UPF Path Management and Restoration

Feature Summary and Revision History

Summary Data

Table 1: Summary Data

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

Revision History

Table 2: Revision History

Revision Details	Release
Heartbeat on Sx	2023.01.0
First introduced.	2020.02.0

Feature Description

The heartbeat monitors the status of a UPF node in terms of its responsiveness. It initiates a bilateral flow of request and response between the SMF and the UPF. It has the following actions:

- The SMF periodically sends a signal in the form of a heartbeat request to the registered UPF node. This action helps in determining if the SMF is in active or not.
- If the SMF doesn't receive a response from the UPF after the exhausted retransmission attempts, then the SMF recognizes a failure instance. It purges the UPF node-mapped subscribers.

You can control the following:

- The number of heartbeat requests that SMF sends to UPF.
- The interval between consecutive requests.
- The duration until which the SMF waits for a response.

The Heartbeat feature is also applicable for SMF with Diameter interfaces.

Standards Compliance

The heartbeat transmission between SMF and UPF complies with the following standards:

- *3GPP TS 23.527*
- *3GPP TS 23.007, version 15.4.0*

How it Works

You can configure the Heartbeat capability at the interface-level, UPF profile group-level, or both. The interface-level configuration is mandatory. If the interface-level configuration is unavailable, then the Heartbeat parameters get configured with the default values. The profile-level configuration overrides the interface-level configuration.

The Heartbeat feature also extends to achieve high-availability for the Node Manager.

Interface and profile-level Heartbeat

The SMF-UPF interaction to detect the UPF path failure using the Heartbeat messages involves the following steps:

1. The SMF sends a Heartbeat request message to the discovered UPF instances or profile groups based on the configured schedule.
2. If the UPF instance or profile is alive, it sends a Heartbeat response to the SMF indicating that it's operational. In case the UPF doesn't send a Heartbeat response, then the SMF retransmits the Heartbeat request. It's based on the configured interval and the number of permitted attempts.

3. After the configured count of Heartbeat message reattempts gets exhausted and the SMF doesn't receive a response from UPF, then the SMF starts the Session release procedure for the subscribers that are associated with that UPF.

Heartbeat and High-availability in Node Manager

Each UPF instance is associated with a primary and secondary Node Manager. The secondary Node Manager acts as a standby system on which the primary manager fails over. The primary Node Manager is responsible for the IP allocation and managing the association-specific messages such as association create, update, or delete request.

Configuration Support for the UPF Path Management and Restoration

This section describes how to configure the support for monitoring the UPF status.

Configuring the support for detecting the UPF status using the Heartbeat feature involves the following steps:

- Configuring the Heartbeat Parameters for the UPF—Lists out the configuration details for the Heartbeat parameters for the UPF at the interface level. For more information, see Configuring the Heartbeat at the Interface Level, on page 3.
- Configuring the Heartbeat Parameters for the UPF Profile—Lists out the configuration details for the Heartbeat parameters for the UPF profile at the profile level. For more information, see Configuring the Heartbeat at the UPF Group Level, on page 4.
- Associating UPF Group to Individual UPF Network Configuration—Lists out the configuration details for associating the UPF group to an individual UPF network. For more information, see Associating UPF Group to Individual UPF Network Configuration, on page 5.
- Configuring the Sx/N4 Path Failure Detection Policy—Lists out the configuration details for the Sx/N4 Path Failure Detection Policy parameter. For more information, see Configuring the Sx/N4 Path Failure Detection Policy, on page 6.

Configuring the Heartbeat at the Interface Level

To configure the Heartbeat at the interface-level, use the following sample configuration:

```
config
   instance instance-id gr_instance_id
      endpoint pfcp
         interface { n4 | sxa }
            heartbeat
               interval interval
                  max-retransmissions max_retry_count
                  retransmission-timeout retry_interval_count
                  end
```

NOTES:

- **instance instance-id** *gr_instance_id*—Specify the GR instance ID.

- **endpoint pfcp**—Specifies the endpoint configuration mode.
- **interface { n4 | sxa }**—Configures the N4 or Sxa interface over which the Heartbeat messages get exchanged between the SMF and the UPF.
- **Heartbeat**—Specifies the Heartbeat configuration.
- **interval** *interval*—Specify the Heartbeat interval in seconds. The accepted range is 60–360. The default value is 60 seconds.

Note Setting the *interval* to 0, disables the Heartbeat feature.

- **max-retransmissions** *max_retry_count*—Specify the maximum retries for the Packet Forwarding Control Protocol (PFCP) Heartbeat request. Must be in the range of 0–10. The default value is 3.
- **retransmission-timeout** *retry_interval_count*—Specify the Heartbeat retransmission timeout in seconds. Must be in the range of 1–20. The default value is 5.

Verifying the Heartbeat Configuration for the SMF

This section describes how to verify the heartbeat configuration for the SMF.

Use the **show running-config instance instance-id** *gr_instance_id* **endpoint pfcp** command to view and verify the feature configuration.

The following is a sample output of the show command.

```
show running-config instance instance-id 1  endpoint pfcp
 instance instance-id 1
  endpoint pfcp
   interface n4
    heartbeat
     interval               61
     retransmission-timeout 3
     max-retransmissions    5
     exit
    exit
   exit
 exit
exit
 interface sxa
  heartbeat
   interval               300
   retransmission-timeout 15
   max-retransmissions    0
   exit
  exit
exit
```

Configuring the Heartbeat at the UPF Group Level

To configure the Heartbeat at the UPF group level, use the following sample configuration:

```
config
   profile upf-group group_name
      heartbeat
```

```
interval interval
retransmission-timeout max_retry
max-retransmissions retry_count
end
```

NOTES:

- **profile upf-group** *group_name*—Specify the UPF group for which the Heartbeat feature must be enabled.
- **interface**—Configures the N4 interface over which the Heartbeat messages get exchanged between the SMF and the UPF.
- **heartbeat** —Specifies the Heartbeat configuration.
- **interval** *interval*—Specify the Heartbeat interval in seconds. Must be in the range of 60–360. The default value is 60 seconds.

  Setting the *interval* to 0, disables the Heartbeat feature.
- **max-retransmissions** *max_retry*—Specify the maximum retries for the Packet Forwarding Control Protocol (PFCP) Heartbeat request. Must be in the range of 0–10. The default value is 3.
- **retransmission-timeout** *retry_count*—Specify the Heartbeat retransmission timeout in seconds. Must be in the range of 1–20. The default value is 5.

Verifying the Heartbeat Configuration for the UPF Group Level

This section describes how to verify the heartbeat configuration for the UPF group level.

Use the **show running-config profile upf-group** command to view and verify the feature configuration.

The following is a sample output of the show command.

```
show running-config profile upf-group
 profile upf-group upfGroup1
  heartbeat
   interval               62
   retransmission-timeout 3
   max-retransmissions    2
   exit
  exit
 exit
```

Associating UPF Group to Individual UPF Network Configuration

This section describes how to associate a UPF group with a UPF configuration.

In this scenario, each UPF network configuration includes the UPF profile that associates every UPF instance with a UPF profile.

To associate an UPF group profile with a network configuration, use the following sample configuration:

```
config
   profile network-element upf upf_profile_name
       upf-group-profile upf_group_name
       end
```

NOTES:

- **profile network-element upf** *upf_profile_name*—Configure the UPF network configuration.
- **upf-group-profile** *upf_group_name*—Specify the UPF group name that must be associated to the specified UPF network configuration.

Verifying the Association of the UPF Group with the Individual UPF

This section describes how to verify the association of the UPF group with the individual UPF.

Use the **show running-config profile network-element upf** command to view and verify the feature configuration.

The following is a sample output of the show command.

```
profile network-element upf upf1
 n4-peer-address ipv4 209.165.200.238
 n4-peer-port      8805
 upf-group-profile upfGroup1
 dnn-list          [ intershat intershat1 intershat2 ]
 capacity          65535
 priority          65535
```

Configuring the Sx/N4 Path Failure Detection Policy

To configure the Sx/N4 Path Failure Detection policy, use the following sample configurations:

Use the following sample configuration to associate the Sx/N4 path failure detection policy:

```
config
   instance instance-id gr_instance_id
      endpoint pfcp
         sx-path-failure sx-detection-policy detection_policy_name
         end
```

Use the following sample configuration to set parameters for the Sx/N4 path failure detection policy:

```
config
   policy sx-path-failure-detection detection_policy_name
      ignore { heartbeat-retry-failure |
heartbeat-recovery-timestamp-change }
         end
```

NOTES:

- **instance instance-id** *gr_instance_id*—Specify the GR instance ID. The instance ID 1 denotes the local instance ID.
- **endpoint pfcp** *endpoint_name*—Specify the endpoint name and the endpoint configuration mode for the selected interface.
- **sx-path-failure sx-detection-policy** *detection_policy_name*—Specify the name of the policy used, when the Sx path failure occurs as a result of the Heartbeat request timeout, and the default Sx action performs the cleanup activities.
- **policy sx-path-failure-detection** *detection_policy_name*—Specify the name of the policy used, when the Sx path failure occurs as a result of the Heartbeat request timeout detection.

- **ignore { heartbeat-retry-failure | heartbeat-recovery-timestamp-change }**—Detect the path failure mode, when there's an attempt to retry the Heartbeat messages time out, or whenever there's a change in the recovery timestamp of the heartbeat request or a response message.

Verifying the Sx/N4 Path Failure Detection Policy

This section describes how to verify the Sx/N4 path failure detection policy.

Verifying the Association of the Sx/N4 Path Failure Detection Policy:

Use the **show running-config instance instance-id** *gr_instance_id* **endpoint pfcp** command to view and verify the association of the feature configuration.

The following is a sample output of the show command.

```
show running-config instance instance-id 1 endpoint pfcp
 instance    instance-id 1
  endpoint    pfcp
   replicas    1
   enable-cpu-optimization    true
   sx-path-failure sx-detection-policy sx1
   interface    n4
   heartbeat
    interval    0
    retransmission-timeout    3
    max-retransmissions    5
    exit
   vip-ip    209.165.201.24
   exit
  interface    gtpu
  vip-ip    209.165.201.24
  exit
 exit
exit
```

Verifying Parameters Settings for the Sx/N4 Path Failure Detection Policy:

To view and verify the configuration parameters settings for the Sx/N4 path failure detection policy, use the following commands:

Use the **show running-config policy sx-path-failure-detection** *detection_policy_name* command to view and verify the configuration parameters settings for the feature.

The following is a sample output of the show command.

```
show running-config policy sx-path-failure-detection
 policy sx-path-failure-detection sx1
 ignore heartbeat-retry-failure
 exit
exit
```

OAM Support

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

Bulk Statistics

The following statistics are supported for the heartbeat-related UPF path management feature.

- **nodemgr_upf_heartbeat_fail_stats**
- **nodemgr_upf_hb_msg_stats**

The SMF maintains these bulk statistics triggered during the heartbeat request and response procedure.

nodemgr_upf_heartbeat_fail_stats

- Description:

  The counter that gets updated per UPF when it fails to respond to a heartbeat request.

- The `nodemgr_upf_heartbeat_fail_stats` counter supports the following labels:

  Labels:

  - Label: **upf_heartbeat_req_tx**

    Label Description: Label for the heartbeat request that the SMF sends.

  - Label: **upf_heartbeat_req_retx**

    Label Description: Label for the retransmitted heartbeat request

  - Label: **upf_heartbeat_rsp_rx**

    Label Description: Label for the heartbeat response that the SMF receives.

nodemgr_upf_hb_msg_stats

- Description:

  The counter for all heartbeat messages for the specified UPF

For more information on bulk statistics support for SMF, see the *UCC 5G SMF Metrics Reference* document.