

Call Flows

This section describes the call flows for the AMF Subscription and Notification feature.

Subscription (PATCH) Call Flow

The NRF updates the subscription to notifications on NF instances to refresh the validity time, when the specified time is due to expire. The AMF can request a new validity time to the NRF. If the operation is successful, the NRF can assign and provide a new validity time to the NF.

Updating the "subscriptionID" resource, initiates the Subscription (PATCH) operation. The operation starts on issuing an HTTP PATCH request on the URI representing the individual resource.

The following figure illustrates the call flow for subscription to NF instances in the same PLMN.

Figure 4: Subscription (PATCH) Call Flow

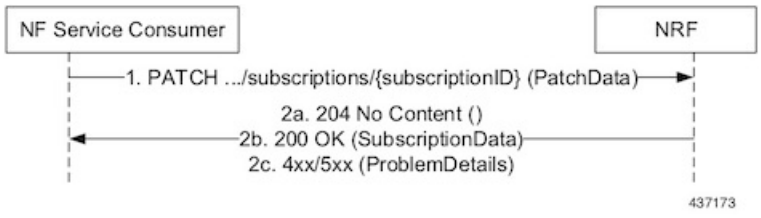


Table 4: Subscription (PATCH) Call Flow

Step	Description
1	The AMF sends a PATCH request to the resource URI identifying the individual subscription resource. The payload body of the PATCH request contains a "replace" operation on the "validityTime" attribute of the SubscriptionData structure. The request also contains a new suggested value for the "validityTime" attribute. This replace operation does not replace any other attribute of the resource.
2a	When a subscription is successful, the NRF sends a "204 No Content" response. This response indicates that the NRF accepts: • Extension of the subscription lifetime • Value of the "validityTime" attribute
2b	If the subscription fails due to errors in the JSON Patch object in the request body, the NRF returns a "400 Bad Request" status code with the problem details.

2c	If the subscription fails due to internal errors in the NRF, the NRF returns a "500 Internal Server Error" with the problem details.
	Example:
	`PATCH .../subscriptions/2a58bf47`
	`Content-Type: application/json-patch+json`
	`[`
	`{ "op": "replace", "path": "/validityTime", "value": "2018-12-30T23:20:50Z" },`
	`]`

Subscription (POST) Call Flow

The Subscription service operation allows to:

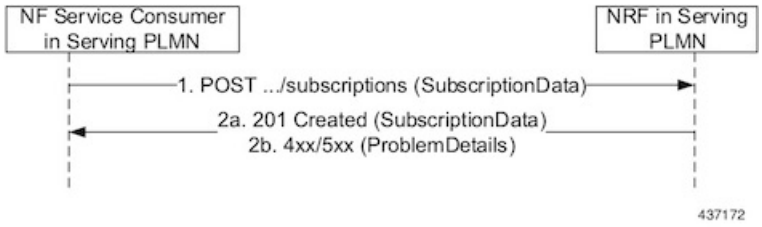
- Create a subscription so that the AMF can request notification (depending on certain filters) in the following scenarios:
  - When there is a registration or deregistration in the NRF.
  - When there is a modification to a profile.
- Create a subscription to a specific NF instance such that the AMF can request notification in the following scenarios:
  - When there is a modification to an NF instance.
  - When there is a deregistration of an NF instance.



Important Currently, AMF only supports the subscription of NF instances that the NF receives as its discovery response.

The following figure illustrates the call flow for subscription to NF instances in the same PLMN.

Figure 5: Subscription (POST) Call Flow



Implementing the subscription to notifications on NF instances creates a new individual resource under the collection resource "subscriptions." Issuing a POST request starts the operation on the Uniform Resource Identifier (URI) representing the "subscriptions" resource.

Table 5: Subscription (POST) Call Flow Description

Step	Description
1	The NF Service Consumer sends a POST request to the resource URI representing the "subscriptions" collection resource. The request body includes data that indicates the type of notifications that the AMF has subscribed to receive. It also contains a callback URI, where the AMF prepares to receive the actual notification from the NRF. The notification contains the AMF suggested validity time, which represents the time span during which the subscription remains active. The subscription request may also include more parameters indicating the list of attributes in the NF Profile to monitor (or to exclude from monitoring). This request determines if the NRF must send a notification, when there is a change in any of the profile attributes. The subscription data also includes the **reqNfType** attribute, which contains the NF type of the NF Service Consumer that requests the creation of the subscription. The NRF uses it for authorizing the request.
2a	When a subscription is successful, the NRF sends a "201 Created" response. This response contains newly created subscription data that includes the NRF-determined validity time beyond which, the subscription is invalid. When the subscription expires, the AMF creates a new subscription in the NRF to continue receiving status notifications.
2b	If the subscription fails due to errors in the subscription data, the NRF returns a "400 Bad Request" status code with the problem details. If the subscription fails due to internal errors in the NRF, the NRF returns a "500 Internal Server Error" with the problem details.

NFStatus Notify Call Flow

When a POST request is issued to each callback URI of the various subscribed NF instances, the AMF initiates the NFStatus Notify operator.

The following figure illustrates the NFStatus Notify call flow.

Figure 6: NFStatus Notify Call Flow

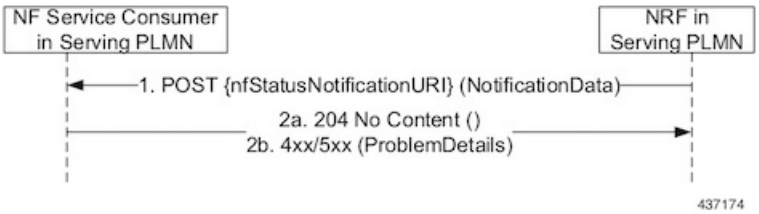


Table 6: NFStatus Notify Call Flow Description

Step	Description
1	The NRF sends a POST request to the callback URI. The request body for a profile change notification request includes the following: • **event**—This attribute indicates the notification type. It can be one of the following: • NF_REGISTERED • NF_DEREGISTERED • NF_PROFILE_CHANGED • **nfInstanceUri**—Uniform Resource Identifier (URI) of the NF instance associated to the notification event. • **nfProfile**—Indicates the new or updated NF profile. • **profileChanges**—This attribute identifies changes on the profile of the NF instance associated to the notification event. This attribute is available when the event notification type is "NF_PROFILE_CHANGED".
2a	When the notification is successful, the NRF sends a "204 No content" response.
2b	If the AMF disregards "nfStatusNotificationURI" as a valid notification URI, the AMF returns a "404 Not Found" status code with the problem details. For example, if the URI does not belong to any of the existing subscriptions that the AMF has created in the NRF.

Limitations

This feature has the following limitations:

- NF status notification supports only NF profile load, NF profile capacity, NF profile status, service load, service capacity, and service status parameter changes.
- AMF supports only the NFPofiile field in the "NotificationData." It does not support the "Change item" field.
- The AMF supports notification of the following parameter changes:
  - nfProfile
    - nfStatus
    - ipv4Address

- ipv6Address
- priority
- capacity
- load

- nfService
  - version



Note Change to a new version is permitted but not the deletion and modification of the existing version.

- scheme



Note Currently, http is only supported

- nfServiceStatus
- ipEndPoints
- apiPrefix
- capacity
- load
- priority

- The AMF currently supports only the ADD, REPLACE, and REMOVE operations as part of the "op" parameter in the "ChangeItem" field.

Configuring NRF for Subscription and Notification

This section describes how to configure the NRF for subscription and notification.



Note For the subscription and notification to work, it is mandatory to configure the NRF interface within SBI interface.

When discovery is done with NRF, a subscription message for the discovered NF instances is sent. The AMF fills the Status Notification URL based on the NRF interface configuration that is specified in the configuration. The notification VIP IP and VIP port are used to frame the status notification URL. The AMF uses the URL that is included in the subscription request message for status notifications.

To configure the NRF interface, vip-ip, vip-port, and loopback port to open the server endpoints for the NF status notification, use the following sample configuration.

```
config
  instance instance-id gr_instance_id
    endpoint sbi
      replicas replica_num
        vip-ip ip_address
      interface nrf
        vip-ip ip_address
        vip-port port_number
        loopbackPort port_number
        end
```

NOTES:

- **interface nrf**: Specify the interface as NRF.
- **vip-ip** *ip_address*: Specify the virtual IP address of the virtual host. The AMF uses this as the listening IP address for the status notification.
- **vip-port** *port_number*: Specify the port number of the virtual host. The AMF uses this as the listening port for the status notification.
- **loopbackPort** *port_number*: Specify the internal port number of the loopback host. The AMF uses this port for the NF status notification.

Standard Compliance

This feature complies to *3GPP TS 29.510, Version 16.4.0*.

NF Profile Update

Feature Description

The AMF invokes the NF Update service operation when there are changes to the NF registration parameters due to the AMF profile configuration change.

The NF Update service updates the NF profile that was previously registered in the NRF by providing the updated profile of the requesting NF to the NRF.

The update operation can be one of the following:

- A whole NF profile update (complete replacement of the existing profile with a new profile)
- An update to only a subset of the NF profile parameters (adding, deleting, or replacing services to the NF profile)

How it Works

This section describes the NF profile update procedure.

Call Flows

This section describes the following call flows:

- NF Profile Complete Replacement Call Flow, on page 17

• NF Registration and NF Update Call Flow, on page 17

NF Profile Complete Replacement Call Flow

The following figure illustrates a call flow representing the complete NF profile replacement.

Figure 7: NF Profile Complete Replacement

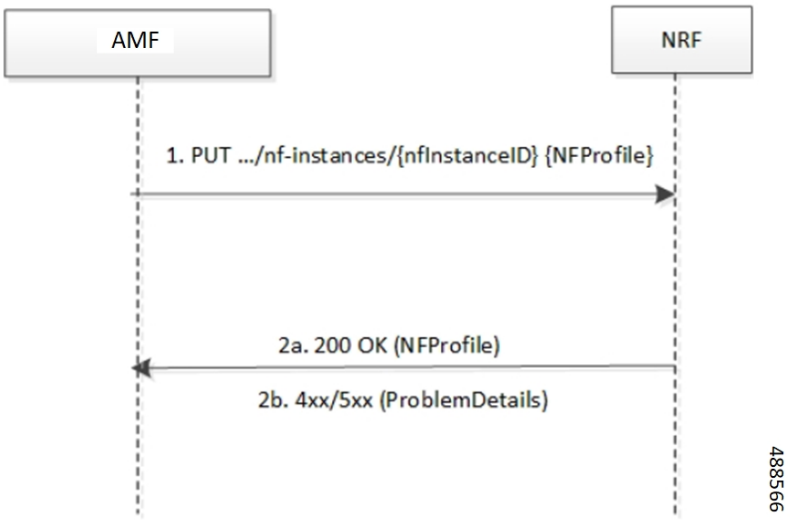


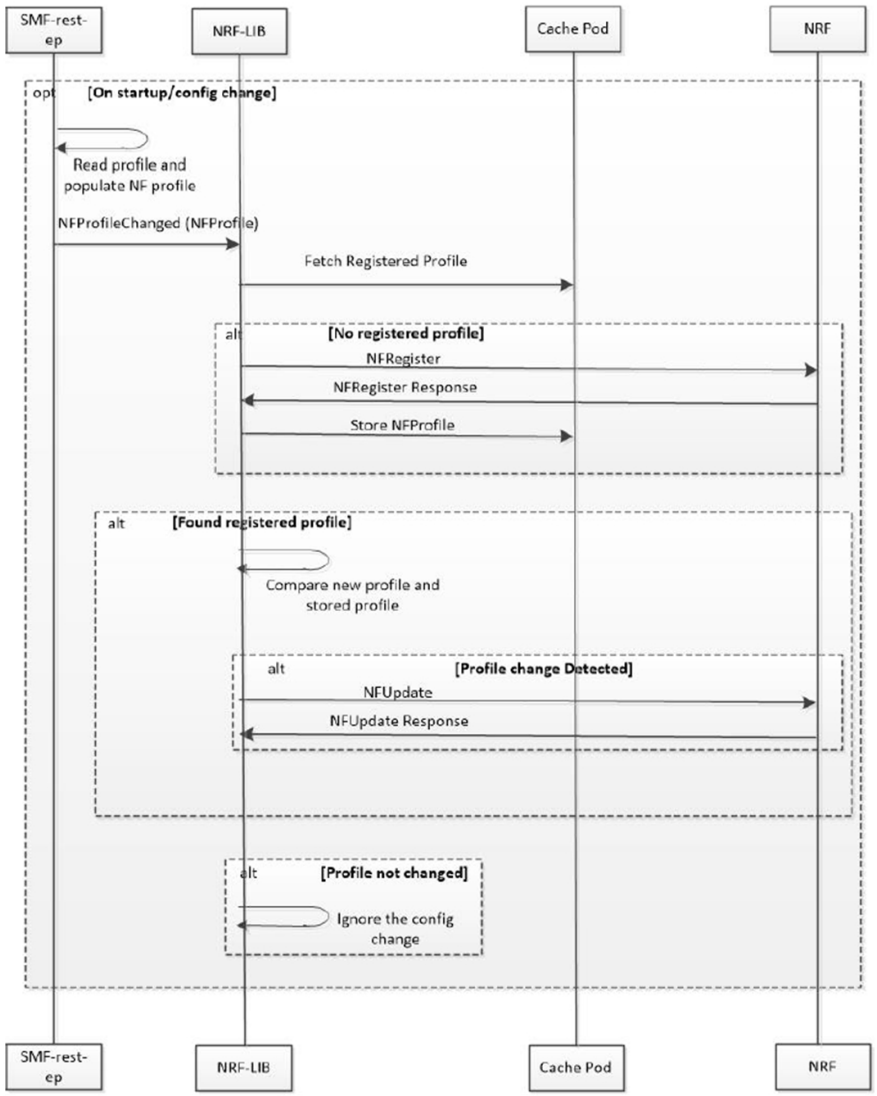
Table 7: NF Profile Complete Replacement Call Flow Description

Step	Description
1	The AMF sends a PUT request to the resource URI representing the NF instance. The payload body of the PUT request contains an update operation on the NF Profile of the NF instance.
2a	On success, if the NF Profile changes, the NRF returns "200 OK" along with the full NF Profile data in the response body.
2b	If the NF instance, identified by the "nfInstanceID", is not found in the list of registered NF instances in the NRF database, the NRF returns 4xx or 5xx status code with the ProblemDetails IE providing details of the error.

NF Registration and NF Update Call Flow

The following figure illustrates the call flow representing the NF registration and NF update messaging from AMF on NF profile change trigger from REST-EP.

Figure 8: NF Registration and NF Update Call Flow



1. The AMF REST-EP, on start-up, reads the AMF profile configuration and accordingly populates the NF management profile. The REST-EP then triggers AMF to indicate the NF Profile change.
2. The AMF maintains the NF registration status and the registered profile in an external cache pod. The AMF detects whether the NF registration with NRF is completed. If the AMF detects that the registration is not completed during NF profile change handling, perform Step 3. If the NF registration is complete, perform Step 4.
3. The AMF sends NF Register to NRF. It allows an NF instance to register its NF profile in the NRF. It includes the registration of the general parameters of the NF instance along with the list of services exposed by the NF instance.
4. The AMF fetches the registered NF profile and then compares it with the new profile.
5. The AMF sends NF update (PUT) request to the NRF when any of the parameters in the NF management profile changes due to AMF profile configuration change.

Load parameter is not set as part of the PUT message. Heartbeat is set as the current active heartbeat interval.

6. The AMF ignores the trigger if there is no change detected.



Important The NF update is sent only from the elected AMF.

Standards Compliance

The NF Profile Update feature complies with the following standards:

- *3GPP TS 29.510, Version 15.4.0 (2019-07) – 5G System; Network function repository services; Stage 3*

Limitations

The NF Profile Update feature has the following limitation:

- Supports only the complete replacement of NF profile.
- Doesn't support capacity.

NF Discovery

Feature Description

The AMF uses the NRF-provided, NF discovery service to discover network functions (NFs), such as Access and Mobile Function (AMF), Unified Data Management (UDM), and Policy Control Function (PCF). The AMF configures the preferred locality as provided in the "profile nf-pair" configuration of Network Repository Function (NRF) in the discovery query.

For each NF, the query parameters, also known as filters, are configurable. Based on these parameters, NRF returns all the NFs matching the query criteria for the AMF to discover NF profiles.



Note The NF discovery and load-balancing capabilities are available only for UDM, PCF, CHF, and AMF.

NF discovery supports dynamic configuration change. With this feature, if the configurations were modified in the middle of the transaction or procedure, the ongoing transactions are not impacted.

The dynamic configuration change feature supports the following:

- NRF transaction or procedure picks a configuration version (v1) and uses the same version until the NRF transaction or procedure completes.
- If you change the configuration during an ongoing NRF transaction, then a new configuration version (v2) is created. However, the new configuration is applied in the new transaction.

The dynamic configuration changes apply to the following data structures:

- NrfFailureProfileSt
- NrfClntProfileSt
- NrfGrpSt
- NrfPairProfileSt
- NrfMgmtGrpSt

How it Works

The service operation is executed by querying the "nf-instances" resource. The request is sent to an NRF in the same PLMN of the AMF.

Call Flows

This section describes the call flow associated with this feature.

Service Discovery Request Call Flow

This section describes the service discovery request call flow.

Figure 9: Service Discovery Request Call Flow

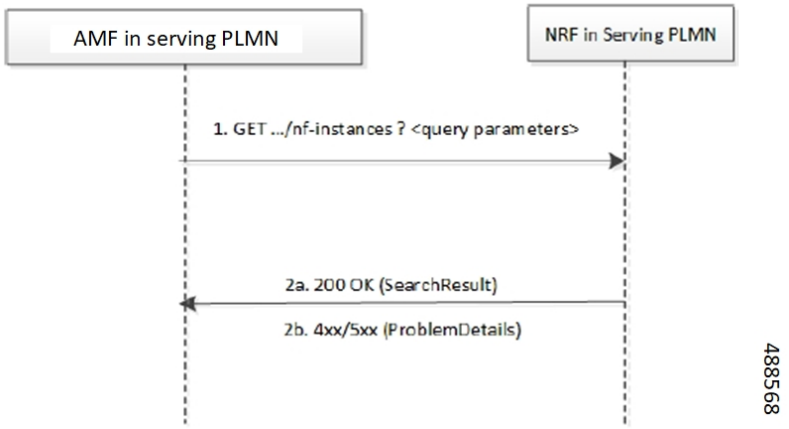


Table 8: Service Discovery Request Call Flow Description

Step	Description
1	The AMF sends an HTTP GET request to the resource URI "nf-instances" collection resource. The input filter criteria for the discovery request exists in query parameters.
2a	On success, "200 OK" is returned. The response body contains a validity period, during which the AMF caches the search result, and an array of NF profile object that satisfy the search filter criteria. For example, all NF instances displaying a certain NF Service name.

Step	Description
2b	If the AMF is not allowed to discover the NF services for the requested NF type provided in the query parameters, the NRF returns "403 Forbidden" response. If the discovery request fails at the NRF due to errors in the input data in the URI query parameters, the NRF returns "400 Bad Request" status code with the "ProblemDetails" IE providing details of the error. If the discovery request fails at the NRF due to NRF internal errors, the NRF returns "500 Internal Server Error" status code with the "ProblemDetails" IE providing details of the error.

The NF profile objects that are returned in a successful result contains generic data of each NF instance, applicable to any NF type. These objects can also contain NF-specific data, for those NF instances belonging to a specific type (for example, the attribute "udrInfo" exists in the NF profile when the type of the NF instance takes the "UDR" value). In addition, the attribute "customInfo" exists in the NF profile for NF instances with custom NF types. For NF instances, the NRF returns the "customInfo" attribute, if available, as part of the NF profiles returned in the discovery response.

The AMF service communicates with different NFs, such as UDM, SMF, PCF, and CHF, when the session is active. The NF discovery is based on set of filters, also called query parameters, which are associated with the session. The AMF service discovers the NFs, matching the filter criteria for the session, to send messages to NF.

The AMF supports the following filters:

- Dnn
- Tai
- TargetNfFqdn
- TargetPlmnList
- TargetNfInstanceId
- Snssais
- Preferred locality

The discovered NFs are cached with the filter as the key. The endpoint selection for sending the message is based on probabilistic load balancing algorithm (IETF RFC 2782) using the priority and capacity parameters. The NF discovery response carries a validity time, which decides the cache validity period.

AMF sends the messages to a target based on the Location header URL in response to initial messages sent to NF.

AMF supports stickiness wherein the endpoint, service instance, and NF instance details of the selected endpoint for a message that is sent, will be provided to the application or REST-EP so that the same can be specified in subsequent message (instead of discovery filter). This operation helps in maintaining stickiness for a session to the selected NF.

Standards Compliance

The NF Discovery feature complies with the following standards:

- *3GPP TS 29.510 version 15.4.0 (2019-07) – 5G; 5G System; Network function repository services; Stage 3*

Limitations

The NRF Discovery feature has the following limitations:

- The cache maintained is local to the library. In case of deployment with multiple replicas of REST-EP, if two Discovery or Send messages with the same discovery filter land on different pods, then both the pods trigger NF discovery.
- This feature supports only the UDM, PCF, CHF, and SMF discovery, and load balancing. It does not support UPF discovery.

Configuring NRF for Discovery

This section provides the configurations that are required to perform the NF discovery.

Registering NRF

To register an NRF, use the following sample configuration.

```
config
nssai name nssai_name
    sst sst ssd ssd
    dnn dnn_name_value
    end
```

NOTES:

- **nssai name** *nssai_name*: Configure the NSSAI name value for the slice. The *nssai_name* value must be a string.



Note AMF supports a maximum of 512 slices to be sent toward NRF.

Configuration Example

The following is an example configuration of the NRF registration.

```
nssai name slice1
 sst 02
 sdt Abf123
 dnn [ dnn1 intershat intershat1 intershat2 intershat3 intershat4 intershat5 intershat6
intershat7 starosupf ]
exit

nssai name slice2
 sst 02
 sdt Abf124
 dnn [ dnn1 intershat intershat1 intershat2 intershat3 intershat4 intershat5 intershat6
intershat7 starosupf ]
exit
```

Discovering NRF

To configure the NRF discovery, use the following sample configuration:

```
config
  profile network-element [ smf amf_profile_name| chf chf_profile_name | pcf
pcf_profile_name | udm udm_profile_name | upf upf_profile_name ]
     query-params requester-snssais
     exit
```

NOTES:

- **query-params requester-snssais**: Specify the list of Single Network Slice Selection Assistance Information (S-NSSAIs) as the query parameter in the NF discovery request towards the NRF.

Configuration Example

The following is an example configuration.

```
config
   profile network-element udm udm1
      query-params requester-snssais
      exit
   profile network-element pcf pcf1
      query-params requester-snssais
      exit
   profile network-element chf chf1
      query-params requester-snssais
      exit
   profile network-element upf upf1
      query-params requester-snssais
      exit
   profile network-element amf amf1
      query-params requester-snssais
      exit
```

Configuring NF Client Profile

To configure the NF endpoints for , CHF, PCF, and UDM, use the following sample configuration:

```
config
  profile nf-client { nf-type { smf smf-profile | chf chf-profile | pcf
pcf-profile | udm udm-profile } nf_profile_name }
  end
```

NOTES:

- **profile nf-client { nf-type { smf smf-profile | chf chf-profile | pcf pcf-profile | udm udm-profile }** *nf_profile_name* **}**: Specify the required NF client profiles and provide the local configuration for any of the following configured NFs:
  - **smf**: Enable the local configuration
  - **chf**: Enable the CHF local configuration
  - **pcf**: Enable the PCF local configuration
  - **udm**: Enable the UDM local configuration

    For example, if you are configuring the **smf smf-profile** keyword, this command enables the local configuration. The same approach applies for the other configured NFs.

    nf_profile_name must be an alphanumeric string representing the corresponding NF client profile name.

- You can configure multiple NF profiles within a given service.
- To disable the configuration, use the **no profile nf-client { nf-type { smf smf-profile | chf chf-profile | pcf pcf-profile | udm udm-profile }** *nf_profile_name* **}** command.

Configuration Example

The following is an example configuration.

```
profile nf-client nf-type pcf
pcf-profile pcf-profile
  locality LOC1
   priority 1
   service name type npcf-smpolicycontrol
    endpoint-profile epprof
     capacity   10
     priority   1
     uri-scheme http
     endpoint-name ep1
      priority 1
      capacity 10
      primary ip-address ipv4 209.165.202.133
      primary ip-address port 8080
     exit
     endpoint-name ep2
      priority 1
      capacity 10
      primary ip-address ipv4 209.165.201.1
      primary ip-address port 8080
     exit
    exit
   exit
  exit
exit
exit
profile nf-client nf-type pcf
pcf-profile pcf-profile
  locality LOC1
   priority 1
   service name type npcf-smpolicycontrol
    endpoint-profile epprof
     capacity   10
     priority   1
     uri-scheme http
     endpoint-name ep1
      priority 1
      capacity 10
      primary ip-address ipv4 209.165.201.2
      primary ip-address port 8080
     exit
```

Associating a Discovery Group with NF Type

To pair a discovery group with NF types, use the following sample configuration.

```
config
   profile nf-pair nf-type nf_type
      nrf-discovery-group nrfdisc_group_name
      end
```

NOTES:

- **nf-type** *nf_type*: Specify the NF client type value as AMF.
- **nrf-discovery-group** *nrfdisc_group_name*: Specify the NRF discovery group name. Discovery group is the logical link to the NRF endpoint groups (nrf-group). For each NF type, you can associate a discovery group and the locality information.

Configuring NF Endpoint Profile Parameters in NRF Discovery Group

The AMF provides CLI for configuring NF endpoints for **nnrf-nfd** (NF discovery).

Note For a discovery group, you can configure only the **nnrf-disc** service.

The CLI configuration allows configuring multiple endpoints under each endpoint profile. The AMF uses the priority and capacity parameters to load balance between these endpoints. All endpoints under an endpoint profile share the session context. That is, when selecting an endpoint profile for initial message of a session, then the AMF sends the subsequent messages (for example, update, delete, and so on) of the session to any of the endpoints in the endpoint profile.

Primary, secondary, and tertiary hosts [ip:port] can be configured within each endpoint. Both IPv4 and IPv6 addresses can be specified. If both are specified, then the IPv4 address is preferred.

AMF provides APIs to discover and send a message to an NF matching a set of filter parameters.

A URI uniquely identifies a resource. In the 5GC SBI APIs, when a resource URI is an absolute URI, the structure is specified as follows:

```
{apiRoot}/{apiName}/{apiVersion}/{apiSpecificResourceUriPart}
```

apiRoot is a concatenation of the following parts:

- scheme ("http" or "https")

Note Both HTTP and HTTPS scheme URIs are allowed. See the *3GPP TS 33.501, subclause 13.1* for more information on security of service-based interfaces.

- fixed string "://"
- authority (host and optional port) as defined in IETF RFC 3986
- an optional deployment-specific string (API prefix) that starts with a "/" character [api-root in CLI]

To configure the NRF endpoints for different services supported by NRF, use the following sample configuration:

```
config
  group nrf discovery discovery_name
    service type nrf nnrf-disc
      endpoint-profile
        name epprofile_name
        api-root api_string
        api-uri-prefix uri_prefix_string
        uri-scheme { http | https }
```

```
          endpoint-name ep_name { capacity capacity | primary ip-address {
ipv4 ipv4_address | ipv6 ipv6_address | port port_num } | secondary ip-address {
 ipv4 ipv4_address | ipv6 ipv6_address| port  port_num } | tertiary ip-address
{ ipv4 ipv4_address| ipv6 ipv6_address | port port_num } }
          version [ uri-version version_num full version version_num ]
          end
```

NOTES:

- **group nrf discovery** *discovery_name* : Configure the NRF discovery group.
- **api-root** *api_string*: Specify the deployment-specific service API prefix that is used within the { apiRoot }.
- **api-uri-prefix** *uri_prefix_string*: Specify the {apiName}. If not configured, it takes the standard API name for the service as per the specification.
- **endpoint-name** *ep_name* **{ capacity** *capacity* **| primary ip-address { ipv4** *ipv4_address* **| ipv6** *ipv6_address* **| port** *port_num* **} | secondary ip-address { ipv4** *ipv4_address* **| ipv6** *ipv6_address* **| port** *port_num* **} | tertiary ip-address { ipv4** *ipv4_address* **| ipv6** *ipv6_address* **| port** *port_num* **} }**: Specify the endpoint name. You can configure the primary, secondary, and tertiary hosts (IP: Port) within each endpoint for NF server failover handling. The server failover configuration accepts both the IPv4 and IPv6 addresses. However, the AMF gives preference to the IPv4 address.
  - **capacity** *capacity*: Specify the node capacity for the endpoint. *capacity* must be an integer in the range of 0-65535.
  - The endpoint selection for sending the message is based on probabilistic load-balancing algorithm (IETF RFC 2782) using the priority and capacity parameters.
  - **primary ip-address { ipv4** *ipv4_address* **| ipv6** *ipv6_address* **| port** *port_num* **}**: Specify the primary endpoint IPv4 address, IPv6 address, or port.
  - **secondary ip-address { ipv4** *ipv4_address* **| ipv6** *ipv6_address* **| port** *port_num* **}**: Specify the secondary endpoint IPv4 address, IPv6 address, or port.
  - **tertiary ip-address { ipv4** *ipv4_address* **| ipv6** *ipv6_address* **| port** *port_num* **}**: Specify the tertiary endpoint IPv4 address, IPv6 address, or port.
  - **priority** *priority_value*: Specify the priority for the service to select the appropriate profile using the load-balancing logic. *priority* must be an integer in the range of 0-65535.
- **uri-scheme { http | https }**: Specify the URI scheme as **http** or **https**.
- **version [uri-version** *version_num* **full version** *version_num* **]**: Specify the API URI version. The full version format is <Major-version>.<Minor-version>.<patch-version>.[alpha-<draft-number>].

Verifying the NRF Endpoints Profile Parameters for NF Discovery

This section describes how to verify the configuration of the NRF endpoints profile parameters.

```
show running-config group nrf
group nrf discovery udmdiscovery
 service type nrf nnrf-disc
  endpoint-profile epprof
   capacity       10
   priority       1
   api-uri-prefix nudm-sdm
```

```
   api-root       root
   uri-scheme     http
   version
    uri-version v1
     full-version 209.165.200.225
    exit
   exit
   endpoint-name endpointName
    priority 1
    capacity 100
    primary ip-address ipv4 209.165.200.237
    primary ip-address port 3021
    fqdn name nrf.cisco.com
    fqdn port 9010
   exit
  exit
 exit
exit
```

Configuring Locality for NF Types

The AMF provides locality aware NF discovery.

A pair profile has the locality values configured with NF type as AMF. A locality has the following values:

- client—Specify the client locality information.
- geo-server—Specify the geo-service locality information.
- preferred-server—Specify the preferred server locality information.

For a profile selection, only the preferred-server and geo-server locality values are considered. Following are the scenarios of these locality values configuration:

- If both the preferred-server and geo-server locality values are configured, then the profiles, which exist in discovery response, matching these locality values are selected. In addition, the profiles with empty locality value are selected. Any other profile with locality other than preferred-server and geo-server locality values are not considered.
- If only the preferred-server locality value is configured, then the profiles, which exist in discovery response, matching this value is selected. In addition, the profiles with an empty locality value are selected. Any other profile with locality other than preferred-server locality value is not considered.
- If only geo-server locality value is configured then the profiles, which exist in discovery response, matching this geo-server locality value is selected. In addition, the profiles with empty locality value is selected. Any other profile with locality other than geo-server locality value is not considered.
- If both preferred-server and geo-server locality values are not configured then all the profiles, which exist in discovery response, are selected.

To configure the locality for NF types, use the following sample configuration.

```
config
  profile nf-pair nf-type nf_type
    locality { client client_name | geo-server geoserver_name | preferred-server
 prefserver_name }
     end
```

NOTES:

- **client** *client_name*: Specify the client locality information. Client locality is the AMF locality and is a mandatory parameter.
- **preferred-server** *prefserver_name*: Specify the preferred server locality information. The preferred server locality is the locality that should be considered as the locality of preference during the corresponding NF discovery.
- **geo-server** *geoserver_name*: Specify the geo-server locality information. The geo-server locality is the geo redundant site for the preferred locality and is generally used as the next best server locality after preferred locality, during NF discovery.



Note **geo-server** *geoserver_name* is not fully qualified.

Verifying the Association of the Discovery Group and Locality Configuration

This section describes how to verify the discovery group association and locality configuration for NF.

```
show running-config profile nf-pair
profile nf-pair nf-type UDM
 nrf-discovery-group DISC1
 locality client LOC1
 locality preferred-server PREF_LOC
 locality geo-server GEO
exit
```

Configuring Locality for AMF

To configure the locality for AMF, use the following sample configuration.

This is a mandatory configuration if the AMF performs the NF discovery using the NRF.

```
config
  profile AMF AMF_profile_name
    locality value
    end
```

NOTES:

- **locality** *value*: Specify the AMF locality. *value* must be an alphanumeric string representing the deployed AMF locality. By default, this CLI command is disabled.
- To disable this configuration, use the **no locality** *value* command.

Configuring NF Profiles for a DNN

To configure the NF profile that the configured Data Network Name (DNN) uses, use the following sample configuration.

```
config
  profile dnn dnn_profile_name
    network-element-profiles { smf | chf | pcf | udm } nf_profile_name
    end
```

NOTES:

- **network-element-profiles { smf | chf | pcf | udm }** *nf_profile_name*: Specify one or more NF types, such as , CHF, PCF, and UDM as the network element profile. *nf_profile_name* must be an alphanumeric string representing the corresponding network element profile name.
- This is an optional configuration. By default, this CLI command is disabled.
- You can configure multiple profiles within a given service.
- To disable the configuration, use the **no network-element-profiles { smf | chf | pcf | udm }** *nf_profile_name* command.

Defining Locality within NF Profile

This section describes how to define the locality of the NF endpoints. For the NF endpoint selection, the AMF first considers the preferred locality that is configured with the **profile nf-pair** CLI command. The admin determines the preferred locality based on the proximity of the locality and the network function. The AMF then uses the geo-server locality configurations as the next preferred locality for the NF discovery. For information on the **profile nf-pair** command, see Configuring Locality for NF Types, on page 27 in the NRF Selection per Peer NF Type, on page 32 section.

The AMF selects the other locality endpoints if the **profile nf-pair** CLI command does not include the preferred server locality configuration, or if the **profile nf-client** CLI command does not include the endpoint configured with the preferred server or geo-server locality. For the other locality endpoint selection, the AMF uses the **priority** configuration within the **locality** CLI command.

To define the locality of the NF endpoints, use the following sample configuration.

```
config
  profile nf-client { nf-type { smf smf-profile | chf chf-profile | pcf
pcf-profile | udm udm-profile } nf_profile_name }
    locality locality_name [ priority priority | service name type service_types
 { endpoint-profile epprofile_name } ]
     end
```

NOTES:

- **locality** *locality_name*: Specify the locality of the NF endpoint. The AMF uses the locality configurations (that is, the preferred server locality and geo-server locality) to select the appropriate NF endpoints.
- **priority** *priority*: Specify the priority for the locality configuration.
- **service name type** *service_types*: Specify the configured NF service types. The service types vary depending on the configured service.
  - SMF service supports "nsmf-comm" as peer communication type.
  - PCF service supports "npcf-am-policy-control" as peer communication type.
  - UDM service supports "nudm-sdm" and "nudm-uecm" as peer communication type.
  - service supports "nsmf-pdusession" as peer communication type.
  - EIR service supports "n5g-eir-eic" as peer communication type.
  - NSSF service supports "nnssf-nsselection" as peer communication type.
  - SMSF service supports "nsmsf-sms" as peer communication type.

- LMF service supports "nlmf-loc" as peer communication type.
- GMLC service supports "ngmlc-loc" as peer communication type.
- AUSF service supports "nausf-auth" as peer communication type.

- **endpoint-profile** *epprofile_name*: Specify the endpoints at a per NF service level. The NF specific services are available within the locality configuration.
- You can configure multiple endpoints per profile name for the configured NF.

Configuring NF Endpoint Profile Parameters in NF Client Profile

This section describes how to configure the NF endpoint profiles within the service and its associated parameters.

The CLI configuration allows configuring multiple endpoints under each endpoint profile. The AMF uses the priority and capacity parameters to load balance between these endpoints. All endpoints under an endpoint profile share the session context. That is, when selecting an endpoint profile for initial message of a session, then the AMF sends the subsequent messages (for example, update, delete, and so on) of the session to any of the endpoints in the endpoint profile.

AMF provides APIs to discover and send a message to an NF matching a set of filter parameters.

A URI uniquely identifies a resource. In the 5GC SBI APIs, when a resource URI is an absolute URI, the structure is specified as follows:

```
{apiRoot}/{apiName}/{apiVersion}/{apiSpecificResourceUriPart}
```

apiRoot is a concatenation of the following parts:

- scheme ("http" or "https")



Important Both HTTP and HTTPS scheme URIs are allowed. See *3GPP TS 33.501, subclause 13.1* for more information on security of service-based interfaces.

- fixed string "://"
- authority (host and optional port) as defined in *IETF RFC 3986*
- an optional deployment-specific string (API prefix) that starts with a "/" character [api-root in CLI]

To configure the NF endpoint profiles within the service and its associated parameters, use the following sample configuration:

```
config

  profile nf-client { nf-type { smf smf-profile | chf chf-profile | pcf
pcf-profile | udm udm-profile }  nf_profile_name }     locality locality_name
[ priority priority | service name type service_type ]
        endpoint-profile epprofile_name
           api-root api_string
           api-uri-prefix uri_prefix_string
           capacity capacity
           endpoint-name ep_name { capacity capacity | primary ip-address {
```

```
ipv4 ipv4_address | ipv6 ipv6_address | port port_num }| secondary ip-address {
ipv4 ipv4_address | ipv6 ipv6_address| port  port_num } | tertiary ip-address {
 ipv4 ipv4_address| ipv6 ipv6_address | port port_num } }
          priority priority_value
          uri-scheme { http | https }
          fqdn { name  fqdn_name | port port_num } }
          version [ uri-version version_num full version version_num ]
          end
```

NOTES:

- **api-root** *api_string*: Specify the deployment-specific service API prefix that is used within the { apiRoot }.
- **api-uri-prefix** *uri_prefix_string*: Specify the {apiName}. If not configured, it takes the standard API name for the service as per the specification.
- **capacity** *capacity*: Specify the profile capacity.
- **endpoint-name** *ep_name* **{ capacity** *capacity* **| primary ip-address { ipv4** *ipv4_address* **| ipv6** *ipv6_address* **| port** *port_num* **} | secondary ip-address { ipv4** *ipv4_address* **| ipv6** *ipv6_address* **| port** *port_num* **} | tertiary ip-address { ipv4** *ipv4_address* **| ipv6** *ipv6_address* **| port** *port_num* **} }**: Specify the endpoint name. You can configure the primary, secondary, and tertiary hosts (IP: Port) within each endpoint for NF server failover handling. The server failover configuration accepts both the IPv4 and IPv6 addresses. However, the AMF gives preference to the IPv4 address.
  - **capacity** *capacity*: Specify the node capacity for the endpoint. *capacity* must be an integer in the range of 0–65535.

    The endpoint selection for sending the message is based on probabilistic load balancing algorithm (*IETF RFC 2782*) using the priority and capacity parameters.
  - **primary ip-address { ipv4** *ipv4_address* **| ipv6** *ipv6_address* **| port** *port_num* **}**: Specify the primary endpoint IPv4 address, IPv6 address, or port.
  - **secondary ip-address { ipv4** *ipv4_address* **| ipv6** *ipv6_address* **| port** *port_num* **}**: Specify the secondary endpoint IPv4 address, IPv6 address, or port.
  - **tertiary ip-address { ipv4** *ipv4_address* **| ipv6** *ipv6_address* **| port** *port_num* **}**: Specify the tertiary endpoint IPv4 address, IPv6 address, or port.
  - **priority** *priority_value*: Specify the priority for the service to select the appropriate profile using the load balancing logic. *priority* must be an integer in the range 0–65535.
  - **fqdn name** *fqdn_name*: Specify the FQDN name.
  - **fqdn port** *fqdn_port*: Specify the FQDN port number. If port is not configured, uses the standard port for FQDN, that is 80 for URI scheme HTTP and 443 for URI scheme HTTPS.
- **uri-scheme { http | https }**: Specify the URI scheme as **http** or **https**.
- **version [uri-version** *version_num* **full version** *version_num* **]**: Specify the API URI version. The full version format is <Major-version>.<Minor-version>.<patch-version>.[alpha-<draft-number>].

NRF Selection per Peer NF Type

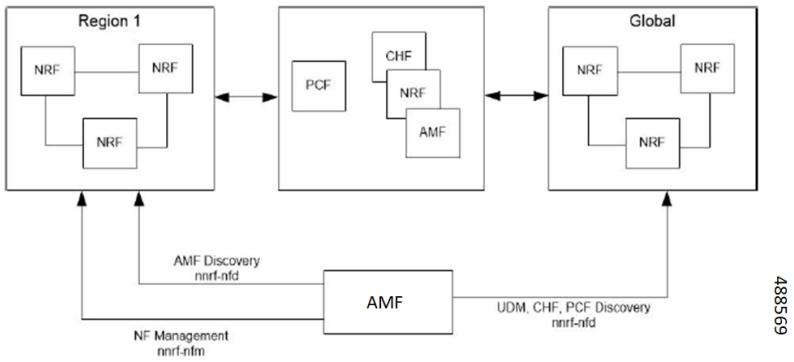
Feature Description

The Network Repository Function (NRF) deployment can be logically segmented as global, regional, and so on, for a reliable network management. You can accomplish this segmentation by specifying different NRF endpoint groups for the discovery of different network functions.

For example, the AMF interacts with Region 1 NRF endpoints for management and AMF discovery. For UDM, CHF, and PCF discovery, the AMF communicates with the global NRF endpoints.

The following figure illustrates the NRF deployment.

Figure 10: NRF Deployment



Standards Compliance

This feature complies with the following standard:

- *3GPP TS 29.510 version 15.4.0—5G System; Network function repository services; Stage 3*

Configuring the NRF Selection per Peer NF Type

This section describes how to configure the NRF selection per peer NF type.

Associating NRF Management and AMF Locality to NRF Endpoint

To configure the NRF management (nrf-group) and AMF locality, and associate them to NRF endpoint, use the following sample configuration.

```
config
  group nf-mgmt mgmt_name
    nrf-mgmt-group nrf_group_name
    locality locality_name
    message-handling-profile message_handling_profile_name
    end
```

NOTES:

- **nrf-mgmt-group** *nrf_group_name*: Specify the NRF management group.
- **locality** *locality_name*: Specify the locality information.

- **message-handling-profile** *message_handling_profile_name*: Specify the message handling profile for NRF.

Verifying the Association of the NRF Management and AMF Locality to NRF Endpoint

This section describes how to verify the configuration that associates the NRF management and AMF locality to NRF endpoint.

```
show running-config group nf-mgmt
group nf-mgmt NFMGMT1
 nrf-mgmt-group MGMT
 locality       LOC1
exit
```

Configuring Locality for AMF

To configure the locality for AMF, use the following sample configuration.

This is a mandatory configuration if the AMF performs NF discovery using the NRF.

```
config
  profile AMF AMF_profile_name

    locality value
    end
```

NOTES:

- **locality** *value*: Specify the AMF locality. *value* must be an alphanumeric string representing the deployed AMF locality. By default, this CLI command is disabled.
- To disable the configuration, use the **no locality** *value* command.

Configuring NF Profiles for a DNN

To configure the NF profile used by the configured Data Network Name (DNN), use the following sample configuration.

```
config
  profile dnn dnn_profile_name

    network-element-profiles { smf | chf | pcf | udm } nf_profile_name
    end
```

NOTES:

- **network-element-profiles { smf | chf | pcf | udm }** *nf_profile_name*: Specify one or more NF types, such as , CHF, PCF, and UDM as the network element profile. *nf_profile_name* must be an alphanumeric string representing the corresponding network element profile name.
- This is an optional configuration. By default, this CLI command is disabled.
- You can configure multiple profiles within a given service.
- To disable the configuration, use the **no network-element-profiles { smf | chf | pcf | udm }** *nf_profile_name* command.

Configuring Network Element Profile Parameters for the NF

To configure the network element profile parameters for the configured NF, use the following sample configuration.

```
config
  profile network-element { { smf | chf | pcf | udm } nf_profile_name }
    nf-client-profile profile_name
    query-params { dnn | limit | max-payload-size | requester-snssais |
 supi | tai | target-nf-instance-id | target-plmn }
    end
```

NOTES:

- **nf-client-profile** *profile_name*: Specify the local NF client profile. *profile_name* must be an alphanumeric string representing the corresponding NF client profile name.
- **query-params { dnn | limit | max-payload-size | requester-snssais | supi | tai | target-nf-instance-id | target-plmn }**: Specify one of the following query parameters to include in the NF discovery request towards the NRF.
  - **dnn**: Specify the DNN as the query parameter in the NF discovery request towards the NRF.
  - **limit**: Specify the limit for the maximum number of profiles that the NRF sends in the NF discovery response.
  - **max-payload-size**: Specify the maximum payload size as the query parameter in the NF discovery request towards the NRF.
  - **requester-snssais**: Specify the list of Single Network Slice Selection Assistance Information (S-NSSAIs) as the query parameter in the NF discovery request towards the NRF.
  - **supi**: Specify the SUPI as the query parameter in the NF discovery request towards the NRF.
  - **tai**: Specify the TAI as the query parameter in the NF discovery request towards the NRF.
  - **target-nf-instance-id**: Specify the target NF instance identifier as the query parameter in the NF discovery request towards the NRF.
  - **target-plmn**: Specify the target PLMN as the query parameter in the NF discovery request towards the NRF.
- This is an optional configuration. By default, the CLI commands are disabled.
- To disable this configuration, use the **no** variant of these commands. For example, **no nf-client-profile** CLI command.

Verifying the Local Configuration for the NRF Interface Per Endpoint

This section describes how to verify the configuration for the NRF interface per endpoint.

The following is an example of the NRF endpoint configuration.

```
show running-config profile dnn cisco
profile dnn cisco
 network-element-profiles chf chf1
 network-element-profiles amf amf1
 network-element-profiles pcf pcf1
```

```
 network-element-profiles udm udm1
 ssc-mode 2 allowed [ 3 ]
 session type IPV4 allowed [ IPV4V6 ]
 upf apn intershat
exit

profile smf smf1
 node-id          12b888e1-8e7d-49fd-9eb5-e2622a57722
 locality         LOC1
 bind-address ipv4 209.165.200.227
 bind-port        8008
instances 1 fqdn cisco.com.apn.epc.mnc456.mcc123
 plmn-id mcc 123
 plmn-id mnc 456
exit

profile network-element amf amf1
 nf-client-profile        AMF-L1
 failure-handling-profile FH1
 query-params [ target-nf-instance-id ]
exit
profile network-element pcf pcf1
 nf-client-profile        PCF-L1
 failure-handling-profile FH1
exit
profile network-element udm udm1
 nf-client-profile        UDM-L1
 failure-handling-profile FH1
exit
profile network-element chf chf1
 nf-client-profile        CHF-L1
 failure-handling-profile FH2
exit
end
```

Caching for Discovered NF Profiles

Feature Description

The AMF provides caching support for discovered caching profiles. It uses the NF discovery (nnrf-disc) function to discover profiles, such as SMF, UDM, PCF, and CHF. The received discovery response is associated with validity time. AMF caches the discovery response and uses the same response for future NF selections until the cache is valid. This caching support helps in reducing the number of NRF interactions during an ongoing session.

Relationships

Caching support for NF Discovery has functional relationship with the following features:

- NRF Support for AMF Subscription and Notification
- NRF Selection per Peer NF Type

How it Works

The AMF maintains the cache data in a cache pod. It uses the cache pod to share the NF discovery cache across multiple instances of SBI pods. The SBI pod periodically updates the cache pod on receiving an NF discovery response. All SBI pods refresh its cache data periodically with the help of the cache pod.

If a message is sent to an NF that meets a specific criterion, the AMF looks up the cache data for further processing. During a cache lookup:

- On a cache hit without an expired entry, the selected cached NF response sends a message for an endpoint selection.
- On a cache hit with an expired entry, the AMF sends NF discovery requests to the NRF to fetch a new list of NF discovery responses.
- If there is a cache miss, the AMF sends NF discovery request to the NRF to retrieve a new list of NF discovery responses.

Call Flows

Cache Lookup Call Flow

This section describes the call flow for Cache Lookup.

AMF maintains a local cache and updates the external cache (cache-pod). The key for a cache is a combination of nfType and filter, which is a string that is prepared from multiple filter parameters in "key1=value, key2=value2" format.

On startup, AMF retrieves all the cache entries that were modified since epoch from cache-pod so that it can build the local cache. After the local cache is built, the same cache is used in the send message flow for lookup. A periodic refresh routine is initiated to refresh the local cache using the cache-pod. Local cache is periodically refreshed by getting all records from the cache-pod that were modified since last refresh. The resultant record list is traversed and the local cache is updated.

When AMF-rest-ep (SBI) triggers a send message to UDM, the AMF looks up the local cache for the cache entry with the nfType and filter key. The NF profiles are load-balanced and a message is sent to the selected endpoint.

Standards Compliance

This feature complies with the following standards:

- *3GPP TS 29.510 version 15.4.0 — 5G System; Network function repository services; Stage 3*

NF Discovery Cache Invalidation

Feature Description

AMF gives higher priority to the NFs that are discovered from NRF over the locally configured NFs. AMF uses the locally configured NFs only if the NRF endpoints are not configured or if no NFs are available as part of the NF discovery response. This response appears after the query filter criteria are met. Each NF discovery response has an associated validity time and AMF caches the NF discovery response, uses the cache for subsequent session activation. AMF performs NF discovery only if matching entries are unavailable for the query filter in its NF discovery response cache or if the entry in cache exists, however with the expired validity.

How it Works

AMF provides configuration to determine the behaviour when the NRF is unreachable and has an expired cache entry. The CLI provides the following options to determine:

- If the cache entry needs to invalidate on expiry.

- If the cache entry needs to be invalidated, along with the duration to retain the cache entry after the validity expiry.

These options are applicable only if the NRF is inactive. The configuration is according to the nf-pair profile. The configuration determines if AMF should use expired cache in case NRF becomes inactive and if it uses the expired cache, along with the duration to retain the cache entry after the validity expiry.

Configuring NF Discovery Cache Invalidation (Purge)

To configure the cache entry invalidation (purge) for the NF discovery cache, use the following sample configuration.

```
config

  profile nf-pair nf-type { smf | chf | pcf | udm }
    cache invalidation { false | true [ timeout integer ] }
    end
```

NOTES:

- **cache invalidation { false | true [timeout** *integer* **] }**: Configure the interval and cache invalidation rule. The default value is false.
  - **false**: Specify that the cache entry will never be invalidated.
  - **true timeout** *integer* : Specify that the cache entry will be invalidated. **timeout***integer* specifies the time period in milliseconds (ms) for controlling the usage of the expired cache entry (when NRF is unreachable). The default value is 0 ms.

The following configuration is an example that sets the cache invalidation to false for the UDM discovery:

```
profile nf-pair nf-type UDM
  cache invalidation false
 end
```

The following configuration is an example that sets the cache invalidation to true for the UDM discovery:

```
profile nf-pair nf-type UDM
  cache invalidation true timeout 10
 end
```

Static Configuration for Peer NF Management

Fallback to Static IP Address Support

Feature Description

The AMF follows a priority order for different NF selection options. The AMF prioritizes the NF discovered from the NRF over the local configuration. The AMF uses the locally configured NFs when the NF discovery response has no valid NFs.

Depending on the deployment, the preferred server and geo locality server are configured for each of the NFs. The general rule is to select NFs in the preferred server locality followed by NFs in the geo locality server in case the preferred server NFs fail.

For each NF, the AMF provides an option to configure preferred and geo server locality through the **profile nf-pair** parameter. For more details, see Configuring Locality for NF Types, on page 27 in the NRF Selection per Peer NF Type, on page 32 section.

In addition, each NF discovery response comes with associated validity time. The AMF caches this NF discovery response and uses it to fetch subsequent sessions.

The AMF performs the NF discovery in the following conditions:

- The NF discovery response cache has no matching entries.
- The NF discovery response cache has matching entries, but the validity has expired.

Relationships

The Fallback to Static IP Address feature has functional relationships with the following features:

- Caching Support for NF Discovery
- NF Discovery, NF Selection, and Load Balancing
- NRF Selection per Peer NF Type

How it Works

The AMF follows this sequence for NF selection if an NRF discovery group is configured:

1. It looks up the local cache (NF discovery response cache) for the NF.
2. If the NF is a valid entry (not expired), it uses that entry. Else, AMF proceeds to Step 3.
3. The AMF reaches NRF for discovery [see, NRF Discovery (Priority 1)]. Else, AMF moves to Step 4.
4. If AMF cannot use the NRF for discovery, it uses the expired NF cache [see, Expired NF Cache (Priority 2)]. If expired NF cache is not available, AMF moves to Step 5.
5. If AMF does not find the NF in the local cache nor is it able to get it in the NRF discovery response, it uses the locally-configured NF [see, NF Local configuration (Priority 3)].

The priority order for NF selection is as follows:

1. **NRF Discovery (Priority 1)**

   The SMS uses the NRF-provided, NF discovery service to discover NFs like AMF, UDM, and PCF. The AMF sets the preferred locality as provided in the "**profile nf-pair**" configuration in the discovery query. (For more details about the "**profile nf-pair nf-type**" CLI configuration, see Configuring Locality for NF Types, on page 27 in the NRF Selection per Peer NF Type, on page 32 section.) For each NF, the query parameters are configurable. (For more details, see Configuring Network Element Profile Parameters for the NF, on page 34 in the NRF Selection per Peer NF Type, on page 32 section). The NRF returns all the NFs matching the query criteria. When available, the NRF prefers NF profiles with a locality attribute that matches the preferred-locality. The NRF could return more NFs in the response, which are not matching the preferred target NF location. This occurs when there is no NF profile that is found matching the preferred target NF location. To avoid this, the NRF could set a lower priority for any additional NFs on the response not matching the preferred target NF location than those matching the preferred target NF location. The locality-aware NF selection logic of AMF is as follows:

   a. If the NF has both the preferred and geo locality server configurations, all the NFs in the response that are matching these are cached. AMF ignores the balance NFs. The load-balancing logic first

selects the preferred locality NFs. If the preferred locality NFs fail, AMF picks the geo locality NFs for a retry. If N retry is allowed, N-1 retries are on the preferred locality and the last retry is on the geo locality NF. If the N-1 endpoints are unavailable in the preferred locality, AMF attempts all the endpoints of the preferred locality. Else, AMF picks up the geo locality endpoints for the remaining retries. Multiple retries on the same host (port) is not attempted.

b. If the NF has only the preferred locality configuration, all the NFs in the response that match the preferred locality are cached. The load-balancing logic selects the endpoints from these NFs.

c. If the NF does not have the preferred locality or geo locality configuration, then SMS caches all the discovery response NFs. The load-balancing logic selects from these NFs.



Note

- The load-balancing logic is based on priority, capacity, and load. The logic is similar to server selection as defined in IETF RFC 2782. However, the weight is considered as "capacity * (100 - load)".
- If AMF selects the NRF-discovered NFs (in any of the three cases), even when all attempts to reach preferred and geo locality fail, the AMF does not fall back to the local configuration NFs for a retry.

2. Expired NF Cache (Priority 2)

The AMF performs an NF discovery only in the following scenarios:

- If the matching entries are not available for the query filter in its NF discovery cache
- If matching entries are available in its NF discovery cache. However, these entries have expired validity.

  The retention of an expired cache entry is configuration-based. If the expired cache entry is available and the NRF is not reachable or returns an error, then AMF uses the expired cache entry for NF selection. You can configure the AMF to control the cache entry usage with the following options:

  - Invalidate the cache entry on expiration of validity.
  - Use the invalidated cache entry for a configurable time period (timeout) and fallback to the static configuration after the timeout expires.



Note The AMF controls the cache entry usage - only when the NRF is down - through these options. The configurations are based on the **profile nf-pair**. Additionally, the AMF provides flexibility in configuring different cache usage rule for different NFs. For instance, the AMF always uses the expired cache to discover PCF when the NRF is down. But, for discovering the UDM, the AMF uses the expired cache for a timeout period of 10 milliseconds (ms) when the NRF is down.

3. NF Local Configuration (Priority 3)

The locally configured NFs are the last option for NF endpoint selection. The local configuration too considers the preferred and geo server locality for NF selection. The priority order is as follows:

a. If the preferred server is configured for the NF [in **profile nf-pair**], AMF selects the NF endpoints under the preferred locality, first. The load-balancing logic is applicable for endpoint profiles and endpoints within the locality as per the configured priority and capacity values.

b. If the geo locality is configured for the NF [in **profile nf-pair**], AMF selects the NF endpoints under the geo locality as the fallback option. That is, if the preferred server locality NF endpoints fail or preferred server locality endpoints are not configured. The load-balancing logic is applicable for endpoint profiles and endpoints within the locality as per the configured priority and capacity values.

c. If the preferred server and geo locality server are not applicable, AMF picks up the locality based on the priority that is configured for each locality in the local NF configuration. The load-balancing logic is applicable for endpoint profiles and endpoints within the locality as per the configured priority and capacity values.



Note The priority under locality is applicable only if the preferred and geo locality servers are not applicable.

The failure template is configurable for each of the NFs. Also, the message type in the template can set the retry count and action for the possible HTTP return codes.

Standards Compliance

The Fallback to Static IP Address feature complies with the following standards:

- *3GPP TS 29.510 version 15.4.0 (2019-07) – 5G System; Network function repository services; Stage 3*

Configuring Fallback to Static IP Address

This section describes how to configure the support for Fallback to Static IP Address.

Configuring NF Client Profile

To configure the NF endpoints for , CHF, PCF, and UDM, use the following sample configuration:

```
config
  profile nf-client { nf-type { smf smf-profile | chf chf-profile | pcf
pcf-profile | udm udm-profile } nf_profile_name }
  end
```

NOTES:

- **profile nf-client { nf-type { smf smf-profile | chf chf-profile | pcf pcf-profile | udm udm-profile }** *nf_profile_name* **}**: Specify the required NF client profiles and provide the local configuration for any of the following configured NFs:
  - **smf**: Enable the local configuration
  - **chf**: Enable the CHF local configuration
  - **pcf**: Enable the PCF local configuration
  - **udm**: Enable the UDM local configuration

  For example, if you are configuring the **smf smf-profile** keyword, this command enables the local configuration. The same approach applies for the other configured NFs.

nf_profile_name must be an alphanumeric string representing the corresponding NF client profile name.

- You can configure multiple NF profiles within a given service.
- To disable the configuration, use the **no profile nf-client { nf-type { smf smf-profile | chf chf-profile | pcf pcf-profile | udm udm-profile }** *nf_profile_name* **}** command.

Configuration Example

The following is an example configuration.

```
profile nf-client nf-type pcf
pcf-profile pcf-profile
  locality LOC1
   priority 1
   service name type npcf-smpolicycontrol
    endpoint-profile epprof
     capacity   10
     priority   1
     uri-scheme http
     endpoint-name ep1
      priority 1
      capacity 10
      primary ip-address ipv4 209.165.202.133
      primary ip-address port 8080
     exit
     endpoint-name ep2
      priority 1
      capacity 10
      primary ip-address ipv4 209.165.201.1
      primary ip-address port 8080
     exit
    exit
   exit
  exit
exit
exit
profile nf-client nf-type pcf
pcf-profile pcf-profile
  locality LOC1
   priority 1
   service name type npcf-smpolicycontrol
    endpoint-profile epprof
     capacity   10
     priority   1
     uri-scheme http
     endpoint-name ep1
      priority 1
      capacity 10
      primary ip-address ipv4 209.165.201.2
      primary ip-address port 8080
     exit
```

Configuring Network Element Profile Parameters for the NF

To configure the network element profile parameters for the configured NF, use the following sample configuration.

```
config
```

```
network-element-profiles { { smf | chf | pcf | udm } nf_profile_name }
  nf-client-profile profile_name
  query-params { dnn  | limit | max-payload-size | requester-snssais
| supi | tai | target-nf-instance-id | target-plmn }
  end
```

NOTES:

- **nf-client-profile** *profile_name*: Specify the local NF client profile. *profile_name* must be an alphanumeric string representing the corresponding NF client profile name.
- **query-params { dnn | limit | max-payload-size | requester-snssais | supi | tai | target-nf-instance-id | target-plmn }**: Specify one of the following query parameters to include in the NF discovery request towards the NRF.
  - **dnn**: Specify a DNN as the query parameter in the NF discovery request towards the NRF.
  - **limit**: Specify a limit for the maximum number of profiles that the NRF sends in the NF discovery response.
  - **max-payload-size**: Specify the maximum payload size as the query parameter in the NF discovery request towards the NRF.
  - **requester-snssais**: Specify the list of Single Network Slice Selection Assistance Information (S-NSSAIs) as the query parameter in the NF discovery request towards the NRF.
  - **supi**: Specify a SUPI as the query parameter in the NF discovery request towards the NRF.
  - **tai**: Specify a TAI as the query parameter in the NF discovery request towards the NRF.
  - **target-nf-instance-id**: Specify a target NF instance Identifier as the query parameter in the NF discovery request towards the NRF.
  - **target-plmn**: Specify a target PLMN as the query parameter in the NF discovery request towards the NRF.
- This is an optional configuration. By default, the CLI commands are disabled.
- To disable the configuration, use the **no** variants of these commands. For example, **no nf-client-profile** CLI command.

Failure Handling

AMF uses the NF registeration messages for tracking the liveliness of management NRF group. If AMF detects a failure in one of the NRFs in the management group, it uses the NRF failure handling mechanism.

Failure handling template is available for each of the NFs and its message types to set the retry count and action for the possible HTTP return codes.

For more information on failure handling, see the Failure/Exception Handling Framework Support section.