Contents

1 Configuring the SCC

1.1 Overview

The Security Control Center (SCC) provides common configuration methods and policy integration for various access control and network security services, so that these services can coexist on one device to meet diversified access and security control requirements in various scenarios.

Typical access control services include 802.1x, web authentication, Address Resolution Protocol (ARP) check, and IP source guard, and typical network security services include access control list (ACL), NFPP, and gateway-targeted ARP spoofing prevention. When two or more access control or network security services are enabled on the same device, the SCC coordinates coexistence based on related policies.

1.2 Configuration Task Summary

All the configuration tasks below are optional. Select the configuration tasks as required.

- Configuring Authentication-Exempted VLANs
- Configuring the IPv4 User Capacity
- Configuring Authenticated User Migration

1.3 Configuring Authentication-Exempted VLANs

1.3.1 Overview

After an authentication-exempted virtual local area network (VLAN) is configured, users in this VLAN can access the Internet without 802.1x or web authentication. When the device detects that a received packet is destined for an authentication-exempted VLAN, the device skips authentication.

The authentication-exempted VLAN function aims to provide easy and convenient network access experience for special groups in networks that require authentication. For example, the headmaster's office in a campus network is configured to be within an authentication-exempted VLAN to ensure network access without authentication.

1.3.2 Restrictions and Guidelines

- When an authentication-exempted VLAN is configured, ensure that the ACL also permits the VLAN. The authentication-exempted VLAN function exempts user packets only from authentication detection. User packets still need to undergo ACL detection. If a specified user or VLAN is denied in the ACL, the specified user or users in the specified VLAN cannot access the Internet.
- A maximum of 100 authentication-exempted VLANs can be configured.
- Configuring authentication-exempted VLANs occupies system resources. If access authentication is disabled on a device, the authentication-exempted VLAN function is meaningless and needs to be disabled.

1.3.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure authentication-exempted VLANs.

direct-vlan *vlan-list*

No authentication-exempted VLAN is configured by default.

1.4 Configuring the IPv4 User Capacity

1.4.1 Overview

The IPv4 user capacity is used to limit the maximum number of IPv4 access users on a port of the device. When the total number of IPv4 access users on a port reaches the limit, new users cannot access the network over this port. You need to select a proper user capacity based on the actual environment to guard against brutal force impacts from unauthorized users and improve the operational stability of the device.

1.4.2 Restrictions and Guidelines

IPv4 users include those generated through 802.1x authentication, web authentication, and other binding functions. IPv4 users on a port may be generated over the port or globally. For example, when a global IPv4 user is bound to a port by running the corresponding command, the user is also calculated as a user on the port.

1.4.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure the IPv4 user capacity on a port.

nac-author-user maximum *max-user-number*

The IPv4 user capacity on a port is not limited by default.

1.5 Configuring Authenticated User Migration

1.5.1 Overview

In actual scenarios, access users usually pass authentication and get online through one physical location, and then switch to another physical location for office or entertainment. For example, an enterprise employee takes a tablet from one office to another office to access the Internet by directly removing the network cable instead of getting offline proactively. If the authenticated user migration function is not configured, the employee cannot pass authentication to access the Internet in the other office because the original account does not get offline.

By default, 802.1x and web authentication users cannot switch from one physical location (access port+VLAN) to another to perform authentication and access the Internet again if they do not get offline. The authenticated user migration function allows users to realize this.

When authenticated user migration is enabled, the 802.1x or web authentication module of the device detects that the port or VLAN corresponding to a user's media access control (MAC) address has changed. Then, the user is forced offline and needs to be authenticated again before getting online. This prevents malicious users from forging online users' MAC addresses to access the Internet and causing authenticated users being forced offline. The authenticated user migration function determines the MAC address authenticity. For a user who gets online through web authentication or 802.1x authentication with IP authorization, the 802.1x or web authentication module sends an ARP request to the original physical location of the user if detecting that the same MAC address is online in another VLAN or on another port. If no response is received within the specified time, the module determines that the user's location has changed and the migration is allowed.

1.5.2 Restrictions and Guidelines

- The authenticated user migration function requires a check of users' MAC addresses, and is invalid for users who have IP addresses only.
- When both 802.1x authentication and port security are enabled on a port, and port security and 802.1x authentication users get online simultaneously, 802.1x authenticated users will fail to be migrated to another port to get online because the same MAC address cannot go online through different ports.
- The user online detection function can kick users offline. When the authentication user migration function is not configured and a user does not proactively get offline, the user may be kicked offline by the online detection function and can implement authentication and get online in another physical location.
- When an online authenticated user moves to a new physical location, the user needs to perform 802.1x or web authentication again.

1.5.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable authenticated user migration.

station-move permit

Authenticated user migration is disabled by default.

1.6 Monitoring

Run the **show** commands to check the running status of a configured function to verify the configuration effect.

Run the **debug** commands to output debugging information.

⚠ **Notice**

The output debugging information occupies system resources. Therefore, disable the debugging switch immediately after use.

Table 1-1 Monitoring

Command	Purpose
show direct-vlan	Displays authentication-exempted VLAN configurations.
show nac-author-user [**interface** *interface-type interface-number*]	Displays IPv4 user entries on a port.
show access-control packet statistics [**interface** *interface-type interface-number* | **vlan** *vlan-id*]	Displays statistics about packets filtered due to access control.
debug scc event	Debugs the SCC running process.
debug scc user	Debugs SCC user entries.
debug scc acl-show summary	Debugs ACL summary stored in the SCC delivered by various services.
debug scc acl-show all	Debugs all ACLs stored in the SCC.