1 RBAC Commands

Command	Function
description	Configure the description of a role.
feature	Add a feature to a feature group.
interface policy deny	Prohibit a role from operating all interface resources.
permit interface	Allow a role to operate a specific interface resource.
permit vlan	Allow a role to operate a specific VLAN resource.
permit vrf	Allow a role to operate a specific VRF resource.
role enable	Enable the RBAC function.
role feature-group name	Configure a feature group and enter the specified feature group configuration mode.
role name	Configure a role and enter a specified role configuration mode.
rule	Configure rule permissions for a role.
show role	Show information about a specific role or all roles.
show role feature	Display the basic information or details about a specific feature or all features.
show role feature-group	Display the basic information or details about a specific feature group or all feature groups.
vlan policy deny	Prohibit a role from operating all VLAN resources on a device.
vrf policy deny	Prohibit a role from operating all VRF resources.

1.1 description

Function

Run the **description** command to configure the description of a role.

Run the **no** form of this command to restore the default description of a role.

Run the **default** form of this command to restore the default configuration.

By default, a predefined role is provided with a default description while a user-defined role is provided with no description.

Syntax

description *description*

no description

default description

Parameter Description

description: Description of a role. It is a string of 1 to 128 characters.

Command Modes

Role configuration mode

Default Level

15

Usage Guidelines

This command is used to configure the description of a role.

Examples

The following example configures description "admin role" for role **admin-role**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# role name admin-role
Hostname(config-role)# description admin role
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- role enable

- role name
- show role

1.2 feature

Function

Run the **feature** command to add a feature to a feature group.

Run the **no** form of this command to remove this configuration.
Run the **default** form of this command to restore the default configuration.

By default, a predefined feature group contains default features while a user-defined feature group contains no feature.

Syntax

feature *feature-name*

no feature *feature-name*

default feature *feature-name*

Parameter Description

feature-name: The feature to be added to a specified feature group. *feature-name* indicates the name of a feature predefined in the system and is case-sensitive.

Command Modes

Feature group configuration mode

Default Level

15

Usage Guidelines

This command is used to add a feature to a feature group.

Examples

The following example adds feature **aaa** to feature group **test-group**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# role feature-group name test-group
Hostname(config-role-featuregrp)# feature aaa
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- role enable
- role feature-group name
- show role feature-group

1.3 interface policy deny

Function

Run the **interface policy deny** command to prohibit a role from operating all interface resources.

Run the **no** form of this command to allow a role to operate all interface resources .

Run the **default** form of this command to restore the default configuration.

By default, a role has the permission to operate all interface resources.

Syntax

interface policy deny

no interface policy deny

default interface policy deny

Parameter Description

N/A

Command Modes

Role configuration mode

Default Level

15

Usage Guidelines

This command is used to prohibit a role from creating, deleting or applying all interface resources.

Examples

The following example prohibits the role **admin-role** from operating all interface resources.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# role name admin-role
Hostname(config-role)# interface policy deny
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **role enable**
- **role name**
- **show role**

1.4 permit interface

Function

Run the **permit interface** command to allow a role to operate a specific interface resource.

Run the **no** form of this command to prohibit a role from operating a specific interface resource or all interface resources.

Run the **default** form of this command to restore the default configuration.

By default, a role is prohibited from operating all interface resources.

Syntax

permit interface *interface-type interface-number-list*

no permit interface [*interface-type interface-number-list*]

default permit interface [*interface-type interface-number-list*]

Parameter Description

interface *interface-type interface-number-list*: Specifies the interface type and interface number list. An interface number list contains one or more interface numbers. Interface numbers are separated by a comma (,). You can specify an interface number range by connecting the first and the last interface numbers with a hyphen (-).

Command Modes

Role interface configuration mode

Default Level

15

Usage Guidelines

This command is used to allow a role to operate interface resources.

Examples

The following example allows role **admin-role** to operate GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# role name admin-role
Hostname(config-role)# interface policy deny
Hostname(config-role-interface)# permit interface gigabitethernet 0/1
```

The following example allows role **admin-role** to operate GigabitEthernet 0/2, GigabitEthernet 0/4, and GigabitEthernet 0/6.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# role name admin-role
Hostname(config-role)# interface policy deny
Hostname(config-role-interface)# permit interface gigabitethernet 0/2, 0/4, 0/6
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **role enable**
- **role name**
- **interface policy deny**
- **show role**

1.5 permit vlan

Function

Run the **permit vlan** command to allow a role to operate a specific VLAN resource.

Run the **no** form of this command to prohibit a role from operating a specific VLAN resource or all VLAN resources.

Run the **default** form of this command to restore the default configuration.

By default, a role is prohibited from operating all VLAN resources.

Syntax

permit vlan *vlan-list*

no permit vlan [*vlan-list*]

default permit vlan [*vlan-list*]

Parameter Description

vlan-list: VLAN list. The value range is from 1 to 4094. The VLAN list can contain one or more VLANs. VLAN IDs are separated by a comma (,). You can specify a VLAN range by connecting the first and the last VLAN IDs with a hyphen (-).

Command Modes

Role VLAN configuration mode

Default Level

15

Usage Guidelines

This command is used to allow a role to operate VLAN resources.

Examples

The following example allows the role **admin-role** to operate VLAN 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# role name admin-role
Hostname(config-role)# vlan policy deny
Hostname(config-role-vlan)# permit vlan 1
```

The following example allows the role **admin-role** to operate VLAN 1, VLAN 3, and VLAN 5.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# role name admin-role
Hostname(config-role)# vlan policy deny
Hostname(config-role-vlan)# permit vlan 1,3,5
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **role enable**
- **role name**
- **vlan policy deny**
- **show role**

1.6 permit vrf

Function

Run the **permit vrf** command to allow a role to operate a specific VRF resource.

Run the **no** form of this command to prohibit a role from operating a specific VRF resource or all VRF resources.

Run the **default** form of this command to restore the default configuration.

By default, a role is prohibited from operating all VRF resources.

Syntax

permit vrf *vrf-name*

no permit vrf [*vrf-name*]

default permit vrf [*vrf-name*]

Parameter Description

vrf-name: VRF instance name.

Command Modes

Role VRF configuration mode

Default Level

15

Usage Guidelines

This command allows a role to operate VRF resources on a device.

Examples

The following example allows the role **admin-role** to operate VRF instance **test** .

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# role name admin-role
Hostname(config-role)# vrf policy deny
Hostname(config-role-vrf)# permit vrf test
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **role enable**
- **role name**
- **vrf policy deny**
- **show role**

1.7 role enable

Function

Run the **role enable** command to enable the RBAC function.

Run the **no** form of this command to disable this feature.

Run the **default** form of this command to restore the default configuration.

The RBAC function is disabled by default.

Syntax

role enable

no role enable

default role enable

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

15

Usage Guidelines

This command is used to enable or disable the RBAC function.

Examples

The following example enables the RBAC function.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# role enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.8 role feature-group name

Function

Run the **role feature-group name** command to configure a feature group and enter the specified feature group configuration mode.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

By default, feature groups **L2** and **L3** are predefined in the system, and these feature groups contain features.

Syntax

role feature-group name *group-name*

no role feature-group name *group-name*

default role feature-group name *group-name*

Parameter Description

group-name: Name of a feature group. It is a case-sensitive string of 1 to 32 characters.

Command Modes

Global configuration mode

Default Level

15

Usage Guidelines

This command is used to create a feature group and enter the feature group configuration mode.

The system predefines feature groups **L2** and **L3**. **L2** contains all commands for functions related to L2 protocols, and **L3** contains all commands for functions related to L3 protocols. The predefined feature groups cannot be deleted or modified. Users can customize up to 64 feature groups and configure features for the feature groups.

Examples

The following example configures feature group **test-group** for a role, and enters the feature group configuration mode.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# role feature-group name test-group
Hostname(config-role-featuregrp)#
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **role enable**
- **show role feature-group**

1.9 role name

Function

Run the **role name** command to configure a role and enter a specified role configuration mode.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

By default, the system predefines 18 roles, including **network-admin**, **network-operator**, and **priv-***n* (0–15). Each role is granted with specific operation permissions.

Syntax

role name *role-name*

no role name *role-name*

default role name *role-name*

Parameter Description

role-name: Name of a role. It is a case-sensitive string of 1 to 64 characters.

Command Modes

Global configuration mode

Default Level

15

Usage Guidelines

This command is used to create a role and enter the role configuration mode.

The system predefines 18 roles, including **network-admin**, **network-operator**, and **priv-***n* (0–15).

System predefined roles cannot be deleted by running the **no** command. The default permission of only the **priv-***n* (0–13) role can be restored by running the **default** command.

Permissions can be added to the **priv-***n* (0–13) role only. System predefined permissions cannot be deleted, and permissions of other roles cannot be modified.

Users can customize up to 64 roles and configure permissions for the roles.

Examples

The following example configures role **admin-role** and enters the role configuration mode.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# role name admin-role
Hostname(config-role)#
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **role enable**
- **show role**

1.10 rule

Function

Run the **rule** command to configure rule permissions for a role.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

By default, predefined roles have predefined rule permissions while user-defined roles have no rule permissions.

Syntax

rule *rule-number* { **permit** | **deny** } { **command** *command-string* | { **read** | **write** | **execute** }* { **feature** [*feature-name*] | **feature-group** *feature-group-name* } }

no rule { *rule-number* | **all** }

default rule { *rule-number* | **all** }

Parameter Description

rule-number: Rule ID. The value range is from 1 to 256.

permit: Allows the user to execute the specified command.

Deny: Prohibits the user from executing the specified command.

command *command-string*: Configures command-based rules. *command-string* indicates a case-sensitive command string of 1 to 128 characters. It can be a specific command or multiple commands that are separated by a semicolon (;). It can also be a type of commands represented by an asterisk (*) wildcard. *command-string* can contain spaces and all printable characters.

read: Indicates a read command, that is, a type of commands that can display system configurations and maintenance information, such as the **show**, **dir**, and **more** commands.

write: Indicates a write command, that is, a type of commands that can configure the system, for example, the **logging on** command.

execute: Indicates an execution command, that is, a type of commands that can execute a specific program or function, for example, the **ping** command.

feature *feature-name*: Configures feature-based rules. *feature-name* indicates the name of a feature predefined in the system and is case-sensitive. If no feature name is specified, the command applies to all features.

feature-group *feature-group-name*: Configures feature group-based rules. *feature-group-name* indicates the name of a feature group. It is a case-sensitive string of 1 to 32 characters.

all: Specifies all permission rules.

Command Modes

Role configuration mode

Default Level

15

Usage Guidelines

This command is used to configure rule permissions for a role. Note:

- During rule configuration, if the specified rule number does not exist, create a rule; otherwise, modify the rule corresponding to the rule number. The modified rule supports newly authenticated users only.
- A user role is allowed to create multiple rules, and permissions executable by this role is a union set of these rules. If permissions defined by these rules conflict with each other, rules with larger serial numbers prevail. For example, if command A is prohibited by rule 1, and command B is prohibited by rule 2, but command A is allowed by rule 3, rule 2 and rule 3 finally take effect. Specifically, command A is allowed and command B is prohibited.
- Predefined rules for predefined roles cannot be deleted or modified. If there is a conflict between system predefined rules and user-defined rules, user-defined rules prevail.
- Up to 256 rules can be configured for each role. A maximum of 1024 rules are configured for all roles on the device.

To configure command-based rules, follow the rules below:

- Division of segments
  - To describe a multi-level mode command, divide the command character string into multiple segments by a semicolon (;). Each segment represents one or a series of commands. The command in the latter segment is used to execute the mode of a command in the preceding segment.
  - A segment must contain at least one printable character.
- Use of semicolons
  - To describe a multi-level mode command, divide the command segments with a semicolon. For example, the character string **config ; logging on** is used to grant a permission over the **logging on** command in configuration mode.
  - The semicolon in the last command segment indicates that the permission is granted over the current mode command. For example, the character string **config ; interface *** grants a permission over only the command in interface configuration mode.
  - The absence of a semicolon in the last command segment indicates that permissions are granted over the current command mode and all commands in this mode. For example, the character string **config ; interface *** is used to grant permissions over all commands in interface mode.
- Use of asterisks
  - Each command segment can contain at least one asterisk (*). An asterisk resides either in the middle or at both ends of a command segment. Each asterisk serves to fuzzily match a command. For example, the character string **config ; *** is used to grant permissions over all commands in configuration mode. The character string **config ; logging * flush** is used to grant a permission over a command starting with

  logging and ending with **flush** in configuration mode. The character string **config ; logging *** is used to grant permissions over all the commands starting with **logging** in configuration mode.

  - When an asterisk resides in the middle of a command segment and the asterisk is used to match the command, the command is matched up to only the first asterisk in the middle, and the subsequent command segments are all considered matched. An execution command must be fully matched.

- Matching of keyword prefixes
  - A prefix matching algorithm is used for the matching between the command keyword and the command character string. That is, if the first several consecutive characters or all characters of a keyword in the command line match the keyword defined in a rule, the command line matches this rule. Therefore, a command character string may include a partial or complete command keyword. For example, if the rule **rule 1 deny command show ssh** is effective, the **show ssh** and **show ssh-session** commands are disabled.

Examples

The following example configures role **admin-role**, which has rule permissions to run all commands in configuration mode.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# role name admin-role
Hostname(config-role)# rule 1 permit command config ; *
```

The following example configures role **admin-role**, which has the permission to read feature **aaa**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# role name admin-role
Hostname(config-role)# rule 2 permit read feature aaa
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- role enable
- role name
- show role

1.11 show role

Function

Run the **show role** command to show information about a specific role or all roles.

Syntax

show role [**name** *role-name*]

Parameter Description

name *role-name*: Displays information about a specific role.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

This command is used to display information about a specific role or all roles.

Examples

The following example displays information about the role **network-admin**.

```
Hostname> enable
Hostname# show role name network-admin
Role: network-admin
  Description: Predefined network admin role has access to all commands
  Interface policy: permit (default)
  VLAN policy: permit (default)
  Vrf policy: permit (default)
  -------------------------------------------------------------------
  Rule    Perm   Type  Scope         Entity
  -------------------------------------------------------------------
  sys-1   permit       command       *
  R:Read W:Write X:Execute
```

Table 1-1Output Fields of the show role name Command

Field	Description
Role	Name of a role.
Description	Description of a role.
Interface policy	Allows a role to operate all interface resources.
VLAN policy	Allows a role to operate all VLAN resources.
Vrf policy	Allows a role to operate all VRF resources.
Rule	Rule ID.
Perm	Allow or prohibit.
Type	Command type. This field is set to **RWX**, indicating that the permissions to read, write, and execute are granted to the command.

Scope	Configures rules. This field is set to the following values: ● **command**: command-based rules ● **feature**: feature-based rules ● **feature-group**: feature-group-based rules
Entity	Rule entity.

Notifications

N/A

Platform Description

N/A

Related Commands

- role name

1.12 show role feature

Function

Run the **show role feature** command to display the basic information or details about a specific feature or all features.

Syntax

show role feature [{ **detail** | **name** *feature-name* }]

Parameter Description

detail: Displays the details about all features.

name *feature-name*: Displays the basic information about a specific feature.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

This command is used to display the basic information or details about a specific feature or all features.

Examples

The following example displays the basic information about all features.

```
Hostname> enable
Hostname# show role feature
Feature: aaa                              (Aaa related commands)
Feature: bfd                              (Bfd related commands)
Feature: bgp                              (Bgp related commands)
```

```
Feature: bridge                           (Bridge related commands)
Feature: ce-mgmt                          (Ce mgmt related commands)
```

Table 1-1Output Fields of the show role feature Command

Field	Description
Feature	Name of a feature

The following example displays the details about all features.

```
Hostname> enable
Hostname# show role feature detail
Feature: aaa                              (Aaa related commands)
  undebug username    (W)
  undebug aaa *    (W)
  debug username    (W)
  debug aaa *    (W)
  clear aaa *    (W)
  username *    (W)
  show aaa *    (R)
  configure ; username *    (W)
  configure ; aaa *    (W)
  configure ; aaa domain * ; authentication *    (W)
  configure ; aaa domain * ; accounting *    (W)
  configure ; aaa domain * ; authorization *    (W)
  configure ; aaa domain * ; state *    (W)
  configure ; aaa domain * ; username-format *    (W)
  configure ; aaa domain * ; access-limit *    (W)
Feature: bfd                              (Bfd related commands)
  undebug bfd *    (W)
  debug bfd *    (W)
  show sbfd *    (R)
  show bfd *    (R)
  configure ; sbfd *    (W)
  configure ; bfd *    (W)
  configure ; interface * ; bfd *    (W)
```

Table 1-2Output Fields of the show role feature detail Command

Field	Description
Feature	Name of a feature
(W)	Write command
(R)	Read command
(X)	Execution command

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.13 show role feature-group

Function

Run the **show role feature-group** command to display the basic information or details about a specific feature group or all feature groups.

Syntax

show role feature-group [{ **detail** | **name** *group-name* [**detail**] }]

Parameter Description

detail: Displays the details about all feature groups.

name *group-name*: Displays the basic information about a specific feature group.

detail: Displays the details about a specific feature group.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

This command is used to display the basic information or details about a specific feature group or all feature groups.

Examples

The following example displays the basic information about the feature group **test**.

```
Hostname> enable
Hostname# show role feature-group name test
Feature group: test
Feature: aaa                              (Aaa related commands)
Feature: snmpd                            (Snmpd related commands)
Feature: syslogd                          (Syslogd related commands)
```

Table 1-1Output Fields of the show role feature-group name Command

Field	Description

Feature group	Name of a feature group
Feature	Name of a feature

Notifications

N/A

Platform Description

N/A

Related Commands

- role feature-group name

1.14 vlan policy deny

Function

Run the **vlan policy deny** command to prohibit a role from operating all VLAN resources on a device.

Run the **no** form of this command to allow a role to operate all VLAN resources on a device.

Run the **default** form of this command to restore the default configuration.

By default, a role has the permission to operate all VLAN resources on a device.

Syntax

vlan policy deny

no vlan policy deny

default vlan policy deny

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

15

Usage Guidelines

This command is used to prohibit a role from creating, deleting or applying all VLAN resources.

Examples

The following example prohibits the role **admin-role** from operating all VLAN resources.

```
Hostname> enable
Hostname# configure terminal
```

```
Hostname(config)# role name admin-role
Hostname(config-role)# vlan policy deny
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- role enable
- role name
- show role

1.15 vrf policy deny

Function

Run the **vrf policy deny** command to prohibit a role from operating all VRF resources.

Run the **no** form of this command to allow a role to operate all VRF resources.

Run the **default** form of this command to restore the default configuration.

By default, a role has the permission to operate all VRF resources.

Syntax

vrf policy deny

no vrf policy deny

default vrf policy deny

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

15

Usage Guidelines

This command is used to prohibit a role from creating, deleting or applying all VRF resources.

Examples

The following example prohibits the role **admin-role** from operating all VRF resources.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# role name admin-role
Hostname(config-role)# vrf policy deny
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- role enable
- role name
- show role