

Network Slicing

- Feature history of network slicing, on page 1
- Network slicing, on page 1
- Configure network slicing, on page 2
- Verify network slicing using CLI, on page 5

Feature history of network slicing

Table 1: Feature History

Feature Name	Release Information	Description
Cellular Network Slicing	Cisco IOS XE Catalyst SD-WAN Release 17.16.1a Cisco Catalyst SD-WAN Manager Release 20.16.1	This feature allows multiple networks to exist on the same physical network to optimize the network for different traffic types.

Network slicing

Network slicing is a network architecture solution that:

- partitions a single physical network into multiple virtual slices
- allows each slice to operate with customized network functions and resources
- allocates dedicated resources for diverse service types or customer requirements.

5G network slicing is supported only on 5G standalone networks. It is not available on 5G non-standalone (NSA) networks. The network provider defines a specific set of network functions and resources for each slice or service type. Service type defines the expected behavior of a network slice, specifying its features and services.

The following service types are supported in network slicing:

- Enhanced Mobile Broadband (eMBB): used for high-bandwidth and low-latency applications.

- Ultra-reliable low latency communications (URLLC): used for highly reliable and low-latency transmission requirements.
- Massive Internet of Things (MIoT): used for sending small quantities of data.

Configure network slicing

Before you begin

Create a configuration group for Cisco Catalyst Cellular Gateways using **Workflows** > **Create Cellular Gateway Group**. On the **Configuration Groups** page, the resulting configuration group is labelled cellular gateway in the **Device Solution** column.

For information about creating configuration groups and applying them to devices, see the Using Configuration Groups section of *Cisco Catalyst SD-WAN Configuration Groups, Cisco IOS XE Catalyst SD-WAN Release 17.x*.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.

Step 2 Create a Configuration Group. A new configuration group is created.

Step 3 In the configuration group, click **Add Profile**.

Step 4 Choose **Transport & Management Profile** from the drop-down list.

Step 5 Click **Edit** to add features to the Transport and Management profile and click **Add New Feature**.

Step 6 Choose **Cellular Controller** from the **Add Feature** drop-down list.

Step 7 Choose **Cellular Profile** from the **Add Fetaure** drop-down list.

Table 2: Cellular Settings

Field	Description
Primary Slot	Choose a SIM slot to designate it as primary. Range: 0, 1 Default: 0
SIM SLOT 0 Cellular Profile	
Profile Id	Profile ID. You can click **Add** to add multiple profiles.
Access Point Name	Access point name, from your service provider.
Authentication Method	Authentication method (**none**, **pap**, **chap**, **pap_or_chap**) indicated by your service provider.
Username	Username for authentication, as indicated by your service provider.

Field	Description
Password	Password for authentication, as indicated by your service provider.
Packet Data Network Type	Packet data network type (**IPv4**, **IPv6**, **IPv4v6**), as indicated by your service provider.
Attach Profile	Choose a attach profile from the defined profiles.
Data Profile	Choose a data profile from the defined profiles. You can use the same profile for the attach profile and data profile.
SIM SLOT 1 Cellular Profile	
See the fields described for SIM slot 0.	

Step 8 For the configured **Cellular Controller**, choose the **Cellular Profile** or click **Add New** to add a new cellular profile.

Step 9 Configure **Cellular Profile** using the following table.

Table 3: Cellular Profile Settings

Field	Description
Type	Choose a feature from the drop-down list.
Feature Name	Enter a name for the feature. The name can be up to 128 characters and can contain only alphanumeric characters.
Description	Enter a description of the feature. The description can be up to 2048 characters and can contain only alphanumeric characters.
Profile ID	Enter the identification number of the profile to use on the router. Range: 1 through 15
Access Point Name	Enter the name of the gateway between the service provider network and the public internet. It can be up to 32 characters long.
Authentication	Choose the authentication method used for the connection to the cellular network. It can be **none**, **pap**, **chap**, or **pap_chap**.
Profile Username	Enter the user name to use when making cellular connections for web services. It can be 1 to 32 characters. It can contain any alphanumeric characters, including spaces.
Profile Password	Enter the user password to use when making cellular connections for web services. The password is case-sensitive and can be clear text, or an AES-encrypted key. From Cisco Catalyst SD-WAN Manager Release 20.15.1, when you enter the password as clear text, Cisco SD-WAN Manager encrypts the password. When you view the configuration preview, the password appears in its encrypted form.
Packet Data Network Type	Choose the packet data network (PDN) type of the cellular network. It can be IPv4, IPv6, or IPv4v6.

Field	Description
No Overwrite	Enable this option to overwrite the profile on the cellular modem. By default, this option is disabled.
Slice Type	Choose the network slice type (SST) for the profile. The options are: • eMBB: Enhanced Mobile Broadband, used for high data throughput. • URLLC: Ultra-Reliable Low Latency Communication, used for high reliability and low latency transmission. • MIoT: Massive IoT, used for many devices transmitting small quantities of data.
Slice Differentiator	Enter the slice differentiator (SD) for the profile. This is an optional value that enables the user equipment (UE) to use multiple slice instances of the same SST. Range: 0 through 16777214
Slot	Enter the associated SIM slot for the profile.

Configure network slicing using CLI

The following example shows how to configure a cellular network slicing using a CLI:

```
Device(config-controller)# profile id 3 apn apn-ns authentication none pdn-type ipv4
   no-overwrite
   slot            Associated sim slot
   slice-type Associated network slice type(SST)

Device(config-controller)# profile id 3 apn apn-ns authentication none pdn-type ipv4 slice-
 type
<1-3>  Slice type number: 1(eMBB), 2(URLLC), 3(MioT)
Device(config-controller)# profile id 3 apn apn-ns authentication none pdn-type ipv4 slice-
 type embb
   slice-differentiator Associated Slice Differentiator(SD)  <--- if SD is bypassed here,"FF
 FF FF" wll be used internally as the SD to indicate that there is no SD associated with
this SST.
   slot                            Associated sim slot

Device(config-controller)# profile id 3 apn apn-ns authentication none pdn-type ipv4 slice
 type
embb slice-differentiator
  <0-16777214>  Slice Differentiator
Device(config-controller)#
Device(config-controller)#$ pdn ipv6  slice-type miot slice-differentiator 6
  slot  Associated sim slot
```

Verify network slicing using CLI

The following is a sample output from the **show cellular** command that displays network slicing configuration and slice type details:

```
Device# show cellular profile 6

Profile 6 = INACTIVE
--------
PDP Type = IPv6
Access Point Name (APN) = TestNSSAI6_URLLC1
Authentication = None
S-NSSAI Slice Type is URLLC
S-NSSAI Slice Differentiator = 1
```