**Syntax Description**

| Parameter | Description | Presence | Default Value | Possible Values |
|---|---|---|---|---|
| `[<class-map-num(1-65535)>]` | Indicates the identifier of the class-map for which configuration information is to be displayed. Do not specify a value for this parameter if you want to view the configuration information for all class-maps. | Optional | N/A | 1-65535 |

**Display Format** (for each class-map if requested for all class-maps)

```
Class map <class map number>
-----------------------------------------------
CoS Value                    : <value>
DSCP Value                   : <value>
```

**Command Modes**

Global command mode

## 3.3.8.2 Managing QoS Classification Rules

QoS classification rules classify packets into flows, based on the following parameters:

- IP address of the host originating the traffic (the IP address assigned to the bearer, internal-management or external-management interface)
- Layer 3 protocol indicating either TCP or UDP
- Layer 4-source port for the application that needs to be marked (for example, FTP, Telnet, SNMP, MIP, or RADIUS)

A class-map can be associated with each flow to define separate DSCP and/or VLAN priority bits for QoS handling of each flow.

**To configure a QoS classification rule:**

1 Enable the ACL configuration mode for ACL 199 (refer to Section 3.3.8.2.1).

**IMPORTANT**

QoS classification rules can be associated only with ACL 199.

2 You can now:

- Configure one or more QoS classification rules (refer to Section 3.3.8.2.2)
- Delete one or more QoS classification rules (refer to Section 3.3.8.2.3)
- Terminate the ACL configuration mode (refer to Section 3.3.8.2.4)

You can, at any time, enable/disable QoS marking (refer to Section 3.3.8.3) or view the configuration information for ACL 199 (refer to Section 3.3.8.4).

### 3.3.8.2.1 Enabling the ACL Configuration Mode for ACL 199

To configure QoS classification rules for host-originating traffic, first enable the extended ACL 199 configuration mode.

**IMPORTANT**

QoS classification rules can be added only to extended ACL 199

Run the following command to enable the extended ACL configuration mode for ACL 199.

```
npu(config)# ip access-list {standard <access-list-number (1-99)> |
extended <access-list-number (100-199)>} [name<string>]
```

After you enable the ACL 199 configuration mode, you can configure one or several QoS classification rules, and associate them with the appropriate class-maps.

| | |
|---|---|
| **Command Syntax** | `npu(config)# ip access-list {standard <access-list-number (1-99)> \| extended <access-list-number (100-199)>} [name <string>]` |
| **Privilege Level** | `10` |

**Syntax Description**

| Parameter | Description | Presence | Default Value | Possible Values |
|---|---|---|---|---|
| **extended** <access-list-number (100-199)> | Indicates the identifier of the extended ACL for which the ACL configuration mode is to be enabled. You must specify 199 to enable configuration of QoS classification rules. | Mandatory | N/A | 199 |
| [**name** <string>] | Indicates the name of the ACL for which the ACL configuration mode is to be enabled.<br>**Note**: If you do not specify the ACL name, the ACL number is used as the default ACL name. | Optional | N/A | String (upto 20 characters) |

**Command Modes** Global configuration mode

### 3.3.8.2.2 Configuring a QoS Classification Rule

You can configure the QoS classification rules for the ACL with respect the following parameters:

- Source IP address for the host-originating application traffic
- Application protocol (TCP or UDP)
- L4 source port of the application traffic
- QoS class-map identifier

By default, there are 8 pre-configured QoS classification rules associated with the 8 pre-configured QoS class-maps:

**Table 3-15: Pre-Configured QoS Classification Rules and Class-Maps**

| IP Interface | Type of Traffic | Protocol | Source Port | Class Map | DSCP | 802.1p |
|---|---|---|---|---|---|---|
| Bearer | RADIUS | UDP | 1812 | 1 | 7 | 7 |

**Table 3-15: Pre-Configured QoS Classification Rules and Class-Maps**

| IP Interface | Type of Traffic | Protocol | Source Port | Class Map | DSCP | 802.1p |
|---|---|---|---|---|---|---|
| Bearer | MobileIP-Agent | UDP | 434 | 2 | 7 | 7 |
| Bearer | WiMAX ASN Control Plane Protocol | UDP | 2231 | 3 | 7 | 7 |
| Internal-Management | OBSAI message exchange between NPU and AU | UDP | 10009 | 4 | 0 | 0 |
| Internal-Management | Trivial File Transfer Protocol | UDP | 69 | 5 | 0 | 0 |
| External-Management | Telnet | TCP | 23 | 6 | 0 | 0 |
| External-Management | SSH Remote Login Protocol | TCP | 22 | 7 | 0 | 0 |
| External-Management | SNMP | UDP | 161 | 8 | 0 | 0 |

After configuring QoS classification rules for this ACL, enable QoS marking for this ACL. By default, QoS marking is disabled. For details, refer to Section 3.3.8.3.

Run the following command to configure a QoS classification rule for this ACL:

```
npu(config-ext-nacl)# qos-mark {{host <src-ip-address>} {{tcp | udp} srcport <short (1-65535)>} qosclassifier <short (1-65535)>}
```

When you execute this command, a new QoS classification rule is added to the ACL for which the configuration mode is enabled.

**IMPORTANT**

An error may occur if:

- You have specified a source port that is not within the range, 1-65535.
- The host IP address or class-map identifier that you have specified do not exist.

**Command Syntax**

```
npu(config-ext-nacl)# qos-mark {{host <src-ip-address>} {{tcp | udp} srcport <short (1-65535)>} qosclassifier <short (1-65535)>}
```

**Privilege Level**

10

**Syntax Description**

| Parameter | Description | Presence | Default Value | Possible Values |
|---|---|---|---|---|
| `{host <src-ip-address>}` | Indicates the IP address of the host interface that generates the traffic for which this classification rule is to be configured. Specify the IP address that you have assigned to the internal-management, external-management, local-management or bearer IP interface. | Mandatory | N/A | Valid IP address (assigned to the internal-management, external-management, local-management or bearer IP interface) |
| `{tcp \| udp}` | Indicates the transport protocol. | Mandatory | N/A | ■ tcp<br>■ udp |
| `srcport <short (1-65535)>` | Indicates the source port number of the application traffic for which this QoS classification rule is to be applied. | Mandatory | N/A | 1-65535 |
| `qosclassifier <class-map-number (1-65535)>` | Indicates the identifier of the QoS class-map to be associated with this classification rule. For more information about configuring class-maps, refer Section 3.3.8.1. | Mandatory | N/A | 1-65535 |

**Command Modes** Extended ACL configuration mode

### 3.3.8.2.3 Deleting a QoS Classification Rule

**IMPORTANT**

You can delete a QoS classification rule only if the associated ACL is INACTIVE. For more information, refer Section 3.3.10.3.

To delete a QoS classification rule for an ACL, run the following command:

```
npu(config-ext-nacl)# no qos-mark {{host <src-ip-address>} {{tcp | udp} srcport <short (1-65535)>} qosclassifier <short (1-65535)>}
```

When you execute this command, the QoS classification rule is deleted from the ACL.

**IMPORTANT**

An error may occur if you specify a combination of parameters that do not match any of the existing QoS classification rules.:

- 

**Command Syntax**

```
npu(config-ext-nacl)# no qos-mark {{host <src-ip-address>} {{tcp | udp}
srcport <short (1-65535)>} qosclassifier <short (1-65535)>}
```

**Privilege Level**

**10**

**Syntax Description**

| Parameter | Description | Presence | Default Value | Possible Values |
|---|---|---|---|---|
| `[host <src-ip-address>]` | Indicates the IP address of the host interface that generates the traffic for which this classification rule is to be deleted. | Mandatory | N/A | Valid IP address (assigned to the internal-management, external-management or bearer IP interface) |
| `{tcp \| udp}` | Indicates the transport protocol. | Mandatory | N/A | ■ tcp<br>■ udp |
| `srcport <short (1-65535)>` | Indicates the source port number of the application traffic for which this QoS classification rule is to be deleted. | Mandatory | N/A | 1-65535 |
| `qosclassifier <class-map-number (1-65535)>` | Indicates the identifier of the QoS class-map associated with the classification rule to be deleted. For more information about class-maps, refer Section 3.3.8.1. | Mandatory | N/A | 1-65535 |

| | |
|---|---|
| **Command Modes** | Extended ACL configuration mode |

#### 3.3.8.2.4 Terminating the ACL Configuration Mode

To terminate the ACL configuration mode, run the following command:

```
npu(config-ext-nacl) # exit
```

| | |
|---|---|
| **Command Syntax** | `npu(config-ext-nacl) # exit` |
| **Privilege Level** | 10 |
| **Command Modes** | Extended ACL configuration mode |

### 3.3.8.3 Enabling/Disabling QoS Marking for ACL 199

You can enable/disable the QoS marking for the ACL. The class-map is applied on traffic matching a QoS classification rule only after you enable the QoS marking for the ACL).

**NOTE**

If you want to modify a QoS class-map, first disable the QoS marking rules for the associated ACL. By default, QoS marking is disabled for the ACL.

Run the following command to enable/disable the QoS marking for the specified ACL:

```
npu(config)# set qos {enable | disable} 199
```

| | |
|---|---|
| **Command Syntax** | `npu(config)# set qos {enable \| disable} 199` |
| **Privilege Level** | `10` |

**Syntax Description**

| Parameter | Description | Presence | Default Value | Possible Values |
|---|---|---|---|---|
| `{enable \| disable}` | Indicates whether QoS marking should be enabled or disabled for a specific ACL. | Mandatory | disable | ■ enable<br>■ disable |
| `199` | Indicates the identifier of the ACL for which the QoS marking is to be activated. You musr specify 199. | Mandatory | N/A | 199 |

**Command Modes**

Global configuration mode

### 3.3.8.4 Displaying ACL 199 Configuration Information

Run the following command to display the configuration information for ACL 199:

```
npu# show access-lists [{199 | <access-list-199-name}]
```

**IMPORTANT**

An error may occur if the ACL name you have specified does not exist.

**Command Syntax**

```
npu# show access-lists [199| <access-list-199-name}]
```

**Privilege Level**

**1**

**Syntax Description**

| Parameter | Description | Presence | Default Value | Possible Values |
|---|---|---|---|---|
| `[199 \| <access-list-199-name}]` | To view configuration information for ACL 199, specify 199 or the name configured for this ACL. | Mandatory for viewing information for ACL 199. | N/A | ■ 199<br>■ String; the name configured for ACL 199. |

**Display Format (Standard)**

```
Extended IP Access List 199
Access List Name(Alias)          : 199

 Interface List                  : NIL
 Status                          : <Active|Inactive>
 Admin-Status                    : <Up|Down>

 Filter Protocol Type            : <UDP|TCP>
 Source IP address               : <IP address>
 Filter Source Port              : <value>
 Rule Action                     : QoS Marking
 QoS Classifier ID               : <value>
 Marking rule status             : <ACTIVE|INACTIVE>
..............
```

## 3.3.9 Configuring Static Routes

**Command Modes** Global command mode

Using the CLI, you can configure the static routes for traffic originating from the NPU. For each static route, you can configure the destination IP address, address mask, and the next hop IP address. The following are the types of traffic originating from the NPU:

- R4/R6 control traffic
- R3 control traffic such as RADIUS or MIP
- NMS traffic

This section describes the commands for:


- “Adding a Static Route” on page 168
- “Deleting a Static Route” on page 169

■ “Displaying the IP Routing Table” on page 170

There are four automatically created static route with the IP addresses of the directly connected Bearer, External Management, Local Management and Internal Management interfaces (the IP address of the Internal Management interface is set to 10.0.0.254. Note that availability of certain interfaces depend on the connectivity mode). These routes cannot be modified or deleted.

In addition, the “Any Destination” entry with Destination 0.0.0.0 and Mask 0.0.0.0 must be created during initial setup and should not be deleted. The Next Hop IP address of this route must be in the same subnet with the interface used for remote management.

### 3.3.9.1 Adding a Static Route

To add a static route, run the following command:

```
npu(config)# ip route <ip_address> <ip_mask> <ip_nexthop>
```

**NOTE**

Refer to Section 3.3.9.3 to display the IP routing table.

For example, run the following command to add an entry for a static route with the destination IP address, 11.0.0.2, and the address mask, 255.255.255.255, and next-hop IP address, 192.168.10.1.

```
npu(config)# ip route 11.0.0.2 255.255.255.255 192.168.10.1
```

**IMPORTANT**

An error may occur if:

- The IP address, address mask or the next-hop IP address are invalid.
- A route with the parameters that you have specified already exists.
- The IP address that you have specified is being used for another interface.
- The next-hop IP address that you have specified is either unreachable or is down.

| | |
|---|---|
| **Command Syntax** | `npu(config)# ip route <ip_address> <ip_mask> <ip_nexthop>` |

**Privilege Level** `10`

**Syntax Description**

| Parameter | Description | Presence | Default Value | Possible Values |
|---|---|---|---|---|
| `<ip_address>` | Indicates the destination host or network IP address, for which the route is to be added. | Mandatory | N/A | Valid IP address |
| `<ip_mask>` | Indicates the address mask for the static route to be added. | Mandatory | N/A | Valid address mask |
| `<ip_nexthop>` | Indicates the next hop IP address, for the route to be added. | Mandatory | N/A | Valid IP address |

**Command Modes** Global configuration mode

**NOTE**

Kernel route is added automatically for default gateway network address of service interface of VLAN type when service interface is attached to a service group and vlan enable is set for the service group. This route is deleted when vlan is disabled for service group.

Also kernel route is added automatically for relay server IP address when service interface of type VLAN is attached to a service group and vlan enable is set for the service group. This route is deleted when vlan is disabled for the service group.

These routes are not displayed by the "show ip route" command.

### 3.3.9.2 Deleting a Static Route

To delete a static route, run the following command:

**`npu(config)# no ip route`** `<ip_address> <ip_mask> <ip_nexthop>`

For example, run the following command to delete an entry for a static route with the destination IP address, 11.0.0.2, and the address mask, 255.255.255.255, and next-hop IP address, 192.168.10.1.

**`npu(config)# no ip route 11.0.0.2 255.255.255.255 192.168.10.1`**

**IMPORTANT**

An error may occur if a route matching the specified parameters does not exist.

**Command Syntax**

```
npu(config)# no ip route <ip_address> <ip_mask> <ip_nexthop>
```

**Privilege Level**

10

**Syntax Description**

| Parameter | Description | Presence | Default Value | Possible Values |
|---|---|---|---|---|
| <ip_address> | Indicates the destination host or network IP address, for which the route is to be deleted. | Mandatory | N/A | Valid IP address |
| <ip_mask> | Indicates the address mask for the static route to be deleted. | Mandatory | N/A | Valid address mask |
| <ip_nexthop> | Indicates the next hop IP address, for the route to be deleted. | Mandatory | N/A | Valid IP address |

**Command Modes**

Global configuration mode

### 3.3.9.3 Displaying the IP Routing Table

To display the IP routing table, run the following command:

```
npu# show ip route
```

**Command Syntax**

```
npu(config)# show ip route
```

**Privilege Level**

1

**Display Format**

```
<IP address/mask>          is directly connected
<IP address/mask>          is directly connected
<IP address/mask>          is directly connected
<IP address/mask>          via <Next-hop IP address>
<IP address/mask>          via <Next-hop IP address>
<IP address/mask>          via <Next-hop IP address>
<IP address/mask>          via <Next-hop IP address>
<IP address/mask>          via <Next-hop IP address>
```

**Command Modes**

Global command mode

## 3.3.10 Configuring ACLs

ACLs are applied on traffic received from the NPU physical interfaces (DATA, MGMT or CSCD ports), and destined towards the following virtual interfaces:

- AUs
- NPU

By default, all traffic destined towards the AUs is denied. Several default ACLs are created automatically to allow some restricted traffic towards the NPU. These ACL rules are applied automatically at the time of NPU startup or upon a change of IP address of various interfaces. You can use the CLI to configure additional ACLs for permitting or denying specific traffic destined towards the NPU or AUs.

You can create the following types of ACLs:

- Standard: Allows you to filter traffic based on the source and destination IP addresses.
- Extended: Allows you to filter traffic based on the source and destination IP addresses, source and destination ports, and protocol.

**IMPORTANT**

You can use extended ACL 199 to configure QoS classification rules for classifying traffic originating from the NPU into different flows. For details, refer "Configuring QoS Marking Rules" on page 152).

You can create the following types of rules for an ACL:

- Permit: Indicates that traffic matching the filter criteria is allowed to reach the NPU or AUs.
- Deny: Indicates that traffic matching the filter criteria is dropped, and not allowed to reach the NPU or AUs.

You can configure multiple rules for each ACL; the priority for these rules is applied with respect to the sequence in which these rules are configured. After you configure an ACL, you can attach the ACL to either the NPU or the AUs or both NPU and AUs.

All ACLs are either in the ACTIVE or INACTIVE state. The ACTIVE state indicates that the ACL is attached to one or more interfaces; the INACTIVE state indicates that the ACL is not attached to any interface.

By default, traffic towards the AUs is not restricted. This is implemented through ACL 1 which is available by default. ACL 1 is attached to AUs, with Rule Action = Permit, Source IP Address = Any and Destination IP Address = Any.

All the following automatically created standard default ACLs are attached to the NPU virtual interface and include a single Permit rule:

**Table 3-16: Default Standard ACLs**

| ACL Number | Rule Action | Source IP Address | Destination IP Address |
|---|---|---|---|
| ACL 96 | Permit | Any | Internal Management IP address |
| ACL 97 | Permit | Any | External Management IP address |
| ACL 98 | Permit | Any | Local Management IP address |

The default Extended ACL 186 attached to the NPU virtual interface includes the following Permit rules allowing certain traffic towards the Bearer interface:

**Table 3-17: Rules of Default ACL 186**

| Rule Action | Source IP Address | Source Port | Destination IP Address | Destination Port | Protocol |
|---|---|---|---|---|---|
| Permit | Any | Any | Bearer IP address | Any | ICMP (1) |

**Table 3-17: Rules of Default ACL 186**

| Rule Action | Source IP Address | Source Port | Destination IP Address | Destination Port | Protocol |
|---|---|---|---|---|---|
| Permit | Any | Any | Bearer IP address | 2231 (used for WiMAX ASN Control Plane Protocol) | UDP (17) |
| Permit | Any | Any | Bearer IP address | 1812-1813 (used for RADIUS Authentication and Accounting) | UDP (17) |
| Permit | Any | Any | Bearer IP address | 69 (used for TFTP) | UDP (17) |
| Permit | Any | Any | Bearer IP address | 1022-1023 (used for software download) | UDP (17) |

Additional Extended ACLs are created automatically for every Service Group that is associated with a VLAN Service Interface and an enabled VLAN Service. Up to 10 ACLs, numbered ACL 187 to ACL 196, can be created, These automatically created/deleted ACLs allow Ping and DHCP traffic on the DHCP Own IP Address interface of the applicable VLAN service:

**Table 3-18: Rules of Default VLAN Service Interfaces ACL 187-196**

| Rule Action | Source IP Address | Source Port | Destination IP Address | Destination Port | Protocol |
|---|---|---|---|---|---|
| Permit | Any | Any | DHCP Own IP Address defined for the applicable Service Group | Any | ICMP (1) |
| Permit | Any | Any | DHCP Own IP Address defined for the applicable Service Group | 67-68 (used for DHCP traffic) | UDP (17) |

**IMPORTANT**

The default pre-configured and automatically created ACLs cannot be deleted and should not be modified.

This section describes the commands for:

- "Configuring an ACL in the Standard/Extended Mode" on page 174
- "Deleting an ACL" on page 198
- "Attaching/De-attaching ACLs to/from an Interface" on page 199
- "Displaying ACL Configuration Information" on page 202

## 3.3.10.1 Configuring an ACL in the Standard/Extended Mode

You can configure an ACL in either of the following modes:

- Standard mode: Use this mode if you want to create Permit or Deny rules for traffic based on source and destination IP addresses.
- Extended mode: Use this mode if you want to create Permit or Deny rules based on source and destination IP addresses, source and destination ports, protocol.

**To configure an ACL:**

1. Enable the standard or extended ACL configuration mode (refer Section 3.3.10.1.1).
2. After you enter the ACL configuration mode, you can:
   - » Configure ACLs in the standard mode (refer Section 3.3.10.1.2).
   - » Configure ACLs in the extended mode (refer Section 3.3.10.1.3).
3. Terminate the ACL configuration mode (refer Section 3.3.10.1.4).
4. After you have configured the ACL, you can attach the ACL with the AUs or NPU refer Section 3.3.10.3.

### 3.3.10.1.1 Enable the ACL Configuration Mode/Creating an ACL

To configure an ACL, first enable either of the following ACL configuration modes:

- Standard
- Extended

**IMPORTANT**

ACL 199 is the default extended ACL that is pre-configured in the system, and is not attached to any interface, that is, it is INACTIVE. However, ACL 199 is reserved for QoS classification rules. You cannot configure Permit/Deny rules for ACL 199.

To view the default configuration information for ACL 199, you can run the following command:

```
npu# show access-lists 199
```

For details on using ACL 199 refer to Section 3.3.8.

To apply this ACL to traffic destined towards the AUs or the NPU, you are required to activate this ACL (for details refer Section 3.3.10.3).

Run the following command to enable the ACL configuration mode. You can also use this command to create a new ACL.

```
npu(config)# ip access-list {standard <access-list-number (1-99)> |
extended <access-list-number (100-199)>}[name<string>]
```

When you run this command, the ACL configuration mode for the newly-created ACL is automatically enabled. If the name is not specified when creating a new ACL, the default name will be the specified ACL number.

For example, run the following command to create ACL 22 in the standard mode:

```
npu(config)# ip access-list standard 22

Standard ACL 22 will be created with the default name 22.
```

For example, run the following command to create ACL 111 in the extended mode, with the name ACL-111:

```
npu(config)# ip access-list extended 111 ACL-111
```

After you create an ACL or enable the ACL configuration mode, you can

- Configure the ACL in the standard mode (refer Section 3.3.10.1.2)
- Configuring the ACL in the extended mode (refer Section 3.3.10.1.3)

**IMPORTANT**

An error may occur if:·

- You specify an invalid ACL number. The ACL number should be between 1 and 99 in the standard mode, and between 100 and 199 in the extended mode.
- The ACL name you have specified is already used for another ACL or is more than 20 characters.

**Command Syntax**

```
npu(config)# ip access-list {standard <access-list-number (1-99)> |
extended <access-list-number (100-199)>}[name<string>]
```

**Privilege Level**

**10**

**Syntax Description**

| Parameter | Description | Presence | Default Value | Possible Values |
|---|---|---|---|---|
| `standard <access-list-number (1-99)> \| extended <access-list-number (100-199)>` | Denotes the number of the standard or extended ACL that is to be created for which the ACL configuration mode is to be enabled. If you are creating a new ACL, the ACL configuration mode is automatically enabled when you execute this command.<br>**Note**: ACL 199 is reserved for QoS classification rules and cannot be used for creating Permit/Deny rules. | Mandatory | N/A | ■ standard 1-99<br>■ extended (100-198) |
| `[name<string>]` | Indicates the name of the ACL to be created for which the ACL configuration mode is to be enabled. | Optional | ACL name | String (upto 20 characters) |

**Command Modes**

Global configuration mode

#### 3.3.10.1.2 Configuring ACLs in the Standard Mode

After you have enabled the standard ACL configuration mode, you can create or delete the Permit/Deny rules for forwarding traffic from/to a particular source/destination IP address.

**IMPORTANT**

You cannot create Permit or Deny rules for an ACL that is associated with a Qos marking rule. You can either associate QoS marking rules or permit/deny rules with an ACL.

This section describes the commands for:

- "Creating a Permit/Deny Rule (Standard Mode)" on page 177
- "Deleting a Permit/Deny Rule (Standard Mode)" on page 179

**IMPORTANT**

After you have configured the rules to be applied on an ACL, you can attach the ACL to the NPU or AUs. The ACL enables filtering of traffic destined to these interfaces. For more information, refer to Section 3.3.10.3.

##### 3.3.10.1.2.1 Creating a Permit/Deny Rule (Standard Mode)

Run the following commands to create the Permit/Deny rules for forwarding traffic from/to a particular source/destination IP address:

```
npu(config-std-nacl)# permit {any | host <src-ip-address> |
<network-src-ip> <mask>} [{any | host <dest-ip-address> |
<network-dest-ip> <mask>}]
```

```
npu(config-std-nacl)# deny {any | host <src-ip-address> |
<network-src-ip> <mask>} [{any | host <dest-ip-address> |
<network-dest-ip> <mask>}]
```

**IMPORTANT**

In the above commands, it is mandatory to specify the source IP address for which the Permit/Deny rule is to be created. If you do not specify the destination IP address/subnet mask, by default, traffic to all destination IP addresses configured for the NPU is permitted/denied.

The following table lists the parameters and their descriptions in these commands.

**Table 3-19: Parameters for Configuring Permit/Deny Rules in the Standard ACL Mode**

| | Parameter | Description | Example |
|---|---|---|---|
| Source IP | any | Indicates that incoming traffic from any source IP address is permitted or denied. | **npu(config-std-nacl)# permit any**<br>**npu(config-std-nacl)# deny any** |
| | host <src-ip-address> | Indicates that incoming traffic from a specific source IP address is permitted or denied. | **npu(config-std-nacl)# permit host 1.1.1.1**<br>**npu(config-std-nacl)# deny host 1.1.1.1** |
| | <network-src-ip> <mask> | Indicates that incoming traffic is to be permitted or denied for a particular subnet. | **npu(config-std-nacl)# permit 1.1.1.0 255.255.255.0**<br>**npu(config-std-nacl)# deny 1.1.1.0 255.255.255.0** |
| Destination IP address | any | Indicates that traffic destined to all NPU IP addresses is permitted or denied. | **npu(config-std-nacl)# permit host 1.1.1.1 any**<br>**npu(config-std-nacl)# deny host 1.1.1.1 any** |
| | host <src-ip-address> | Indicates that traffic destined to a specific destination IP address is permitted or denied. | **npu(config-std-nacl)# permit any host 1.1.1.1**<br>**npu(config-std-nacl)# deny any host 1.1.1.1** |
| | <network-src-ip> <mask> | Indicates that traffic destined to a particular subnet is to be permitted or denied. | **npu(config-std-nacl)# permit any 1.1.1.0 255.255.255.0**<br>**npu(config-std-nacl)# deny any 1.1.1.0 255.255.255.0** |

**Command Syntax**

**npu(config-std-nacl)# permit** { **any** | **host** <src-ip-address> | <network-src-ip> <mask> } [ { **any** | **host** <dest-ip-address> | <network-dest-ip> <mask> } ]

**npu(config-std-nacl)# deny** { **any** | **host** <src-ip-address> | <network-src-ip> <mask> } [ { **any** | **host** <dest-ip-address> | <network-dest-ip> <mask> } ]

**Syntax Description**

| Parameter | Description | Presence | Default Value | Possible Values |
|---|---|---|---|---|
| `{ any \| host <src-ip-address> \| <network-src-ip> <mask> }` | Indicates the source IP address/subnet for which incoming traffic is permitted/denied. | Mandatory | N/A | For details, refer Table 3-19 |
| `[ { any \| host <dest-ip-address> \| <network-dest-ip> <mask> } ]` | Indicates the destination IP address/subnet for which traffic is permitted/denied | Optional | any | For details, refer Table 3-19 |

**Command Modes**

Standard ACL configuration mode

### 3.3.10.1.2.2 Deleting a Permit/Deny Rule (Standard Mode)

Run the following commands to delete the Permit/Deny rule for incoming traffic from/to a specific IP address/subnet.

```
npu(config-std-nacl)# no permit {any | host <src-ip-address> |
<network-src-ip> <mask>} [{any | host <dest-ip-address> |
<network-dest-ip> <mask>}]
```

```
npu(config-std-nacl)# no deny {any | host <src-ip-address> |
<network-src-ip> <mask>} [{any | host <dest-ip-address> |
<network-dest-ip> <mask>}]
```

**Command Syntax**

```
npu(config-std-nacl)# no permit { any | host <src-ip-address> |
<network-src-ip> <mask> }  [ { any | host <dest-ip-address> |
<network-dest-ip> <mask> } ]
```

```
npu(config-std-nacl)# no deny { any | host <src-ip-address> |
<network-src-ip> <mask> }  [ { any | host <dest-ip-address> |
<network-dest-ip> <mask> } ]
```

**Privilege Level**

**10**

**Syntax Description**

| Parameter | Description | Presence | Default Value | Possible Values |
|---|---|---|---|---|
| `{ any \| host <src-ip-address> \| <network-src-ip> <mask> }` | Indicates the source IP address/subnet for which the Permit/Deny rule is to be deleted. | Mandatory | N/A | For details, refer Table 3-19 |
| `[ { any \| host <dest-ip-address> \| <network-dest-ip> <mask> } ]` | Indicates the destination IP address/subnet for which the Permit/Deny rule is to be deleted. | Optional | any | For details, refer Table 3-19 |

**Command Modes**

Standard ACL configuration mode

### 3.3.10.1.3 Configuring ACLs in the Extended Mode

After you have enabled the extended ACL configuration mode, you can create Permit/Deny rules based on source/destination IP address, protocol and source/destination port numbers.

**IMPORTANT**

You cannot create Permit or Deny rules for an ACL that is associated with a Qos marking rule. You can either associate QoS marking rules or permit/deny rules with an ACL.

This section describes the commands to be used for:

- “Configuring Permit/Deny Rules from/to a Specific Protocol and Source/Destination IP Addresses” on page 181
- “Configuring Permit/Deny Rules for TCP/UDP Traffic” on page 185
- “Configuring Permit/Deny Rules for ICMP Traffic” on page 194

**IMPORTANT**

After you have configured the rules to be applied on an ACL, you can attach the ACL to the NPU or AUs. The ACL enables filtering of traffic destined to these interfaces. For more information, refer to Section 3.3.10.3.

#### 3.3.10.1.3.1 Configuring Permit/Deny Rules from/to a Specific Protocol and Source/Destination IP Addresses

After you have created an ACL, you can configure Permit/Deny rules to be applied for traffic from/to a particular source/destination IP address/subnet, with respect to a specific protocol.

**IMPORTANT**

You cannot configure Permit or Deny rules for an ACL that is associated with a Qos marking rule. You can either associate QoS marking rules or permit/deny rules with an ACL.

This section describes the commands to be used for:

- "Creating a Permit/Deny Rule for Specific Protocols/IP Addresses (Extended Mode)" on page 181
- "Deleting a Permit/Deny Rule for Specific Protocols/IP Addresses (Extended Mode)" on page 184

##### *3.3.10.1.3.1.1 Creating a Permit/Deny Rule for Specific Protocols/IP Addresses (Extended Mode)*

You can create the Permit or Deny rule for traffic from/to a source/ destination IP address/subnet with respect to the following protocols:

- IP
- OSPF
- Protocol Independent Multicast (PIM)
- Any other protocol

Run the following commands to create the Permit/Deny rule for traffic from and to a specific IP address/subnet for a particular protocol:

```
npu(config-ext-nacl)# permit {ip | ospf | pim | <protocol-type
(1-255)>} {any | host <src-ip-address> | <src-ip-address> <mask>}
{any | host <dest-ip-address> | <dest-ip-address> <mask>}
```

```
npu(config-ext-nacl)# deny {ip | ospf | pim | <protocol-type
(1-255)>} {any | host <src-ip-address> | <src-ip-address> <mask>}
{any | host <dest-ip-address> | <dest-ip-address> <mask>}
```

In the above commands, it is mandatory to specify the protocol and source IP address for which the Permit/Deny rule is to be created. If you do not specify the destination IP address/subnet mask, by default, traffic to all destination IP addresses is permitted/denied.

The following table lists the parameters and their descriptions in these commands:

**Table 3-20: Parameters for Configuring Permit/Deny Rules for Traffic from/to Specific IP Addresses**

| | Parameter | Description | Example |
|---|---|---|---|
| Protocol | `ip` | Indicates that the Permit/Deny rule to be created is to be applied for the IP-in-IP packets. | **`npu(config-ext-nacl)# permit ip any`** |
| | `ospf` | Indicates that the Permit/Deny rule to be created is to be applied to OSPF packets. | **`npu(config-ext-nacl)# permit ospf any`** |
| | `pim` | Indicates that the Permit/Deny rule to be created is to be applied to the PIM packets. | **`npu(config-ext-nacl)# permit pim any`** |
| | `<protocol-type (1-255)>` | Indicates that the Permit/Deny rule to be created is to be applied to traffic from/to any protocol (including IP, OSPF, PIM). Use standard IANA values to specify the values of these protocols | **`npu(config-ext-nacl)# permit 11 any`** |
| Source IP address | `any` | Indicates that incoming traffic from any source IP address is permitted or denied. | **`npu(config-std-nacl)# permit ip any`**<br>**`npu(config-std-nacl)# deny ip any`** |
| | `host <src-ip-address>` | Indicates that incoming traffic from a specific source IP address is permitted or denied. | **`npu(config-std-nacl)# permit ip host 1.1.1.1`**<br>**`npu(config-std-nacl)# deny ip host 1.1.1.1`** |
| | `<network-src-ip> <mask>` | Indicates that incoming traffic is to be permitted or denied for a particular source IP address and subnet mask. | **`npu(config-std-nacl)# permit ip 1.1.1.0 255.255.255.0`**<br>**`npu(config-std-nacl)# deny ip 1.1.1.0 255.255.255.0`** |

**Table 3-20: Parameters for Configuring Permit/Deny Rules for Traffic from/to Specific IP Addresses**

| | Parameter | Description | Example |
|---|---|---|---|
| Destination IP address | any | Indicates that traffic to any destination IP address is permitted or denied. any is the default destination IP address. | **npu(config-std-nacl)# permit ip host 1.1.1.1 any**<br>**npu(config-std-nacl)# deny ip host 1.1.1.1 any** |
| | host <dst-ip-address> | Indicates that traffic destined to a specific destination IP address is permitted or denied. | **npu(config-std-nacl)# permit ip any host 1.1.1.1**<br>**npu(config-std-nacl)# deny ip any host 1.1.1.1** |
| | <network-dst-ip> <mask> | Indicates that traffic destined to a particular subnet is to be permitted or denied. | **npu(config-std-nacl)# permit ip any 1.1.1.0 255.255.255.0**<br>**npu(config-std-nacl)# deny ip any 1.1.1.0 255.255.255.0** |

**Command Syntax**

**npu(config-ext-nacl)# permit** { **ip** | **ospf** | **pim** | <protocol-type (1-255)>} { **any** | **host** <src-ip-address> | <src-ip-address> <mask> } { **any** | **host** <dest-ip-addresq> | <dest-ip-address> <mask> }

**npu**(config-ext-nacl)# **deny** { **ip** | **ospf** | **pim** | <protocol-type (1-255)>} { **any** | host <src-ip-address> | <src-ip-address> <mask> } { **any** | **host** <dest-ip-addresq> | <dest-ip-address> <mask> }

**Privilege Level**

**10**

**Syntax Description**

| Parameter | Description | Presence | Default Value | Possible Values |
|---|---|---|---|---|
| { ip \| ospf \| pim \| <protocol-type (1-255)>} | Indicates the type of protocol for which incoming traffic is permitted. | Mandatory | N/A | For details, refer Table 3-20 |
| { any \| host <src-ip-address> \| <src-ip-address> <mask> } | Indicates the source IP address/subnet for which incoming traffic is permitted/denied. | Mandatory | N/A | For details, refer Table 3-20 |

| | | | | | |
|---|---|---|---|---|---|
| | `{ any \| host <dest-ip-addresq> \| <dest-ip-address> <mask> }` | Indicates the destination IP address/subnet for which traffic is permitted/denied | Optional | any | For details, refer Table 3-20 |

**Command Modes** Extended ACL configuration mode

### 3.3.10.1.3.1.2 Deleting a Permit/Deny Rule for Specific Protocols/IP Addresses (Extended Mode)

Run the following commands to delete the Permit/Deny rule for traffic from to a specific IP address/subnet for a particular protocol:

```
npu(config-ext-nacl)# no permit {ip | ospf | pim | <protocol-type (1-255)>} {any | host <src-ip-address> | <src-ip-address> <mask>} {any | host <dest-ip-address> | <dest-ip-address> <mask>}

npu(config-ext-nacl)# no deny {ip | ospf | pim | <protocol-type (1-255)>} {any | host <src-ip-address> | <src-ip-address> <mask>} {any | host <dest-ip-address> | <dest-ip-address> <mask>}
```

**Command Syntax**

```
npu(config-ext-nacl)# no permit { ip | ospf | pim | <protocol-type (1-255)>} { any | host <src-ip-address> | <src-ip-address> <mask> } { any | host <dest-ip-addresq> | <dest-ip-address> <mask> }

npu(config-ext-nacl)# no deny { ip | ospf | pim | <protocol-type (1-255)>} { any | host <src-ip-address> | <src-ip-address> <mask> } { any | host <dest-ip-addresq> | <dest-ip-address> <mask> }
```

**Privilege Level** 10

**Syntax Description**

| Parameter | Description | Presence | Default Value | Possible Values |
|---|---|---|---|---|
| `{ ip \| ospf \| pim \| <protocol-type (1-255)>}` | Indicates the type of protocol for which the Permit/Deny rule is to be deleted. | Mandatory | N/A | For details, refer Table 3-20 |

| | | | | | |
|---|---|---|---|---|---|
| | `{ any \| host <src-ip-address> \| <src-ip-address> <mask> }` | Indicates the source IP address/subnet for which the Permit/Deny rule is to be deleted. | Mandatory | N/A | For details, refer Table 3-20 |
| | `{ any \| host <dest-ip-address> \| <dest-ip-address> <mask> }` | Indicates the destination IP address/subnet for which the Permit/Deny rule is to be deleted. | Optional | any | For details, refer Table 3-20 |

**Command Modes** Extended ACL configuration mode

### 3.3.10.1.3.2 Configuring Permit/Deny Rules for TCP/UDP Traffic

After you have created an ACL, you can configure Permit/Deny rules for TCP and UDP traffic from/to specific source and destination IP address and port.

**IMPORTANT**

You cannot configure Permit or Deny rules for an ACL that is associated with a Qos marking rule. You can either associate QoS marking rules or permit/deny rules with an ACL.

This section describes the commands to be used for:

- “Creating a Permit/Deny Rule for TCP/UDP Traffic (Extended Mode)” on page 185
- “Deleting a Permit/Deny Rule for TCP/UDP Traffic (Extended Mode)” on page 191

#### *3.3.10.1.3.2.1 Creating a Permit/Deny Rule for TCP/UDP Traffic (Extended Mode)*

Run the following commands to specify the Permit rule for TCP/UDP traffic from/to a specific source/destination IP address/port:

```
npu(config-ext-nacl)# permit tcp {any | host <src-ip-address> |
<src-ip-address> <src-mask>} [{gt <port-number (1-65535)> | lt
<port-number (1-65535)> |eq <port-number (1-65535)> | range
<port-number (1-65535)> <port-number (1-65535)>}] {any | host
<dest-ip-address> | <dest-ip-address> <dest-mask>} {gt <port-number
(1-65535)>   | lt <port-number (1-65535)> | eq <port-number
(1-65535)> | range <port-number (1-65535)> <port-number
(1-65535)>}]
```

```
npu(config-ext-nacl)# permit udp {any | host <src-ip-address> |
<src-ip-address> <src-mask>} [{gt <port-number (1-65535)> | lt
<port-number (1-65535)> |eq <port-number (1-65535)> | range
<port-number (1-65535)> <port-number (1-65535)>}] {any | host
<dest-ip-address> | <dest-ip-address> <dest-mask>} {gt <port-number
(1-65535)>   | lt <port-number (1-65535)> | eq <port-number
(1-65535)> | range <port-number (1-65535)> <port-number
(1-65535)>}]
```

Run the following commands to specify the Deny rule for TCP/UDP traffic from/to a specific source/destination IP address/port:

```
npu(config-ext-nacl)# deny tcp {any | host <src-ip-address> |
<src-ip-address> <src-mask>} [{gt <port-number (1-65535)> | lt
<port-number (1-65535)> |eq <port-number (1-65535)> | range
<port-number (1-65535)> <port-number (1-65535)>}] {any | host
<dest-ip-address> | <dest-ip-address> <dest-mask>} {gt <port-number
(1-65535)>   | lt <port-number (1-65535)> | eq <port-number
(1-65535)> | range <port-number (1-65535)> <port-number
(1-65535)>}]
```

```
npu(config-ext-nacl)# deny udp {any | host <src-ip-address> |
<src-ip-address> <src-mask>} [{gt <port-number (1-65535)> | lt
<port-number (1-65535)> |eq <port-number (1-65535)> | range
<port-number (1-65535)> <port-number (1-65535)>}] {any | host
<dest-ip-address> | <dest-ip-address> <dest-mask>} {gt <port-number
(1-65535)>   | lt <port-number (1-65535)> | eq <port-number
(1-65535)> | range <port-number (1-65535)> <port-number
(1-65535)>}]
```

In the above commands, it is mandatory to specify the source and destination IP address for which the Permit/Deny rule is to be created.

**IMPORTANT**

To increase the granularity of the Permit/Deny rule you are creating, specify the source and destination port numbers for the source and destination IP addresses.

The following table lists the parameters and their descriptions in these commands:

**Table 3-21: Parameters for Configuring Permit/Deny Rules for TCP/UDP Traffic**

| | Parameter | Description | Example |
|---|---|---|---|
| Source IP address | `any` | Indicates that incoming TCP/UDP traffic from any source IP address is permitted or denied. | **`npu(config-ext-nacl)# permit tcp any any`**<br>**`npu(config-ext-nacl)# deny udp any`** |
| | `host <src-ip-address>` | Indicates that incoming TCP/UDP traffic from a specific source IP address is permitted or denied. | **`npu(config-ext-nacl)# permit tcp host 1.1.1.1 any`**<br>**`npu(config-ext-nacl)# deny udp host 1.1.1.1`** |
| | `<network-src-ip> <mask>` | Indicates that incoming TCP/UDP traffic is to be permitted or denied for a particular subnet. | **`npu(config-ext-nacl)# permit tcp 1.1.1.0 255.255.255.0 any`**<br>**`npu(config-ext-nacl)# deny udp 1.1.1.0 255.255.255.0`** |
| Source port | `[{gt <port-number (1-65535)>` | Indicates that incoming TCP/UDP traffic is to be permitted or denied from the source port for which the port number is greater than the value of this parameter. | **`npu(config-ext-nacl)# permit tcp 1.1.1.0 255.255.255.0 gt 1111`**<br>**`npu(config-ext-nacl)# deny udp host 1.1.1.1 gt 1010`** |
| | `[{lt <port-number (1-65535)>` | Indicates that incoming TCP/UDP traffic is to be permitted or denied from the source port for which the port number is less than the value of this parameter. | **`npu(config-ext-nacl)# permit tcp 1.1.1.0 255.255.255.0 lt 1111`**<br>**`npu(config-ext-nacl)# deny udp host 1.1.1.1 lt 1010`** |
| | `[{eq <port-number (1-65535)>` | Indicates that incoming TCP/UDP traffic is to be permitted or denied from the source port for which the port number is equal to the value of this parameter. | **`npu(config-ext-nacl)# permit tcp 1.1.1.0 255.255.255.0 eq 8080`**<br>**`npu(config-ext-nacl)# deny udp host 1.1.1.1 eq 4040`** |
| | `range <port-number (1-65535)> <port-number (1-65535)> }]` | Indicates that incoming TCP/UDP traffic is to be permitted or denied from the source port for which the port number is within the range specified by this parameter. | **`npu(config-ext-nacl)# permit tcp 1.1.1.0 255.255.255.0 range 1010 8080`**<br>**`npu(config-ext-nacl)# deny udp host 1.1.1.1 range 1010 4040`** |

**Table 3-21: Parameters for Configuring Permit/Deny Rules for TCP/UDP Traffic**

| | Parameter | Description | Example |
|---|---|---|---|
| Destination IP address | `any` | Indicates that TCP/UDP traffic to all NPU interface IP addresses is permitted or denied. | **`npu(config-ext-nacl)# permit tcp 1.1.1.1 host any`**<br>**`npu(config-ext-nacl)# deny udp any any`** |
| | `host <src-ip-address>` | Indicates that TCP/UDP traffic to a specific NPU interface IP address is permitted or denied. | **`npu(config-ext-nacl)# permit tcp any host 1.1.1.1 host host 1.1.1.1`**<br>**`npu(config-ext-nacl)# deny udp any host 1.1.1.1`** |
| | `<network-src-ip> <mask>` | Indicates that TCP/UDP traffic is to be permitted or denied for a particular NPU interface subnet. | **`npu(config-ext-nacl)# permit tcp any host 1.1.1.0 255.255.255.0`**<br>**`npu(config-ext-nacl)# deny udp any host 1.1.1.0 255.255.255.0`** |

**Table 3-21: Parameters for Configuring Permit/Deny Rules for TCP/UDP Traffic**

| | Parameter | Description | Example |
|---|---|---|---|
| Destination port | [{gt <port-number (1-65535)> | Indicates that TCP/ UDPtraffic is to be permitted or denied to the NPU interface source port for which the port number is greater than the value of this parameter. | **npu(config-ext-nacl)# permit tcp host 1.1.1.1 host any gt 8080**<br>**npu(config-ext-nacl)# deny udp any any** |
| | [{lt <port-number (1-65535)> | Indicates that TCP/ UDP traffic is to be permitted or denied to the NPU interface source port for which the port number is less than the value of this parameter. | **npu(config-ext-nacl)# permit tcp host 1.1.1.0 255.255.255.0 any lt 1111**<br>**npu(config-ext-nacl)# deny udp any host 1.1.1.1 lt 1010** |
| | [{eq <port-number (1-65535)> | Indicates that TCP/ UDP traffic is to be permitted or denied to the NPU interface source port for which the port number is equal to the value of this parameter. | **npu(config-ext-nacl)# permit tcp any 1.1.1.0 255.255.255.0 eq 8080**<br>**npu(config-ext-nacl)# deny udp any host 1.1.1.1 eq 4040** |
| | range <port-number (1-65535)> <port-number (1-65535)> }] | Indicates that TCP/ UDP traffic is to be permitted or denied the NPU interface source port for which the port number is within the range specified by this parameter. | **npu(config-ext-nacl)# permit tcp host 1.1.1.1 host 1.1.1.0 255.255.255.0 range 1010 8080**<br>**npu(config-ext-nacl)# deny udp host 1.1.1.1 any range 1010 4040** |

**Command Syntax**

**npu(config-ext-nacl)# deny tcp** {any | **host** <src-ip-address> | <src-ip-address> <src-mask> } [{gt <port-number (1-65535)> | **lt** <port-number (1-65535)> |**eq** <port-number (1-65535)> | **range** <port-number (1-65535)> <port-number (1-65535)>}] {**any** | **host** <dest-ip-address> | <dest-ip-address> <dest-mask>} {**gt** <port-number (1-65535)> | **lt** <port-number (1-65535)> | **eq** <port-number (1-65535)> | **range** <port-number (1-65535)> <port-number (1-65535)>}]

**npu(config-ext-nacl)# deny udp** {any | **host** <src-ip-address> | <src-ip-address> <src-mask> } [{gt <port-number (1-65535)> | **lt** <port-number (1-65535)> |**eq** <port-number (1-65535)> | **range** <port-number (1-65535)> <port-number (1-65535)>}] {**any** | **host** <dest-ip-address> | <dest-ip-address> <dest-mask>} {**gt** <port-number (1-65535)> | **lt** <port-number (1-65535)> | **eq** <port-number (1-65535)> | **range** <port-number (1-65535)> <port-number (1-65535)>}]

**Privilege Level** `10`

**Syntax Description**

| Parameter | Description | Presence | Default Value | Possible Values |
|---|---|---|---|---|
| `any \| host <src-ip-address> \| <src-ip-address> <src-mask>` | Indicates the source host for which incoming TCP/UDP traffic is permitted/denied. | Mandatory | N/A | For details, refer Table 3-21 |
| `[{gt <port-number (1-65535)> \| lt <port-number (1-65535)> \|eq <port-number (1-65535)> \| range <port-number (1-65535)> <port-number (1-65535)>}]` | Indicates the source port from which incoming TCP/UDP traffic is permitted/denied. | Optional | 0-65535 | For details, refer Table 3-21 |
| `any \| host <dest-ip-address> \| <dest-ip-address> <dest-mask>` | Indicates the destination IP address/subnet for which TCP/UDP traffic is permitted/denied. | Mandatory | N/A | For details, refer Table 3-21 |

| | | | | | |
|---|---|---|---|---|---|
| | {gt <port-number (1-65535)> \| lt <port-number (1-65535)> \| eq <port-number (1-65535)> \| range <port-number (1-65535)> <port-number (1-65535)>}] | Indicates the destination port to which TCP/UDP traffic is permitted/denied. | Optional | 0-65535 | For details, refer Table 3-21 |

**Command Modes** Extended ACL configuration mode

### 3.3.10.1.3.2.2Deleting a Permit/Deny Rule for TCP/UDP Traffic (Extended Mode)

Run the following commands to delete a Permit rule for TCP/UDP traffic from/to a specific IP address/port:

```
npu(config-ext-nacl)# no permit tcp {any | host <src-ip-address> |
<src-ip-address> <src-mask>} [{gt <port-number (1-65535)> | lt
<port-number (1-65535)> |eq <port-number (1-65535)> | range
<port-number (1-65535)> <port-number (1-65535)>}] {any | host
<dest-ip-address> | <dest-ip-address> <dest-mask>} {gt <port-number
(1-65535)>   | lt <port-number (1-65535)> | eq <port-number
(1-65535)> | range <port-number (1-65535)> <port-number
(1-65535)>}]
```

```
npu(config-ext-nacl)# no permit udp {any | host <src-ip-address> |
<src-ip-address> <src-mask>} [{gt <port-number (1-65535)> | lt
<port-number (1-65535)> |eq <port-number (1-65535)> | range
<port-number (1-65535)> <port-number (1-65535)>}] {any | host
<dest-ip-address> | <dest-ip-address> <dest-mask>} {gt <port-number
(1-65535)>   | lt <port-number (1-65535)> | eq <port-number
(1-65535)> | range <port-number (1-65535)> <port-number
(1-65535)>}]
```

Run the following commands to delete a Deny rule for TCP/UDP traffic from/to a specific IP address/port:

**npu(config-ext-nacl)# no deny tcp** {any | **host** <src-ip-address> | <src-ip-address> <src-mask>} [{gt <port-number (1-65535)> | **lt** <port-number (1-65535)> |**eq** <port-number (1-65535)> | **range** <port-number (1-65535)> <port-number (1-65535)>}] {**any** | **host** <dest-ip-address> | <dest-ip-address> <dest-mask>} {**gt** <port-number (1-65535)> | **lt** <port-number (1-65535)> | **eq** <port-number (1-65535)> | **range** <port-number (1-65535)> <port-number (1-65535)>}]

**npu(config-ext-nacl)# no deny udp** {any | **host** <src-ip-address> | <src-ip-address> <src-mask>} [{gt <port-number (1-65535)> | **lt** <port-number (1-65535)> |**eq** <port-number (1-65535)> | **range** <port-number (1-65535)> <port-number (1-65535)>}] {**any** | **host** <dest-ip-address> | <dest-ip-address> <dest-mask>} {**gt** <port-number (1-65535)> | **lt** <port-number (1-65535)> | **eq** <port-number (1-65535)> | **range** <port-number (1-65535)> <port-number (1-65535)>}]

**Command Syntax (for Permit Rule)**

**npu(config-ext-nacl)# no permit tcp** {any | **host** <src-ip-address> | <src-ip-address> <src-mask> } [{gt <port-number (1-65535)> | **lt** <port-number (1-65535)> |**eq** <port-number (1-65535)> | **range** <port-number (1-65535)> <port-number (1-65535)>}] {**any** | **host** <dest-ip-address> | <dest-ip-address> <dest-mask>} {**gt** <port-number (1-65535)> | **lt** <port-number (1-65535)> | **eq** <port-number (1-65535)> | **range** <port-number (1-65535)> <port-number (1-65535)>}]

**npu(config-ext-nacl)# no permit udp** {any | **host** <src-ip-address> | <src-ip-address> <src-mask> } [{gt <port-number (1-65535)> | **lt** <port-number (1-65535)> |**eq** <port-number (1-65535)> | **range** <port-number (1-65535)> <port-number (1-65535)>}] {**any** | **host** <dest-ip-address> | <dest-ip-address> <dest-mask>} {**gt** <port-number (1-65535)> | **lt** <port-number (1-65535)> | **eq** <port-number (1-65535)> | **range** <port-number (1-65535)> <port-number (1-65535)>}]

**Command Syntax (for Deny Rule)**

```
npu(config-ext-nacl)# no deny tcp {any | host <src-ip-address> |
<src-ip-address> <src-mask> } [{gt <port-number (1-65535)>  | lt
<port-number (1-65535)> |eq <port-number (1-65535)>  | range <port-number
(1-65535)> <port-number (1-65535)>}] {any | host <dest-ip-address> |
<dest-ip-address> <dest-mask>} {gt <port-number (1-65535)>   | lt
<port-number (1-65535)> | eq <port-number (1-65535)>  | range
<port-number (1-65535)> <deny-number (1-65535)>}]
```

```
npu(config-ext-nacl)# no deny udp {any | host <src-ip-address> |
<src-ip-address> <src-mask> } [{gt <port-number (1-65535)>  | lt
<port-number (1-65535)> |eq <port-number (1-65535)>  | range <port-number
(1-65535)> <port-number (1-65535)>}] {any | host <dest-ip-address> |
<dest-ip-address> <dest-mask>} {gt <port-number (1-65535)>   | lt
<port-number (1-65535)> | eq <port-number (1-65535)>  | range
<port-number (1-65535)> <port-number (1-65535)>}]
```

**Privilege Level**

**10**

**Syntax Description**

| Parameter | Description | Presence | Default Value | Possible Values |
|---|---|---|---|---|
| any \| host <src-ip-address> \| <src-ip-address> <src-mask> | Indicates the source host for which the Permit/Deny rule for incoming TCP/UDP traffic is to be deleted. | Mandatory | N/A | For details, refer Table 3-21 |
| [{gt <port-number (1-65535)> \| lt <port-number (1-65535)> \|eq <port-number (1-65535)> \| range <port-number (1-65535)> <port-number (1-65535)>}] | Indicates the source port for which the Permit/Deny rule for incoming TCP/UDP traffic is to be deleted. | Optional | 1-65535 | For details, refer Table 3-21 |

| | | | | | |
|---|---|---|---|---|---|
| | `any \| host <dest-ip-address> \| <dest-ip-address> <dest-mask>` | Indicates the NPU IP address/subnet for which the Permit/Deny rule for TCP/UDP traffic is to be deleted. | Mandatory | N/A | For details, refer Table 3-21 |
| | `[{gt <port-number (1-65535)> \| lt <port-number (1-65535)> \|eq <port-number (1-65535)> \| range <port-number (1-65535)> <port-number (1-65535)>}]` | Indicates the NPU interface port for which the Permit/Deny rule for incoming TCP/UDP traffic is to be deleted. | Optional | 1-65535 | For details, refer Table 3-21 |

**Command Modes** Extended ACL configuration mode

### 3.3.10.1.3.3 Configuring Permit/Deny Rules for ICMP Traffic

After you have created an ACL, you can configure Permit/Deny rules for ICMP traffic from/to specific a source and destination IP address/subnet.

**IMPORTANT**

You cannot configure Permit or Deny rules for an ACL that is associated with a Qos marking rule. You can either associate QoS marking rules or permit/deny rules with an ACL.

This section describes the commands to be used for:

- "Creating a Permit/Deny Rule for ICMP Traffic (Extended Mode)" on page 194
- "Deleting a Permit/Deny Rule for ICMP Traffic (Extended Mode)" on page 197

#### *3.3.10.1.3.3.1 Creating a Permit/Deny Rule for ICMP Traffic (Extended Mode)*

Run the following commands to specify the Permit/Deny rule for ICMP traffic from/to a specific source/destination IP address/subnet:

```
npu(config-ext-nacl)# permit icmp {any | host <src-ip-address> |
<src-ip-address> <mask>} {any | host <dest-ip-address> |
<dest-ip-address> <mask>}
```

```
npu(config-ext-nacl)# deny icmp {any | host <src-ip-address> |
<src-ip-address> <mask>} {any | host <dest-ip-address> |
<dest-ip-address> <mask>}
```

In the above commands, it is mandatory to specify the source IP address for which the Permit/Deny rule is to be created. If you do not specify the destination IP address/subnet mask, by default, traffic to all destination IP addresses is permitted/denied.

The following table lists the parameters and their descriptions in these commands:

**Table 3-22: Parameters for Configuring Permit/Deny Rules for ICMP Traffic**

| | Parameter | Description | Example |
|---|---|---|---|
| Source IP | any | Indicates that incoming ICMP traffic from any source IP address is permitted or denied. | **npu(config-ext-nacl)#permit icmp any**<br>**npu(config-ext-nacl)#deny icmp any** |
| | host <src-ip-address> | Indicates that incoming ICMP traffic from a specific source IP address is permitted or denied. | **npu(config-ext-nacl)#permit icmp host 1.1.1.1**<br>**npu(config-ext-nacl)#deny icmp host 1.1.1.1** |
| | <network-src-ip> <mask> | Indicates that incoming ICMP traffic is to be permitted or denied for a particular subnet. | **npu(config-ext-nacl)#permit icmp 1.1.1.0 255.255.255.0**<br>**npu(config-ext-nacl)#deny icmp host 1.1.1.0 255.255.255.0** |

**Table 3-22: Parameters for Configuring Permit/Deny Rules for ICMP Traffic**

| | Parameter | Description | Example |
|---|---|---|---|
| Destination IP address | any | Indicates that ICMP traffic destined to the NPU interface IP address is permitted or denied. | **npu(config-ext-nacl)#permit icmp host 1.1.1.1 any**<br>**npu(config-std-nacl)# deny host 1.1.1.1 host any** |
| | host <src-ip-address> | Indicates that ICMP traffic destined to the NPU interface destination IP address is permitted or denied. | **npu(config-std-nacl)# permit host any host 1.1.1.1**<br>**npu(config-ext-nacl)#deny icmp any host 1.1.1.1** |
| | <network-src-ip> <mask> | Indicates that ICMP traffic to the NPU interface subnet is to be permitted or denied. | **npu(config-ext-nacl)#permit icmp host any host 1.1.1.0 255.255.255.0**<br>**npu(config-ext-nacl)#deny icmp host any host 1.1.1.0 255.255.255.0** |

**Command Syntax**

**npu(config-ext-nacl)# permit icmp** { **any** | **host** <src-ip-address> | <src-ip-address> <mask> } { **any** | **host** <dest-ip-address> | <dest-ip-address> <mask> }

**npu(config-ext-nacl)# deny icmp** { **any** | **host** <src-ip-address> | <src-ip-address> <mask> } { **any** | **host** <dest-ip-address> | <dest-ip-address> <mask> }

**Privilege Level**

**10**

**Syntax Description**

| Parameter | Description | Presence | Default Value | Possible Values |
|---|---|---|---|---|
| { **any** \| **host** <src-ip-address> \| <src-ip-address> <mask> } | Indicates the source IP address/subnet for which incoming ICMP traffic is permitted/denied. | Mandatory | N/A | For details Table 3-22 |
| { **any** \| **host** <dest-ip-address> \| <dest-ip-address> <mask> } | Indicates the destination IP address/subnet for which ICMP traffic is permitted/denied. | Optional | any | For details Table 3-22 |

**Command Modes** Global command mode

### 3.3.10.1.3.3.2Deleting a Permit/Deny Rule for ICMP Traffic (Extended Mode)

Run the following commands to delete a Permit/Deny rule for ICMP traffic from/to a specific IP address/subnet:

```
npu(config-ext-nacl)# no permit icmp {any | host <src-ip-address> |
<src-ip-address> <mask>} {any | host <dest-ip-address> |
<dest-ip-address> <mask>}
```

```
npu(config-ext-nacl)# no deny icmp {any | host <src-ip-address> |
<src-ip-address> <mask>} {any | host <dest-ip-address> |
<dest-ip-address> <mask>}
```

**Command Syntax**

```
npu(config-ext-nacl)# no permit icmp { any | host <src-ip-address> |
<src-ip-address> <mask> }  { any | host <dest-ip-address> |
<dest-ip-address> <mask> }
```

```
npu(config-ext-nacl)# no deny icmp { any | host <src-ip-address> |
<src-ip-address> <mask> }  { any | host <dest-ip-address> |
<dest-ip-address> <mask> }
```

**Privilege Level** **10**

**Syntax Description**

| Parameter | Description | Presence | Default Value | Possible Values |
|---|---|---|---|---|
| { **any** \| **host** <src-ip-address> \| <src-ip-address> <mask> } | Indicates the source IP address/subnet for which the Permit/Deny rule for incoming ICMP traffic is to be deleted. | Mandatory | N/A | For details Table 3-22 |
| { **any** \| **host** <dest-ip-address> \| <dest-ip-address> <mask> } | Indicates the destination IP address/subnet for which the Permit/Deny rule for ICMP traffic is to be deleted. | Optional | any | For details Table 3-22 |

**Command Modes** Extended ACL configuration mode

#### 3.3.10.1.4 Terminating the ACL Configuration Mode

To terminate the standard ACL configuration mode and return to the global configuration mode, run the following command:

```
npu(config-std-nacl)# exit
```

To exit the extended ACL configuration mode and return to the global configuration mode, run the following command:

```
npu(config-ext-nacl)# exit
```

| | |
|---|---|
| **Command Syntax** | **npu(config-std-nacl)# exit**<br>**npu(config-ext-nacl) # exit** |
| **Privilege Level** | 10 |
| **Command Modes** | Standard/Extended ACL configuration mode |

### 3.3.10.2 Deleting an ACL

**To delete an ACL:**

1. Check if the ACL is attached to the interface. For more information about this command, refer Section 3.3.10.4.
2. Enable the interface configuration mode and de-attach the ACL. For details, refer Section 3.3.10.3.
3. Terminate the interface configuration mode to return to the global configuration mode (refer Section 3.3.10.3.4).
4. Run the following command to delete the ACL:

```
npu(config)# no ip access-list {standard <access-list-number
(1-99)> | extended <access-list-number (100-199)>}
```

**IMPORTANT**

An error may occur if:

- The ACL you are trying to delete is INACTIVE.
- The ACL number you have specified does not exist.

**Command Syntax**

```
npu(config)# no ip access-list {standard <access-list-number (1-99)> |
extended <access-list-number (100-199)>}
```

**Privilege Level**

**10**

**Syntax Description**

| Parameter | Description | Presence | Default Value | Possible Values |
|---|---|---|---|---|
| `{ standard <access-list-number (1-99)> \| extended <access-list-number (100-199)> }` | Indicates the ACL number of the standard or extended ACL to be deleted. | Mandatory | N/A | ■ Standard (1-99)<br>■ Extended (100-199) |

**Command Modes**

Global configuration mode

**IMPORTANT**

The default pre-configured and automatically created ACLs cannot be deleted and should not be modified.

### 3.3.10.3 Attaching/De-attaching ACLs to/from an Interface

You can attach or de-attach an ACL to/from the following virtual interfaces.

- NPU
- All the AU interfaces

When an ACL is attached to an interface, it is in the ACTIVE state; it is in the INACTIVE state when it is de-attached from an interface.

**To attach/de-attach an ACL:**

1. Enable the interface configuration mode (refer Section 3.3.10.3.1).
2. You can now execute either of the following tasks:
   - » Attach an ACL to an interface (refer Section 3.3.10.3.2).
   - » De-attach an ACL from an interface (refer Section 3.3.10.3.3).
3. Terminate the interface configuration mode (refer Section 3.3.10.3.4).

### 3.3.10.3.1 Enabling the Interface Configuration Mode

ACLs are applied on traffic received from the DATA, MGMT or CSCD ports, and destined towards the following virtual interfaces:

- AUs
- NPU

Run the following command to enable the interface configuration mode for the NPU:

```
npu(config)# interface npu-host
```

Run the following command to enable the interface configuration mode for all AUs:

```
npu(config)# interface all-au
```

After you have enabled the interface configuration mode, you can:

- Attach an ACL to an interface (Section 3.3.10.3.2)
- De-attach an ACL from an interface (Section 3.3.10.3.3)

### 3.3.10.3.2 Attaching an ACL to an interface

After you have enabled the interface configuration mode, run the following command to attach an ACL with an interface:

```
npu(config-if)# ip access-group {<access-list-number (1-199)> |
<access-list-name>}
```

**IMPORTANT**

An error may occur if the ACL number/name that you have specified does not exist or is already attached to this interface.

**Command Syntax**

```
npu(config-if)# ip access-group {<access-list-number (1-199)> |
<access-list-name>}
```

**Privilege Level**

**10**

**Syntax Description**

| Parameter | Description | Presence | Default Value | Possible Values |
|---|---|---|---|---|
| {<access-list-number (1-199)> \| <access-list-name>} | Indicates the number or name of the ACL to be attached to this interface. | Mandatory | N/A | ■ 1-[a]99<br>■ String |

**Command Modes**

Interface configuration mode

### 3.3.10.3.3 Deattaching an ACL from an Interface

Run the following command to de-attach an ACL from an interface:

```
npu(config-if)# no ip access-group {<access-list-number (1-199)> |
<access-list-name>}
```

**IMPORTANT**

An error may occur if the ACL number/name that you have specified does not exist or is already attached to this interface.

**Command Syntax**

```
npu(config-if)# no ip access-group {<access-list-number (1-199)> |
<access-list-name>}
```

**Privilege Level**

**10**

**Syntax Description**

| Parameter | Description | Presence | Default Value | Possible Values |
|---|---|---|---|---|
| `{<access-list-number (1-199)> \| <access-list-name>}` | Indicates the number/name of the ACL to be deattached from this interface. | Mandatory | N/A | ■ 1-199<br>■ String |

**Command Modes** Interface configuration mode

### 3.3.10.3.4 Terminating the Interface Configuration Mode

To exit the interface configuration mode and return to the global configuration mode, run the following command:

```
npu(config-if)# exit
```

**Command Syntax**

```
npu(config-if)# exit
```

**Privilege Level** 10

**Command Modes** Interface configuration mode

## 3.3.10.4 Displaying ACL Configuration Information

Run the following command to display the configuration information for a specific ACL:

```
npu# show access-lists [{<access-list-number (1-199)> |
<access-list-name}]
```

**IMPORTANT**

An error may occur if the ACL number/name you have specified does not exist.

**Command Syntax**

```
npu# show access-lists [{<access-list-number (1-199)> |
<access-list-name}]
```

**Privilege Level**

**1**

**Syntax Description**

| Parameter | Description | Presence | Default Value | Possible Values |
|---|---|---|---|---|
| [{<access-list-number (1-199)> \| <access-list-name}] | Indicates the number or name of the ACL for which configuration information is to be displayed. If you do not provide the ACL number or name, configuration information is displayed for all ACLs. | Optional | N/A | ■ 1-199<br>■ String |

**Display Format (Standard)**

```
Standard IP Access List                 <ACL number>
------------------------------------------------------------------------
Access List Name(Alias)              :<ACL Name>
Interface List                       : <Interface Name>, <Interface Name>
Status                               : <value>
Source IP address                    : <value>
Source IP address mask               : <value>
Destination IP address               : <value>
Destination IP address mask          : <value>
Rule Action                          : <value>
Packet Match Count                   : <value>
Rule Row Status                      : <value>
```

**Display Format (Extended)**

```
Extended IP Access List          <ACL Number>
----------------------------
Access List Name(Alias)          : <ACL Name>
Interface List                   : <Interface>, <Interface>
Status                           : <value>
Filter Protocol Type             : <value>
Source IP address                : <value>
Filter Source Port               : <value>
Rule Action                      : <value>
QoS Classifier ID                : <value>
Marking rule status              : <value>
```

**Command Modes**

Global command mode

## 3.3.11 Configuring the ASN-GW Functionality

**IMPORTANT**

Execute the procedures described in this section only if you are operating the NPU in the ASN-GW mode. Skip this section if you are operating the NPU in the Transparent mode.

The ASN-GW functionality indicates that the NPU executes the following functions:

- Network Decision Point (NWDP): Includes the following non-bearer plane functions:
  - » Implementation of EAP Authenticator and AAA client
  - » Termination of RADIUS protocol against the selected CSN AAA server (home or visited AAA server) for MS authentication and per-MS policy profile retrieval
  - » Storage of the MS policy profile for as long as the MS is authenticated/authorized and remains in the ASN controlled by the specific ASN-GW
  - » Generation of authentication key material
  - » QoS service flow authorization entity
  - » AAA accounting client
- Network Enforcement Point (NWEP) functions: Includes the following bearer plane functions:
  - » Classification of downlink data into generic routing encapsulation (GRE) tunnels
  - » Packet header suppression functionality
  - » DHCP functionality
  - » Handover functionality

The ASN-GW functionality is disabled if you are operating the NPU in the Transparent mode. If you are operating the NPU in the ASN-GW mode, you can choose to operate the NPU in either of the following modes:

- With HA support, that is, MIP services are implemented (not supported in the current release)
- Without HA support, that is, MIP services are not implemented.

**IMPORTANT**

The ASN-GW mode with HA support is not implemented because MIP services are not supported in the current release.

The following table lists the tasks for configuring the ASN-GW functionality.

**Table 3-23: Tasks to be Executed for Configuring the ASN-GW Functionality**

| Task | Required for Operating the NPU with HA Support | Required for Operating the NPU without HA Support |
|---|---|---|
| "Configuring the Next-hop IP Address-Network ID Mapping" on page 207 | Yes | Yes |
| "Managing the IGMP Functionality" on page 210<br>**Note**: This feature is not supported in the current release. | Yes | Yes |
| "Managing the MIP-Foreign Agent Functionality" on page 211<br>**Note**: This feature is not supported in the current release. | Yes | No |
| "Managing the Proxy-MIP Client Functionality" on page 211<br>**Note**: This feature is not supported in the current release. | Yes | No |
| "Managing the ASN Interface" on page 211 | Yes | Yes |
| "Managing the Authenticator Function" on page 212 | Yes | Yes |
| "Managing the Data Path Function" on page 214 | Yes | Yes |
| "Managing the Context Function" on page 216 | Yes | Yes |
| "Managing the MS State Change Functionality" on page 217 | Yes | Yes |

**Table 3-23: Tasks to be Executed for Configuring the ASN-GW Functionality**

| Task | Required for Operating the NPU with HA Support | Required for Operating the NPU without HA Support |
|---|---|---|
| "Managing the Connectivity Service Network Interface" on page 218 | Yes | Yes |
| "Configuring Bearer Plane QoS Marking Rules" on page 219 | Yes | Yes |
| "Managing Service Interfaces" on page 228 | Yes | Yes |
| "Configuring the AAA Client Functionality" on page 239 | Yes | Yes |
| "Managing Service Groups" on page 246 | Yes | Yes |
| "Configuring the Service Flow Authorization Functionality" on page 281 | Yes<br>(Configure only DHCP Proxy for a service group) | Yes<br>(Configure DHCP server, proxy or relay for a service group) |
| "Configuring PHS Rules" on page 333 | Yes | Yes |
| "Managing the ASN-GW Keep-Alive Functionality" on page 339 | Yes | Yes |

### 3.3.11.1 Configuring the Next-hop IP Address-Network ID Mapping

The NPU maintains the mapping of the BS network ID to the next-hop IP address. The next-hop IP address can be the IP address of an intermediate ASN-GW or the destination BS. Using this mapping, the NPU resolves the BS-ID to IP address.

This section describes the commands to be used for:

- "Configuring the Next-hop IP Address" on page 208
- "Displaying the Next-hop IP Address-Network ID Mapping" on page 209
- "Displaying the Next-hop IP Address-Network ID Mapping" on page 209

#### 3.3.11.1.1 Configuring the Next-hop IP Address

To map the next-hop IP address for a specific network ID, run the following command:

```
npu(config)# idip <nw-id> <next-hop-ipaddr>
```

For example, run the following command to map the MAC address of the BS with the next-hop IP address:

```
npu(config)# idip 112233445566 10.0.0.1
```

**NOTE**

Refer to Section 3.3.11.2 for a list of existing next-hop IP address-network ID mappings.

**Command Syntax**

```
npu(config)# idip <nw-id> <next-hop-ipaddr>
```

**Privilege Level**

10

**Syntax Description**

| Parameter | Description | Presence | Default Value | Possible Values |
|---|---|---|---|---|
| <nw-id> | Denotes the BS ID. This parameter is a MAC address, and should be specified without colons. | Mandatory | N/A | 6-byte ID |
| <next-hop-ipaddr> | Denotes the next hop IP address for a particular BS. | Mandatory | N/A | Valid IP Address |

**Command Modes**

Global configuration mode

#### 3.3.11.1.2 Deleting Next-hop IP Address-Network ID Mappings

To delete a specific or all next-hop IP address-network ID mappings, run the following command:

```
npu(config)# no idip [<nw-id>]
```

**CAUTION**

Specify the network ID if you want to delete a specific next-hop IP address-network ID mapping. Otherwise all the configured mappings are deleted.

**Command Syntax**

```
npu(config)# no idip [<nw-id>]
```

**Privilege Level**

10

**Syntax Description**

| Parameter | Description | Presence | Default Value | Possible Values |
|---|---|---|---|---|
| <nw-id> | Denotes the network ID(s) for which an IDIP context is to be removed.<br>Specify this parameter only if you want to delete a specific network ID.<br>If you do not specify a value for this parameter, all configured network IDs are deleted. | Optional | null | 6-byte ID or null |

**Command Modes**

Global configuration mode

### 3.3.11.1.3 Displaying the Next-hop IP Address-Network ID Mapping

To display the next-hop-IP address mapped to a network ID or all network IDs, run the following command:

```
npu# show idip [<nw-id>]
```

Specify the network ID if you want to display a particular the next-hop-IP address-network ID mapping. Do not specify a value for this parameter if you want to view all the next-hop-IP address-network ID mappings.

**Command Syntax**

```
npu# show idip [<nw-id>]
```

**Privilege Level**

1

**Syntax Description**

| Parameter | Description | Presence | Default Value | Possible Values |
|---|---|---|---|---|
| [<nw-id>] | Denotes the network ID (s) for which you want to view the next-hop IP addresses already mapped to it.<br>Specify a value for this parameter if you want to view the next-hop IP address(es) defined for a specific network ID. If you do not specify any value for this parameter, all the existing entries for mappings of network IDs-next-hop IP addresses are displayed. | Optional | N/A | 6-byte ID |

**Display Format**

```
nw-id        next-hop-ip address
<Network ID 1>    <Ip Address>
<Network ID 2>    <Ip Address>
```

**Command Modes**

Global command mode

## 3.3.11.2 Managing the IGMP Functionality

**IMPORTANT**

The IGMP functionality is not supported in the current release.
The following commands are not applicable:
npu# show igmp
npu# show igmp-membership

### 3.3.11.3 Managing the MIP-Foreign Agent Functionality

**IMPORTANT**

The MIP-Foreign Agent functionality is not supported in the current release.
The command npu# show mip-fa is not applicable.

### 3.3.11.4 Managing the Proxy-MIP Client Functionality

**IMPORTANT**

The Proxy-MIP client functionality is not supported in the current release.
The command npu# show mip-client is not applicable.

### 3.3.11.5 Managing the ASN Interface

The ASN interface is the NPU interface that is exposed towards the BS or another ASN gateway.

For the current release, the `bearer` interface IP address is used as the value of the `ip-intf` parameter.

ASN Interface parameters can be configured only by the vendor.

To display the parameters of the IP interface (R4/R6) of the ASN interface, run the following command:

**`npu# show asnif`**

| | |
|---|---|
| **Command Syntax** | **`npu# show asnif`** |
| **Privilege Level** | 1 |
| **Display Format** | `% Asn-gateway ASNIF config`<br>`Alias bearer`<br>`ASNIF IPAddr <value>`<br>`ASNIF Mtu <value>` |

| | |
|---|---|
| **Command Modes** | Global command mode |

### 3.3.11.6 Managing the Authenticator Function

The Authenticator function of the NPU manages MS authentication for accessing WiMAX network resources. It also maintains context information for each MS that has accessed or is trying to access the network. For this, it handles all key derivations and distribution. In addition, it uses AAA client functions to send RADIUS messages on the R3 interface.

Authenticator function parameters can be configured only by the vendor.

To display configuration information for the Authenticator function, run the following command:

```
npu# show authenticator
```

| | |
|---|---|
| **Command Syntax** | `npu# show authenticator` |
| **Privilege Level** | 1 |

**Display Format**

```
Authenticator Function Configuration :
e
eapTimerIdReq <value>
eapCounterIdReqMax <value>
authTimerNtwEntryHold <value>
eapTimerTransfer <value>
eapCounterTransferMax <value>
eapCounterReAuthAttemptMax <value>
authTimerReauthCmpltHold <value>
eapCounterRndTripsMax <value>
authTimerPmkLifetime <value>
authTimerPmkGaurd <value>
authCounterNtwEntryMax <value>
authTimerAuthFailureHold <value>
```

**Command Modes**

Global command mode

The following table provides some details on these parameters:

| Parameter | Description |
|---|---|
| `eapTimerIdReq` | The period, in milliseconds, the NPU waits for the EAP Transfer response. |
| `eapCounterIdReqMax` | The period, in milliseconds, for which the NPU should wait for the response to the request for the EAP ID. |
| `authTimerNtwEntryHold` | The period, in seconds, within which the MS should be authenticated for initial entry into the network. If the MS is not authenticated within this period, the NPU terminates the request for network entry. |
| `eapTimerTransfer` | The maximum number of times the MS can attempt for initial entry to the network. If the number of EAP transfers exceeds the value of this parameter, the NPU de-registers the MS. |
| `eapCounterTransferMax` | The number of times the NPU can retransmit the EAP ID request until it receives a EAP ID response. |

| | |
|---|---|
| `eapCounterReAuthAttemptMax` | The maximum number of times the NPU may handle a an MS/network-initiated re-authentication request. When the number of re-authentication attempts exceeds the value of this parameter, the MS is de-registered. |
| `authTimerReauthCmpltHold` | The period, in milliseconds, within which, re-authentication of the MS should be complete. If the MS is not authenticated within this period, the NPU reinitiates MS authentication. |
| `eapCounterRndTripsMax` | The number EAP roundtrips in one authentication/re-authentication process. |
| `authTimerPmkLifetime` | The period, in seconds, for which the MS authentication key is valid. At the end of this period, the NPU de-registers the MS. |
| `authTimerPmkGaurd` | The duration of the guard timer for the MS authentication keys. the NPU initiates re-authentication for the MS after the pmk guard timer has expired. (The value of this timer is `pmk-lifetime` - `pmk-guardtime`.)<br>If the value of this parameter is 0, the guard timer is not started. |
| `authTimerAuthFailureHold` | The period, in seconds, for which the MS context is retained after authentication failure. |
| `authCounterNtwEntryMax` | The maximum number of times that the NPU may handle a network entry request from an MS, after prior attempts for that MS has already failed. After the NPU has handled `max-ntwentry` number of attempts and its value is 0, the MS is assigned the unauthenticated mode. |

### 3.3.11.7 Managing the Data Path Function

The Data Path function controls the creation, maintenance, and deletion of data paths within the NPU. Data Path function parameters can be configured only by the vendor.

To display configuration information for the Data Path function, run the following command:

**`npu# show datapath`**

| | |
|---|---|
| **Command Syntax** | **`npu# show datapath`** |
| **Privilege Level** | 1 |

**Display Format**

```
Data Path Function Configuration :
dpTimerInitPathRegReq <value>
dpCounterInitPathRegReqMax <value>
dpTimerMsDeregReq <value>
dpCounterMsDeregReqMax <value>
dpTimerPathRegReq <value>
dpCounterPathRegReqMax <value>
dpTimerPathRegRsp <value>
 dpCounterPathRegRspMax <value>
dpTimerPathRegStart <value>
dpTimerMipWaitDhcp <value>
```

**Command Modes**

Global command mode

The following table provides some details on these parameters:

| Parameter | Description |
|---|---|
| dpTimerInitPathRegReq | The interval, in milliseconds, after which the request for initial path registration should be complete. If the initial path registration request is not completed within this period, the NPU may retransmit the initial path registration request. |
| dpCounterInitPathRegReqMax | The maximum number of initial path registration request retransmissions that may be sent by the NPU. After the number of retransmissions has exceeded the value of this parameter, the MS de-registration procedure is initiated. |
| dpTimerMsDeregReq | The MS deregistration response timeout, in milliseconds. |
| dpCounterMsDeregReqMax | The maximum number of MS deregistration request retransmissions, after which the MS is de-registered. |
| dpTimerPathRegReq | The period, in milliseconds, with which the NPU should wait for the path registration response. If a response is not received within this period, the NPU retransmits the request. |
| dpCounterPathRegReqMax | The maximum number of times the NPU may retransmit the path registration request. |

| | |
|---|---|
| dpTimerPathRegRsp | The period, in milliseconds, within which the NPU should wait for an acknowledgement for the registration response. If a response is not received within this period, the NPU retransmits the response. |
| dpCounterPathRegRspMax | The maximum number of times the NPU may retransmit the path response. |
| pdpTimerPathRegStart | Indicates the period, in milliseconds, within which the path registration procedure is initiated, after the path pre-registration procedure is complete. If the path registration procedure is not completed within the period specified by this parameter, the MS is de-registered. |
| dpTimerMipWaitDhcp | The period, in seconds, for allocating the IP address, after the path registration procedure is complete. |

### 3.3.11.8 Managing the Context Function

The context function manages the contexts of various authenticated MSs. You can specify parameters pertaining to context creation and reports.

Context function parameters can be configured only by the vendor.

To display configuration information for the context function, run the following command:

```
npu# show contextfn
```

**Command Syntax**

```
npu# show contextfn
```

**Privilege Level**

1

**Display Format**

```
Context Function Configuration :
ctxtfnTimerContextReq <value>
ctxtfnCounterContextReqMax <value>
ctxtfnTimerContextRprt <value>
ctxtfnCOUNTerContextRprtMax <value>
```

**Command Modes**

Global command mode

The following table provides some details on these parameters:

| Parameter | Description |
|---|---|
| ctxtfnTimerContextReq | The period, in milliseconds, for which the NPU waits for a response to the context request. If the NPU does not receive a response to this request within the period specified by this timer, the NPU retransmits this request. |
| ctxtfnCounterContextReqMax | The maximum number of times the NPU will retransmit a context request. |
| ctxtfnTimerContextRprt | The period, in milliseconds, for which the NPU waits for the context report acknowledgement. At the end of this period, the NPU retransmits the context report. |
| ctxtfnCOUNTerContextRprtMax | The maximum number of times, the NPU retransmits the context report. |

### 3.3.11.9 Managing the MS State Change Functionality

The MS state change functionality manages MS states within an MS context.

MS State Change parameters can be configured only by the vendor.

To display configuration information for the MS state change functionality, run the following command:

**npu# show msscfn**

**Command Syntax**

**npu# show msscfn**

**Privilege Level**

1

**Display Format**

```
MS State Change Function Configuration :
msscfnTimerMsscRsp <value>
msscfnCounterMsscRspMax <value>
msscfnTimerSbcHold <value>
msscfnTimerRegHold <value>
msscfnTimerMsscDrctvReq <value>
msscfnCounterMsscDrctvReqMax <value>
```

**Command Modes**

Global command mode

The following table provides some details on these parameters:

| Parameter | Description |
|---|---|
| msscfnTimerMsscRsp | The period, in milliseconds for which the NPU waits for an acknowledgement for the MS state change response. If the NPU does not receive an acknowledgement within this period, it retransmits the MS state change response. |
| msscfnCounterMsscRspMax | The maximum number of times, the NPU retransmits the MS state change response. |
| msscfnTimerSbcHold | The period, in milliseconds, within which the basic capabilities negotiation procedure should be completed. At the end of this period, the NPU starts the authentication/ registration procedure for the MS, depending on accepted authentication policy. |
| msscfnTimerRegHold | The interval, in seconds, for the MS registration procedure timeout. After this interval, the NPU changes the MS state to the registered state, and initiates the data path creation procedure (for authenticated MSs). |
| msscfnTimerMsscDrctvReq | The period, in milliseconds, for which the NPU waits for an acknowledgement for the MS state change directive. If the NPU does not receive an acknowledegment within this period, it retransmits the state change directive. |
| msscfnCounterMsscDrctvReqMax | The maximum number of times, the NPU may retransmit the MS state change directive. |

### 3.3.11.10 Managing the Connectivity Service Network Interface

The Connectivity Service Network (CSN) interface provides IP connectivity services for a set of subscribers. The gateway uses the CSN interface for R3 control traffic and R3 data traffic towards the core network. You can configure the parameters for the IP interface to be used as the network interface for R3 control traffic.

CSN parameters can be configured only by the vendor.

To display configuration information for the CSN interface, run the following command:

```
npu# show csnif
```

| | |
|---|---|
| **Command Syntax** | `npu# show csnif` |
| **Privilege Level** | 1 |

**Display Format**

```
CSN Interface Configuration :
i
Alias bearer
CSNIF IPAddr <value>
CSNIF Mtu <value>
TUNNEL CheckSum <Enabled/Disabled>
TunIpipMtu  <value>
```

**Command Modes**

Global command mode

The following table provides some details on these parameters:

| Parameter | Description |
|---|---|
| `Alias` | A pre-defined IP interface to be used as a network interface for R3 control traffic and R3 data traffic. Must be the Bearer. |
| `CSNIF IPAddr` | The IP address of the Alias interface (Bearer) |
| `CSNIF Mtu` | The MTU of the Alias interface (Bearer) |
| `TUNNEL CheckSum` | Indicates if the tunnel checksum feature is enabled. or disabled. If this feature is enabled, the checksum of the inner header is to be verified. |
| `TunIpipMtu` | The MTU for the IP-in-IP tunnel (used for R3 data traffic) on this interface. |

## 3.3.11.11 Configuring Bearer Plane QoS Marking Rules

The Bearer Plane QoS Marking Rules enables defining QoS marking rules for the bearer plane' traffic, based on parameters such as traffic priority, the type of service, media, and interface (R3 or R6). For each marking rule, you can define the output parameters (outer-DSCP and VLAN-priority values) to be applied on service flows using best-match logic. For example, if we have the following two marking rules for BE traffic (Traffic Type set to BE):

A. Interface Type set to Internal (R6) interface, All other parameters set to ANY.

B. All other parameters (including interface type) are set to ANY.

Than Rule A will apply to all BE traffic transmitted on the internal (R6) interface. Rule B will apply to all other BE traffic, meaning traffic transmitted on the external (R3) interface.

Up to a maximum of 20 Bearer Plane QoS Marking Rules can be defined.

**To configure one or more QoS bearer plane marking rules:**

1. Enable the bearer plane QoS marking rules configuration mode (refer to Section 3.3.11.11.1)
2. You can now execute any of the following tasks:
   - » Configure the output parameters for bearer plane QoS marking rules (refer to Section 3.3.11.11.2)
   - » Restore the default parameters for bearer plane QoS marking rules (refer to Section 3.3.11.11.3)
3. Terminate the bearer plane QoS marking rules configuration mode (refer to Section 3.3.11.11.4)

In addition, you can, at any time, display configuration information (refer to Section 3.3.11.11.6) or delete an existing bearer plane QoS marking rule (refer to Section 3.3.11.11.5).

### 3.3.11.11.1 Enabling the Bearer Plane QoS Marking Rule Configuration Mode\Creating a Bearer Plane QoS Marking Rule

To configure the parameters for the bearer plane QoS marking rules, first enable the bearer plane QoS marking rule configuration mode. Run the following command to enable the bearer plane QoS marking rules configuration mode. You can also use this command to create and enable the configuration mode for a new bearer plane QoS marking rule.

```
npu(config)# bearerqos <qos-alias> [<intf-type((1<R3> - 0<R6>)|
255<ANY>)> <srvc-type(0<UGS> | 1<RTVR> | 2<NRTVR> | 3<BE> |
4<ERTVR> | 255<ANY>)> <trfc-priority((0-7)|255)> <media-type> ]
```

**NOTE**

You can display configuration information for the bearer plane QoS marking rules. For details, refer to Section 3.3.11.11.6.

**IMPORTANT**

An error may occur if you provide an invalid value for any of these parameters. Refer the syntax description for more information about the appropriate values and format for configuring these parameters.

If you use this command to create a new QoS marking rule, the configuration mode for this rule is automatically enabled, after which you can execute any of the following tasks:

- Configure the output parameters for bearer plane QoS marking rules (refer to Section 3.3.11.11.2)
- Restore the default parameters for bearer plane QoS marking rules (refer to Section 3.3.11.11.3)

After executing the above tasks, you can terminate the bearer plane QoS marking rules configuration mode (refer to Section 3.3.11.11.4) and return to the global configuration mode.

**NOTE**

The granularity of the QoS definition to be applied to packets transmitted on the bearer plane depends upon the number of parameters that you specify. If any parameter is to be excluded from the definition, specify the value 255 for that parameter.

**Command Syntax**

```
npu(config)# bearerqos <qos-alias> [<intf-type((1<R3> - 0<R6>)| 255<ANY>)>
<srvc-type(0<UGS> | 1<RTVR> | 2<NRTVR> | 3<BE> | 4<ERTVR> | 255<ANY>)>
<trfc-priority((0-7)|255)> <media-type>]
```

**Privilege Level**

10

**Syntax Description**

| Parameter | Description | Presence | Default Value | Possible Values |
|---|---|---|---|---|
| <qos-alias> | Denotes the QoS alias of the QoS marking rule for which you want to enable the bearer plane QoS marking rules configuration mode. If you want to create a new QoS marking rule, specify a new alias and define the type of interface, service, and traffic priority that is applicable for that rule. | Mandatory | N/A | String (1 to 30 characters) |

| | | | | |
|---|---|---|---|---|
| <intf-type((1<R3> - 0<R6>)\|255<ANY>)> | Denotes the type of interface for which you are defining the bearer plane QoS rule. | Mandatory when creating a new Bearer Plane QoS Rule. | N/A | ■ 0: Indicates the R6 (internal) interface<br>■ 1: Indicates the R3 (external interface))<br>■ 255: Indicates that the parameter should be ignored for packets transmitted on both internal and external interfaces. |
| <srvc-type(0<UGS> \| 1<RTVR> \| 2<NRTVR> \| 3<BE> \| 4<ERTVR> \| 255<ANY>)> | Denotes the service type of the service flow (see “Specifying Service Flow Configuration Parameters” on page 288) provided as an input classification parameter for the bearer plane QoS rule. This parameter is used to match the outer-DSCP and VLAN-priority values for a service flow | Mandatory when creating a new Bearer Plane QoS Rule | N/A | ■ 0 (UGS)<br>■ 1 (RTVR)<br>■ 2 (NRTVR)<br>■ 3 (BE)<br>■ 4 ERTVR<br>■ 255 (ANY): Indicates that the parameter should be ignored for packets transmitted on both internal and external interfaces. |

| | | | | | |
|---|---|---|---|---|---|
| | <trfc-priority ((0-7)\|255)> | Denotes the traffic priority of the service flow (see "Specifying Service Flow Configuration Parameters" on page 288) provided as an input classification parameter for the bearer plane QoS rule. This parameter is used to match the outer-DSCP and VLAN-priority values for a service flow. | Mandatory when creating a new Bearer Plane QoS Rule | N/A | ■ 0-7, where 7 is highest<br>■ 255 (ANY): Indicates that the parameter should be ignored for packets transmitted on both internal and external interfaces. |
| | <media-type> | Denotes the media type of the service flow (see "Specifying Service Flow Configuration Parameters" on page 288) provided as an input classification parameter for the bearer plane QoS rule. This parameter is used to match the outer-DSCP and VLAN-priority values for a service flow. | Mandatory when creating a new Bearer Plane QoS Rule | N/A | ■ String (1 to 30 characters)<br>■ ANY: Indicates that the parameter should be ignored for packets transmitted on both internal and external interfaces. |

**Command Modes** Global configuration mode

### 3.3.11.11.2 Configuring the Output Parameters for Bearer Plane QoS Marking Rules

After enabling the bearer plane QoS marking rules configuration mode you can configure the output parameters that should be applied on packets (that are created using the parameters specified in Section 3.3.11.11.1). Output parameters are a combination of the Outer-DSCP and VLAN priority values. These are populated in the outer DSCP and VLAN priority fields in the IP and Ethernet headers of these packets.

**NOTE**

Note that for traffic associated with a VLAN Service Interface only the VLAN Priority marking is applicable.

**IMPORTANT**

Enable the bearer plane QoS marking rule that you are configuring. By default, all bearer plane QoS marking rules are disabled.

Run the following command to configure the output parameters for this bearer plane QoS marking rule:

**npu(config-bqos)# config** [**outer-dscp** <integer(0-63>] [**vlan-priority** <integer(0-7>] [**qos enable**]

**NOTE**

You can display configuration information for the bearer plane QoS marking rules. For details, refer to Section 3.3.11.11.6.

**IMPORTANT**

An error may occur if you provide an invalid value for any of these parameters. Refer the syntax description for more information about the appropriate values and format for configuring these parameters.

**Command Syntax**

**npu(config-bqos)# config** [**outer-dscp** <integer(0-63>] [**vlan-priority** <integer(0-7>] [**qos enable**]

**Privilege Level**

10

**Syntax Description**

| Parameter | Description | Presence | Default Value | Possible Values |
|---|---|---|---|---|
| [outer-dscp <integer(0-63> ] | Denotes the Differentiated Service Code Point (DSCP) value to be used for marking the packets, if the packet complies with the marking rules specified in Section 3.3.11.11.1. | Optional | 0 | ■ 0-63<br>■ |
| [vlan-priority <integer(0-7>] | Denotes the VLAN priority to be assigned to the packets if the packet meets the requirements of the marking rules specified in Section 3.3.11.11.1. | Optional | 0 | ■ 0-7, where 7 is the highest<br>■ |

| | | | | | |
|---|---|---|---|---|---|
| | `[qos enable]` | Indicates whether this QoS marking rule should be enabled. The absence of this flag indicates that this QoS flag is disabled. By default, a bearer plane QoS marking rule is disabled.<br><br>If you enable this QoS marking rule, packets on bearer plane that were created using the parameters in Section 3.3.11.11.1, the Outer DSCP and VLAN Priority fields in the IP header and Ethernet header, respectively are populated with the values you specify for the `outer-dscp` and `vlan-priority` parameters. | Optional | By default, the QoS marking rule is disabled. | The presence/absence of this flag indicates that this QoS flag is enabled/disabled. |

**Command Modes** Bearer plane QoS marking rules configuration mode

### 3.3.11.11.3 Restoring the Default Configuration Parameters for the Bearer Plane QoS Output Marking Rules

Run the following command to restore the default configuration for this bearer plane QoS marking rule:

```
npu(config-bqos)# no {outer-dscp | vlan-priority | qos enable}
```

When you execute this command, it automatically disables this QoS marking rule.

**NOTE**

Refer to Section 3.3.11.11.2 for a description and default values of these parameters.

**Command Syntax** `npu(config-bqos)# no {outer-dscp | vlan-priority | qos enable}`

**Privilege Level** 10

| | |
|---|---|
| **Command Modes** | Bearer plane QoS marking rules configuration mode |

### 3.3.11.11.4 Terminating the QoS Marking Rules Configuration Mode

Run the following command to terminate the marking rules configuration mode:

```
npu(config-bqos)# exit
```

| | |
|---|---|
| **Command Syntax** | `npu(config-bqos)# exit` |
| **Privilege Level** | 10 |
| **Command Modes** | Bearer plane QoS marking rules configuration mode |

### 3.3.11.11.5 Deleting Bearer Plane QoS Marking Rules

Run the following command to delete the a QoS marking rule:

```
npu(config)# no bearerqos [<qos-alias>]
```

**CAUTION**

Specify the QoS alias if you want to delete a specific bearer plane qoS marking rule. Otherwise all the configured bearer plane QoS marking rules are deleted except "int_default" and "ext_default" ..

| | |
|---|---|
| **Command Syntax** | `npu(config)# no bearerqos [<qos-alias>]` |
| **Privilege Level** | 10 |

**Syntax Description**

| Parameter | Description | Presence | Default Value | Possible Values |
|---|---|---|---|---|
| `[<qos-alias>]` | Denotes the QoS alias of the bearer QoS marking rule that you want to delete. Specify a value for this parameter if you want to delete a specific bearer QoS marking rule.<br><br>Do not specify a value for this parameter if you want to delete all bearer QoS marking rules except "int_default" and "ext_default".. | Optional | N/A | String |

**Command Modes**

Global configuration mode

### 3.3.11.11.6 Displaying Configuration Information for the Bearer Plane QoS Marking Rules

To display configuration information for specific or all bearer plane QoS marking rules, run the following command:

**`npu# show bearerqos`** `[<qos-alias>]`

Specify the QoS alias if you want to display configuration information for a particular bearer plane QoS marking rule. Do not specify a value for this parameter if you want to view configuration information for all bearer plane QoS marking rules.

**Command Syntax**

**`npu# show bearerqos`** `[<qos-alias>]`

**Privilege Level**

1

**Syntax Description**

| Parameter | Description | Presence | Default Value | Possible Values |
|---|---|---|---|---|
| `[<qos-alias>]` | Denotes the QoS alias of the bearer QoS marking rule that you want to display.<br>Specify a value for this parameter if you want to display a specific bearer QoS marking rule. Do not specify a value for this parameter if you want to display all bearer QoS marking rules. | Optional | N/A | String |

**Display Format**

```
Bearer QoS Configuration :

qos-alias  intf-type srvc-type trfc-priority media-type inner-dscp
outer-dscp vlan-priority status

voip     <value>  <value>  <value>   <value>   <value>   <value>   enabled
```

**Command Modes**

Global command mode

### 3.3.11.12 Managing Service Interfaces

A Service Interface defines the parameters of the interface used by the ASN-GW on the network side for services specified in the applicable Service Group.

The following types of Service Interface are available:

- IP-IP: The Service Interface defines the parameters on the ASN-GW side of a point-to-point tunnel to be used for the applicable traffic.
- VLAN: The Service Interface defines the VLAN ID to be added/removed by the ASN-GW to/from the applicable traffic.
- QinQ: Applicable only for special applications requiring local support of unauthenticated mode. The QinQ Service Interface is applicable only for supporting VLAN CS Service Flows associated with a QinQ Service Group.

Up to 10 Service Interfaces may be defined.

**To configure a Service Interface:**

1. Enable the Service Interface configuration mode for the selected Service Interface (refer to Section 3.3.11.12.1)
2. You can now execute any of the following tasks:
   - Configure one or more of the parameters of the Service Interface (refer to Section 3.3.11.12.2)
   - Restore the default values of the Service Interface parameters (refer to Section 3.3.11.12.3)
   - Terminate the Service Interface configuration mode (refer to Section 3.3.11.12.4)

In addition, you can, at any time, display configuration information for one or all existing Service Interfaces (refer to Section 3.3.11.12.6) or delete an existing Service Interface (refer to Section 3.3.11.12.5).

### 3.3.11.12.1 Enabling the Service Interface Configuration Mode\Creating a Service Interface

To configure the parameters of a Service Interface, first enable the Service Interface configuration mode for the specific Service Interface. Run the following command to enable the Service Interface configuration mode. You can also use this command to create a new Service Interface.

```
npu(config)# srvc-intf [<string>] [{IP-IP|VLAN|QinQ}]
```

For example, to define a new IP-IP Service Interface named SI1, run the following command:

```
npu(config)# srvc-intf SI1 IP-IP
```

To enable the configuration mode for an existing Service Interface named SI1, run the following command:

```
npu(config)# srvc-intf SI1
```

If you use this command to create a new Service Interface, the configuration mode for this Service Interface is automatically enabled.

**NOTE**

The Bearer IP Interface (refer to "Configuring IP interfaces" on page 118) must be configured prior to creating IP-IP or VLAN service interfaces.

After enabling the configuration mode for a Service Interface you can execute any of the following tasks:

- Configure one or more of the Service Interface parameters (refer to Section 3.3.11.12.2)
- Restore the default values of non-mandatory parameters of the Service Interface (refer to Section 3.3.11.12.3)

After executing the above tasks, you can terminate the Service Interface configuration mode (refer to Section 3.3.11.12.4) and return to the global configuration mode.

**Command Syntax**

```
npu(config)# srvc-intf [<string>] [{IP-IP|VLAN|QinQ}]
```

**Privilege Level**

10

**Syntax Description**

| Parameter | Description | Presence | Default Value | Possible Values |
|---|---|---|---|---|
| `[<string>]` | The Service Interface alias of the Service Interface for which you want to enable the configuration mode. If you want to create a new Service Interface, specify a new alias and define the type of service interface (see below). | Mandatory | N/A | String (1 to 30 characters) |
| `[{IP-IP\|VLAN\|QinQ}]` | The Service Interface's type. | Optional | IP-IP | ■ IP-IP<br>■ VLAN<br>■ QinQ |

**Command Modes**

Global configuration mode

### 3.3.11.12.2 Configuring Service Interface Parameters

This section describes the commands for:

- "Configuring Parameters for IP-IP Service Interface"
- "Configuring Parameters for VLAN Service Interface"

### 3.3.11.12.2.1 Configuring Parameters for IP-IP Service Interface

After enabling the IP-IP Service Interface configuration mode, run the following command to configure the IP-IP service interface parameters:

This command shall configure one or more parameters of the IP-IP Service Interface.

**npu(config-srvcif-ipip)# config tunnel** ([**descr** <string>] [**srcaddr** <ip4addr>] {**dstaddr** <ipv4addr>} [**mtu** <size(556-1804)>] [**chksm**])

**Command Syntax**

**npu(config-srvcif-ip-ip)# config tunnel** ([**descr** <string>] [**srcaddr** <ip4addr>] {**dstaddr** <ipv4addr>} [**mtu** <size(556-1804)>] [**chksm**])

**Privilege Level**

10

**Syntax Description**

| Parameter | Description | Presence | Default Value | Possible Values |
|---|---|---|---|---|
| [descr <string>] | A description of the Service Interface. | Optional | null | String (up to 70 characters) |
| [srcaddr <ip4addr>] | The source IP address that indicates the point of origination of the tunnel for the service interface.<br>Must be the same as the Bearer IP Address. | Mandatory | N/A | IP Address of Bearer Interface. |
| {dstaddr <ipv4addr>} | The destination IP address that indicates the point of termination of the tunnel for the service interface. | Mandatory | N/A | Valid IP Address. |
| [mtu <size(556-1804)>] | Denotes the MTU. | Optional | 1480 | 556-1804 |

| | | | | | |
|---|---|---|---|---|---|
| | [chksm] | Indicates that end-to-end checksumming mechanism on ServiceTunnel Interface is enabled. | Optional | By default, this feature is disabled. | The presence/absence of this flag indicates that this feature is enabled/ disabled. |

**Command Modes** IP-IP Service Interface configuration mode

### 3.3.11.12.2.2 Configuring Parameters for VLAN Service Interface

After enabling the VLAN Service Interface configuration mode, run the following command to configure the VLAN service interface parameters:

This command shall configure one or more parameters of the VLAN Service Interface.

**npu(config-srvcif-vlan)# config** ([**descr** <string>] [**vlan-id** <size(1-9 | 11-4094>] [**dflt-gw-ip** <ipaddress> <mask>] [**mtu** <size(556-1804)>])

**Command Syntax** **npu(config-srvcif-vlan)# config** ([**descr** <string>] [**vlan-id** <size(1-9 | 11-4094>] [**dflt-gw-ip** <ip address> <mask>] [**mtu** <size(556-1804)>])

**Privilege Level** 10

**Syntax Description**

| Parameter | Description | Presence | Default Value | Possible Values |
|---|---|---|---|---|
| descr <string> | Aa description of the service interface. | Optional | null | String (up to 70 characters) |
| vlan-id <size(1-9 \| 11-4094>] | A Service Interface VLAN ID shall not conflict with other instances of Service Interface VLAN ID and VLAN IDs of Bearer, Local-Management, External-Management and AU Maintenance interfaces. Shall also not conflict with CVID of any transparent MS with L2 service. | Mandatory | N/A | 1-9, 11-4094 |

| | | | | | |
|---|---|---|---|---|---|
| | [dflt-gw-ip <ip address> <mask>] | The IP Address and subnet mask of the Default Gateway.<br>The IP address shall be unique among all the Host Interfaces IP's (Bearer, Local-Management, Internal-Management, External-Management) and existing instances of Service Interface's Tunnel Destination IP Address and Default Gateway IP Address.<br>Interface mask should be configured in such a way that the resulting subnet should not overlap with an existing Interface subnet (host interfaces, other service interfaces).<br>Should be in the same subnet.with the IP Address of the DHCP server/proxy/relay to be assigned to a service group using this service interface. | Mandatory | N/A | valid IP address and mask |
| | [mtu <size(556-1804)>] | The MTU size in bytes | Optional | 1480 | 556-1804 |

**Command Modes** VLAN Service Interface configuration mode

### 3.3.11.12.2.3 Configuring Parameter for QinQ Service Interface

After enabling the QinQ Service Interface configuration mode, run the following command to configure the QinQ service interface parameters:

This command shall configure one or more parameters of the QinQ Service Interface.

**npu(config-srvcif-QinQ)# config** ([**descr** <string>] [**vlan-id** <size(1-4094>])

**Command Syntax** **npu(config-srvcif-QinQ)# config** ([**descr** <string>] [**vlan-id** <size(1-4094>]])

**Privilege Level** 10

**Syntax Description**

| Parameter | Description | Presence | Default Value | Possible Values |
|---|---|---|---|---|
| descr <string> | A description of the service interface. | Optional | null | String (up to 70 characters) |
| vlan-id <size(1-4094>] | A Service Interface VLAN ID shall not conflict with other instances of Service Interface VLAN ID and VLAN IDs of Bearer, Local-Management and External-Management interaces. Shall also not conflict with CVID of any transparent MS.<br>Note that the default (0) is not a valid value. | Optional | 0 | 1-9, 11-4094 |

**Command Modes** QinQ Service Interface configuration mode

### 3.3.11.12.3 Restoring the Default Configuration Parameters for a Service Interface

This section describes the commands for:

- "Restoring the Default Configuration Parameters for an IP-IP Service Interface"
- "Restoring the Default Configuration Parameters for a VLAN Service Interface"

#### 3.3.11.12.3.1 Restoring the Default Configuration Parameters for an IP-IP Service Interface

Run the following command to restore the default configuration for IP-IP service interface tun-mtu and/or tun-chksm parameters:

**npu(config-srvcif-ipip)# no tunnel [mtu] [chksm]**

You can restore only one parameter to its default values by specifying only that parameter. To restore both parameters to their default value, run the command **npu(config-srvcif-ipip)# no tunnel.**

**NOTE**

Refer to Section 3.3.11.12.2.1 for a description and default values of these parameters.

| | |
|---|---|
| **Command Syntax** | **`npu(config-srvcif-ipip)# no tunnel [mtu] [chksm]`** |
| **Privilege Level** | 10 |
| **Command Modes** | IP-IP Service Interface configuration mode |

### 3.3.11.12.3.2 Restoring the Default Configuration Parameters for a VLAN Service Interface

Run the following command to restore the default configuration for a VLAN service interface tun-mtu parameter:

**`npu(config-srvcif-vlan)# no tunnel mtu`**

**NOTE**

Refer to Section 3.3.11.12.2.2 for a description and default values of this parameter.

| | |
|---|---|
| **Command Syntax** | **`npu(config-srvcif-vlan)# no tunnel mtu`** |
| **Privilege Level** | 10 |
| **Command Modes** | VLAN Service Interface configuration mode |

## 3.3.11.12.4 Terminating a Service Interface Configuration Mode

This section describes the commands for:


- "Terminating the IP-IP Service Interface Configuration Mode" on page 236
- "Terminating the VLAN Service Interface Configuration Mode" on page 236
- "Terminating the QinQ Service Interface Configuration Mode" on page 236

#### 3.3.11.12.4.1 Terminating the IP-IP Service Interface Configuration Mode

Run the following command to terminate the IP-IP service interface configuration mode:

```
npu(config-srvcif-ipip)# exit
```

| | |
|---|---|
| **Command Syntax** | `npu(config-srvcif-ipip)# exit` |
| **Privilege Level** | 10 |
| **Command Modes** | IP-IP Service interface configuration mode |

#### 3.3.11.12.4.2 Terminating the VLAN Service Interface Configuration Mode

Run the following command to terminate the vlan service interface configuration mode:

```
npu(config-srvcif-vlan)# exit
```

| | |
|---|---|
| **Command Syntax** | `npu(config-srvcif-vlan)# exit` |
| **Privilege Level** | 10 |
| **Command Modes** | VLAN Service interface configuration mode |

#### 3.3.11.12.4.3 Terminating the QinQ Service Interface Configuration Mode

Run the following command to terminate the QinQ service interface configuration mode:

```
npu(config-srvcif-QinQ)# exit
```

| | |
|---|---|
| **Command Syntax** | `npu(config-srvcif-QinQ)# exit` |

| | |
|---|---|
| **Privilege Level** | 10 |

| | |
|---|---|
| **Command Modes** | QinQ Service interface configuration mode |

### 3.3.11.12.5 Deleting a Service Interface

You can, at any time, run the following command to delete service interface:

npu(config)# no srvc-intf [<intf-alias>]

**NOTE**

A Service Interface cannot be deleted if it is assigned to any Service Group.
A QinQ Service Interface cannot be deleted if it is assigned to a Service Flow (with a VPWS-QinQ Service Group). For details refer to "Configuring Service Flows" on page 285.

| | |
|---|---|
| **Command Syntax** | **npu(config)# no srvc-intf** [intf-alias>] |

| | |
|---|---|
| **Privilege Level** | 10 |

**Syntax Description**

| Parameter | Description | Presence | Default Value | Possible Values |
|---|---|---|---|---|
| [intf-alias>] | The alias of the Service interface which needs to be deleted | Mandatory | N/A | String |

| | |
|---|---|
| **Command Modes** | Global configuration mode |

### 3.3.11.12.6 Displaying Configuration Information for the Service Interface

To display configuration information for one or all service interfaces, run the following command:

**npu# show srvc-intf** <intf-alias>

Specify a value for the `intf-alias` parameter if you want to display configuration information for a particular service interface. Do not specify a value for this parameter if you want to view configuration information for all service interfaces.

**Command Syntax**

```
npu# show srvc-intf intf-alias>
```

**Privilege Level**

1

**Syntax Description**

| Parameter | Description | Presence | Default Value | Possible Values |
|---|---|---|---|---|
| <intf-alias> | The alias of the service interface that you want to display. If you do not specify a value for this parameter, all the services interfaces that are configured, are displayed. | Optional | N/A | String |

**Display Format**

**IP-IP Service Interface**

```
% Asn-gateway Srvc Intf config
 Srvcif-Alias <string>
 SrvcifDescr <string>
 intf-type IP-IP
 SrvcifTunSrcIpAddr <IP address>
 SrvcifTunDstIpAddr <IP address>
 Tunnel-Chksum is <Disable/Enable>
 TunIPIPMTU <size>
if-alias <string>
if-descr <string>
intf-type IP-IP
tun-src-ip <IP address>
tun-dst-ip <IP address>
tun-chksum  <Enable/Disable>
tun-mtu <value>
```

| | |
|---|---|
| **Display Format** | `% Asn-gateway Srvc Intf config` |
| **VLAN Service Interface** | `if-alias <string>`<br>`if-descr <string>`<br>`intf-type VLAN`<br>`if-vlan-id <value>`<br>`if-dflt-gw-ip <value>` |
| **Command Modes** | Global command mode |

## 3.3.11.13 Configuring the AAA Client Functionality

The AAA client functionality enables configuration of one RADIUS client. The RADIUS client encapsulates the messages destined for the AAA server in RADIUS messages or decapsulates messages sent by the AAA server for the MS.

In addition, you can also configure certain RADIUS parameters such as the NAS ID and the time zone offset that are applicable for all AAA clients. In the current release a single AAA client is supported.

This section describes the commands for:

- "Managing AAA Client Configuration" on page 239
- "Managing Global RADIUS Configuration Parameters" on page 243

### 3.3.11.13.1 Managing AAA Client Configuration

**To configure the AAA client:**

1. Enable the AAA client configuration mode (`refer` to Section 3.3.11.13.1.1)
2. You can now execute any of the following tasks:
   - » Configure the AAA client parameters (refer to Section 3.3.11.13.1.2)
   - » Terminate the AAA client configuration mode (refer to Section 3.3.11.13.1.3)

In addition, you can, at any time, display the AAA client configuration information (refer to Section 3.3.11.13.1.4). The AAA client cannot be deleted.

#### 3.3.11.13.1.1 Enabling the AAA Client Configuration Mode

To configure the AAA client parameters, first enable the AAA client configuration mode. Run the following command to enable the AAA client configuration mode.

**`npu(config)# aaa-client`** `<client-alias>`

The system is supplied with a pre-configured AAA client with the following properties that cannot be modified:

client-alias: default

src-intf: Bearer

After enabling the AAA client configuration mode you can execute any of the following tasks:

- Configure the AAA client parameters (refer to Section 3.3.11.13.1.2)
- Terminate the AAA client configuration mode and return to the global configuration mode (refer to Section 3.3.11.13.1.3).

**Command Syntax**

**`npu(config)# aaa-client`** `<client-alias>`

**Privilege Level**

10

**Syntax Description**

| Parameter | Description | Presence | Default Value | Possible Values |
|---|---|---|---|---|
| `<client-alias>` | Denotes the client-alias of the AAA client for which the configuration mode is to be enabled.<br>In the current release a single AAA client is supported, with client-alias “default”. | Mandatory | N/A | default |

**Command Modes**

Global configuration mode

### 3.3.11.13.1.2 Configuring Parameters for the AAA Client

After enabling the AAA client configuration mode, run the following command to configure the parameters for the AAA client:

```
npu(config-aaa)# config ([src-intf <ip-intf>] [primary-serveraddr
<ipv4addr>] [rad-sharedsecret <string>] [rad-CallingStationId
{Binary | UTF-8}])
```

**IMPORTANT**

An error may occur if you provide an invalid value for any of these parameters. Refer the syntax description for more information about the appropriate values and format for configuring these parameters.

**IMPORTANT**

If the bearer interface IP address is being modified after aaa-client configuration, you must re-configure the src-intf parameter to "bearer" so that the aaa-client will attach itself to the new bearer interface IP address.

**Command Syntax**

```
npu(config-aaa)# config ([src-intf <ip-intf>] [primary-serveraddr
<ipv4addr>] [rad-sharedsecret <string>] [rad-CallingStationId {Binary |
UTF-8}])
```

**Privilege Level**

10

**Syntax Description**

| Parameter | Description | Presence | Default Value | Possible Values |
|---|---|---|---|---|
| [src-intf <ip-intf>] | Indicates the interface providing RADIUS client functionality. Must be the bearer interface. | Optional | bearer | bearer |
| [primary-serveraddr <ipv4addr>] | Denotes IPv4 address of the primary AAA server (in the current release an alternate server is not supported). | Mandatory | 172.16.0.10 | Valid IP Address |

| | | | | | |
|---|---|---|---|---|---|
| | `[rad-sharedsecret <string>]` | Denotes the shared secret between the AAA client and the AAA server. | Optional | default | String (1 to 49 characters) |
| | `[rad-CallingStationId {Binary \| UTF-8}]` | The format of the MAC address used to define the Calling Station ID | Optional | UTF-8 | ■ Binary<br>■ UTF-8 |

**Command Modes** AAA client configuration mode

### 3.3.11.13.1.3 Terminating the AAA Client Configuration Mode

Run the following command to terminate the AAA client configuration mode:

**`npu(config-aaa)# exit`**

**Command Syntax** **`npu(config-aaa)# exit`**

**Privilege Level** 10

**Command Modes** AAA client configuration mode

### 3.3.11.13.1.4 Displaying Configuration and Status Information for the AAA Client

To display one or all AAA clients, run the following command:

**`npu# show aaa-client`** `<client-alias>`

**Command Syntax** **`npu# show aaa-client`** `<client-alias>`

**Privilege Level** 1

**Syntax Description**

| Parameter | Description | Presence | Default Value | Possible Values |
|---|---|---|---|---|
| [<client-alias>] | Denotes the client-alias for which the associated AAA client information is to be displayed. In the current release the client-alias of the supported client is default. | Optional | N/A | String |

**Display Format**

```
AAA-client              :
Src-intf(IP)            :
Primary-ServerAddr      :
Radius Shared Secret    : <not available for display>
Server-Mac-Format       :
```

**Command Modes**

Global command mode

### 3.3.11.13.2 Managing Global RADIUS Configuration Parameters

Global RADIUS configuration parameters for AAA clients determine how AAA clients should send access requests. This section describes the commands to be used for:


- "Configuring Global RADIUS Parameters" on page 243
- "Restoring the Default Global RADIUS Configuration Parameters" on page 245
- "Displaying Global RADIUS Configuration Parameters" on page 246


#### 3.3.11.13.2.1 Configuring Global RADIUS Parameters

To configure the global RADIUS configuration parameters to be used for all AAA clients, run the following command:

```
npu(config)# radius <[accessreq-retries <retransmissions>]
[accessreq-interval <timeout>] [nasid <nas-identifier>]
[timezone-offset <time-offset(0-86400)>] [mtu <framed mtu
```

size(1020-2000)>][**RadiusAtrbtTypeServiceProfileName** <AtrbtTypeId(1-255)>] [**alrmAaaSwitchoverRetryFailThrshld**(1-250)>]>

**NOTE**

You can display configuration information for global RADIUS parameters. For details, refer to Section 3.3.11.13.2.3

**IMPORTANT**

An error may occur if you provide an invalid value for any of these parameters. Refer the syntax description for more information about the appropriate values and format for configuring these parameters.

**Command Syntax**

**npu(config)# radius <**[**accessreq-retries** <retransmissions>] [**accessreq-interval** <timeout>] [**nasid** <nas-identifier>] [**timezone-offset** <time-offset(0-86400)>] [**mtu** <framed mtu size(1020-2000)>] [**RadiusAtrbtTypeServiceProfileName** <AtrbtTypeId(1-255)>] [alrmAaaSwitchoverRetryFailThrshld(1-250)>]>

**Privilege Level**

10

**Syntax Description**

| Parameter | Description | Presence | Default Value | Possible Values |
|---|---|---|---|---|
| [accessreq-retries <retransmissions>] | Denotes the maximum number of times the AAA client can resend the access request. | Optional | 3 | 0-5 |
| [accessreq-interval <timeout>] | Denotes the interval, in seconds, after which the AAA client can resend the access request. | Optional | 500 | 10-100000 |
| [nasid <nas-identifier>] | Denotes the unique identifier of the ASNGW NAS. Sent in Access Request message only if configured. Should be in FQDN format. | Optional | null | String (up to 64 characters) |
| [timezone-offset <time-offset(0-86400)>] | Denotes the time zone offset, in seconds, from GMT at the NAS. | Optional | 0 | 0-86400 |

| | | | | | |
|---|---|---|---|---|---|
| | `[mtu <framed mtu size(1020-2000)>]` | Denotes the MTU to be used for the AAA client functionality. | Optional | 2000 | 1020-2000 |
| | `[RadiusAtrbtTypeServiceProfileName <AtrbtTypeId(1-255)>]` | Denotes the RADIUS attribute in which the ASN-GW shall expect to get the service profile name. For example, configure 11 if AAA uses Filter ID as the container of service profile name,<br>Use only unassigned freetext-type RADIUS attributes. | Optional | 11 | 1-255 |
| | `[alrmAaaSwitchoverRetryFailThrshld(1-250)>]` | Threshold to set alarm when the number of AAA switchover "unsuccessful access to primary + secondary" failed events for a measured period (PM interval of 15 minutes) exceeds the provisioned number. | Optional | 250 | 1 - 250 |

**Command Modes** Global configuration mode

### 3.3.11.13.2.2 Restoring the Default Global RADIUS Configuration Parameters

To restore the default global RADIUS configuration used for AAA clients, run the following command:

**`npu(config)# no radius [accessreq-retries] [accessreq-interval] [nasid] [timezone-offset] [mtu]`**

**NOTE**

Refer Section 3.3.11.13.2.1 for a description and default values of these parameters.

**Command Syntax** **`npu(config)# no radius [accessreq-retries] [accessreq-interval] [nasid] [timezone-offset] [mtu]`**

**Privilege Level** 10

| | |
|---|---|
| **Command Modes** | Global configuration mode |

#### 3.3.11.13.2.3 Displaying Global RADIUS Configuration Parameters

To display global RADIUS configuration parameters used for all AAA clients, run the following command:

```
npu# show radius
```

| | |
|---|---|
| **Command Syntax** | `npu# show radius` |
| **Privilege Level** | 1 |
| **Display Format** | `TimeOut <value>`<br>`accessReq-retries <value>`<br>`NAS-ID <value>`<br>`TimeZone Offset <value>`<br>`framed MtuSize <value>`<br>`Profile AtrbtType <value>`<br>`alrmAaaSwitchoverRetryFailThrshld <value>` |
| **Command Modes** | Global command mode |

## 3.3.11.14 Managing Service Groups

A service group is a group of MSs that are served by the same service provider or service flows that belong to the same service class.

The following service group types are supported:

- **IP**: This type of service group is used only for IP CS flows. Once service group is configured as type IP, additional IP allocation configuration is also required (such as DHCP mode, IP pool, IP Subnet, etc). This type of service group must be associated with either IP-IP (encapsulated IP packets) or VLAN type of R3 service interface. An IP service group can be configured to support time based or volume and time based accounting. In addition, an IP service group can be

configured to support direct communication between MSs belonging to the service group.

- **VPWS-Transparent**: This type of service group is used only for VLAN CS flows. Once service group is configured as VPWS-Transparent type, IP allocation configuration is not required. This type of service group is not associated with any R3 service interface as vlan-tagged MS traffic is transferred transparently on the on the R3 interface. A VPWS-Transparent service group can be configured to support time based accounting.

- **VPWS-QinQ**: This type of service group is used only for VLAN CS flows. Once service group is configured as type VPWS-QinQ type, IP allocation configuration is not required. This type of service group is not associated with any R3 service interface as double-tagged MS traffic is transferred transparently on the on the R3 interface. The QinQ VLAN used by the MS should be received from the AAA server in Access-Accept messages. A VPWS-QinQ service group can be configured to support time based accounting.

- **VPWS-Mapped**: This type of service interface is intended for special needs were VLAN CS service flows from multiple MSs use the same VLAN ID. Once service group is configured as VPWS- Mapped type, IP allocation configuration is not required. This type of service group makes the mapping between a unique MS flow VLAN ID used on R3 interface and a CVID. The CVID can be missing. For this service group type a VLAN pool need to configured. The ASNGW will uniquely allocate a VLAN from the configured pool to each MS flow to be used on R3 interface. A VPWS-Mapped service group can be configured to support time based accounting.

You can configure up to 10 service groups, where each of the IP Service Groups is:

- Associated with a separate service IP or VLAN service interface.

- Configured as any one of the following:
  - » DHCP server that allocates an IP address to the MS from the local pool (in the non-HA mode).
  - » DHCP relay that obtains the IP address using an external DHCP server (in the non-HA mode).
  - » DHCP proxy for either of the following boot modes:
    - ◊ Non-HA mode: The DHCP proxy assigns the MS the IP address that was received from AAA in the MS profile (in FRAMED-IP attribute or R3 Descriptors) or
    - ◊ HA mode: The DHCP proxy assigns the MS, the IP address received in the MS profile or obtains the IP address from HA using the mobile IP

**To configure a service group:**

1. Enable the service group configuration mode (refer to Section 3.3.11.14.1)
2. You can now execute any of the following tasks:
   - » Configure the common parameters of an IP service group (refer to Section 3.3.11.14.2)
   - » Enable/Disable the VLAN Interface of an IP Service Group (refer to Section 3.3.11.14.3)
   - » Enable the service group DHCP operation mode and configure the DHCP server/proxy/relay-specific parameters (refer to Section 3.3.11.14.4)
   - » Configure the parameters of a VPWS-Transparent Service Group (refer to Section 3.3.11.14.5)
   - » Configure the parameters of a VPWS-QinQ Service Group (refer to Section 3.3.11.14.6)
   - » Configure the parameters of a VPWS-Mapped Service Group (refer to Section 3.3.11.14.7)
   - » Terminate the service group configuration mode (refer to Section 3.3.11.14.8)

In addition, you can, at any time, display configuration information (refer to Section 3.3.11.14.10) or delete an existing service group (refer to Section 3.3.11.14.9).

### 3.3.11.14.1 Enabling the Service Group Configuration Mode\ Creating a New Service Group

To configure the parameters for the service group, first enable the service group configuration mode. Run the following command to enable the service group configuration mode or create the service group.

```
npu(config)# srvc-grp <grp-alias> [ServiceGrpType {IP | VPWS-QinQ |
VPWS-Transparent | VPWS-Mapped}]
```

If you use this command to create a new service group, the configuration mode for this group is automatically enabled after which you can configure or restore the default parameters for this service group.

After enabling the service group configuration mode, you can execute any of the following tasks:

- Configure the common parameters for an IP service group (refer to Section 3.3.11.14.2)
- Enable/Disable the VLAN Interface of an IP Service Group (refer to Section 3.3.11.14.3)
- Enable the service group operation mode and configure the DHCP server/proxy/relay-specific parameters (refer to Section 3.3.11.14.4)
- Configure the parameters of a VPWS-Transparent Service Group (refer to Section 3.3.11.14.5)
- Configure the parameters of a VPWS-Transparent Service Group (refer to Section 3.3.11.14.6)
- Configure the parameters of a VPWS-Transparent Service Group (refer to Section 3.3.11.14.7)

After executing these tasks, you can terminate the service group configuration mode (refer to Section 3.3.11.14.8).

**NOTE**

You can display configuration information for specific or all service groups. For details, refer to Section 3.3.11.15.2.

**Command Syntax**

```
npu(config)# srvc-grp <grp-alias> [ServiceGrpType {IP | VPWS-QinQ |
VPWS-Transparent | VPWS-Mapped}]
```

**Privilege Level**

10

**Syntax Description**

| Parameter | Description | Presence | Default Value | Possible Values |
|---|---|---|---|---|
| `srvc-grp <grp-alias>` | Denotes the group-alias of the service group for which the service group configuration mode is to be enabled. If you want to create a new service group, specify the group alias to be assigned to the srevice group. | Mandatory | N/A | String (1 to 30 characters) |
| `[ServiceGrpType {IP \| VPWS-QinQ \| VPWS-Transparent \| VPWS-Mapped}]` | The Service group's type. | Optional | IP | ■ IP<br>■ VPWS-QinQ<br>■ VPWS-Transparent<br>■ VPWS-Mapped |

**Command Modes**

Global configuration mode

### 3.3.11.14.2 Configuring Common Parameters of an IP Service Group

After enabling the service group configuration mode for an IP service group, run the following command to configure common parameters for the service group:

```
npu(config-srvcgrp)# config {{[srvcif-alias <service interface>]
[waitdhcp-holdtime <timeout>] [dhcp-ownaddr <ipv4addr>]} |
```

```
{server|proxy|relay} |{[<acct (none|time|volumeTime)>]}|{[<ms-loop
(enable|disable)>] | [acctInterimTmr <integer(0|5-1600)>]}
```

```
This commands comprises 5 sub-commands:
```

1. npu(config-srvcgrp)# config {[srvcif-alias <service interface>] [waitdhcp-holdtime <timeout>] [dhcp-ownaddr <ipv4addr>]}
2. npu(config-srvcgrp)# config {server|proxy|relay}
3. npu(config-srvcgrp)# config {[<acct (none|time|volumeTime)>]}
4. npu(config-srvcgrp)# config {[<ms-loop (enable|disable)>]}
5. npu(config-srvcgrp)# config {[acctInterimTmr <integer(0|5-1600)>]}

**NOTE**

You can display configuration information for the service group. For details, refer to Section 3.3.11.15.2.

**IMPORTANT**

An error may occur if you provide an invalid value for any of these parameters. Refer the syntax description for more information about the appropriate values and format for configuring these parameters.

**Command Syntax**

```
npu(config-srvcgrp)# config {{[srvcif-alias <service interface>]
[waitdhcp-holdtime <timeout>] [dhcp-ownaddr <ipv4addr>]} |
{server|proxy|relay} |{[<acct (none|time|volumeTime)>]}|{[<ms-loop
(enable|disable)>] | [acctInterimTmr <integer(0|5-1600)>]}
```

**Privilege Level**

10

**Syntax Description**

| Parameter | Description | Presence | Default Value | Possible Values |
|---|---|---|---|---|
| `[srvcif-alias <service interface>]` | Denotes the pre-defined IP or VLAN service interface alias to be used as the data path for traffic towards the core network.<br><br>Note that a Service Interface alias can be associated only to a single Service Group. | Mandatory | N/A | String |
| `[waitdhcp-holdtime <timeout>]` | Denotes the period, in seconds, for which the NPU waits for an IP address allocation trigger (MIP registration request / DHCP discover) from the MS.<br><br>If you specify the value of this parameter as 0, no timer is started and the NPU will wait infinitely for the IP address allocation trigger. | Optional | 0 | 0-86400 |
| `[dhcp-ownaddr <ipv4addr>]` | Denotes the IPv4 address of the DHCP server/ relay/ proxy.<br><br>Must be unique in the network.<br><br>For a service group using a VLAN service interface, should be in same subnet with the Default Gateway configured for the service interface associated with the service group. Subnet mask is taken as the default subnet mask i.e 255.255.255.0.<br><br>Note: In DHCP Server mode, the DHCP server IP address must be in the same subnet but outside the range allocated for users address pool as provisioned in the DHCP Server. | Mandatory | N/A | Valid IP Address |

| | | | | | |
|---|---|---|---|---|---|
| | `{server\|proxy\|relay}` | Mode of IP address allocation used for subscribers: DHCP Server/ Proxy/ Relay. | Mandatory | N/A | ■ dhcp-server<br>■ dhcp-proxy<br>■ dhcp-relay |
| | `{acct {none\|time\|volumeTime}}` | The Accounting mode for the service interface:<br>none: No accounting support.<br>time: The ASN-GW send RADIUS Accounting Start/Stop Requests. The ASN-GW shall also send Interim Accounting requests to AAA server using RADIUS Accounting Interim messages on a preconfigured or negotiated interval. AAA server can send negotiated time interval in Access-Accept message. If ASN GW defined value (see acctInterimTmr below) is zero and there is no Acct-Interim-Interval in Access Accept, interim updates should be deactivated.<br>volumeTime: Same as for time option above. In addition, this mode supports postpaid accounting by supporting IP Session Volume Based Accounting. The ASN-GW will report the cumulative volume counters for each MS IP Session. The counters will be collected per MS Service Flow and will be cumulated in order to get the MS IP Session counters. | Optional | time | ■ none<br>■ time<br>■ volumeTime |

| | | | | |
|---|---|---|---|---|
| {ms-loop {enable\| disable}} | Denotes whether MS loopback (direct communication between two MSs belonging to the same service group) is enabled or disabled for the service interface | Optional | Disable | ■ Enable<br>■ Disable |
| [acctInterim Tmr <integer(0\|5-1600)>] | Applicable only if acct (see above) mode is set to either time or volumeTime. The default interval in minutes for Accounting Interim reports to be used if Acct-Interim-Interval is not received from the AAA server.<br>Value "0" means interim reports are deactivated unless Acct-Interim-Interval is sent by the AAA server in Access Accept messages. | Optional | 5 | ■ 0<br>■ 5-1600 |

**Command Modes** IP Service group configuration mode

### 3.3.11.14.3 Enabling/Disabling VLAN Service Interface for an IP Service Group

This command is applicable only for an IP service group associated with a VLAN service interface.

Run the following commands to enable/disable the creation of a data-path for a VLAN Service:

To enable: **npu(config-srvcgrp)# set vlan-enable**

To disable: **npu(config-srvcgrp)# no vlan-enable**

**IMPORTANT**

The default is **disabled**

**Command Syntax**

```
npu(config-srvcgrp)# set vlan-enable
npu(config-srvcgrp)# no vlan-enable
```

| | |
|---|---|
| **Privilege Level** | 10 |

| | |
|---|---|
| **Command Modes** | IP Service group configuration mode |

### 3.3.11.14.4 Configuring the DHCP Server/Proxy/Relay

**To configure the DHCP server/proxy/relay:**

1. Enable the service group operation mode for DHCP server/relay/proxy (refer to Section 3.3.11.14.4.1)
2. You can now execute one of the following tasks according to the selected DHCP mode:
   - » Configure the DHCP server (refer to Section 3.3.11.14.4.2)
   - » Configure the DHCP proxy (refer to Section 3.3.11.14.4.3)
   - » Configure the DHCP relay (refer to Section 3.3.11.14.4.4)

#### 3.3.11.14.4.1 Enabling the Service Group Operation Mode for DHCP Server//Proxy/Relay

Run the following command enable the DHCP (server/relay/proxy) configuration mode.

```
npu(config-srvcgrp)# config {server|proxy|relay}
```

When you run this command, the DHCP server/proxy/relay configuration mode is enabled, after which you can execute the following tasks:

- Configure the DHCP server (refer to Section 3.3.11.14.4.2)
- Configure the DHCP proxy (refer to Section 3.3.11.14.4.3)
- Configure the DHCP relay (refer to Section 3.3.11.14.4.4)

**NOTE**

You cannot modify the configured DHCP mode. To change the DHCP mode you should first delete the Service Group and configure it again.

**Command Syntax**

```
npu(config-srvcgrp)# config {server|proxy|relay}
```

**Privilege Level**

10

**Syntax Description**

| Parameter | Description | Presence | Default Value | Possible Values |
|---|---|---|---|---|
| `{server\|proxy\|relay}` | Indicates whether the service group operation mode is to be enabled for the DHCP server, proxy or relay. | Mandatory | N/A | ■ server<br>■ proxy<br>■ relay |

**Command Modes**

Service group configuration mode

### 3.3.11.14.4.2 Configuring the DHCP Server

After enabling the service group operation mode for the DHCP server, you can execute any of the following tasks:

- “Configuring DHCP Server Parameters” on page 256
- “Restoring Configuration Parameters for the DHCP Server” on page 260
- “Configuring Exclude IP Addresses for the DHCP Server” on page 260
- “Deleting Exclude IP Addresses for the DHCP Server” on page 261

**NOTE**

Before executing these tasks, ensure that you have enabled the DHCP server configuration mode. For details, refer to “Enabling the Service Group Operation Mode for DHCP Server//Proxy/Relay” on page 255.

#### *3.3.11.14.4.2.1Configuring DHCP Server Parameters*

Run the following command to configure the DHCP server:

```
npu(config-srvcgrp-dhcpserver)# config ([pool-minaddr <string>]
[pool-maxaddr <string>] [pool-subnet <string>] [dflt-gwaddr
```

**<string>] [lease-interval <integer(24-4294967295)>] [renew-interval <integer>] [rebind-interval <integer>] [dnssrvr-addr <string>] [offerreuse-holdtime <integer>] [opt60 <string(30)>] [opt43 {[Name <string(64)>] [Value <string(64)>]}] [Sname <string(64)>] [File <string(128)>] [dnssrvr-addr2 <string>])**

**IMPORTANT**

An error may occur if you provide an invalid value for any of these parameters. Refer the syntax description for more information about the appropriate values and format for configuring these parameters.

**Command Syntax**

**npu(config-srvcgrp-dhcpserver)# config ([pool-minaddr <string>] [pool-maxaddr <string>] [pool-subnet <string>] [dflt-gwaddr <string>] [lease-interval <integer(24-4294967295)>] [renew-interval <integer>] [rebind-interval <integer>] [dnssrvr-addr <string>] [offerreuse-holdtime <integer>] [opt60 <string(30)>] [opt43 {[Name <string(64)>] [Value <string(64)>]}] [Sname <string(64)>] [File <string(128)>] [dnssrvr-addr2 <string>])**

**Privilege Level**

10

**Syntax Description**

| Parameter | Description | Presence | Default Value | Possible Values |
|---|---|---|---|---|
| **[pool-minaddr <string>]** | Denotes the minimum (lowest) IP address of the address pool to be used for address allocation for MSs from this Service Group.<br><br>DHCP address in the pool shall not overlap with the DHCP address pool defined in an existing service group and with ip addresses of host interfaces(Bearer, External mgmt, Internal mgmt amd Local mgmt). | Optional | 0.0.0.0 | Valid IP Address |

| | | | | | |
|---|---|---|---|---|---|
| | [**[pool-maxaddr <string>]** | Denotes the maximum (highest) IP address of the address pool configuration.<br>DHCP address in the pool shall not overlap with the DHCP address pool defined in an existing service group and with ip addresses of host interfaces(Bearer, External mgmt, Internal mgmt amd Local mgmt). | Optional | 255.255.255.255 | Valid IP Address |
| | **[pool-subnet <string>]** | The IP subnet mask to be provided by local DHCP Service with IP address for MSs from this Service Group. | Optional | 255.255.255.255 | IP subnet |
| | **[dflt-gwaddr <string>]** | IP address of Default Gateway to be provided by local DHCP Service with IP address for MS from this Service Group. | Optional | 0.0.0.0 (none) | Valid IP Address |
| | **[lease-interval <integer(24-4294967295)>]** | Lease time in seconds of IP address allocated for MS from this Service Group. | Optional | 86400 | **24-4294967295** |
| | **[renew-interval <integer>]** | Denotes the period, after which, the MS can request for renewal of the lease which has expired. Specify the value of this parameter as a percentage of the `lease-interval` parameter.<br>The renew-interval must be lower than rebind-interval. | Optional | 50 | 1-100 |
| | **[rebind-interval <integer>]** | Denotes the rebind interval maintained as a percentage of the lease interval. This is passed to the MS (DHCP client). | Optional | 75 | 1-99 |

| | | | | |
|---|---|---|---|---|
| **[dnssrvr-addr <string>]** | IP Address of the first DNS Server to be provisioned to MS from this Group. | Optional | 0.0.0.0 (none) | Valid IP Address |
| **[offerreuse-holdtime <integer>]** | Denotes the Offer Reuse time in seconds of IP address offered to MS from this Service Group. | Optional | 5 | 1-120 |
| **[opt60 <string(30)>]** | Configures option 60.<br>An empty string (null) means that DHCP Option 60 is disabled. | Optional | <dslforum.org> | String (up to 30 characters).<br>Null (empty string) disables Option 60. |
| **[opt43 {[Name <string(64)>]** | Configures option 43 Name | Optional | InternetGatewayDevice.ManagementServer.URL | String (up to 64 characters) |
| **[Value <string(64)>]** | Configures option 43 Value | Optional | empty string | String (up to 64 characters) |
| **[Sname <string(64)>]** | Configures the server host name. This parameter is sent in dhcp-offer / dhcp-ack messages and may be used by certain CPEs. | Optional | empty string | String (up to 64 characters) |
| **[File <string(128)>]** | Configures the boot file name. This parameter is sent in dhcp-offer / dhcp-ack messages and may be used by certain CPEs. | Optional | empty string | String (up to 128 characters) |
| **[dnssrvr-addr2 <string>]** | IP Address of the second DNS Server to be provisioned to MS from this Group. | Optional | 0.0.0.0 (none) | Valid IP address |

**Command Modes** Service Group-DCHP server configuration mode

### 3.3.11.14.4.2.2Restoring Configuration Parameters for the DHCP Server

Run the following command to restore the default values of one or several DHCP server parameters. This command can be used to delete the DNS server address configuration (if specified).

**npu(config-srvcgrp-dhcpserver)# no [lease-interval] [renew-interval] [rebind-interval] [dnssrvr-addr] [offerreuse-holdtime] [dnssrvr-addr2]**

Specify one or several parameters to restore the specified parameters to their default values. Do not specify any parameter to restore all of these parameters to their default values.

**NOTE**

Refer to Section 3.3.11.14.4.2.1 for a description and default values of these parameters.

| | |
|---|---|
| **Command Syntax** | **npu(config-srvcgrp-dhcpserver)# no [lease-interval] [renew-interval] [rebind-interval] [dnssrvr-addr] [offerreuse-holdtime] [dnssrvr-addr2]** |
| **Privilege Level** | 10 |
| **Command Modes** | Service group-DHCP server configuration mode |

### 3.3.11.14.4.2.3Configuring Exclude IP Addresses for the DHCP Server

Run the following command to configure exclude IP addresses for the DHCP server:

**npu(config-srvcgrp-dhcpserver)# exclude-addr** <no. of Addrs (1-9)> <ipv4addr> [<ipv4addr>] ….

In each command you may add up to 9 IP addresses to be excluded. The total number of excluded IP addresses is up to a maximum of 16384.

**IMPORTANT**

An error may occur if you provide an invalid IP address. Refer the syntax description for more information about the appropriate values and format for configuring this parameters.

**Command Syntax**

```
npu(config-srvcgrp-dhcpserver)# exclude-addr <no. of Addrs (1-9)>
<ipv4addr> [<ipv4addr>] ….
```

**Privilege Level**

10

**Syntax Description**

| Parameter | Description | Presence | Default Value | Possible Values |
|---|---|---|---|---|
| <no. of Addrs (1-9)> | The number of IP addresses to be excluded | Mandatory | N/A | 1-9 |
| <ipv4addr> | Denotes the exclude IP address that will not be assigned to an MS by the DHCP server.<br>The number of IP address entries must match the value defined by the no. of Addrs parameter. | Mandatory | N/A | Valid IP address |

**Command Modes**

Service group-DCHP server configuration mode

### *3.3.11.14.4.2.4Deleting Exclude IP Addresses for the DHCP Server*

Run the following command to delete one or several excluded IP addresses for the DHCP server:

```
npu(config-srvcgrp-dhcpserver)# no exclude-addr <no. of Addrs
(1-9)> <ipv4addr> [<ipv4addr>] …
```

Run the following command (without specifying the parameters) to delete all excluded IP addresses for the DHCP server:

```
npu(config-srvcgrp-dhcpserver)# no exclude-addr
```

The deleted exclude IP addresses are no longer excluded when the DHCP server allocates the IP addresses. That is, the server may allocate these IP addresses to the MS.

**Command Syntax**

```
npu(config-srvcgrp-dhcpserver)# no exclude-addr no. of Addrs (1-9)>
<ipv4addr> [<ipv4addr>] …
```

**Privilege Level** 10

**Syntax Description**

| Parameter | Description | Presence | Default Value | Possible Values |
|---|---|---|---|---|
| <no. of Addrs (1-9)> | The number of excluded IP addresses to be deleted.<br>Do not specify any value if you want to remove all the exclude IP addresses specified for that DHCP server. | Optional | N/A | 1-9 |
| <ipv4addr> | Denotes an IP address that you want to remove from the list of exclude IP addresses.<br>The number of IP address entries must match the value defined by the no. of Addrs parameter.<br>Do not specify any value if you want to remove all the exclude IP addresses specified for that DHCP server. | Optional | N/A | Valid IP address |

**Command Modes** Service group-DHCP server configuration mode

### *3.3.11.14.4.2.5Terminating the DHCP Server Configuration Mode*

Run the following command to terminate the DHCP server configuration mode:

```
npu(config-srvcgrp-dhcpserver)# exit
```

**Command Syntax**

```
npu(config-srvcgrp-dhcpserver)# exit
```

**Privilege Level** 10

| | |
|---|---|
| **Command Modes** | Service group-DHCP server configuration mode |

### 3.3.11.14.4.3 Configuring the DHCP Proxy

After enabling the service group operation mode for the DHCP proxy, you can execute the following tasks:

- "Specifying DHCP Proxy Configuration Parameters" on page 263
- "Restoring the Default Configuration Parameters for the DHCP Proxy" on page 266
- "Terminating the DHCP Proxy Configuration Mode" on page 267

#### *3.3.11.14.4.3.1 Specifying DHCP Proxy Configuration Parameters*

Run the following command to configure the DHCP proxy:

```
npu(config-srvcgrp-dhcpproxy)# config ([offerreuse-holdtime
<integer>] [lease-interval <integer>] [dnssrvr-addr <string>]
[pool-subnet <string>] [dflt-gwaddr <string>] [renew-interval
<integer>] [rebind-interval <integer>] [opt60 <string(30)>] [opt43
{[Name <string(64)>] [Value <string(64)>]}] [Sname <string(64)>]
[File <string(128)>]) [dnssrvr-addr2 <string>]
```

**IMPORTANT**

An error may occur if you provide an invalid value for any of these parameters. Refer the syntax description for more information about the appropriate values and format for configuring these parameters.

| | |
|---|---|
| **Command Syntax** | `npu(config-srvcgrp-dhcpproxy)# config ([offerreuse-holdtime <integer>] [lease-interval <integer>] [dnssrvr-addr <string>] [pool-subnet <string>] [dflt-gwaddr <string>] [renew-interval <integer>] [rebind-interval <integer>] [opt60 <string(30)>] [opt43 {[Name <string(64)>] [Value <string(64)>]}] [Sname <string(64)>] [File <string(128)>] [dnssrvr-addr2 <string>])` |
| **Privilege Level** | 10 |

**Syntax Description**

| Parameter | Description | Presence | Default Value | Possible Values |
|---|---|---|---|---|
| **[offerreuse-holdtime <integer>]** | Denotes the duration in seconds within which the MS should send a DHCP request to accept the address sent by the NPU.<br>If the MS does not accept the address within this period, the MS is deregistered. | Optional | 5 | 0-120 |
| **[lease-interval <integer>]** | Lease time in seconds of IP address allocated for MS from this Service Group.<br>In the Proxy mode, this value is used if appropriate parameter is not received in RADIUS Access-Accept. | Optional | 86400 | 24 - 4294967295 |
| **[dnssrvr-addr <string>]** | IP Address of the first DNS Server to be provisioned to MS from this Group.<br>In the Proxy mode, this value is used if appropriate parameter is not received in RADIUS Access-Accept. | Optional | 0.0.0.0 (none) | Valid IP Address |
| **[pool-subnet <string>]** | The IP subnet mask to be provided by local DHCP Service with IP address for MSs from this Service Group. In the Proxy mode, this value is used if appropriate parameter is not received in RADIUS Access-Accept. | Optional | 255.255.255.255 | IP subnet |

| | | | | | |
|---|---|---|---|---|---|
| | **[dflt-gwaddr <string>]** | IP address of Default Gateway to be provided by local DHCP Service with IP address for MS from this Service Group.<br>In theProxy mode, this value is used if appropriate parameter is not received in RADIUS Access-Accept. | Optional | 0.0.0.0 (none) | Valid IP Address |
| | **[renew-interval <integer>]** | Denotes the period, after which, the MS can request for renewal of the lease which has expired. Specify the value of this parameter as a percentage of the `lease-interval` parameter.<br>This value is used if appropriate parameter is not received in RADIUS Access-Accept. | Optional | 50 | 1-100 |
| | **[rebind-interval <integer>]** | Denotes the rebind interval maintained as a percentage of the lease interval. This is passed to the MS (DHCP client).<br>This value is used if appropriate parameter is not received in RADIUS Access-Accept. | Optional | 75 | 1-99 |
| | **[opt60 <string(30)>]** | Configures option 60. | Optional | <dslforum.org> | String (up to 30 characters) |
| | **[opt43 {[Name <string(64)>]** | Configures option 43 Name | Optional | Internet Gateway Device. ManagementServer.URL | String (up to 64 characters) |
| | **[Value <string(64)>]** | Configures option 43 Value | Optional | empty string | String (up to 64 characters) |

| | | | | | |
|---|---|---|---|---|---|
| | **[Sname <string(64)>]** | Configures the proxy host name. This parameter is sent in dhcp-offer / dhcp-ack messages and may be used by certain CPEs. | Optional | empty string | String (up to 64 characters) |
| | **[File <string(128)>]** | Configures the boot file name. This parameter is sent in dhcp-offer / dhcp-ack messages and may be used by certain CPEs. | Optional | empty string | String (up to 128 characters) |
| | **[dnssrvr-addr2 <string>]** | IP Address of the second DNS Server to be provisioned to MS from this Group.<br>In the Proxy mode, this value is used if appropriate parameter is not received in RADIUS Access-Accept. | Optional | 0.0.0.0 (none) | Valid IP address |

| | |
|---|---|
| **Command Modes** | Service group-DHCP proxy configuration mode |

### *3.3.11.14.4.3.2Restoring the Default Configuration Parameters for the DHCP Proxy*

Run the following command to restore the default values of one or several DHCP proxy parameters. This command can also be used to delete the configured DNS server address (if specified).

**npu(config-srvcgrp-dhcpproxy)# no [offerreuse-holdtime] [lease-interval] [dnssrvr-addr][renew-interval] [rebind-interval] [dnssrvr-addr2]**

Specify one or several parameters to restore the specified parameters to their default values. Do not specify any parameter to restore all of these parameters to their default values.

**NOTE**

Refer Section 3.3.11.14.4.3.1 for a description and default values of these parameters.

| | |
|---|---|
| **Command Syntax** | **npu(config-srvcgrp-dhcpproxy)# no [offerreuse-holdtime] [lease-interval] [dnssrvr-addr][renew-interval] [rebind-interval] [dnssrvr-addr2]** |
| **Privilege Level** | 10 |
| **Command Modes** | Service group-DHCP proxy configuration mode |

#### *3.3.11.14.4.3.3Terminating the DHCP Proxy Configuration Mode*

Run the following command to terminate the DHCP proxy configuration mode:

**npu(config-srvcgrp-dhcpproxy)# exit**

| | |
|---|---|
| **Command Syntax** | **npu(config-srvcgrp-dhcpproxy)# exit** |
| **Privilege Level** | 10 |
| **Command Modes** | Service group-DHCP proxy configuration mode |

### 3.3.11.14.4.4 Configuring the DHCP Relay

After enabling the service group operation mode for the DHCP relay, you can execute any of the following tasks:


- "Configuring the DHCP Relay Parameters" on page 267
- "Terminating the DHCP Relay Configuration Mode" on page 272


#### *3.3.11.14.4.4.1Configuring the DHCP Relay Parameters*

Run the following command to configure the DHCP server address for the DHCP relay:

**npu(config-srvcgrp-dhcprelay)# config ([server-addr** <ipV4Addr>] [{**EnableOpt82|DisableOpt82**}])

**IMPORTANT**

An error may occur if you provide an invalid value for the DHCP server address. Refer the syntax description for more information about the appropriate values and format for configuring this parameters.

**Command Syntax**

```
npu(config-srvcgrp-dhcprelay)# config ([server-addr <ipV4Addr>]
[{EnableOpt82|DisableOpt82}])
```

**Privilege Level**

10

**Syntax Description**

| Parameter | Description | Presence | Default Value | Possible Values |
|---|---|---|---|---|
| [server-addr <ipv4addr>] | Denotes the IP address of the external DHCP server, | Mandatory | N/A | Valid IP Address |
| [{EnableOpt82\|DisableOpt82}] | Denotes whether DHCP option 82 is enabled or disabled. | Optional | Disable Opt82 | ■ EnableOpt82<br>■ DisableOpt82 |

**Command Modes**

Service group-DHCP relay configuration mode

### *3.3.11.14.4.4.2Configuring the DHCP Relay Option 82 Parameters*

If Option 82 for the DHCP Relay is enabled, run the following command to configure suboptions of option 82 of DHCP messages:

npu(config-srvcgrp-dhcprelay-Opt82)# config ([Subopt1value {Default | MSID | BSID | NASID | NASIP | Full-NAI | Domain | AsciiFrStrng <string(32)> | BinFrStrng <string(32)>}] [Subopt2value {Default | MSID | BSID | NASID | NASIP | Full-NAI | Domain | AsciiFrStrng <string(32)> | BinFrStrng <string(32)>}] [Subopt6value {Default | MSID | BSID | NASID | NASIP | Full-NAI | Domain | AsciiFrStrng <string(32)> | BinFrStrng <string(32)>}] [{Subopt7value [service-type] [vendor-specific] [session-timeout]}] [{EnableUnicast | DisableUnicast}])

**IMPORTANT**

- For DhcpRlOpt82SubOpt1BinFrstrng value, enter hex string without spaces.
- If Opt82Unicast is enabled then DHCP relay agent appends option 82 to all DHCP messages (unicast and broadcast).
- If Opt82Unicast is disabled (default) then DHCP relay agent appends option 82 only to broadcast DHCP request messages.

**Command Syntax**

npu(config-srvcgrp-dhcprelay-Opt82)# config ([Subopt1value {Default | MSID | BSID | NASID | NASIP | Full-NAI | Domain | AsciiFrStrng <string(32)> | BinFrStrng <string(32)>}] [Subopt2value {Default | MSID | BSID | NASID | NASIP | Full-NAI | Domain | AsciiFrStrng <string(32)> | BinFrStrng <string(32)>}] [Subopt6value {Default | MSID | BSID | NASID | NASIP | Full-NAI | Domain | AsciiFrStrng <string(32)> | BinFrStrng <string(32)>}] [{Subopt7value [service-type] [vendor-specific] [session-timeout]}] [{EnableUnicast | DisableUnicast}])

**Privilege Level**

10

**Syntax Description**

| Parameter | Description | Presence | Default Value | Possible Values |
|---|---|---|---|---|
| [Subopt1value {Default \| MSID \| BSID \| NASID \| NASIP \| Full-NAI \| Domain \| AsciiFrStrng <string(32)> \| BinFrStrng <string(32)>}] | Configures the suboption 1 (Agent Circuit ID) of DHCP option 82.<br>For AsciiFrStrng (string enter up to 32 characters,<br>For BinFrStrng (string enter a string of up to 32 hexadecimal digits (no spaces). | Optional | Not Set | ■ Default<br>■ MSID<br>■ BSID<br>■ NASID<br>■ NASIP<br>■ Full-NAI<br>■ Domain<br>■ AsciiFrStrng (string32)<br>■ BinFrStrng (string32) |

| | | | | | |
|---|---|---|---|---|---|
| | [Subopt2value {Default \| MSID \| BSID \| NASID \| NASIP \| Full-NAI \| Domain \| AsciiFrStrng <string(32)> \| BinFrStrng <string(32)>} | Configures the suboption 2 (Agent Remote ID) of DHCP option 82.<br>For AsciiFrStrng (string enter up to 32 characters,<br>For BinFrStrng (string enter a string of up to 32 hexadecimal digits (no spaces). | Optional | Not Set | ■ Default<br>■ MSID<br>■ BSID<br>■ NASID<br>■ NASIP<br>■ Full-NAI<br>■ Domain<br>■ AsciiFrStrng (string32)<br>■ BinFrStrng (string32) |
| | [Subopt6value {Default \| MSID \| BSID \| NASID \| NASIP \| Full-NAI \| Domain \| AsciiFrStrng <string(32)> \| BinFrStrng <string(32)>}] | Configures the suboption 6 (Agent Subscriber ID )of DHCP option 82.<br>For AsciiFrStrng (string enter up to 32 characters,<br>For BinFrStrng (string enter a string of up to 32 hexadecimal digits (no spaces). | Optional | Not Set | ■ Default<br>■ MSID<br>■ BSID<br>■ NASID<br>■ NASIP<br>■ Full-NAI<br>■ Domain<br>■ AsciiFrStrng (string32)<br>■ BinFrStrng (string32) |

| | | | | | |
|---|---|---|---|---|---|
| | [{Subopt7value [service-type] [vendor-specific] [session-timeout]}] | Configures the suboption 7 of DHCP option 82.<br>Allows enabling/disabling the use of suboption 7 by specifying it. In addition, allows enabling/disabling the following attributes (by specifying attributes to be enabled) if suboption 7 is enabled:<br>■ service-type (attribute 6)<br>■ vendor-specific (attribute 26)<br>■ session-timeout (attribute 27) | Optional | | |
| | [{EnableUnicast\|DisableUnicast}]) | Indicates whether the Unicast parameter is enabled or disabled. | Optional | Disable | ■ Enable<br>■ Disable |

**Command Mode** Service group-DHCP relay-option 82 configuration mode

### *3.3.11.14.4.4.3Removing the DHCP Relay suboption values*

Run the following command to remove one, several or all of the Suboption values configured by the user for DHCP Option 82.

npu(config-srvcgrp-dhcprelay-opt82)# no [Subopt1value] [Subopt2value] [Subopt6value] [Subopt7value]

**Command Syntax** npu(config-srvcgrp-dhcprelay-opt82)# no [Subopt1value] [Subopt2value] [Subopt6value] [Subopt7value]

**Privilage Level** 10

**Syntax Description**

| Parameter | Description | Presence | Default Value | Possible Values |
|---|---|---|---|---|
| no [Subopt1value] [Subopt2value] [Subopt6value] [Subopt7value] | Indicates the removal status of DHCP Option 82 suboptions.<br>If no suboption is specified, the values of all suboptions will be removed. | Optional | N/A | N/A |

**Command Mode** Service group-DHCP relay-Option 82 configuration mode

#### *3.3.11.14.4.4.4Terminating the DHCP Relay Configuration Mode*

Run the following command to terminate the DHCP relay configuration mode for this service group:

```
npu(config-srvcgrp-dhcprelay)# exit
```

**Command Syntax**

```
npu(config-srvcgrp-dhcprelay)# exit
```

**Privilege Level** 10

**Command Modes** Service group-DHCP relay configuration mode

### 3.3.11.14.5 Configuring the Parameters of a VPWS-Transparent Service Group

After enabling the service group configuration mode for a VPWS-Transparent service group, run the following command to configure the accounting parameters for the service group:

```
npu(config-srvcgrp-VPWS)# config {acct {none|time} | acctInterimTmr
<integer(0|5-1600)>}
```

**NOTE**

You can display configuration information for the service group. For details, refer to Section 3.3.11.15.2.

**Command Syntax**

```
npu(config-srvcgrp)# config {acct {none|time} | acctInterimTmr
<integer(0|5-1600)>}
```

**Privilege Level**

10

**Syntax Description**

| Parameter | Description | Presence | Default Value | Possible Values |
|---|---|---|---|---|
| `{acct {none\|time}}` | The Accounting mode for the service interface:<br>none: No accounting support.<br>time: The ASN-GW send RADIUS Accounting Start/Stop Requests. The ASN-GW shall also send Interim Accounting requests to AAA server using RADIUS Accounting Interim messages on a preconfigured or negotiated interval. AAA server can send negotiated time interval in Access-Accept message. If ASN GW defined value (see acctInterimTmr below) is zero and there is no Acct-Interim-Interval in Access Accept, interim updates should be deactivated. | Optional | time | ■ none<br>■ time |

| | | | | | |
|---|---|---|---|---|---|
| | `[acctInterimTmr <integer(0\|5-1600)>]` | Applicable only if acct (see above) mode is set to time. The default interval in minutes for Accounting Interim reports to be used if Acct-Interim-Interval is not received from the AAA server.<br><br>Value “0” means interim reports are deactivated unless Acct-Interim-Interval is sent by the AAA server in Access Accept messages. | Optional | 5 | ■ 0<br>■ 5-1600 |

**Command Modes** VPWS-Transparent Service group configuration mode

### 3.3.11.14.6 Configuring the Parameters of a VPWS-QinQ Service Group

After enabling the service group configuration mode for a VPWS-QinQ service group, run the following command to configure the accounting parameters for the service group:

```
npu(config-srvcgrp-VPWS)# config {acct {none|time} | acctInterimTmr <integer(0|5-1600)>}
```

**NOTE**

You can display configuration information for the service group. For details, refer to Section 3.3.11.15.2.

**Command Syntax**

```
npu(config-srvcgrp)# config {acct {none|time} | acctInterimTmr <integer(0|5-1600)>}
```

**Privilege Level** 10

**Syntax Description**

| Parameter | Description | Presence | Default Value | Possible Values |
|---|---|---|---|---|

| | | | | |
|---|---|---|---|---|
| {acct {none\|time}} | The Accounting mode for the service interface:<br>none: No accounting support.<br>time: The ASN-GW send RADIUS Accounting Start/Stop Requests. The ASN-GW shall also send Interim Accounting requests to AAA server using RADIUS Accounting Interim messages on a preconfigured or negotiated interval. AAA server can send negotiated time interval in Access-Accept message. If ASN GW defined value (see acctInterimTmr below) is zero and there is no Acct-Interim-Interval in Access Accept, interim updates should be deactivated. | Optional | time | ■ none<br>■ time |
| [acctInterimTmr <integer(0\|5-1600)>] | Applicable only if acct (see above) mode is set to time. The default interval in minutes for Accounting Interim reports to be used if Acct-Interim-Interval is not received from the AAA server.<br>Value “0” means interim reports are deactivated unless Acct-Interim-Interval is sent by the AAA server in Access Accept messages. | Optional | 5 | ■ 0<br>■ 5-1600 |

**Command Modes** VPWS-QinQ Service group configuration mode

### 3.3.11.14.7 Configuring the Parameters of a VPWS-Mapped Service Group

After enabling the service group configuration mode for a VPWS-Mapped service group, you can configure the following parameters for the service group:

Accounting parameters (see Section 3.3.11.14.7.1)

VID Map Range parameters (see Section 3.3.11.14.7.2)

### 3.3.11.14.7.1 Configuring the Accounting Parameters of a VPWS-Mapped Service Group

run the following command to configure the accounting parameters for the service group:

```
npu(config-srvcgrp-VPWS-Mapped)# config {acct {none|time} |
acctInterimTmr <integer(0|5-1600)>}
```

**NOTE**

You can display configuration information for the service group. For details, refer to Section 3.3.11.15.2.

**Command Syntax**

```
npu(config-srvcgrp-VPWS-Mapped)# config {acct {none|time} |
acctInterimTmr <integer(0|5-1600)>}
```

**Privilege Level**

10

**Syntax Description**

| Parameter | Description | Presence | Default Value | Possible Values |
|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| | `{acct {none\|time}}` | The Accounting mode for the service interface:<br>none: No accounting support.<br>time: The ASN-GW send RADIUS Accounting Start/Stop Requests. The ASN-GW shall also send Interim Accounting requests to AAA server using RADIUS Accounting Interim messages on a preconfigured or negotiated interval. AAA server can send negotiated time interval in Access-Accept message. If ASN GW defined value (see acctInterimTmr below) is zero and there is no Acct-Interim-Interval in Access Accept, interim updates should be deactivated. | Optional | time | ■ none<br>■ time |
| | `[acctInterimTmr <integer(0\|5-1600)>]` | Applicable only if acct (see above) mode is set to time. The default interval in minutes for Accounting Interim reports to be used if Acct-Interim-Interval is not received from the AAA server.<br>Value “0” means interim reports are deactivated unless Acct-Interim-Interval is sent by the AAA server in Access Accept messages. | Optional | 5 | ■ 0<br>■ 5-1600 |

**Command Modes** VPWS-Mapped Service group configuration mode

### 3.3.11.14.7.2 Configuring the VID Map Range Parameters of a VPWS-Mapped Service Group

run the following commands to configure the vid-map-range parameters for the service group:

To configure the start vlan id run the command:
**npu(config-srvcgrp-VPWS-Mapped)# config vid-map-range-start vlan-id** <size(1-4094)>.

To configure the end vlan id run the command:
**npu(config-srvcgrp-VPWS-Mapped)# config vid-map-range-end vlan-id** <size(1-4094)>.

**IMPORTANT**

When creating a new VPWS-Mapped service group, both start vlan-id and end vlan-id must be defined.

**NOTE**

You can display configuration information for the service group. For details, refer to Section 3.3.11.15.2.

**Command Syntax**

```
npu(config-srvcgrp-VPWS-Mapped)# config vid-map-range-start vlan-id <size(1-4094)>
npu(config-srvcgrp-VPWS-Mapped)# config vid-map-range-end vlan-id <size(1-4094)>
```

**Privilege Level**

10

**Syntax Description**

| Parameter | Description | Presence | Default Value | Possible Values |
|---|---|---|---|---|
| vid-map-range-start vlan-id <size(1-4094)> | The start value of the range of VLAN IDs for mapping.<br>None of the value within the range shall overlap with any existing infrastructue (host interfaces) VLAN IDs. None of the value within the range shall overlap with VID mapping ranges of other existing Service Groups | Mandatory | N/A | 1-4094 |

| | | | | | |
|---|---|---|---|---|---|
| | `vid-map-range-end vlan-id <size(1-4094)>` | The start value of the range of VLAN IDs for mapping.<br>Cannot be lower than vid-map-range-start vlan-id<br>None of the value within the range shall overlap with any existing infrastructue (host interfaces) VLAN IDs. None of the value within the range shall overlap with VID mapping ranges of other existing Service Groups | Mandatory | N/A | 1-4094 |

**Command Modes** VPWS-Mapped Service group configuration mode

### 3.3.11.14.8 Terminating the Service Group Configuration Mode

Run the following command to terminate the service group configuration mode:

```
npu(config-srvcgrp)# exit
npu(config-srvcgrp-VPWS)# exit
npu(config-srvcgrp-VPWS-Mapped)# exit
```

**Command Syntax**

```
npu(config-srvcgrp)# exit
npu(config-srvcgrp-VPWS)# exit
npu(config-srvcgrp-VPWS-Mapped)# exit
```

**Privilege Level** 10

**Command Modes** IP/VPWS-Transparent/VPWS-QinQ/VPWS-Mapped Service group configuration mode

### 3.3.11.14.9 Deleting a Service Group

You can, at any time, run the following command to delete a service group:

```
npu(config)# no srvc-grp <grp-alias>
```

**NOTE**

A Service Group cannot be deleted if it is assigned to a Service Flow. For details refer to "Configuring Service Flows" on page 285.

To delete a VLAN service group (associated with a VLAN service interface), first execute the "no vlan-enable" command (refer to Section 3.3.11.14.3).

**Command Syntax**

```
npu(config)# no srvc-grp <grp-alias>
```

**Privilege Level**

10

**Syntax Description**

| Parameter | Description | Presence | Default Value | Possible Values |
|---|---|---|---|---|
| <grp-alias> | Denotes the group-alias for which the service group to be deleted. | Mandatory | N/A | String |

**Command Modes**

Global configuration mode

### 3.3.11.14.10 Displaying Configuration Information for the Service Group

To display configuration information for one service group or for all service groups, run the following command:

```
npu# show srvc-grp [<grp-alias>]
```

**Command Syntax**

```
npu# show srvc-grp [<grp-alias>]
```

**Privilege Level**

1

**Syntax Description**

| Parameter | Description | Presence | Default Value | Possible Values |
|---|---|---|---|---|
| `[<grp-alias>]` | Denotes the group-alias for which the service group to be displayed.<br>If no grp-alias is specified, the parameters of all service groups will be displayed. | Optional | N/A | String |

**Display Format**

```
According to Service Group type and (for IP Service Group) the configured
DHCP mode.
```

## 3.3.11.15 Configuring the Service Flow Authorization Functionality

The Service Flow Authorization (SFA) functionality handles creation/ maintenance of pre-provisioned service flows for MS. It maps the AAA parameters (service profile name) received from the AAA server to pre-configured WiMAX-specific QoS parameters in the NPU. The SFA functionality enables you to configure multiple service profiles with multiple service flows and classification rules.

This section describes the commands to be used for:

- “Configuring the SFA PHS Functionality” on page 281
- “Displaying Configuration Information for the SFA PHS Functionality” on page 282
- “Configuring Service Profiles” on page 282
- “Configuring Classification Rules” on page 301

### 3.3.11.15.1 Configuring the SFA PHS Functionality

To configure the SFA functionality with respect to PHS Rules, run the following command:

To enable PHS: npu(config)# sfa phs-enable

To disable PHS: npu(config)# no sfa phs-enable

The default configuration is PHS Disable.

**NOTE**

You can display configuration information for the SFA functionality. For details, refer Section 3.3.11.15.2.

For details on PHS Rules, refer to "Configuring PHS Rules" on page 333.

| | |
|---|---|
| **Command Syntax** | **npu(config)# sfa phs-enable**<br>**npu(config)# no sfa phs-enable** |
| **Privilege Level** | 10 |
| **Command Modes** | Global configuration mode |

### 3.3.11.15.2 Displaying Configuration Information for the SFA PHS Functionality

To display the current configuration information for the SFA PHS functionality, run the following command:

**npu# show sfa**

| | |
|---|---|
| **Command Syntax** | **npu# show sfa** |
| **Privilege Level** | 1 |
| **Display Format** | SFA Configuration :<br>PHS <Enable/Disable> |
| **Command Modes** | Global command mode |

### 3.3.11.15.3 Configuring Service Profiles

The NPU allows for guaranteed end-to-end QoS for user traffic across the ASN. The QoS approach is connection-oriented, whereby user traffic is classified into "service flows." A service flow is a unidirectional stream of packets, either in the downlink or uplink direction, associated with a certain set of QoS requirements

such as maximum latency. The QoS requirements for service flows are derived from "service profiles" defined by the operator. A service profile is a set of attributes shared by a set of service flows. For instance, an operator might define a service profile called "Internet Gold" that will include QoS and other definitions to be applied to service flows associated with users subscribed to the operator's "Internet Gold" service package.

The factory default configuration includes an ‘empty” (no defined Service Flows) Service Profile with the name Default. If enabled, it will be used if profile descriptor is missing in service provisioning or if received profile descriptor is disabled (unauthenticated mode). Up to 63 additional Service Profiles may be created.

**To configure one or more service profiles:**

1. Enable the service profile configuration mode (refer to Section 3.3.11.15.3.1)
2. You can now execute any of the following tasks:
   - Configure the parameters for this service profile (refer to Section 3.3.11.15.3.2)
   - Manage service flow configuration for this service profile (refer to Section 3.3.11.15.3.3)
   - Delete service flows (refer to Section 3.3.11.15.3.3.7)
3. Terminate the service profile configuration mode (refer to Section 3.3.11.15.3.4)

You can, at any time, display configuration information (refer to Section 3.3.11.15.3.5) or delete an existing service profile (refer to Section 3.3.11.15.3.6).

### 3.3.11.15.3.1 Enabling the Service Profile Configuration Mode\Creating a New Service Profile

To configure the parameters for a service profile, first enable the service profile configuration mode. Run the following command to enable the service profile configuration mode. You can also use this command to create a new service profile.

```
npu(config)# srvc-profile <profile-name> [dgwPrfl]
```

**NOTE**

The dgwPrfl option is for future use. Do not use this option. In the rest of this section this option will be ignored.

If you use this command to create a new service profile, the configuration mode for this rule is automatically enabled, after which you can execute any of the following tasks:

- Configure the parameters for this service profile (refer to Section 3.3.11.15.3.2)
- Manage service flow configuration for this service profile (refer to Section 3.3.11.15.3.3)
- Delete service flows (refer to Section 3.3.11.15.3.3.7)

After you have executed these tasks, terminate the service profile configuration mode (refer to Section 3.3.11.15.3.4) to return to the service group configuration mode.

**Command Syntax**

```
npu(config)# srvc-profile <profile-name>
```

**Privilege Level**

10

**Syntax Description**

| Parameter | Description | Presence | Default Value | Possible Values |
|---|---|---|---|---|
| <profile-name> | Denotes the name of the service profile for which the configuration mode is to be enabled.<br>If you are creating a new service profile, specify the name of the new service profile. The configuration mode is automatically enabled for the new service profile. | Mandatory | N/A | String (1 to 30 characters) |

| | |
|---|---|
| **Command Modes** | Global configuration mode |

### 3.3.11.15.3.2 Enabling/Disabling the Service Profile

After enabling the service profile configuration mode, run the following command to enable this service profile:

```
npu(config-srvcprfl)# config profile-enable
```

A service profile can be enabled only if at least one service flow is configured.

To disable this service profile, run the following command:

```
npu(config-srvcprfl)# no profile-enable
```

```
The default mode is Disabled.
```

**NOTE**

You can display configuration information for specific or all service profiles. For details, refer to Section 3.3.11.15.3.5.

| | |
|---|---|
| **Command Syntax** | `npu(config-srvcprfl)# config profile enable`<br>`npu(config-srvcprfl)# no profile enable` |
| **Privilege Level** | 10 |
| **Command Modes** | Service profile configuration mode |

### 3.3.11.15.3.3 Configuring Service Flows

Service flows are unidirectional stream of packets, either in the downlink or uplink direction, associated with a certain set of QoS requirements such as maximum latency and minimum rate. Based on certain classification rules, service flows are transported over the R1 air interface in 802.16e connections, identified by connection IDs, and identified by GRE keys over the R6 interface in GRE tunnels. In addition, the ASN-GW can mark outgoing traffic in the R3 interface for further QoS processing within the CSN.

The system supports two types of service flows according to the convergence sublayer (CS) type: IP CS and VLAN CS. An IP CS service flow can be associated

only with an IP service group. A VLAN CS service flow can be associated only with a VPWS (Transparent/QinQ/Mapped) service group. Typically VLAN CS service flows should be managed (created/modified/deleted) only by the AAA server. However, to support special needs, it is possible to define VLAN CS service flows for the Default Service Profile.

Up to 12 Service Flows can be defined for each Service Profile.

**After enabling the service profile configuration mode, execute the following tasks to configure service flows within this service profile:**

1. Enable the service flow configuration mode (refer to Section 3.3.11.15.3.3.1)
2. You can now execute any of the following tasks:
   - » Configure the parameters for this service flow (refer to Section 3.3.11.15.3.3.2)
   - » Restore the default parameters for this service flow (refer to Section 3.3.11.15.3.3.3)
   - » Configure uplink/downlink classification rule names (refer to Section 3.3.11.15.3.3.4)
3. Terminate the service flow configuration mode (refer to Section 3.3.11.15.3.3.6)

You can, at any time delete an existing service flow (refer to Section 3.3.11.15.3.3.7).

### *3.3.11.15.3.3.1Enabling the Service Flow Configuration Mode\ Creating a New Service Flow*

To configure the parameters for a service flow, first enable the service flow configuration mode. Run the following command to enable the service flow configuration mode. You can also use this command to create a new service flow.

```
npu(config-srvcprfl)# flow [<flow-id (1-255)] [grp-alias
<srvc-grp-alias>] [if-alias <string>] [mcast-sfid <integer(0-65535)>
{[mcastipv4add <string(15)>]}] [<string>]
```

**NOTE**

The mcast-sfid and mcastipv4add parameter are for future use with a DGW profile (not supported in the current release). Do not use these parameters. In the following sections these parameters will be ignored.

If you use this command to create a new service flow, the configuration mode for this service flow is automatically enabled, after which you can execute any of the following tasks:

- Configure the parameters for this service flow (refer to Section 3.3.11.15.3.3.2)
- Restore the default parameters for this service flow (refer to Section 3.3.11.15.3.3.3)
- Configure uplink/downlink classification rule names (refer to Section 3.3.11.15.3.3.4)

After you have executed these tasks, you can terminate the service flow configuration mode, and return to the service profile configuration mode (refer to Section 3.3.11.15.3.3.6).

**Command Syntax**

```
npu(config-srvcprfl)#flow [<flow-id (1-255)] [grp-alias <srvc-grp-alias>]
[if-alias <string>]
```

**Privilege Level**

10

**Syntax Description**

| Parameter | Description | Presence | Default Value | Possible Values |
|---|---|---|---|---|
| `flow [<flow-id (1-255)]` | Denotes the flow ID of the service flow for which the service flow configuration mode is to be enabled. If you are creating a new service flow, specify the service flow ID of the new service flow. The configuration mode is automatically enabled for the new service flow. | Mandatory | N/A | 1-255 |

| | | | | |
|---|---|---|---|---|
| [grp-alias <srvc-grp-alias>] | Indicates the Reference Name for an existing service group to be used by the service flow.<br>VPWS Service Groups are applicable only for VLAN CS Service Flows of the Default Service Profile. | Mandatory when creating a new flow | N/A | An existing Service Group Alias. |
| [if-alias <string>] | Indicates the Reference Name for an existing QinQ service interface.<br>Applicable only if the assigned Service Group is of type VPWS-QinQ (in a VLANCS Service Flow of the Default Service Profile). | Mandatory when creating a new flow, only if the type of the specified grp-alias is VPWS-QinQ. | N/A | An existing QinQ Service Interface. |

### 3.3.11.15.3.3.2Specifying Service Flow Configuration Parameters

**Command Modes** Service profile configuration mode

After enabling the service flow configuration mode, run the following command to configure the parameters for this service flow:

```
npu(config-srvcprfl-flow)# config ([flow-type <type (1)>] [cs-type
<type (1 | 4)>] [media-type <string>] [uldatadlvry-type
<type(0<UGS> | 1<RTVR> | 2<NRTVR> | 3<BE> | 4<ERTVR> | 255<ANY>)>]
[ulqos-maxsustainedrate <value(10000-40000000)>]
[ulqos-trafficpriority <value(0-7)>] [dldatadlvry-type
<type(0<UGS> | 1<RTVR> | 2<NRTVR> | 3<BE> | 4<ERTVR> | 255<ANY>)>]
[dlqos-maxsustainedrate <value(10000-40000000)>]
[dlqos-trafficpriority <value(0-7)>] [ul-rsrv-rate-min
<integer(0-40000000)>] [ul-latency-max <integer>]
[ul-tolerated-jitter <integer)>] [ul-unsol-intrvl
<integer(0-65535)>] [dl-rsrv-rate-min <integer(0-40000000)>]
[dl-latency-max <integer>] [dl-tolerated-jitter <integer>])
```

**IMPORTANT**

An error may occur if you provide an invalid value for any of these parameters. Refer the syntax description for more information about the appropriate values and format for configuring these parameters.

**Command Syntax**

```
npu(config-srvcprfl-flow)# config ([flow-type <type (1)>] [cs-type <type
(1 | 4)>] [media-type <string>] [uldatadlvry-type <type(0<UGS> | 1<RTVR>
| 2<NRTVR> | 3<BE> | 4<ERTVR> | 255<ANY>)>] [ulqos-maxsustainedrate
<value(10000-40000000)>] [ulqos-trafficpriority <value(0-7)>]
[dldatadlvry-type <type(0<UGS> | 1<RTVR> | 2<NRTVR> | 3<BE> | 4<ERTVR> |
255<ANY>)>] [dlqos-maxsustainedrate <value(10000-40000000)>]
[dlqos-trafficpriority <value(0-7)>] [ul-rsrv-rate-min
<integer(0-40000000)>] [ul-latency-max <integer>] [ul-tolerated-jitter
<integer)>] [ul-unsol-intrvl <integer(0-65535)>] [dl-rsrv-rate-min
<integer(0-40000000)>] [dl-latency-max <integer>] [dl-tolerated-jitter
<integer>])
```

**Privilege Level**

10

**Syntax Description**

| Parameter | Description | Presence | Default Value | Possible Values |
|---|---|---|---|---|
| `[flow-type <type (1)>]` | Denotes the type of flow, that is, bi-directional (1) or multicast (2).<br>multicast (2) is not supported in current release. | Optional | 1 | ■ 1: Indicates bi-directional |
| `[cs-type <type (1 \| 4)>]` | Convergence Sublayer Type. This parameter is applied to both UL and DL Service Flows.<br>Must match the type of service group referenced by ServiceGrpAlias during creation of the flow: IPv4CS should be selected if the assigned Service Group is of type IP. VLANCS should be selected if the assigned Service Group is of type VPWS. | Optional | 1 (IPv4CS) | ■ 1: IPv4CS<br>■ 4: VLANCS |
| `[media-type <string>]` | Describes the type of media carried by the service flow. | Optional | Null | String, up to 32 characters |

| | | | | |
|---|---|---|---|---|
| [uldatadlvry-type <type(0<UGS> \| 1<RTVR> \| 2<NRTVR> \| 3<BE> \| 4<ERTVR> \| 255<ANY>)>] | Denotes the data delivery type for uplink traffic carried by the service flow. | Optional | 3 (BE) | 0-4 or 255 for ANY. |
| [ulqos-maxsustainedrate <value(10000-40000000)>] | Denotes the maximum sustained traffic rate, in bps, for uplink traffic carried by the service flow.<br>Although available for all service flows, applicable only for service flows with the appropriate uplink data delivery type (NRTVR, RTVR, BE, ERTVR, ANY) | Optional | 250000 | 10000-40000000 bps |
| [ulqos-trafficpriority <value(0-7)>] | Denotes the traffic priority to be applied to the uplink traffic carried by the service flow.<br>Although available for all service flows, not applicable for service flows with UGS uplink data delivery type. | Optional | 0 | 0-7, where 0 is lowest and 7 is highest |
| [dldatadlvry-type <type(0<UGS> \| 1<RTVR> \| 2<NRTVR> \| 3<BE> \| 4<ERTVR> \| 255<ANY>)>] | Denotes the data delivery type for the downlink traffic carried by the service flow. | Optional | 3 (BE) | ■ 0 (UGS)<br>■ 1 (RTVR)<br>■ 2 (NRTVR)<br>■ 3 (BE)<br>■ 4 (ERTVR)<br>■ 255 (ANY) |
| [dlqos-maxsustainedrate <value(10000-40000000)>] | Denotes the maximum sustained traffic rate, in bps, for the downlink traffic carried by the service flow.<br>Although available for all service flows, applicable only for service flows with the appropriate downlink data delivery type (NRTVR, RTVR, BE, ERTVR, ANY) | Optional | 250000 | 10000-40000000 bps |

| | | | | | |
|---|---|---|---|---|---|
| | `[dlqos-traffic priority <value(0-7)>]` | Denotes the traffic priority to be applied to the downlink traffic carried by the service flow.<br><br>Although available for all service flows, not applicable for service flows with UGS uplink data delivery type. | Optional | 0 | 0-7, where 7 is highest |
| | `[ul-rsrv-rate-min <integer(0-40000000)>]` | tthe minimum rate in bps reserved for this uplink service flow.<br><br>Although available for all service flows, applicable only for service flows with the appropriate uplink data delivery type (UGS, NRTVR, RTVR, ERTVR).<br><br>For NRTVER, RTVR and ERTVR-cannot be higher than ulqos-maxsustainedrate. | Optional | 250000 | 0- 40000000 |
| | `[ul-latency-max <integer>]` | The maximum latency in ms allowed in the uplink.<br><br>Although available for all service flows, applicable only for service flows with the appropriate uplink data delivery type (UGS, RTVR, ERTVR).<br><br>If uplink data delivery type is ERTVR or UGS,the default value should be 90ms. | Optional | 500 | 0- 4294967295 |
| | `[ul-tolerated-jitter <integer)>]` | the maximum delay variation (jitter) in milliseconds for this uplink service flow.<br><br>Although available for all service flows, applicable only for service flows with the appropriate uplink data delivery type (UGS, ERTVR) | Optional | 0 | 0- 4294967295 |

| | | | | | |
|---|---|---|---|---|---|
| | `[ul-unsol-intrvl <integer(0-65535)>]` | The nominal interval in ms between successive data grant opportunities for this uplink service flow.<br><br>Although available for all service flows, applicable only for service flows with the appropriate uplink data delivery type (UGS, ERTVR).<br><br>Must be lower than ul-latency-max. | Optional | 20 | 0-65535 |
| | `[dl-rsrv-rate-min <integer(0-40000000)>]` | tthe minimum rate in bps reserved for this downlink service flow.<br><br>Although available for all service flows, applicable only for service flows with the appropriate downlink data delivery type (UGS, NRTVR, RTVR, ERTVR)<br><br>For NRTVER, RTVR and ERTVR-cannot be higher than dlqos-maxsustainedrate. | Optional | 250000 | 0- 40000000 |
| | `[dl-latency-max <integer>]` | The maximum latency in ms allowed in the downlink.<br><br>Although available for all service flows, applicable only for service flows with the appropriate downlink data delivery type (UGS, RTVR, ERTVR).<br><br>If uplink data delivery type is ERTVR or UGS,the default value should be 90ms. | Optional | 500 | 0- 4294967295 |
| | `[dl-tolerated-jitter <integer)>]` | the maximum delay variation (jitter) in milliseconds for this downlink service flow.<br><br>Although available for all service flows, applicable only for service flows with the appropriate downlink data delivery type (UGS, ERTVR) | Optional | 0 | 0- 4294967295 |

**Command Modes** Service profile-service flow configuration mode

### 3.3.11.15.3.3.3Restoring the Default Service Flow Configuration Parameters

Run the following command to restore the default values of one or several parameters for this service flow:

```
npu(config-srvcprfl-flow)#  no [cs-type] [media-type]
[uldatadlvry-type] [ulqos-maxsustainedrate]
[ulqos-trafficpriority] [dldatadlvry-type]
[dlqos-maxsustainedrate] [dlqos-trafficpriority][ul-rsrv-rate-min]
[ul-latency-max] [ul-tolerated-jitter] [ul-unsol-intrvl]
[dl-rsrv-rate-min] [dl-latency-max] [dl-tolerated-jitter]
```

Do not specify any parameter to restore all parameters to their default values.

**NOTE**

Refer to Section 3.3.11.15.3.3.2 for a description and default values of these parameters.

**Command Syntax**

```
npu(config-srvcprfl-flow)# no [cs-type] [media-type]
[uldatadlvry-type] [ulqos-maxsustainedrate]
[ulqos-trafficpriority] [dldatadlvry-type]
[dlqos-maxsustainedrate]
[dlqos-trafficpriority][ul-rsrv-rate-min] [ul-latency-max]
[ul-tolerated-jitter] [ul-unsol-intrvl] [dl-rsrv-rate-min]
[dl-latency-max] [dl-tolerated-jitter]
```

**Privilege Level** 10

**Command Modes** Service profile-service flow configuration mode

### 3.3.11.15.3.3.4Configuring Uplink/Downlink Classification Rule Names

After enabling the service flow configuration mode, run the following commands to configure up to a maximum of 6 uplink and 6 downlink classification rules:

```
npu(config-srvcprfl-flow)# ulclsf-rulename <num_of_rule_names
(1-6)> <rulename> [<rulename>] [...]
```

```
npu(config-srvcprfl-flow)# dlclsf-rulename <num_of_rule_names
(1-6)> <rulename> [<rulename>] [...]
```

After you have executed these tasks, you can terminate the service flow configuration mode, and return to the service profile configuration mode (Section 3.3.11.15.3.3.6). For more information about configuring classification rules, refer "Configuring Classification Rules" on page 301.

**Command Syntax**

```
npu(config-srvcprfl-flow)# ulclsf-rulename <num_of_rule_names (1-6)>
<rulename> [<rulename>] [...]
```

```
npu(config-srvcprfl-flow)# dlclsf-rulename <num_of_rule_names (1-6)>
<rulename> [<rulename>] [...]
```

**Privilege Level**

10

**Syntax Description**

| Parameter | Description | Presence | Default Value | Possible Values |
|---|---|---|---|---|
| <num_of_rule_names (1-6)> | Indicates the number of uplink/downlink classification rules to be created | Mandatory | N/A | 1-6 |

| | | | | | |
|---|---|---|---|---|---|
| | <rulename> | Indicates the name of the uplink/downlink classification rule to be linked to this service flow. Use the classification rule name to reference the appropriate classification rule.<br><br>For VLANCS service flows the linked uplink and downlink classification rules should be the same. This is because the VLANCS classificaion rules define the CVID (Customer VLAN ID), that should be the same for uplink and downlink flows.<br><br>The number of rule name entries must match the number defined in num_of_rule_names.<br><br>For more information about creating classification rules, refer to Section 3.3.11.15.4.1. | Mandatory | N/A | Valid classification rule name |

**Command Modes** Service profile-service flow configuration mode

### *3.3.11.15.3.3.5Deleting Uplink/Downlink Classification Rule Names*

After enabling the service flow configuration mode, run the following commands to delete uplink/downlink classification rules:

**npu(config-srvcprfl-flow)# no ulclsf-rulename** [<num_of_rulenames (1-6)> <rulename> [<rulename>] ...]

**npu(config-srvcprfl-flow)# no dlclsf-rulename** [<num_of_rulenames (1-6)> <rulename> [<rulename>] ...]

After you have executed these commands, you can terminate the service flow configuration mode, and return to the service profile configuration mode (refer to Section 3.3.11.15.3.3.6)

**Command Syntax**

**npu(config-srvcprfl-flow)# no ulclsf-rulename** [<num_of_rulenames (1-6)> <rulename> [<rulename>] ...]

**npu(config-srvcprfl-flow)# no dlclsf-rulename** [<num_of_rulenames (1-6)> <rulename> [<rulename>] ...]

**Privilege Level**

10

**Syntax Description**

| Parameter | Description | Presence | Default Value | Possible Values |
|---|---|---|---|---|
| [<num_of_rulenames (1-6)> | Indicates the number of uplink/downlink classification rules to be deleted. | Mandatory | N/A | 1-6 |
| <rulename> | Indicates the name of the uplink/downlink classification rule to be deleted from to this service flow. Use the classification rule name to reference the appropriate classification rule.<br>The number of rule name entries must match the number defined in num_of_rule_names. | Mandatory | N/A | Valid classification rule name |

**Command Modes**

Service profile-service flow configuration mode

### *3.3.11.15.3.3.6Terminating the Service Flow Configuration Mode*

Run the following command to terminate the service flow configuration mode:

**npu(config-srvcprfl-flow)# exit**

**Command Syntax**

**npu(config-srvcprfl-flow)# exit**

**Privilege Level** 10

**Command Modes** Service profile-service flow configuration mode

### *3.3.11.15.3.3.7Deleting Service Flows*

You can, at any time, run the following command to delete one or all service flows:

```
npu(config-srvcprfl)# no flow [<flow-id>]
```

**CAUTION**

Specify the flow ID if you want to delete a specific service flow. Otherwise all the configured service flows are deleted.

**Command Syntax**

```
npu(config-srvcprfl)# no flow [<flow-id>]
```

**Privilege Level** 10

**Command Syntax**

```
npu(config-srvcprfl)# no flow [<flow-id>]
```

**Syntax Description**

| Parameter | Description | Presence | Default Value | Possible Values |
|---|---|---|---|---|
| [<flow-id>] | Denotes the flow ID of the service flow to be deleted.<br>If you do nort specify a value for this parameter, all the service flows are deleted. | Optional | N/A | 0-255 |

**Command Modes** Service profile configuration mode

### 3.3.11.15.3.4 Terminating the Service Profile Configuration Mode

Run the following command to terminate the service profile configuration mode:

```
npu(config-srvcprfl)# exit
```

| | |
|---|---|
| **Command Syntax** | **npu(config-srvcprfl)# exit** |
| **Privilege Level** | 10 |
| **Command Modes** | Service profile configuration mode |

### 3.3.11.15.3.5 Displaying Configuration Information for Service Profiles

To display all or specific service profiles, run the following command:

**npu# show srvc-profile** [<profile-name>]

Specify the profile name if you want to display configuration information for a particular service profile. Do not specify a value for this parameter if you want to view configuration information for all service profile.

**IMPORTANT**

An error may occur if you provide an invalid service profile name. Refer the syntax description for more information about the appropriate values and format for configuring this parameter.

| | |
|---|---|
| **Command Syntax** | **npu# show srvc-profile** [<profile-name>] |
| **Privilege Level** | 1 |

**Syntax Description**

| Parameter | Description | Presence | Default Value | Possible Values |
|---|---|---|---|---|
| `[<profile-name>]` | Indicates the name of the service profile for which configuration information is to be displayed.<br><br>If you do not specify a value for this parameter, configuration information is displayed for all service profiles. | Optional | N/A | String |

**Display Format**

```
Srvc Profile  <value>
status <value>
flow-id <value>
flow-type <value>
srvc-grp <value>
Service-If <value or null>
CS-type <value>
Media-Type <value>
UL-flowDataDeliveryType <value>
UL-flowQosMaxSustainedRate <value>
UL-flowQosTrafficPrority <value>
DL-flowDataDeliveryType <value>
DL-flowQosMaxSustainedRate <value>
DL-flowQosTrafficPrority <value>
UL-MinReservedTrafficRate <value>
UL-MaxLatencey <value>
UL-ToleratedJitter <value>
UL-UnsolicitedGrantInterval <value>
DL-MinReservedTrafficRate <value>
DL-MaxLatencey <value>
DL-ToleratedJitter <value>
UL-Rulenames :<value>, <value>.....
DL-Rulenames :<value>, <value>....
flow-id <value>............
```

**Command Modes** Global configuration mode

### 3.3.11.15.3.6 Deleting Service Profiles

Run the following command to delete one or all service profiles:

```
npu(config)# no srvc-profile [<profile-name>]
```

**NOTE**

The Default Service Profile cannot be deleted.

**CAUTION**

Specify the profile name if you want to delete a specific service profile. Otherwise all the configured service profiles (excluding the Default Service Profile) are deleted.

**Command Syntax**

```
npu(config)# no srvc-profile [<profile-name>]
```

**Privilege Level**

10

**Syntax Description**

| Parameter | Description | Presence | Default Value | Possible Values |
|---|---|---|---|---|
| [<profile-name>] | Denotes the name of the service profile you want to delete. Specify this parameter only if you want to delete a specific service profile. | Optional | N/A | String |

**Command Modes**

Global configuration mode

### 3.3.11.15.4 Configuring Classification Rules

Classification rules are user-configurable rules that are used to classify packets transmitted on the bearer plane. You can associate one or more classification rules with a particular service profile (For details, refer to Section 3.3.11.15.3.3.4).

You can define an L3 classification rule with respect to the following criteria:

- IP ToS/DSCP
- IP protocol (such as UDP or TCP)
- IP source address (an address mask can be used to define a range of addresses or subnet)

- IP destination address (an address mask can be used to define a range of addresses or subnet)
- Source port range
- Destination port range

You can define an L2 classification rule based on the Customer VLAN ID (CVID).

Classification rules can be specified for:

- Downlink data is classified by the ASN-GW into GRE tunnels, which, in turn, are mapped into 802.16e connections in the air interface
- Uplink data is classified by the MS into 802.16e connections, and with respect to classification rules defined in the service profile provisioned in the ASN-GW and downloaded to the MS when establishing a connection.

For instance, you can define an L3 downlink classification rule that will classify traffic to a certain MS with a DSCP value of 46 into a UGS connection, and all other traffic to the MS into a best effort connection. In addition, an uplink L3 classification rule can be defined that will classify traffic from this MS with a UDP destination port higher than 5000 into a UGS connection, and all other traffic from the MS into a best effort connection.

Up to a maximum of 100 classification rules can be created.

**To configure one or more L3 classification rules:**

1. Enable the L3 classification rules configuration mode (refer to Section 3.3.11.15.4.1)

2 You can now execute any of the following tasks:

- Configure the parameters for this classification rule (refer to Section 3.3.11.15.4.2)
- Restore the default parameters for this classification rule (refer to Section 3.3.11.15.4.3)
- Manage protocol configuration (refer to Section 3.3.11.15.4.4)
- Manage source address configuration (seeSection 3.3.11.15.4.5)
- Manage destination address configuration (refer to Section 3.3.11.15.4.6)
- Manage source port configuration (refer to Section 3.3.11.15.4.7)
- Manage destination port configuration (refer to Section 3.3.11.15.4.8)

3 Terminate the L3 classification rules configuration mode (refer to Section 3.3.11.15.4.9)

You can, at any time, display configuration information (refer to Section 3.3.11.15.4.13) or delete an existing classification rule (refer to Section 3.3.11.15.4.14), protocol lists (refer to Section 3.3.11.15.4.4.5), source addresses (refer to Section 3.3.11.15.4.5.5), destination addresses (refer to Section 3.3.11.15.4.6.5), source ports (refer to Section 3.3.11.15.4.7.5), or destination ports (refer to Section 3.3.11.15.4.8.5) configured for this classification rule.

**To configure one or more L2 classification rules:**

1 Enable the L2 classification rules configuration mode (refer to Section 3.3.11.15.4.1)

2 You can now execute any of the following tasks:

- Configure the parameters for this classification rule (refer to Section 3.3.11.15.4.10)
- Clear the configuration of this classification rule (refer to Section 3.3.11.15.4.11)
- Terminate the L2 classification rules configuration mode (refer to Section 3.3.11.15.4.12)

You can, at any time, display configuration information (refer to Section 3.3.11.15.4.13) or delete an existing classification rule (refer to Section 3.3.11.15.4.14).

### 3.3.11.15.4.1 Enabling the Classification Rule Configuration Mode\ Creating a New Classification Rule

To configure the parameters for a classification rule, first enable the classification rule configuration mode. Run the following command to enable the classification rule configuration mode. You can also use this command to create a new classification rule.

```
npu(config)# clsf-rule <rulename> [clsfRuleType {L2 | L3}]
```

If you use this command to create a new classification rule, the configuration mode for this rule is automatically enabled.

After enabling the classification rule configuration mode for an L3 rule you can execute any of the following tasks:

- Configure the parameters for this classification rule (refer to Section 3.3.11.15.4.2).
- Restore the default parameters for this classification rule (refer to Section 3.3.11.15.4.3)
- Manage protocol configuration (refer to Section 3.3.11.15.4.4)
- Manage source address configuration (refer to Section 3.3.11.15.4.5)
- Manage destination address configuration (refer to Section 3.3.11.15.4.6)
- Manage source port configuration (refer to Section 3.3.11.15.4.7)
- Manage destination port configuration (refer to Section 3.3.11.15.4.8)

After you have executed these tasks, you can terminate the classification rules configuration mode (refer to Section 3.3.11.15.4.9).

After enabling the classification rule configuration mode for an L2 rule you can execute any of the following tasks:

- Configure the parameters for this classification rule (refer to Section 3.3.11.15.4.10).

- Clear the current configuration of this classification rule (refer to Section 3.3.11.15.4.11)

After you have executed these tasks, you can terminate the classification rules configuration mode (refer to Section 3.3.11.15.4.12).

**Command Syntax**

```
npu(config)# clsf-rule <rulename> [clsfRuleType {L2 | L3}]
```

**Privilege Level**

10

**Syntax Description**

| Parameter | Description | Presence | Default Value | Possible Values |
|---|---|---|---|---|
| <rulename> | Denotes the name of the classification rule. | Mandatory | N/A | String (1 to 30 characters) |
| [clsfRuleType {L2 \| L3}] | The type of classifier: L2 or L3. | Optional when creating a new rule. | L3 | ■ L2<br>■ L3 |

**Command Modes**

Global configuration mode

### 3.3.11.15.4.2 Specifying Configuration Parameters for the L3 Classification Rule

After enabling the classification rules configuration mode for an L3 classification rule, run the following command to configure the parameters for this classification rule:

```
npu(config-clsfrule)# config [priority <priority(0-255)>]
[phs-rulename <rulename>] [iptos-low <value(0-63)>] [iptos-high
<value(0-63)>] [iptos-mask <value(0-63)>] [iptos-enable]
```

**NOTE**

You can display configuration information for specific or all classification rules. For details, refer to Section 3.3.11.15.4.13.

**Command Syntax**

```
npu(config-clsfrule)# config [priority <priority(0-255)>] [phs-rulename
<rulename>] [iptos-low <value(0-63)>] [iptos-high <value(0-63)>]
[iptos-mask <value(0-63)>] [iptos-enable]
```

**Privilege Level**

10

**Syntax Description**

| Parameter | Description | Presence | Default Value | Possible Values |
|---|---|---|---|---|
| [priority <priority(0-255)>] | Denotes the priority level to be assigned to the classification rule. | Optional | 0 | 0-255 |
| [phs-rulename <rulename>] | Indicates the Packet Header Suppression (PHS) rule name to be associated with the classification rule. Specify the PHS rulename if you want to perform PHS for this flow. For more information about configuring PHS rules, refer Section 3.3.11.16. | Optional | None | String<br>An existing PHS rule name. |
| [iptos-low <value(0-63)>] | Denotes the value of the lowest IP TOS field to define the lowest value where the range can begin.<br>Cannot be higher than iptos-high.<br>Can be modified only when IP TOS classification is disabled (see iptos-enable below). If set to a value higher than iptos-high, IP TOS classification cannot be enabled. | Optional | 0 | 0-63 |

| | | | | | |
|---|---|---|---|---|---|
| | `[iptos-high <value(0-63)>]` | Denotes the value of highest IP TOS field to define the highest value where the range can end.<br>Cannot be lower than iptos-low.<br>Can be modified only when IP TOS classification is disabled (see iptos-enable below). If set to a value lower than iptos-low, IP TOS classification cannot be enabled. | Optional | 0 | 0-63 |
| | `[iptos-mask <value(0-63)>]` | Denotes the mask for IP TOS value.This mask is applied to the TOS field received in the IP header to be matched within the TOS range configured. | Optional | 0 | 0-63 |
| | `[iptos-enable]` | Indicates whether the use of TOS-based classification is to be enabled. | Optional | By default, the use of TOS-based classification is disabled. | The presence/absence of this flag indicates that the use of TOS-based classification should be enabled/disabled. |

**Command Modes** L3 Classification rules configuration mode

### 3.3.11.15.4.3 Restoring the Default Parameters for the L3 Classification Rule

Run the following command to restore the default configuration for this classification rule.

```
npu(config-clsfrule)# no [priority] [iptos-low] [iptos-high]
[iptos-mask] [iptos-enable][phs-rulename]
```

**NOTE**

Refer to Section 3.3.11.15.4.3 for a description and default values of these parameters.

| | |
|---|---|
| **Command Syntax** | **npu(config-clsfrule)# no [priority] [iptos-low] [iptos-high] [iptos-mask] [iptos-enable]** [phs-rulename] |
| **Privilege Level** | 10 |
| **Command Modes** | L3 Classification rules configuration mode |

### 3.3.11.15.4.4 Managing Protocol Configuration for the L3 Classification Rule

L3 classification rules can classify the packet, based on the value of IP protocol field. You can configure the value of IP protocol for a given classification rule.

**To configure one or more IP protocols:**

1. Enable the IP protocol configuration mode (refer to Section 3.3.11.15.4.4.1)
2. Enable/disable protocol lists (refer to Section 3.3.11.15.4.4.2 and Section 3.3.11.15.4.4.3)
3. Terminate the protocol configuration mode (refer to Section 3.3.11.15.4.4.4)

In addition, you can, at any time, delete an existing protocol list (refer to Section 3.3.11.15.4.4.5).

The following example illustrates the (sequence of) commands for enabling the IP protocol configuration mode, enabling IP protocol 100, and then terminating the protocol lists configuration mode:

```
npu(config-clsfrule)# ip-protocol
npu(config-clsfrule-protocol)# protocol-enable 1 100
npu(config-clsfrule-protocol)# exit
```

#### *3.3.11.15.4.4.1Enabling the IP Protocol Configuration Mode*

Run the following command to enable the IP protocol configuration mode.

```
npu(config-clsfrule)# ip-protocol
```

You can now enable or disable a protocol list (refer to Section 3.3.11.15.4.4.2 and Section 3.3.11.15.4.4.3).

| | |
|---|---|
| **Command Syntax** | **npu(config-clsfrule)# ip-protocol** |
| **Privilege Level** | 10 |
| **Command Modes** | L3 Classification rules configuration mode |

### 3.3.11.15.4.4.2Enabling Protocol Lists

After enabling the protocol configuration mode, run the following command to enable one or more IP protocol lists:

**npu(config-clsfrule-protocol)# protocol-enable** <number of protocols(1-6)> <protocol1> [<protocol2>] [...]

**IMPORTANT**

If destination port range (see Section 3.3.11.15.4.8.2) is enabled, then:
IP protocol (protocol-enable) is set to enabled.
Protocol can be either 6 (TCP) or 17 (UDP).

| | |
|---|---|
| **Command Syntax** | **npu(config-clsfrule-protocol)# protocol-enable** <number of protocols(1-6)> <protocol1> [<protocol2>] [...] |
| **Privilege Level** | 10 |

**Syntax Description**

| Parameter | Description | Presence | Default Value | Possible Values |
|---|---|---|---|---|
| <number of protocols(1)> | Indicates the number of protocol lists to be enabled. In the current release, only one protocol can be enabled per classification rule. | Mandatory | N/A | 1 |

| | | | | | |
|---|---|---|---|---|---|
| | <protocol1> [<protocol2>] [...] | Indicates the IP protocols to be enabled. In the current release, only one protocol can be enabled per classification rule. | Mandatory | N/A | 0-255 (Using standard IANA protocol values) |

**Command Modes** L3 Classification rules-IP protocol configuration mode

### 3.3.11.15.4.4.3Disabling Protocol Lists

After enabling the protocol configuration mode, run the following command to disable one or more IP protocol lists:

**npu(config-clsfrule-protocol)# no protocol-enable** <number of protocols(1-6)> <protocol1> [<protocol2>] [...]

**Command Syntax** **npu(config-clsfrule-protocol)# no protocol-enable** <number of protocols(1-6)> <protocol1> [<protocol2>] [...]

**Privilege Level** 10

**Syntax Description**

| Parameter | Description | Presence | Default Value | Possible Values |
|---|---|---|---|---|
| <number of protocols(1-6)> | Indicates the number of protocol lists to be disabled.<br>In the current release, only one protocol can be enabled per classification rule. | Mandatory | N/A | 1 |
| <protocol1> [<protocol2>] [...] | Indicates the protocols to be disabled. You are required to specify at least one protocol that is to be disabled.<br>In the current release, the single previously enabled protocol should be defined. | Mandatory | N/A | 0-255 |

| | |
|---|---|
| **Command Modes** | L3 Classification rules-IP protocol configuration mode |

#### *3.3.11.15.4.4.4Terminating the Protocol Configuration Mode*

Run the following command to terminate the IP protocol configuration mode:

```
npu(config-clsfrule-protocol)# exit
```

| | |
|---|---|
| **Command Syntax** | `npu(config-clsfrule-protocol)# exit` |
| **Privilege Level** | 10 |
| **Command Modes** | L3 Classfication rule-IP protocol configuration mode |

#### *3.3.11.15.4.4.5Deleting Protocol Lists*

You can, at any time, run the following command to delete all protocol lists:

```
npu(config-clsfrule)# no ip-protocol
```

| | |
|---|---|
| **Command Syntax** | `npu(config-clsfrule)# no ip-protocol` |
| **Privilege Level** | 10 |
| **Command Modes** | L3 Classfication rule-IP protocol configuration mode |

### 3.3.11.15.4.5 Managing Source Address Configuration for the L3 Classification Rule

Classification rules can classify the packet, based on the source address of the packet. You can configure the value of source address for a given classification rule.

**To configure one or more source addresses:**

1. Enable the source address configuration mode (refer to Section 3.3.11.15.4.5.1)
2. You can now execute any of the following tasks:
   - » Configure the address mask (refer to Section 3.3.11.15.4.5.2)
   - » Disable the source address (refer to Section 3.3.11.15.4.5.3)
3. Terminate the source address configuration mode (refer to Section 3.3.11.15.4.5.4)

You can, at any time, delete an existing source address (refer to Section 3.3.11.15.4.5.5).

The following example illustrates the (sequence of) commands for enabling the source address configuration mode, configuring the address mask, and then terminating the source address configuration mode:

```
npu(config-clsfrule)# srcaddr 10.203.155.20

npu(config-clsfrule-srcaddr)# config addr-enable addr-mask
255.255.0.0

npu(config-clsfrule-srcaddr)# exit
```

#### *3.3.11.15.4.5.1Enabling the Source Address Configuration Mode\ Creating a New Source Address*

To configure the parameters for a source address, first enable the source address configuration mode. Run the following command to enable the source address configuration mode. You can also use this command to create a new source address.

```
npu(config-clsfrule)# srcaddr <ipv4addr>
```

If you use this command to specify a new source address, the configuration mode for the newly created source address is automatically enabled, after which you can execute any of the following tasks:

- Configure the address mask (refer to Section 3.3.11.15.4.5.2)
- Disable the source address (refer to Section 3.3.11.15.4.5.3)

After you have executed these tasks, terminate the source address configuration mode to return to the service classification rule configuration mode (refer to Section 3.3.11.15.4.5.4).

**IMPORTANT**

An error may occur if you provide an invalid source IP address. Refer the syntax description for more information about the appropriate value and format for configuring this parameter.

**Command Syntax**

```
npu(config-clsfrule)# srcaddr <ipv4addr>
```

**Syntax Description**

| Parameter | Description | Presence | Default Value | Possible Values |
|---|---|---|---|---|
| <ipv4addr> | Denotes the IPv4 address of the source address for which the configuration mode is to be enabled. If you want to create a new source address, specify the value for the new source address. The source address configuration mode is automatically enabled. | Mandatory | N/A | Valid IP Address |

**Privilege Level**

10

**Command Modes**

L3 Classification rules configuration mode

### *3.3.11.15.4.5.2Configuring the Address Mask*

After enabling the source address configuration mode, run the following command to configure the address mask for the source address.

```
npu(config-clsfrule-srcaddr)# config [addr-enable] [addr-mask <value>]
```

You can also run this command to enable a source address that is currently disabled. For details, refer to “Disabling the Source Address” on page 314.

**IMPORTANT**

An error may occur if you provide an invalid address mask for the source address. Refer the syntax description for more information about the appropriate value and format for this parameter.

**Command Syntax** `npu(config-clsfrule-srcaddr)# config [addr-enable] [addr-mask <value>]`

**Privilege Level** 10

**Syntax Description**

| Parameter | Description | Presence | Default Value | Possible Values |
|---|---|---|---|---|
| `[addr-enable]` | Indiactes that the use of the associated source address is enabled for the classification rule that you are configuring. If the use of this address is disabled, the associated source address is ignored while classifying the packet. | Optional | By default, the use of the associated source address is disabled. | The presence/absence of this flag indicates that the use of the associated source address is enabled/disabled. |
| `[addr-mask <value>]` | Denotes the mask field that is used to specify a range of source addresses. | Optional | 255.255.255.255 | Valid address mask |

**Command Modes** L3 Classification rules-source address configuration mode

### 3.3.11.15.4.5.3Disabling the Source Address

You can run the following command to disable the source address that is currently enabled:

**`npu(config-clsfrule-srcaddr)# no addr-enable`**

**IMPORTANT**

To enable this source address, run the following command:
**`npu(config-clsfrule-srcaddr)# config [addr-enable] [addr-mask <value>]`**
For details, refer to “Configuring the Address Mask” on page 313.

**Command Syntax** **`npu(config-clsfrule-srcaddr)# no addr-enable`**

| | |
|---|---|
| **Privilege Level** | 10 |

| | |
|---|---|
| **Command Modes** | L3 Classification rules-source address configuration mode |

### 3.3.11.15.4.5.4Terminating the Source Address Configuration Mode

Run the following command to terminate the source address configuration mode:

```
npu(config-clsfrule-srcaddr)# exit
```

| | |
|---|---|
| **Command Syntax** | `npu(config-clsfrule-srcaddr)# exit` |

| | |
|---|---|
| **Privilege Level** | 10 |

| | |
|---|---|
| **Command Modes** | L3 Classfication rule-source address configuration mode |

### 3.3.11.15.4.5.5Deleting Source Addresses

You can, at any time, run the following command to delete one or all source addresses

```
npu(config-clsfrule)# no srcaddr [<ip-Addr>]
```

**CAUTION**

Specify the IP address if you want to delete a specific source address. Otherwise all the configured source addresses are deleted.

| | |
|---|---|
| **Command Syntax** | `npu(config-clsfrule)# no srcaddr [<ip-Addr>]` |

| | |
|---|---|
| **Privilege Level** | 10 |

**Syntax Description**

| Parameter | Description | Presence | Default Value | Possible Values |
|---|---|---|---|---|
| `[<ip-Addr>]` | Denotes the IPv4 address of the source address that you want to delete from a classification rule.<br>Specify this parameter only if you want to delete a specific source address. If you do not specify a value for this parameter, all the configured source addresses of the classification rule will be deleted. | Optional | N/A | Valid IP Address |

**Command Modes** L3 Classification rules configuration mode

### 3.3.11.15.4.6 Managing Destination Address Configuration for the L3 Classification Rule

Classification rules can classify the packet, based on the destination address of the packet. You can configure the value of destination address for a given classification rule.

**To configure one or more destination addresses:**

1. Enable the destination address configuration mode (refer to Section 3.3.11.15.4.6.1)
2. You can now execute any of the following tasks:
   - Configure the address mask (refer to Section 3.3.11.15.4.6.2)
   - Disable the destination address (refer to Section 3.3.11.15.4.6.3)
3. Terminate the destination address configuration mode (refer to Section 3.3.11.15.4.6.4)

In addition, you can, at any time, delete an existing destination address (refer to Section 3.3.11.15.4.6.5).

The following example illustrates the (sequence of) commands for enabling the source address configuration mode, configuring the address mask, and then terminating the destination address configuration mode:

```
npu(config-clsfrule)# dstaddr 10.203.155.22

npu(config-clsfrule-dstaddr)# config addr-enable addr-mask
0.0.255.255

npu(config-clsfrule-srcaddr)# exit
```

### 3.3.11.15.4.6.1Enabling the Destination Address Configuration Mode\ Creating a New Destination Address

To configure the parameters for a destination address, first enable the destination address configuration mode. Run the following command to enable the destination address configuration mode. You can also use this command to create a new destination address.

```
npu(config-clsfrule)# dstaddr <ipv4addr>
```

If you use this command to specify a new destination address, the configuration mode for the newly created destination address is automatically enabled, after which you can execute any of the following tasks:

- Configure the address mask (refer to Section 3.3.11.15.4.6.2)k
- Disable the destination address (refer to Section 3.3.11.15.4.6.3)

After you execute these tasks, you can terminate the destination address configuration mode (refer to Section 3.3.11.15.4.6.4) and return to the classification rules configuration mode.

**IMPORTANT**

An error may occur if you provide an invalid destination IP address. Refer the syntax description for more information about the appropriate values and format for configuring this parameter.

| | |
|---|---|
| **Command Syntax** | `npu(config-clsfrule)# dstaddr <ipv4addr>` |
| **Privilege Level** | 10 |

**Syntax Description**

| Parameter | Description | Presence | Default Value | Possible Values |
|---|---|---|---|---|
| `<ipv4addr>` | Denotes the IPv4 address of the destination address for which the configuration mode is to be enabled. If you want to create a new destination address, specify the value for the new destination address. The destination address configuration mode is automatically enabled. | Mandatory | N/A | Valid IP Address |

**Command Modes** L3 Classification rules configuration mode

### *3.3.11.15.4.6.2Configuring the Address Mask*

Run the following command to configure the address mask for the destination address.

**`npu(config-clsfrule-dstaddr)# config [addr-enable] [addr-mask <value>]`**

You can also run this command to enable a destination address that is currently disabled. For details, refer to "Disabling the Destination Address" on page 319.

**IMPORTANT**

An error may occur if you provide an invalid address mask. Refer the syntax description for more information about the appropriate values and format for configuring this parameter.

**Command Syntax** **`npu(config-clsfrule-dstaddr)# config [addr-enable] [addr-mask <value>]`**

**Privilege Level** 10

**Syntax Description**

| Parameter | Description | Presence | Default Value | Possible Values |
|---|---|---|---|---|
| `[addr-enable]` | Indicates that the use of the associated destination address is enabled for the classification rule that you are configuring. If the use of this address is disabled, the associated destination address is ignored while classifying the packet. | Optional | By default, the use of the associated destination address is disabled. | The presence/absence of this flag indicates that the use of the associated destination address is enabled/disabled. |
| `[addr-mask <value>]` | Denotes the mask field that is used to specify a range of destination addresses. | Optional | 255.255.255.255 | Valid address mask |

**Command Modes** L3 Classification rules-destination address configuration mode

### *3.3.11.15.4.6.3Disabling the Destination Address*

Run the following command to disable the destination address that is currently enabled:

```
npu(config-clsfrule-dstaddr)# no addr-enable
```

**Command Syntax** `npu(config-clsfrule-dstaddr)# no addr-enable`

**Privilege Level** 10

**Command Modes** L3 Classification rules-destination address configuration mode

### 3.3.11.15.4.6.4Terminating the Destination Address Configuration Mode

Run the following command to terminate the destination address configuration mode:

```
npu(config-clsfrule-dstaddr)# exit
```

| | |
|---|---|
| **Command Syntax** | `npu(config-clsfrule-dstaddr)# exit` |
| **Privilege Level** | 10 |
| **Command Modes** | L3 Classfication rule-destination address configuration mode |

### 3.3.11.15.4.6.5Deleting Destination Addresses

You can, at any time, run the following command to delete one or all destination addresses

```
npu(config-clsfrule)# no dstaddr [<ip-Addr>]
```

**IMPORTANT**

An error may occur if you provide an invalid IP address. Refer the syntax description for more information about the appropriate values and format for configuring this parameter.

| | |
|---|---|
| **Command Syntax** | `npu(config-clsfrule)# no dstaddr [<ip-Addr>]` |
| **Privilege Level** | 10 |

**Syntax Description**

| Parameter | Description | Presence | Default Value | Possible Values |
|---|---|---|---|---|
| `[<ip-Addr>]` | Denotes the IPv4 address of the destination address that you want to delete from a classification rule.<br>Specify this parameter only if you want to delete a specific destination address. | Optional | N/A | Valid IP Address |

**Command Modes** L3 Classification rules configuration mode

### 3.3.11.15.4.7 Managing Source Port Configuration for the L3 Classification Rule

Classification can be based on the source port of the packet. You can configure the value of a source port for a given classification rule.

**To configure one or more source ports:**

1. Enable the source port configuration mode (refer to Section 3.3.11.15.4.7.1)
2. Enable/disable the source port range (refer to Section 3.3.11.15.4.7.2/Section 3.3.11.15.4.7.3)
3. Terminate the source port configuration mode (refer to Section 3.3.11.15.4.7.4)

In addition, you can, at any time, delete an existing source port configuration (refer to Section 3.3.11.15.4.7.5).

The following example illustrates the (sequence of) commands for enabling the source port configuration mode, enabling the source port range, and then terminating the source port configuration mode:

```
npu(config-clsfrule)# srcport 20 50
npu(config-clsfrule-srcport)# port-enable
npu(config-clsfrule-srcport)# exit
```

### *3.3.11.15.4.7.1Enabling the Source Port Configuration Mode\ Creating a New Source Port*

To configure the parameters for a source port, first enable the source port configuration mode. Run the following command to enable the source port configuration mode. You can also use this command to create a new source port.

```
npu(config-clsfrule)# srcport <start-port> <end-port>
```

**IMPORTANT**

An error may occur if you provide an invalid value for any of these parameters. Refer the syntax description for more information about the appropriate values and format for configuring these parameters.

If you use this command to specify a new source port, the configuration mode for the newly created source port is automatically enabled, after which you can enable/disable the source port range (refer to Section 3.3.11.15.4.7.2/Section 3.3.11.15.4.7.3).

You can then terminate the source port configuration mode (refer to Section 3.3.11.15.4.7.4) and return to the classification rules configuration mode.

**Command Syntax**

```
npu(config-clsfrule)# srcport <start-port> <end-port>
```

**Privilege Level**

10

**Syntax Description**

| Parameter | Description | Presence | Default Value | Possible Values |
|---|---|---|---|---|
| <start-port> | Denotes the starting value of port range to be configured.<br>Cannot be higher than end-port. | Mandatory | N/A | 1-65535 |
| <end-port> | Denotes the end value of port range to be configured.<br>Cannot be lower than start-port. | Mandatory | N/A | 1-65535 |

| | |
|---|---|
| **Command Modes** | L3 Classification rules configuration mode |

### 3.3.11.15.4.7.2Enabling the Source Port Range

Run the following command to enable the source port range:

```
npu(config-clsfrule-srcport)# port-enable
```

You can also run this command to enable a source port range that is currently disabled. For details, refer to “Disabling the Source Port Range” on page 323.

**IMPORTANT**

If source port range is enabled, then:
IP protocol (protocol-enable) is set to enabled.
Protocol can be either 6 (TCP) or 17 (UDP).
For details on these parameters refer to Section 3.3.11.15.4.4.2.

| | |
|---|---|
| **Command Syntax** | `npu(config-clsfrule-srcport)# port-enable` |
| **Privilege Level** | 10 |
| **Command Modes** | L3 Classification rules-source port configuration mode |

### 3.3.11.15.4.7.3Disabling the Source Port Range

Run the following command to disable the source port range that is currently enabled:

```
npu(config-clsfrule-srcport)# no port-enable
```

**IMPORTANT**

To enable this source port range, run the following command:
`npu(config-clsfrule-srcport)# port-enable`
For details, refer to “Enabling the Source Port Range” on page 323.

| | |
|---|---|
| **Command Syntax** | `npu(config-clsfrule-srcport)# no port-enable` |

| | |
|---|---|
| **Privilege Level** | 10 |

| | |
|---|---|
| **Command Modes** | L3 Classification rules-source port configuration mode |

### 3.3.11.15.4.7.4Terminating the Source Port Configuration Mode

Run the following command to terminate the source port configuration mode:

```
npu(config-clsfrule-srcport)# exit
```

| | |
|---|---|
| **Command Syntax** | `npu(config-clsfrule-srcport)# exit` |

| | |
|---|---|
| **Privilege Level** | 10 |

| | |
|---|---|
| **Command Modes** | L3 Classfication rule-source port configuration mode |

### 3.3.11.15.4.7.5Deleting Source Ports

Run the following command to delete one or all source ports

```
npu(config-clsfrule)# no srcport [<start-port> <end-port>]
```

**IMPORTANT**

An error may occur if you provide an invalid value for the `start-port` and `end-port` parameters. Refer the syntax description for more information about the appropriate values and format for configuring these parameters.

| | |
|---|---|
| **Command Syntax** | `npu(config-clsfrule)# no srcport [<start-port> <end-port>]` |

| | |
|---|---|
| **Privilege Level** | 10 |

**Syntax Description**

| Parameter | Description | Presence | Default Value | Possible Values |
|---|---|---|---|---|
| <start-port> | Denotes the starting value of port range to be deleted. | Optional | N/A | 1-65535 |
| <end-port> | Denotes the end value of port range to be deleted. | Optional | N/A | 1-65535 |

**Command Modes** L3 Classification rules configuration mode

### 3.3.11.15.4.8 Managing Destination Port Configuration for the L3 Classification Rule

Classification can be based on the destination port of the packet. You can configure the value of a destination port for a given classification rule.

**To configure one or more destination ports:**

1. Enable the destination port configuration mode (refer to Section 3.3.11.15.4.8.1)
2. Enable/disable the destination port range (refer to Section 3.3.11.15.4.8.2/Section 3.3.11.15.4.8.3)
3. Terminate the destination port configuration mode (refer to Section 3.3.11.15.4.8.4)

In addition, you can, at any time, delete an existing destination port configuration (refer to Section 3.3.11.15.4.8.5).

The following example illustrates the (sequence of) commands for enabling the destination port configuration mode, enabling the destination port range, and then terminating the destination port configuration mode:

```
npu(config-clsfrule)# dstport 50 400
npu(config-clsfrule-dstport)# port-enable
npu(config-clsfrule-dstport)# exit
```

### 3.3.11.15.4.8.1 Enabling the Destination Port Configuration Mode\ Creating a New Destination Port

To configure the parameters for a destination port, first enable the destination port configuration mode. Run the following command to enable the destination port configuration mode. You can also use this command to create a new destination port.

```
npu(config-clsfrule)# dstport <start-port> <end-port>
```

If you use this command to specify a new destination port, the configuration mode for the newly created destination port is automatically enabled, after which you can enable/disable the destination port range (refer to Section 3.3.11.15.4.8.2/Section 3.3.11.15.4.8.3). After executing these tasks, you can terminate the destination port configuration mode (refer to Section 3.3.11.15.4.8.4).

**IMPORTANT**

An error may occur if you provide an invalid value for the `start-port` and `end-port` parameters. Refer the syntax description for more information about the appropriate values and format for configuring these parameters.

**Command Syntax**

```
npu(config-clsfrule)# dstport <start-port> <end-port>
```

**Privilege Level**

10

**Syntax Description**

| Parameter | Description | Presence | Default Value | Possible Values |
|---|---|---|---|---|
| `<start-port>` | Denotes the starting value of port range to be configured.<br>Cannot be higher than end-port. | Mandatory | N/A | 1-65535 |
| `<end-port>` | Denotes the end value of port range to be configured.<br>Cannot be lower than start-port. | Mandatory | N/A | 1-65535 |

| | |
|---|---|
| **Command Modes** | L3 Classification rules configuration mode |

### 3.3.11.15.4.8.2Enabling the Destination Port Range

You can run the following command to enable the destination port range:

```
npu(config-clsfrule-dstport)# port-enable
```

You can also run this command to enable a destination port range that is currently disabled. For details, refer to "Disabling the Destination Port Range" on page 327.

**IMPORTANT**

If destination port range is enabled, then:
IP protocol (protocol-enable) is set to enabled.
Protocol can be either 6 (TCP) or 17 (UDP).
For details on these parameters refer to Section 3.3.11.15.4.4.2.

| | |
|---|---|
| **Command Syntax** | `npu(config-clsfrule-dstport)# port-enable` |
| **Privilege Level** | 10 |
| **Command Modes** | L3 Classification rules-destination port configuration mode |

### 3.3.11.15.4.8.3Disabling the Destination Port Range

You can run the following command to disable the destination port range that is currently enabled:

```
npu(config-clsfrule-dstport)# no port-enable
```

**IMPORTANT**

To enable this destination port range, run the following command:
`npu(config-clsfrule-dstport)# port-enable`
For details, refer to "Enabling the Destination Port Range" on page 327.

| | |
|---|---|
| **Command Syntax** | **`npu(config-clsfrule-srcport)# no port-enable`** |
| **Privilege Level** | 10 |
| **Command Modes** | L3 Classification rules-destination port configuration mode |

### 3.3.11.15.4.8.4Terminating the Destination Port Configuration Mode

Run the following command to terminate the destination port configuration mode:

**`npu(config-clsfrule-dstport)# exit`**

| | |
|---|---|
| **Command Syntax** | **`npu(config-clsfrule-dstport)# exit`** |
| **Privilege Level** | 10 |
| **Command Modes** | L3 Classfication rule-destination port configuration mode |

### 3.3.11.15.4.8.5Deleting Destination Ports

Run the following command to delete one or all destination ports

**`npu(config-clsfrule)# no dstport`** `[<start-port> <end-port>]`

**IMPORTANT**

An error may occur if you provide an invalid value for the `start-port` and `end-port` parameters. Refer the syntax description for more information about the appropriate values and format for configuring these parameters.

| | |
|---|---|
| **Command Syntax** | **`npu(config-clsfrule)# no dstport`** `[<start-port> <end-port>]` |
| **Privilege Level** | 10 |

**Syntax Description**

| Parameter | Description | Presence | Default Value | Possible Values |
|---|---|---|---|---|
| <start-port> | Denotes the starting value of port range to be deleted. | Optional | N/A | 1-65535 |
| <end-port> | Denotes the end value of port range to be deleted. | Optional | N/A | 1-65535 |

**Command Modes** L3 Classification rules configuration mode

### 3.3.11.15.4.9 Terminating the L3 Classification Rule Configuration Mode

Run the following command to terminate the L3 classification rules configuration mode:

```
npu(config-clsfrule)# exit
```

**Command Syntax** `npu(config-clsfrule)# exit`

**Command Modes** L3 Classification rules configuration mode

### 3.3.11.15.4.10 Specifying Configuration Parameters for the L2 Classification Rule

After enabling the classification rules configuration mode for an L2 classification rule, run the following command to configure the parameters for this classification rule:

```
npu(config-clsfrule-L2)# cvid <value(1-4094)>
```

**NOTE**

You can display configuration information for specific or all classification rules. For details, refer to Section 3.3.11.15.4.13.

**Command Syntax** `npu(config-clsfrule-L2)# cvid <value(1-4094)>`

**Privilege Level** 10

**Syntax Description**

| Parameter | Description | Presence | Default Value | Possible Values |
|---|---|---|---|---|
| `cvid <value(1-4094)>` | Denotes the Customer VLAN ID value to be assigned to the classification rule. | Mandatory | N/A | 1-4094 |

**Command Modes** L2 Classification rules configuration mode

### 3.3.11.15.4.11 Clearing the configuration of the L2 Classification Rule

Run the following command to clear the configuration of this classification rule (removing the configured cvid):

```
npu(config-clsfrule-L2)# no cvid
```

After clearing the configuration you can define a new cvid for this classification rule.

**Command Syntax** `npu(config-clsfrule-L2)# no cvid`

**Privilege Level** 10

**Command Modes** L2 Classification rules configuration mode

### 3.3.11.15.4.12 Terminating the L2 Classification Rule Configuration Mode

Run the following command to terminate the L2 classification rules configuration mode:

```
npu(config-clsfrule-L2)# exit
```

**Command Syntax** `npu(config-clsfrule-L2)# exit`

**Command Modes** L2 Classification rules configuration mode

### 3.3.11.15.4.13 Displaying Configuration Information for Classification Rules

To display all or specific classification rules, run the following command:

```
npu# show clsf-rule [<rulename>]
```

Specify the classification rule name if you want to display configuration information for a particular rule. Do not specify a value for this parameter if you want to view configuration information for all classification rules.

**IMPORTANT**

An error may occur if you provide an invalid value for the `rulename` parameter. Refer the syntax description for more information about the appropriate values and format for configuring this parameters.

**Command Syntax**

```
npu# show clsf-rule [<rulename>]
```

**Privilege Level**

1

**Syntax Description**

| Parameter | Description | Presence | Default Value | Possible Values |
|---|---|---|---|---|
| `[<rulename>]` | Denotes the name of the classification rule that you want to display.<br>Specify this parameter only if you want to display a specific classification rule. If you do not specify a rule name, it displays all configured classification rules. | Optional | N/A | String |

| | |
|---|---|
| **Display Format for each L3 rule** | `Classification Rule Configuration :`<br>`ClsfRulename <value>`<br>`clsfRuleType: L3`<br>`Priority <value>`<br>`Phs rulename <value>`<br>`IpTosLow <value> IpTosHigh <value> IpTosMask <value> IpTosEnable <0/1>`<br>`clsfRuleSrcAddr <value> clsfRuleMask <value> SrcAddrEnable <0/1>`<br>`clsfRuleDstAddr <value> clsfRuleAddrMask <value> DstAddrenable <0/1>`<br>`clsfRuleSrcPort Start <value> clsfRuleSrcPort End <value> clsfRulePortEnable <0/1>`<br>`clsfRuleDstPort Start <value> clsfRuleDstPort End <value> clsfRulePortEnable <0/1>` |
| **Display Format for each L2 rule** | `ClsfRulename <value>`<br>`clsfRuleType: L2`<br>`Cvid <value>` |

| | |
|---|---|
| **Command Modes** | Global command mode |

### 3.3.11.15.4.14 Deleting Classification Rules

Run the following command to delete one or all classification rules:

**`npu(config)# no clsf-rule`** `[<rulename>]`

**CAUTION**

Specify the rule name if you want to delete a specific classification. Otherwise all the configured classification rules are deleted.

| | |
|---|---|
| **Command Syntax** | **`npu(config)# no clsf-rule`** `[<rulename>]` |

| | |
|---|---|
| **Privilege Level** | 10 |

**Syntax Description**

| Parameter | Description | Presence | Default Value | Possible Values |
|---|---|---|---|---|
| `[<rulename>]` | Denotes the name of the classification rule that you want to delete. Specify this parameter only if you want to delete a specific classification rule, otherwise all configured classification rules are deleted. | Optional | N/A | String |

**Command Modes**

Global configuration mode

## 3.3.11.16 Configuring PHS Rules

Packet Header Suppression (PHS) is a mechanism that conserves air-interface bandwidth by removing parts of the packet header that remain constant along the traffic session. PHS operates by allowing the MS and ASN-GW to associate PHS rules to each service flow.

When PHS is enabled, a repetitive portion of the payload headers of higher layers is suppressed in the MAC SDU by the sending entity and restored by the receiving entity. At the uplink, the sending entity is the MS and the receiving entity is the NPU. At the downlink, the sending entity is the NPU, and the receiving entity is the MS. If PHS is enabled at the MAC connection, each MAC SDU is prefixed with a PHSI, which references the Payload Header Suppression Field (PHSF).

For instance, the ASN-GW will associate a PHS rule to each provisioned service flow intended for VoIP traffic that will suppress the IP address field from the IP header and other unvarying fields (e.g. protocol version) from the IP and RTP headers. The PHS rules are provisioned on a per-service profile name basis. (For details, refer Section 3.3.11.15.4.)

PHS rules define:

- Header fields that need to be suppressed
- Static values that can be configured for the suppressed header fields

**To configure one or more PHS rules:**

1. Enable the PHS rules configuration mode (refer to Section 3.3.11.16.1)
2. Configure the parameters for the PHS rule (refer to Section 3.3.11.16.2)
3. Terminate the PHS rules configuration mode (refer to Section 3.3.11.16.3)

You can, at any time, display configuration information (refer to Section 3.3.11.16.5) or delete an existing PHS rules (refer to Section 3.3.11.16.4).

The following example illustrates the (sequence of) commands for enabling the PHS rules configuration mode, configuring the parameters of a PHS rule, and then terminating the PHS configuration mode, should be executed as shown in the example below:

```
npu(config)# phs-rule phs-rule1

npu(config-phsrule)# config field
00000000000000000000000FFFFFFFF00000000 mask 000F00 verify 0 size
20

npu(config-phsrule)# exit
```

### 3.3.11.16.1 Enabling the PHS Rules Configuration Mode /Creating a New PHS Rule

To configure the parameters for a PHS rule, first enable the PHS rules configuration mode. Run the following command to enable the PHS rules configuration mode. You can also use this command to create a new PHS rule.

```
npu(config)# phs-rule <rulename>
```

If you use this command to create a new PHS rule, the configuration mode for this PHS rule is automatically enabled, after which you can configure the parameters for the PHS rule (refer to Section 3.3.11.16.2). You can then terminate the PHS rules configuration mode (refer to Section 3.3.11.16.3) and return to the global configuration mode.

| | |
|---|---|
| **Command Syntax** | `npu(config)# phs-rule <rulename>` |
| **Privilege Level** | 10 |

**Syntax Description**

| Parameter | Description | Presence | Default Value | Possible Values |
|---|---|---|---|---|
| `<rulename>` | Denotes the PHS rule for which the PHS configuration mode is to be enabled. | Mandatory | N/A | String (1 to 30 characters) |

**Command Modes**

Global configuration mode

### 3.3.11.16.2 Configuring Parameters for the PHS Rule

Run the following command to configure the parameters of the PHS rule:

**`npu(config-phsrule)# config <[field <value>] [mask <value>] [verify <value>] [size <value>]>`**

**NOTE**

You can display configuration information for specific or all PHS rules. For details, refer Section 3.3.11.16.5.

**IMPORTANT**

An error may occur if you provide an invalid value for any of these parameters. Refer the syntax description for more information about the appropriate values and format for configuring these parameters.

**Command Syntax**

**`npu(config-phsrule)# config <[field <value>] [mask <value>] [verify <value>] [size <value>]>`**

**Privilege Level**

10

**Syntax Description**

| Parameter | Description | Presence | Default Value | Possible Values |
|---|---|---|---|---|
| `[field <value>]` | Denotes the PHSF value, that is, the header string to be suppressed. | Mandatory | N/A | String. This parameter is of format "0x00000000000000000000000000000000000000". Here Octet(x), x=20 bytes, each Byte will represent two characters when used as string like in xml file. |
| `[mask <value>]` | Indicates the PHSM, which contains the bit-mask of the PHSF with the bits set that is to be suppressed. | Mandatory | N/A | String This parameter is of format "0x000000". Here Octet(x), x=3 bytes, each Byte will represent two characters when used as string like in xml file. |
| `[verify <value>]` | Indicates whether the PHS header is to be verified. | Optional | 0 (No) | ■ 0: Indicates that the PHS header should be verified.<br>■ 1: Indicates that the PHS header should not be verified. |
| `[size <value>]` | Indicates the size in bytes of the header to be suppressed. | Mandatory | N/A | 0-20 |

| | |
|---|---|
| **Command Modes** | PHS rules configuration mode |

### 3.3.11.16.3 Terminating the PHS Rules Configuration Mode

Run the following command to terminate the PHS rules configuration mode:

```
npu(config-phsrule)# exit
```

| | |
|---|---|
| **Command Syntax** | `npu(config-phsrule)# exit` |
| **Privilege Level** | 10 |
| **Command Modes** | PHS rules configuration mode |

### 3.3.11.16.4 Deleting PHS Rules

Run the following command to delete one or all PHS rules:

```
npu(config)# no phs-rule [<rulename>]
```

**CAUTION**

Specify the rule name if you want to delete a specific PHS rule. Otherwise all the configured PHS rules are deleted.

| | |
|---|---|
| **Command Syntax** | `npu(config)# no phs-rule [<rulename>]` |
| **Privilege Level** | 10 |

**Syntax Description**

| Parameter | Description | Presence | Default Value | Possible Values |
|---|---|---|---|---|
| `[<rulename>]` | Denotes the rule name of the PHS rule that you want to delete.<br><br>Specify a value for this parameter if you want to delete a specific PHS rule. Do not specify a value for this parameter, if you want to delete all PHS rules. | Optional | N/A | String |

**Command Modes**

Global configuration mode

### 3.3.11.16.5 Displaying Configuration Information for PHS Rules

To display all or specific PHS rules, run the following command:

**`npu# show phs-rule`** `[<rulename>]`

Specify the rule name if you want to display configuration information for a particular PHS rule. Do not specify a value for this parameter if you want to view configuration information for all PHS rule.

**IMPORTANT**

An error may occur if you provide an invalid value for the `rulename` parameter. Refer the syntax description for more information about the appropriate values and format for configuring this parameter.

**Command Syntax**

**`npu# show phs-rule`** `[<rulename>]]`

**Privilege Level**

1

**Syntax Description**

| Parameter | Description | Presence | Default Value | Possible Values |
|---|---|---|---|---|
| `[<rulename>]` | Denotes the rule name of the PHS rule that you want to display.<br>Specify a value for this parameter if you want to display the parameters of a specific PHS rule. Do not specify a value for this parameter, if you want to display all PHS rules. | Optional | N/A | String |

**Display Format**

```
PHS Configuration :
rulename field    mask   verify   size
<value>  <value> <value> <value> <value>
…….
```

**Command Modes**

Global command mode

## 3.3.11.17 Managing the ASN-GW Keep-Alive Functionality

Once an MS enters the network, its context is stored in ASN entities (BS, ASN-GW). Dynamically, MS context could be transferred/updated (during HO and re-authentication) to other entities or duplicated to other entities (separation between anchor functions such as Authenticator, Data Path and Relay Data Path).

In certain cases, such as entity reset, other entities are not aware of service termination of an MS in that entity, and keep maintaining the MS context. This may result in service failure, excessive consumption of memory resources and accounting mistakes.

The keep-alive mechanism should be used to clear MS context from all network entities when it is de-attached from the BS, and de-register MS from the network when its context becomes unavailable in one of its serving function locations.

When the keep-alive mechanism is enabled the ASN-GW periodically polls other ASN entities-of-interest (BSs) and waits for their responses. In case of no

keep-alive response, the ASN-GW shall make further actions, such as clearing the applicable MS(s) context.

The ASN-GW builds a list of BS-of-interest which it must poll. The list shall be dynamically updated; the ASN-GW tracks all BSID(s) in all MS(s) contexts it holds, and dynamically updates the list of BSs-of-interest. When a new MS is attached to a BS that does not exist in the list, it will be added it to the list. When the last MS(s) with specific BSID makes network exit, the ASN-GW shall remove the BS from the list.

The ASN-GW periodically polls the BS(s) for keep-alive. The polling mechanism is independent and unrelated for every BS-of-interestthe ASN-GW polls.

The keep-alive mechanism uses configurable retry timer and retries counter. Upon expiration of the retry timer, the ASN-GW resends the ASN Keep-Alive request message. Upon expiration of the retries counter, the ASN-GW assumes failure of the polled BS and clears the contexts of all MS(s) served by that BS.

In addition, the ASN-GW verifies that for each polled entity that the "Last-Reset-Time" UTC value of poll N+1 is equal to the value of poll N. If the "Last-Reset-Time" UTC value of poll N+1 is higher than the value of poll N, this mean that the BS went through reset state during the interval between two consecutive polls. In this case, the ASN-GW shall clear all MS(s) contexts, served by that specific BS that are "older" than BS life after reset (through calculation of difference between polled entity "Last-Reset-Time" received on poll N+1 and MS network entry time stamp on ASNGW).

If the ASN-GW is the authenticator for the MS(s) the failing BS served, then in addition to context clearance it also sends R3 Accounting-Request (Stop) message including a release indication to AAA.

When keep-alive fails, ASN-GW generates an event.

Regardless of the enable/disable status of the keep-alive mechanism in the ASN-GW, it replies to ASN_Keep_Alive_Req received from other BSs with ASN_Keep_Alive_Rsp. that includes also its "Last-Reset-Time". It responds only if all its functions operate properly. In case one of the functions fails, the ASN-GW shall not respond to the keep-alive poll.

#### 3.3.11.17.1 Configuring ASN-GW Keep-Alive Parameters

To configure one or several keep-alive parameters, run the following command:

**npu(config)# keep-alive (**[**asn-ka** <enable|disable>] **[period** <integer (10-1000)>] [**rtx-cnt** <integer (1-10)>] [**rtx-time** <integer (5000-10000)>] )

**IMPORTANT**

An error may occur if you provide configuration values that do not satisfy following condition: 'period*1000 >= rtx-time * (rtx-cnt + 1)'"

**Command Syntax**

```
npu(config)# keep-alive ([asn-ka <enable|disable>] [period <integer (10-1000)>] [rtx-cnt <integer (1-10)>] [rtx-time <integer (5000-10000)>])
```

**Privilege Level**

10

**Syntax Description**

| Parameter | Description | Presence | Default Value | Possible Values |
|---|---|---|---|---|
| [asn-ka <enable\|disable>] | Enable/Disable the ASN-GW keep-alive mechanism. | Optional | disable | ■ enable<br>■ disable |
| [period <integer (10-1000)>] | The period In seconds between polling sessions.<br>period x 1000 (value in milliseconds) cannot be lower than rtx-time x (rtx-cnt +1). | Optional | 60 | 10-1000 |
| [rtx-cnt <integer (1-10)>] | Maximum number of retries if rtx-time has expired without getting a response. | Optional | 3 | 1-10 |
| **[rtx-time** <integer (5000-10000)>**]** | Time in milliseconds to wait for a response before initiating another polling attempt or reaching a decision that the polled entity has failed (if the maximum number of retries set by rtx-cnt has been reached). | Optional | 5000 | 5000-10000 |

**Command Modes**

Global configuration mode

### 3.3.11.17.2 Displaying Configuration Information for ASN-GW Keep-Alive Parameters

To display the ASN-GW keep-alive parameters, run the following command:

```
npu# show keep-alive
```

| | |
|---|---|
| **Command Syntax** | **npu# show keep-alive** |
| **Privilege Level** | 1 |
| **Display Format** | % Asn-gateway Keep Alive Configuration<br>asn-ka : <enable/disable><br>period : <value><br>rtx-cnt : <value><br>rtx-time : <value> |
| **Command Modes** | Global command mode |

## 3.3.12 Configuring Logging

Logs can be generated to record events that occur with respect to the following system modules:

- System startup procedures: Refers to all procedures/events that occur during system startup.
- NPU/AU upgrade procedures: Refers to all the procedures executed while upgrading the NPU/AU.
- Fault management procedures: Refers to internal processes that are executed for monitoring erroneous conditions or fault conditions.
- System performance procedures: Refers to internal processes that are executed for monitoring system performance.
- Shelf management procedures: Refers to internal processes that are executed for monitoring the health and temperature of all hardware components (other than the NPU) such as the AU, PIU and PSU.

- WiMAX signaling protocols: Refers to all the protocols that implement the ASN-GW functionality.
- User interface: Refers to the command line or remote management interface used for executing all user-initiated events such as system shut down or reset.
- AU Manager: Refers to all internal processes used for fault, configuration, and performance management for AU.

**IMPORTANT**

The Syslog utility is used to implement the logging feature for 4Motion.

You can specify the severity level for which log messages are to be generated for each module. Logs are generated for events for which the severity level is equal to or higher than the configured level. The following are the severity levels that you can configure for each module:

- Emergency
- Alert
- Critical
- Error
- Warning
- Notice
- Information

By default, system-level logging is enabled. The system stores a maximum of 1000 log and trace messages. The system stores log and trace messages using the cyclic buffer method. That is, when there are more than 1000 messages, the system overwrites the oldest log and trace messages.

**IMPORTANT**

It is recommended that you periodically make backups of log messages before these are overwritten. For details, refer to “Making a Backup of Log Files on the NPU Flash” on page 350.

To configure logging, first specify system-level logging that is applicable across the entire system. You can then configure logging, individually for each system module. This section describes the commands to be used for:


- "Managing System-level Logging" on page 344
- "Configuring Module-level Logging" on page 353


## 3.3.12.1 Managing System-level Logging

System-level logging refers to all the procedures to be executed for managing logging for the entire system. To manage system-level logging:

- Enable/disable logging across the entire system, and specify the destination (a file on the local system or on an external server) where logs are to be maintained.
- Make periodic backups of log files.

You can, at any time, view the current log destination or delete log files from the NPU flash. After you have enabled/disabled system-level logging and specified the destination for storing log messages, you can configure logging separately for each module. This section describes the commands to be used for:


- "Enabling System-level Logging" on page 344
- "Disabling Logging to File or Server" on page 346
- "Displaying System-level Logs" on page 348
- "Displaying the Current Log Destination" on page 349
- "Making a Backup of Log Files on the NPU Flash" on page 350
- "Deleting Backup Log Files from the NPU Flash" on page 352


### 3.3.12.1.1 Enabling System-level Logging

You can enable logging for the entire system and specify the destination where logs should be written. The destination can be either written to:

- File

- External server (Log files are sent to the external server in the Syslog log format. The Syslog daemon on the external server can save these log messages in the appropriate format depending upon the server configuration.)

By default, system-level logging is enabled. To view whether the system-level logging is enabled/disabled for logging to file or server. For details, refer Section 3.3.12.1.4.

The system maintains a maximum of 1000 log and trace messages. The system stores log and trace messages using the cyclic buffer method. That is, when there are more than 1000 messages, the system overwrites the oldest log and trace messages.

**IMPORTANT**

If you have enabled writing of log messages to file, it is recommended that you periodically make a backup of this log file. This is because log messages that are written to file are deleted after system reset. For more information about making backups of log files on the NPU flash, refer to Section 3.3.12.1.5.

To enable system-level logging, run the following command:

```
npu(config)# log destination {file | server <IP address>}
```

**NOTE**

After you execute this command, logging is enabled for the entire system. You may also configure logging separately for each system module. For details, refer to Section 3.3.12.2.

**IMPORTANT**

An error may occur if:

- Logging is already enabled for the requested destination (file or server).
- Logging is enabled to a server with a different IP address. Because logging can be enabled to only one external server, you can specify another server IP address after you disable logging to the existing server IP address. For more information about disabling logging to server, refer "Disabling Logging to File or Server" on page 346.
- An internal error has occurred.
- You have specified the IP address in an invalid format. Specify the IP address in the format, XXX.XXX.XXX.XXX.

| | |
|---|---|
| **Command Syntax** | `npu(config)# log destination {file \| server <IP address>}` |

**Privilege Level** 10

**Syntax Description**

| Parameter | Description | Presence | Default Value | Possible Values |
|---|---|---|---|---|
| `{file\|server <IP address>}` | Indicates whether logs are to be written to a file or server. | Mandatory | N/A | ■ **`file`**: Indicates that logs are to be written to a file. (Logs written to file are not maintained after system reset; periodically save the log file to flash.) For details, refer to Section 3.3.12.1.5.<br>■ **`server`**: Indicates that logs are to be written to an external server. Specify the server IP address of the server in the format, XXX.XXX.XXX.XXX. |

**Command Modes** Global configuration mode

### 3.3.12.1.2 Disabling Logging to File or Server

To disable logging to file or server, run the following command:

```
npu(config)# no log destination {file | server <IP address>}
```

**IMPORTANT**

An error may occur if:

- Logging is already disabled for the requested destination (file or server).
- An internal error has occurred.
- The server IP address that you have specified does not exist.

| | |
|---|---|
| **Command Syntax** | **npu(config)# no log destination** {**file** \| **server** <IP address>} |
| **Privilege Level** | 10 |

**Syntax Description**

| Parameter | Description | Presence | Default Value | Possible Values |
|---|---|---|---|---|
| `{file\|server <IP address>}` | Indicates whether the system-level logs are to be disabled for a file or server. | Mandatory | N/A | ■ `file`: Indicates that system-level logging to a file is to be disabled.<br>■ `server<ip address>`: Indicates that system-level logging to a server is to be disabled. Specify the IP address if you want to disable logging to a specific server. Otherwise logging is disabled for the server that was last enabled for logging. Provide the IP address in the format, XXX.XXX.XXX.XXX. |

**Command Modes**

Global configuration mode

### 3.3.12.1.3 Displaying System-level Logs

To display system-level logs, run the following command:

```
npu# show logs
```

When you run this command, all the log messages are displayed. (4Motion maintains a maximum of 1000 log and trace messages.) If you want to filter log messages to be displayed, run the following command to specify the filter criteria:

```
npu# show logs [filter | grep <string>]
```

For example, if you want to view log messages pertaining to only Error logs, run the following command:

```
npu# show logs filter|grep ERROR
```

**IMPORTANT**

An error may occur if:

- There are no logs to be displayed.
- The log files are inaccessible or an internal error occurred while processing the result.

**Command Syntax**

```
npu# show logs [filter | grep <string>]
```

**Privilege Level**

1

**Syntax Description**

| Parameter | Description | Presence | Default Value | Possible Values |
|---|---|---|---|---|
| `[filter \| grep <string>]` | Indicates the criteria for filtering the log messages to be displayed. | Optional | N/A | String |

**Command Modes**

Global command mode

### 3.3.12.1.4 Displaying the Current Log Destination

To view the current log destination, that is, whether logs are written to file or an external server, run the following command:

```
npu# show log destination
```

**IMPORTANT**

An error may occur if an internal error occurs when you execute this command.

| | |
|---|---|
| **Command Syntax** | **npu# show log destination** |
| **Privilege Level** | 1 |
| **Display Format** | Logfile(<file name>) : Enabled/Disabled<br>Log Server(<IP address>) : Enabled/Disabled |
| **Command Modes** | Global command mode |

### 3.3.12.1.5 Making a Backup of Log Files on the NPU Flash

The system stores a maximum of 1000 log and trace messages in the log file, after which the oldest messages are overwritten. This log file resides in the TFTP boot directory (/tftpboot/management/system_logs/) of the NPU. You can TFTP this file from the NPU flash. You can display the list of log files residing on the NPU flash. For details, refer Section 3.3.12.1.7.

In addition, logs written to file are not maintained after system reset. If you have enabled writing of logs to file, it is recommended that you periodically make a backup of log messages on the NPU flash.

**IMPORTANT**

You can display a list of log files that are currently residing on the NPU flash. For details, refer Section 3.3.12.1.7.

When you make a backup of log files on the NPU flash, the last 1000 log and trace messages are stored in a compressed file, which is saved on the NPU flash. There is no limit on the number of log files that can be saved unless there is inadequate space on the NPU flash.

**IMPORTANT**

Trace messages are also written to the same file as log messages (provided you have enabled writing of trace messages to file.) When you make a backup of log files written to file, the backup file also contains trace messages (provided you have enabled writing of trace messages to file). For more information about configuring traces, refer Section 3.11.1.1.

Run the following command to make a backup of the log and trace messages (written to file), on the NPU flash:

```
npu(config)# save log file <file name.gz>
```

When you run this command, the last 1000 log and trace messages are stored in the compressed file, which is saved on the NPU flash.

**IMPORTANT**

An error may occur if:

- You have specified the file name in an invalid format. Because the backup log file is a compressed file, always suffix the file name with **.gz**.
- The length of the file name has exceeded 255 characters.
- The system was unable to compress the file or save the compressed file to flash.
- A processing error has occurred.

**Command Syntax**

```
npu(config)# save log file <file name>
```

**Privilege Level**

10

**Syntax Description**

| Parameter | Description | Presence | Default Value | Possible Values |
|---|---|---|---|---|
| <file name> | Indicates the name of the compressed file that contains the last 1000 log and trace messages. Always suffix the file name with **.gz**. | Mandatory | N/A | <file name>.gz<br>file name string can contain 1 to 50 printable characters. |

| | |
|---|---|
| **Command Modes** | Global configuration mode |

### 3.3.12.1.6 Deleting Backup Log Files from the NPU Flash

You can delete the backup log files from the NPU flash. It is recommended that you periodically make a backup of these log files, and delete these from the NPU flash.

**IMPORTANT**

Trace and log messages are stored in the same backup file on the NPU flash. When you execute this procedure, trace messages are also deleted from the NPU flash. For details, refer to "Managing System-level Tracing" on page 667.

To delete log and trace backup files from the NPU flash, run the following command:

```
npu(config)# erase log file [<file name>]
```

**CAUTION**

Specify the file name if you want to delete a specific backup file. Otherwise all the backup files residing in the NPU flash are deleted.

**IMPORTANT**

An error may occur if:

- The file name that you have specified does not exist.
- A processing error has occurred.

| | |
|---|---|
| **Command Syntax** | `npu(config)# erase log file [<file name>]` |
| **Privilege Level** | 10 |

**Syntax Description**

| Parameter | Description | Presence | Default Value | Possible Values |
|---|---|---|---|---|
| `[<file name>]` | Indicates the name of the compressed log file to be deleted. If you do not specify the file name, all the log files residing in the NPU flash are deleted.<br>Always suffix the file name with **.gz**. | Optional | N/A | <file name>.gz |

**Command Modes**

Global configuration mode

#### 3.3.12.1.7 Displaying Log Files Residing on the NPU Flash

You can display a list of log files that are residing on the NPU flash. For details, refer Section 3.10.4.

### 3.3.12.2 Configuring Module-level Logging

You can configure logging (enable/disable) separately for the following modules, and define the severity level for which logging is required:

- System startup procedures
- NPU/AU upgrade procedures
- Fault management procedures
- System performance procedures
- Shelf management procedures
- WiMAX signaling protocols
- User interface
- AU management procedures

This section describes the commands to be used for:

- "Configuring the Log Severity Level" on page 354
- "Displaying Configuration Information for Module-level Logging" on page 356
- "Disabling Module-level Logging" on page 357


#### 3.3.12.2.1 Configuring the Log Severity Level

You can configure the severity level for logs to be generated for each module. This means that if an event occurs for a module for which the severity level is equal to or higher than the configured level, a log is generated. The following are the severity levels (highest to lowest) that can be configured for each module:

- Emergency
- Alert
- Critical
- Error
- Warning
- Notice
- Information

**IMPORTANT**

By default, logging is enabled for all modules, and the severity level is Error. The severity levels recorded in 4Motion log messages are defined in RFC 3164.

To specify the severity level for each module for which logs are to be created, run the following command:

```
npu(config)# log level
[{StartupMgr|SWDownload|FaultMgr|PerfMgr|ShelfMgr|SIGASN|UserIF|AU
Mgr}] {EMERG|ALERT|CRIT|ERROR|WARN|NOTICE|INFO}
```

The parameters in this command correspond to the system modules/procedures listed in the following table:

**Table 3-24: Modules for which Logging can be Enabled**

| Parameter | Refers to... |
|---|---|
| StartupMgr | System startup procedures |
| SWDownload | Software upgrade procedures |
| FaultMgr | Fault management procedures |
| ShelfMgr | Shelf management procedures |
| SIGASN | WiMAX signaling protocols |
| UserIF | User-initiated procedures |
| AUMgr | Internal processes used for managing AU |
| PerfMgr | Performance management procedures |

Specify the module name if you want to configure the severity level separately for this module. If you do not specify the name of the module, the severity level that you configure in this command is applied to all modules.

For example, run the following command if you want logs to be created for WiMAX signaling protocols when the severity level is Warning or higher:

```
npu(config)# log level SIGASN WARN
```

Or run the following command to set the severity level to Error for all modules:

```
npu(config)# log level ERROR
```

**NOTE**

You can display the currently configured severity levels for each module. For details, refer Section 3.3.12.2.2.

**Command Syntax**

```
npu(config)# log level
[{StartupMgr|SWDownload|FaultMgr|PerfMgr|ShelfMgr|SIGASN|UserIF|AUMgr}]
{EMERG|ALERT|CRIT|ERROR|WARN|NOTICE|INFO}
```

**Privilege Level**

10

**Syntax Description**

| Parameter | Description | Presence | Default Value | Possible Values |
|---|---|---|---|---|
| `[{StartupMgr\|SWDownload\|FaultMgr\|PerfMgr\|ShelfMgr\|SIGASN\|UserIF\|AUMgr}]` | Indicates the name of the module for which the severity level is to be specified.<br>If you do not specify any value for this parameter, the severity level that you specify is applied for all modules. For more information about these parameters, refer Table 3-24. | Optional | N/A | ■ StartupMgr<br>■ SWDownload<br>■ FaultMgr<br>■ PerfMgr<br>■ ShelfMgr<br>■ SIGASN<br>■ UserIF<br>■ AUMgr |
| `{EMERG\|ALERT\|CRIT\|ERROR\|WARN\|NOTICE\|INFO}` | Indicates the severity level to be applied to a particular or all modules. | Mandatory | Error | ■ EMERG<br>■ ALERT<br>■ CRIT<br>■ ERROR<br>■ WARN<br>■ NOTICE<br>■ INFO |

**Command Modes**

Global configuration mode

### 3.3.12.2.2 Displaying Configuration Information for Module-level Logging

To display the log level configured for one or all modules, run the following command.

**`npu(config)# show log level [{StartupMgr|SWDownload|FaultMgr|PerfMgr|ShelfMgr|SIGASN|UserIF|AUMgr}]`**

Specify the module for which you want to view the configured severity level. If you do not specify the name of the module, the log level configured for all modules is displayed.

**Command Syntax**

```
npu(config)# show log level
[{StartupMgr|SWDownload|FaultMgr|PerfMgr|ShelfMgr|SIGASN|UserIF|AUMgr}]
```

**Privilege Level**

1

**Syntax Description**

| Parameter | Description | Presence | Default Value | Possible Values |
|---|---|---|---|---|
| [{StartupMgr\|SWDownload\|FaultMgr\|PerfMgr\|ShelfMgr\|SIGASN\|UserIF\|AUMgr}] | Indicates the name of the module for which you want to view the configured severity level. For more information about these parameters, refer Table 3-24.<br>If you do not specify any value for this parameter, the severity level is displayed for all modules. | Optional | N/A | ■ StartupMgr<br>■ SWDownload<br>■ FaultMgr<br>■ PerfMgr<br>■ ShelfMgr<br>■ SIGASN<br>■ UserIF<br>■ AUMgr |

**Display Format**

```
Module Name     :   Log level
<Module Name>   :   <Log Level>
```

**Command Modes**

Global configuration mode

### 3.3.12.2.3 Disabling Module-level Logging

To disable logging for one or all system modules, run the following command:

```
npu(config)# no log level
[{StartupMgr|SWDownload|FaultMgr|PerfMgr|ShelfMgr|SIGASN|UserIF|AUMgr}]
```

Specify the name of the module if you want to disable logging for a specific module. If you do not specify the module name, logging is disabled for all modules.

**Command Syntax**

```
npu(config)# no log level
[{StartupMgr|SWDownload|FaultMgr|PerfMgr|ShelfMgr|SIGASN|UserIF|AUMgr}]
```

**Privilege Level**

10

**Syntax Description**

| Parameter | Description | Presence | Default Value | Possible Values |
|---|---|---|---|---|
| `[{StartupMgr\|SWDownload\|FaultMgr\|PerfMgr\|ShelfMgr\|SIGASN\|UserIF\|AUMgr}]` | Indicates the name of the module for which logging is to be disabled.<br>If you do not specify any value for this parameter, logging is disabled for all parameters. For more information about these modules, refer Table 3-24. | Optional | N/A | ■ StartupMgr<br>■ SWDownload<br>■ FaultMgr<br>■ PerfMgr<br>■ ShelfMgr<br>■ SIGASN<br>■ UserIF<br>■ AUMgr |

**Command Modes**

Global configuration mode

## 3.3.13 Configuring Performance Data Collection

You can configure 4Motion to periodically collect and store performance counters with respect to the following groups: