Network Slicing

Feature Summary and Revision History

Summary Data

Table 1: Summary Data

Applicable Product(s) or Functional Area	PCF
Applicable Platform(s)	SMI
Feature Default Setting	Enabled – Configuration required to disable
Related Documentation	Not Applicable

Revision History

Table 2: Revision History

Revision Details	Release
Enhancement introduced. PCF to support metrics and statistcs counters based on Slice -ID.	2022.03.0
Enhancement introduced. Configuration updated for N5 interface service.	2022.02.0
First introduced.	2021.04.0

Feature Description

The network slicing solution allows the service providers to partition the 5G physical network into multiple virtual network slices.

PCF implements network virtualization by registering the Single–Network Slice Selection Assistance Information (S-NSSAIs) with the NRF. The S-NSSAI enables PCF to identify a network slice. After the registration is complete, SMF and AMF can discover the PCF instances serving the specific slices.

Note PCF supports only soft slicing, slice-based policy control, without isolating the system resources belonging to different slices.

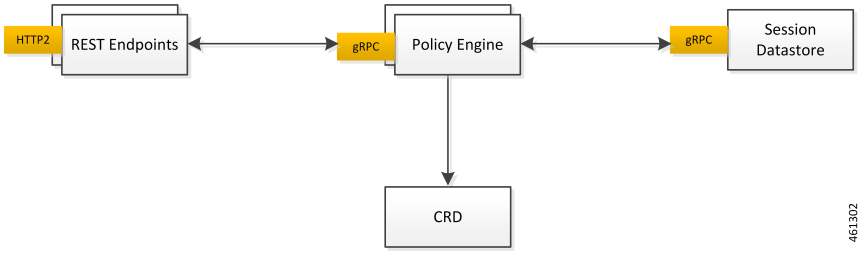
PCF Supports the Statistics counters to provide volume of TPS per Service based interfaces (SBI) with slice-ID as one of the labels.

Architecture

The REST endpoint performs the slice validation based on the requests from the client using HTTP2. The REST endpoint interacts with the Policy Engine to retrieve the policy status and the slice information over gRPC.

Slice information associated with the PDU session can be bound to CRD to generate the slice-specific policies.

Figure 1: Network Slice Architecture



How it Works

This section describes how this feature works.

Call Flows

This section describes the key call flows for this feature.

Slice Validation and Slice-Specific Policy Generation Call Flow

This section describes the Slice Validation and Slice-Specific Policy Generation call flow.

Figure 2: Slice Validation and Slice-Specific Policy Generation Call Flow

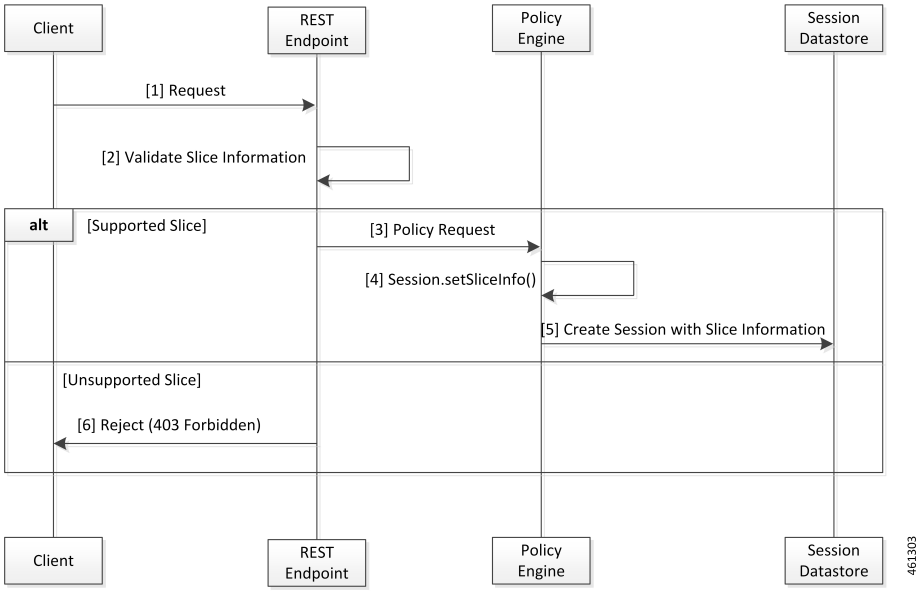


Table 3: Slice Validation and Slice-Specific Policy Generation Call Flow Description

Step	Description
1	The Client sends a request to validate the slice information to the REST endpoint.
2	The REST endpoint validates the slice information.
3	If the slice validation is successful, the REST endpoint sends a policy request to Policy Engine.
4	Policy Engine processes the request with the Session.setSliceInfo() message.
5	Policy Engine sends the Create Session request with the slice information to the Session Datastore.
6	If the slice validation is unsuccessful, the REST endpoint sends the Reject (403 Forbidden) message to the Client.

Configuring the Network Slicing Feature

Configuring this feature involves the following steps:

Configuring the Reject Requests Capability

This section describes how to enable the capability to reject requests from a slice that PCF does not support.

To enable PCF to reject requests, use the following configuration:

```
config
   advance-tuning slicing access-control [ enabled | disabled ]
   end
```

NOTES:

- **slicing access-control [enabled | disabled]**—Enable or disable PCF to reject the requests from the unsupported slices with the HTTP error code.

Configuring the Custom Error Codes

This section describes how to configure the error codes for the requests that PCF rejects.

To configure the custom error codes, use the following configuration:

```
config
   advance-tuning slice-access-control rejection-status-code error_code
   end
```

NOTES:

- **advance-tuning slice-access-control rejection-status-code** *error_code*—Specify the error code that must be displayed when PCF rejects a request. It must be an integer in the range of 100-599.
- If the error code is not configured, the default error code is 403.

Configuring the Allowed NSSAIs

This section describes how to configure the allowed NSSAIs in the PCF Registration Profile.

To configure allowed-NSSAIs, use the following configuration:

```
config
  service-registration
    profile
      allowed-nssais snssai_name sst sst_value [ sd sd_value ]
    services
      afService
        allowed-nssais snssai_name sst sst_value [ sd sd_value ]
      smfService
        allowed-nssais snssai_name sst sst_value [ sd sd_value ]
        end
```

NOTES:

- **allowed-nssais** *snssai_name* **sst** *sst_value* **[sd** *sd_value* **]**—Configures the SNSSAI. The *snssai_name* name is a logical identifier that is local to PCF. This name is not used in the PCF NFProfile when registering with NRF.

  To configure multiple slices per service, configure SNSSAI with same SST and different SD values.

  The **allowed-nssais** configured for smfService takes precedence over the allowed-nssais value configured at the profile-level.

Note Ensure to configure the allowed-nssais at the profile-level.

Configuration changes to the allowed-nssai of services do not affect the PDU sessions that are created before the configuration is modified.

Configuration Example

The following is an example configuration.

```
service-registration profile snssais embb-1
   sst 1
exit
service-registration profile snssais embb-2 sst 1
   sd 0000a1
exit
service-registration profile allowed-nssais name embb-1
   sst 1
exit
service-registration profile allowed-nssais name embb-2
   sst 1
   sd 0000a1
exit
service-registration services smfService
  allowed-nssais name embb-2 sst 1
     sd 0000a1
    exit
exit
```

Network Slicing OA&M Support

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

Statistics

This section provides the counter that gets generated for the network slicing scenarios.

- inbound_request_slice_rejected: Captures the requests initiated for specific slices and the requests rejected for the slices that PCF does not support. The inbound_request_slice_rejected counter monitors requests that contain the slice information (Npcf_SMPolicyControl_Create).

Note The inbound_request_slice_rejected does not determine the traffic on the slice.

The inbound_request_slice_rejected counter supports the following labels:

- interface_name—Indicates the name of the Service Based Interface (SBI) such as N7.
- service_name—Indicates the name of the service such as npcf-smpolicycontrol.
- operation_name—Indicates the name of the service operation such as Npcf_SMPolicyControl_Create.
- command—Indicates the command type such as Create.
- slice—Indicates the S-NSSAI that corresponds to the slice such as 1:0000ab.

- incoming_request_slice_total—The incoming_request_slice_total includes all create, update, and delete actions and indicates the total number of incoming requests per slice on the N7 and N5 interfaces.

The incoming_request_slice_total counter supports the following labels:

- interface_name—Indicates the name of the Service Based Interface (SBI) such as N5, N7, nNRF, and N28.
- service_name—Indicates the name of the service such as nchf-spendinglimitcontrol.
- result—Success and Error. Indicates that the request is success or error.
- slice—Indicates the allowed-nssais that corresponds to the slice such as 1:0000ab.
- outgoing_request_slice_total—The outgoing_request_slice_total includes all subscribe and unsubscribe/notify operations and indicates the total volume of outgoing requests per slice on N28/N7 interfaces.

The outgoing_request_slice_total counter supports the following labels:

- interface_name—Indicates the name of the Service Based Interface (SBI) such as N5, N7, nNRF, and N28.
- service_name—Indicates the name of the service such as nchf-spendinglimitcontrol.
- result—Success and Error. Indicates that the request is success or error.
- slice—Indicates the allowed-nssais that corresponds to the slice such as 1:0000ab.