Contents

Configuring portal authentication

The term "interface" in this chapter refers to VLAN interfaces.

Overview

Portal authentication controls user access to the Internet. Portal authenticates a user by the username and password the user enters on a portal authentication page. Therefore, portal authentication is also known as Web authentication. When portal authentication is deployed on a network, an access device redirects unauthenticated users to the website provided by a portal Web server. The users can access the resources on the website without authentication. If the users want to access the Internet, they must pass authentication on the website.

Portal authentication is classified into the following types:

- **Active authentication**—Users visit the authentication website provided by the portal Web server and enter their username and password for authentication.
- **Forced authentication**—Users are redirected to the portal authentication website for authentication when they visit other websites.

Portal authentication flexibly imposes access control on the access layer and vital data entries. It has the following advantages:

- Allows users to perform authentication through Web pages without installing client software.
- Provides ISPs with diversified management choices and extended functions. For example, the ISPs can place advertisements, provide community services, and publish information on the authentication page.
- Supports multiple authentication modes. For example, re-DHCP authentication implements a flexible address assignment scheme and saves public IP addresses. Cross-subnet authentication can authenticate users who reside in a different subnet than the access device.

The device supports Portal 1.0, Portal 2.0, and Portal 3.0.

Extended portal functions

By forcing patching and anti-virus policies, extended portal functions help hosts to defend against viruses. Portal supports the following extended functions:

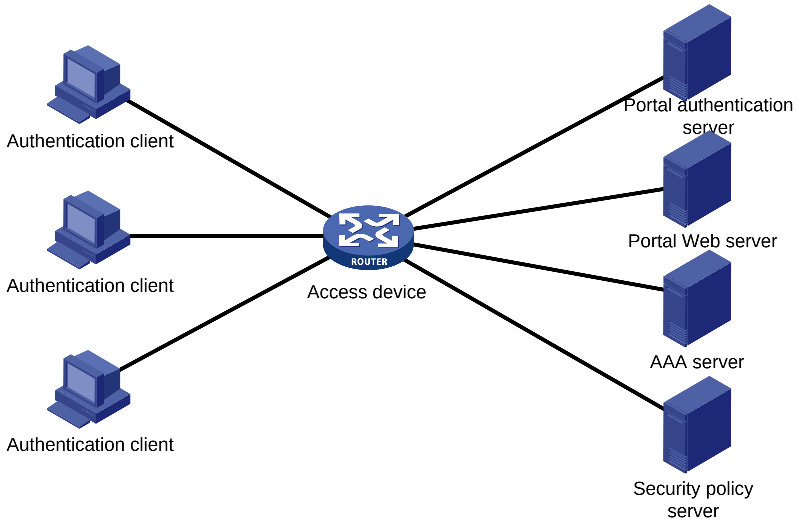
- **Security check**—Detects after authentication whether or not a user host installs anti-virus software, virus definition file, unauthorized software, and operating system patches.
- **Resource access restriction**—Allows an authenticated user to access certain network resources such as the virus server and the patch server. Users can access more Internet resources after passing security check.

Security check must cooperate with the H3C IMC security policy server and the iNode client.

Portal system components

A typical portal system consists of these basic components: authentication client, access device, portal authentication server, portal Web server, AAA server, and security policy server.

Figure 1 Portal system components



Authentication client

An authentication client is a Web browser that runs HTTP/HTTPS or a user host that runs a portal client application. Security check for the user host is implemented through the interaction between the portal client and the security policy server.

Access device

An access device refers to a broadband access device such as a switch or a router. An access device has the following functions:

- Redirects all HTTP requests of unauthenticated users to the portal Web server.
- Interacts with the portal authentication server and the AAA server to complete authentication, authorization, and accounting.
- Allows users that pass portal authentication to access authorized Internet resources.

Portal authentication server

The portal authentication server receives authentication requests from authentication clients and interacts with the access device to authenticate users.

Portal Web server

The portal Web server pushes the Web authentication page to authentication clients and forwards user authentication information (username and password) to the portal authentication server. The access device also redirects HTTP requests from unauthenticated users to the portal Web server.

The portal Web server can be integrated with the portal authentication server or an independent server.

AAA server

The AAA server interacts with the access device to implement authentication, authorization, accounting for portal users. Now only a RADIUS server can act as an AAA server in a portal system.

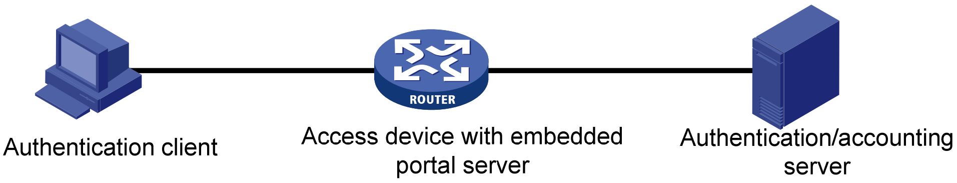
Security policy server

The security policy server interacts with the portal client and the access device for security check and authorization for users.

Portal system using the local portal Web server

The access device supports the local portal Web server feature. Using this feature, the access device also acts as the portal Web server and the portal authentication server to perform local portal authentication on portal users. In this case, the portal system consists of only three components: authentication client, access device, and authentication/accounting server, as shown in Figure 2.

Figure 2 Portal system using the local portal Web server


Authentication client
ROUTER
Access device with embedded portal server
Authentication/accounting server

The authentication client cannot be an H3C iNode client. Local portal authentication only supports authenticating Web clients.

No security policy server is needed because local portal authentication does not support extended portal functions.

The local portal Web server feature implements only some simple portal server functions. It only allows users to log in and log out through the Web interface. It cannot take the place of independent portal Web and authentication servers.

Client and local portal Web server interaction protocols

HTTP and HTTPS can be used for interaction between an authentication client and a local portal Web server. If HTTP is used, there are potential security problems because HTTP packets are transferred in plain text. If HTTPS is used, secure data transmission is ensured because HTTP packets are secured by SSL.

Portal page customization

To perform local portal authentication, you must customize a set of authentication pages that the device will push to users. You can customize multiple sets of authentication pages, compress each set of the pages to a .zip file, and upload the compressed files to the storage medium of the device. On the device, you must specify one of the files as the default authentication page file by using the **default-logon-page** command.

For more information about authentication page customization, see "Customizing authentication pages." For more information about the default-logon-page command, see Security Command Reference.

Interaction between portal system components

The components of a portal system interact as follows:

1. An unauthenticated user initiates authentication by accessing an Internet website through a Web browser. When receiving the HTTP request, the access device redirects it to the Web authentication page provided by the portal Web server. The user can also visit the authentication website to log in. The user must log in through the H3C iNode client for extended portal functions.
2. The user enters the authentication information on the authentication page/dialog box and submits the information. The portal Web server forwards the information to the portal authentication server. Then the portal authentication server processes the information and forwards it to the access device.
3. The access device interacts with the AAA server to implement authentication, authorization, accounting for the user.

4. If security policies are not imposed on the user, the access device allows the authenticated user to access the Internet. If security policies are imposed on the user, the portal client, the access device, and the security policy server interact to check the user host. If the user passes the security check, the security policy server authorizes the user to access resources based on the check result. Portal authentication through Web does not support security check for users. To implement security check, the client must be the H3C iNode client.

NOTE:

Portal authentication supports NAT traversal whether it is initiated by a Web client or an H3C iNode client. NAT traversal must be configured when the portal client is on a private network and the portal server is on a public network. As a best practice for portal authentication with NAT traversal, use an interface's public IP address as the source address of outgoing portal packets.

Portal authentication modes

Portal authentication has three modes: direct authentication, re-DHCP authentication, and cross-subnet authentication. In direct authentication and re-DHCP authentication, no Layer 3 forwarding devices exist between the authentication client and the access device. In cross-subnet authentication, Layer 3 forwarding devices can exist between the authentication client and the access device.

Direct authentication

A user manually configures a public IP address or obtains a public IP address through DHCP. Before authentication, the user can access only the portal Web server and predefined authentication-free websites. After passing authentication, the user can access other network resources. The process of direct authentication is simpler than that of re-DHCP authentication.

Re-DHCP authentication

Before a user passes authentication, DHCP allocates an IP address (a private IP address) to the user. The user can access only the portal Web server and predefined authentication-free websites. After the user passes authentication, DHCP reallocates an IP address (a public IP address) to the user. The user then can access other network resources. No public IP address is allocated to users who fail authentication. Re-DHCP authentication saves public IP addresses. For example, an ISP can allocate public IP addresses to broadband users only when they access networks beyond the residential community network.

Only the H3C iNode client supports re-DHCP authentication. IPv6 portal authentication does not support the re-DHCP authentication mode.

Cross-subnet authentication

Cross-subnet authentication is similar to direct authentication, except it allows Layer 3 forwarding devices to exist between the authentication client and the access device.

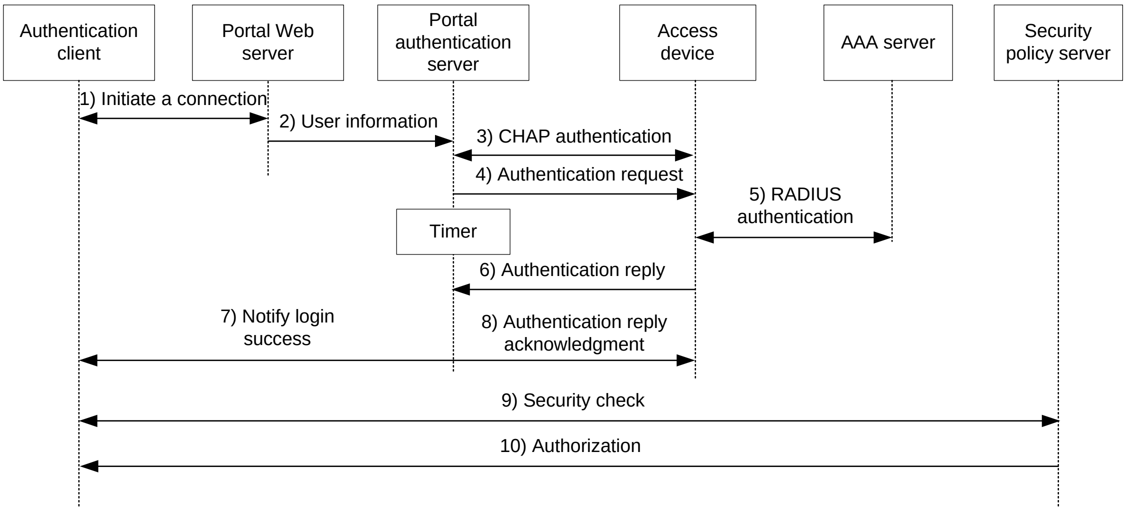
In direct authentication, re-DHCP authentication, and cross-subnet authentication, a user's IP address uniquely identifies the user. After a user passes authentication, the access device generates an ACL for the user based on the user's IP address to control forwarding of the packets from the user. Because no Layer 3 forwarding device exists between authentication clients and the access device in direct authentication and re-DHCP authentication, the access device can learn the user MAC addresses. The access device can enhance its capability of controlling packet forwarding by using the learned MAC addresses.

Portal authentication process

Direct authentication and cross-subnet authentication share the same authentication process. Re-DHCP authentication has a different process as it has two address allocation procedures.

Direct authentication/cross-subnet authentication process (with CHAP/PAP authentication)

Figure 3 Direct authentication/cross-subnet authentication process



The direct/cross-subnet authentication process is as follows:

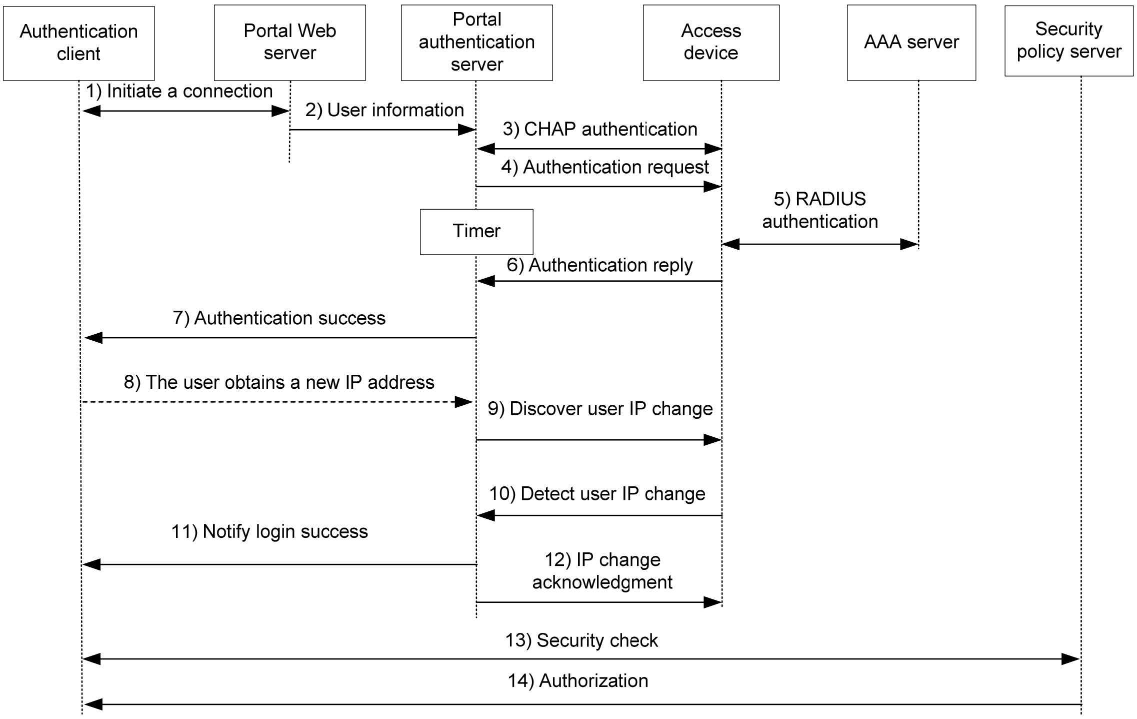
1. A portal user access the Internet through HTTP, and the HTTP packet arrives at the access device.
    - If the packet matches a portal free rule, the access device allows the packet to pass.
    - If the packet does not match any portal-free rule, the access device redirects the packet to the portal Web server. The portal Web server pushes the Web authentication page to the user for him to enter his username and password.
2. The portal Web server submits the user authentication information to the portal authentication server.
3. The portal authentication server and the access device exchange CHAP messages. This step is skipped for PAP authentication. The portal authentication server decides the method (CHAP or PAP) to use.
4. The portal authentication server adds the username and password into an authentication request packet and sends it to the access device. Meanwhile, the portal authentication server starts a timer to wait for an authentication reply packet.
5. The access device and the RADIUS server exchange RADIUS packets.
6. The access device sends an authentication reply packet to the portal authentication server to notify authentication success or failure.
7. The portal authentication server sends an authentication success or failure packet to the client.
8. If the authentication is successful, the portal authentication server sends an authentication reply acknowledgment packet to the access device.

If the client is an iNode client, the authentication process includes step 9 and step 10 for extended portal functions. Otherwise the authentication process is complete.

9. The client and the security policy server exchange security check information. The security policy server detects whether or not the user host installs anti-virus software, virus definition files, unauthorized software, and operating system patches.
10. The security policy server authorizes the user to access certain network resources based on the check result. The access device saves the authorization information and uses it to control access of the user.

Re-DHCP authentication process (with CHAP/PAP authentication)

Figure 4 Re-DHCP authentication process



The re-DHCP authentication process is as follows:

Step 1 through step 7 are the same as those in the direct authentication/cross-subnet authentication process.

8. After receiving the authentication success packet, the client obtains a public IP address through DHCP. The client then notifies the portal authentication server that it has a public IP address.

9. The portal authentication server notifies the access device that the client has obtained a public IP address.

10. The access device detects the IP change of the client through DHCP and then notifies the portal authentication server that it has detected an IP change of the client IP.

11. After receiving the IP change notification packets sent by the client and the access device, the portal authentication server notifies the client of login success.

12. The portal authentication server sends an IP change acknowledgment packet to the access device.

Step 13 and step 14 are for extended portal functions.

13. The client and the security policy server exchanges security check information. The security policy server detects whether or not the user host installs anti-virus software, virus definition files, unauthorized software, and operating system patches.

14. The security policy server authorizes the user to access certain network resources based on the check result. The access device saves the authorization information and uses it to control access of the user.

Portal configuration task list

Tasks at a glance
(Required.) Configuring a portal authentication server

Tasks at a glance
(Required.) Configuring a portal Web server
(Required.) Enabling portal authentication on an interface
(Required.) Referencing a portal Web server for an interface
(Optional.) Controlling portal user access • Configuring a portal-free rule • Configuring an authentication source subnet • Configuring an authentication destination subnet • Setting the maximum number of portal users • Specifying a portal authentication domain • Enabling outgoing packets filtering on a portal-enabled interface
(Optional.) Enabling outgoing packets filtering on a portal-enabled interface
(Optional.) Configuring portal detection features • Configuring online detection of portal users • Configuring portal authentication server detection • Configuring portal Web server detection • Configuring portal user synchronization
(Optional.) Configuring the portal fail-permit feature
(Optional.) Configuring BAS-IP for portal packets sent to the portal authentication server
(Optional.) Applying a NAS-ID profile to an interface
(Optional.) Enabling portal roaming
(Optional.) Logging out portal users
(Optional.) Configuring the local portal Web server feature

Configuration prerequisites

The portal feature provides a solution for user identity authentication and security check. To complete user identity authentication, portal must cooperate with RADIUS.

The prerequisites for portal authentication configuration are as follows:

- The portal authentication server, portal Web server, and RADIUS server have been installed and configured properly.
- To use the re-DHCP portal authentication mode, make sure the DHCP relay agent is enabled on the access device, and the DHCP server is installed and configured properly.
- The portal client, access device, and servers can reach each other.
- To use the remote RADIUS server, configure usernames and passwords on the RADIUS server, and configure the RADIUS client on the access device. For information about RADIUS client configuration, see "Configuring AAA."
- To implement extended portal functions, install and configure CAMS EAD or IMC EAD. Make sure the ACLs configured on the access device correspond to the isolation ACL and the security ACL on the security policy server. For information about security policy server configuration on the access device, see "Configuring AAA." For installation and configuration about the security policy server, see *CAMS EAD Security Policy Component User Manual* or *IMC EAD Security Policy Help*.

Configuring a portal authentication server

Perform this task to configure the following portal authentication server parameters:

- IP address of the portal authentication server
- VPN instance of the portal authentication server
- Shared encryption key used between the device and the portal authentication server
- Destination UDP port number used by the device to send unsolicited portal packets to the portal authentication server

The device supports multiple portal authentication servers.

Do not delete a portal authentication server in use. Otherwise, users authenticated by that server cannot log out normally.

To configure a portal authentication server:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Create a portal authentication server, and enter its view.	**portal server** *server-name*	By default, no portal authentication server is created.
3. Specify the IP address of the portal authentication server.	• To specify an IPv4 portal server: **ip** *ipv4-address* [**vpn-instance** *vpn-instance-name*] [**key** { **cipher** | **simple** } *key-string*] • To specify an IPv6 portal server: **ipv6** *ipv6-address* [**vpn-instance** *vpn-instance-name*] [**key** { **cipher** | **simple** } *key-string*]	Specify an IPv4 portal authentication server, an IPv6 authentication portal server, or both. By default, no portal authentication server is specified.
4. (Optional.) Configure the UDP port used by the device to send unsolicited portal packets to the portal authentication server.	**port** *port-id*	By default, the UDP port number is 50100. This port number must be the same as the listening port number specified on the portal authentication server.

Configuring a portal Web server

Perform this task to configure the following portal Web server parameters:

- VPN instance of the portal Web server
- URL of the portal Web server
- Parameters carried in the URL when the device redirects the URL to users

The device supports multiple portal Web servers.

To configure a portal Web server:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Create a portal Web server and enter its view.	**portal web-server** *server-name*	By default, no portal Web server is created.

Step	Command	Remarks
3. Specify the VPN instance to which the portal Web server belongs.	**vpn-instance** *vpn-instance-name*	By default, the portal Web server belongs to the public network.
4. Specify the URL of the portal Web server.	**url** *url-string*	By default, no URL is specified.
5. Configure the parameters to be carried in the URL when the device redirects it to users.	**url-parameter** *param-name* { **original-url** | **source-address** | **source-mac** | **value** *expression* }	By default, no redirection URL parameters are configured.

Enabling portal authentication on an interface

You must first enable portal authentication on an access interface before it can perform portal authentication for connected clients.

When a portal-enabled interface receives a portal packet, it checks the source IP address and VPN information of the packet. If the packet matches a locally configured portal authentication server, the interface regards the packet valid and sends an authentication response packet to the portal authentication server. Otherwise, the interface drops the packet. After a user logs in to the device, the user interacts with the portal authentication server as needed.

Configuration restrictions and guidelines

When you enable portal authentication on an interface, follow these restrictions and guidelines:

- Make sure the interface has a valid IP address before you enable re-DHCP portal authentication on the interface.
- Cross-subnet authentication mode (**layer3**) does not require Layer 3 forwarding devices between the access device and the portal authentication clients. However, if a Layer 3 forwarding device exists between the authentication client and the access device, you must use the cross-subnet portal authentication mode.
- With re-DHCP portal authentication, configure authorized ARP on the interface as a best practice to make sure only valid users can access the network. With authorized ARP configured on the interface, the interface learns ARP entries only from the users who have obtained a public address from DHCP.
- An IPv6 portal server does not support the re-DHCP portal authentication mode.
- You can enable both IPv4 portal authentication and IPv6 portal authentication on an interface.

Configuration procedure

To enable portal authentication on an interface:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter interface view.	**interface** *interface-type interface-number*	The interface must be a Layer 3 interface.

Step	Command	Remarks

3. Enable portal authentication on the interface.	- To enable IPv4 portal authentication:
	portal enable method { **direct** | **layer3** | **redhcp** }
	- To enable IPv6 portal authentication:
	portal ipv6 enable method { **direct** | **layer3** }
		Enable IPv4 portal authentication, IPv6 portal authentication, or both on the interface.

Referencing a portal Web server for an interface

After you reference a portal Web server for an interface, the device redirects the HTTP requests of the portal users on the interface to the portal Web server.

An interface can reference both an IPv4 portal Web server and an IPv6 portal Web server.

To reference a portal Web server for an interface:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter interface view.	**interface** *interface-type interface-number*	The interface must be a Layer 3 interface.
3. Reference a portal Web server for the interface.	- To reference an IPv4 portal Web server: **portal apply web-server** *server-name* [**fail-permit**] - To reference an IPv6 portal Web server: **portal ipv6 apply web-server** *server-name* [**fail-permit**]	Reference an IPv4 portal Web server, an IPv6 portal Web server, or both for the interface. By default, the interface does not reference any portal Web server.

Controlling portal user access

Configuring a portal-free rule

A portal-free rule allows specified users to access specified external websites without portal authentication.

The matching items for a portal-free rule include the source/destination IP address, TCP/UDP port number, source MAC address, access interface, and VLAN. Packets matching a portal-free rule will not trigger portal authentication, so users sending the packets can directly access the specified external websites.

You cannot configure two or more portal-free rules with the same filtering criteria. Otherwise, the system prompts that the rule already exists.

Regardless of whether portal authentication is enabled or not, you can only add or remove a portal-free rule. You cannot modify it.

To configure an IP-based portal-free rule:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A

Step	Command	Remarks
2. Configure an IPv4-based portal-free rule.	**portal free-rule** *rule-number* { **destination ip** { *ip-address* { *mask-length* | *mask* } | **any** } [**tcp** *tcp-port-number* | **udp** *udp-port-number*] | **source ip** { *ip-address* { *mask-length* | *mask* } | **any** } [**tcp** *tcp-port-number* | **udp** *udp-port-number*] } *	By default, no IPv4-based portal-free rule exists.
3. Configure an IPv6-based portal-free rule.	**portal free-rule** *rule-number* { **destination ipv6** { *ipv6-address prefix-length* | **any** } [**tcp** *tcp-port-number* | **udp** *udp-port-number*] | **source ipv6** { *ipv6-address prefix-length* | **any** } [**tcp** *tcp-port-number* | **udp** *udp-port-number*] } *	By default, no IPv6-based portal-free rule exists.

To configure a source-based portal-free rule:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Configure a source-based portal-free rule.	**portal free-rule** *rule-number* **source** { **interface** *interface-type interface-number* | **mac** *mac-address* | **vlan** *vlan-id* } *	By default, no source-based portal-free rule exists. If you specify both a VLAN and an interface, the interface must belong to the VLAN. Otherwise, the portal-free rule does not take effect.

Configuring an authentication source subnet

By configuring authentication source subnets, you specify that only HTTP packets from users on the authentication source subnets can trigger portal authentication. If an unauthenticated user is not on any authentication source subnet, the access device discards all the user's HTTP packets that do not match any portal-free rule.

When you configure a portal authentication source subnet, follow these restrictions and guidelines:

- Authentication source subnets apply only to cross-subnet portal authentication.
- In direct or re-DHCP portal authentication mode, a portal user and its access interface (portal-enabled) are on the same subnet. It is not necessary to specify the subnet as the authentication source subnet. If the specified authentication source subnet is different from the access subnet of the users, the users will fail the portal authentication.
    - In direct mode, the access device regards the authentication source subnet as any source IP address.
    - In re-DHCP mode, the access device regards the authentication source subnet on an interface as the subnet to which the private IP address of the interface belongs.
- If both authentication source subnets and destination subnets are configured on an interface, only the authentication destination subnets take effect.
- You can configure multiple authentication source subnets. If the source subnets overlap, the subnet with the largest address scope (with the smallest mask or prefix) takes effect.

To configure an IPv4 portal authentication source subnet:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter interface view.	**interface** *interface-type interface-number*	N/A
3. Configure an IPv4 portal authentication source subnet.	**portal layer3 source** *ipv4-network-address* { *mask-length* | *mask* }	By default, no IPv4 portal authentication source subnet is configured, and users from any subnets must pass portal authentication.

To configure an IPv6 portal authentication source subnet:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter interface view.	**interface** *interface-type interface-number*	N/A
3. Configure an IPv6 portal authentication source subnet.	**portal ipv6 layer3 source** *ipv6-network-address prefix-length*	By default, no IPv6 portal authentication source subnet is configured, and IPv6 users from any subnets must pass portal authentication.

Configuring an authentication destination subnet

By configuring authentication destination subnets, you specify that users trigger portal authentication only when they accessing the specified subnets (excluding the destination IP addresses and subnets specified in portal-free rules). Users can access other subnets without portal authentication.

If both authentication source subnets and destination subnets are configured on an interface, only the authentication destination subnets take effect.

You can configure multiple authentication destination subnets. If the destination subnets overlap, the subnet with the largest address scope (with the smallest mask or prefix) takes effect.

To configure an IPv4 portal authentication destination subnet:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter interface view.	**interface** *interface-type interface-number*	N/A
3. Configure an IPv4 portal authentication destination subnet.	**portal free-all except destination** *ipv4-network-address* { *mask-length* | *mask* }	By default, no IPv4 portal authentication destination subnet is configured, and users accessing any subnets must pass portal authentication.

To configure an IPv6 portal authentication destination subnet:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter interface view.	**interface** *interface-type interface-number*	N/A

Step	Command	Remarks
3. Configure an IPv6 portal authentication destination subnet.	**portal ipv6 free-all except destination** *ipv6-network-address prefix-length*	By default, no IPv6 portal authentication destination subnet is configured, and users accessing any subnets must pass portal authentication.

Setting the maximum number of portal users

Perform this task to control the total number of login IPv4 and IPv6 portal users in the system.

If the maximum number of portal users you set is less than that of the current login portal users, the limit can be set successfully and does not impact the login portal users. However, the system does not allow new portal users to log in until the number drops down below the limit.

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Set the maximum number of portal users.	**portal max-user** *max-number*	By default, no limit is set on the number of portal users.

Specifying a portal authentication domain

An authentication domain defines a set of authentication, authorization, and accounting policies. Each portal user belongs to an authentication domain and is authenticated, authorized, and accounted in the domain.

After you specify a portal authentication domain on an interface, the device uses the specified authentication domain for AAA of all portal users on the interface, ignoring the domain names carried in the usernames. This allows for flexible portal access control.

The device selects the authentication domain for a portal user on an interface in this order:

1. ISP domain specified for the interface.
2. ISP domain carried in the username.
3. System default ISP domain. For information about the default ISP domain, see "Configuring AAA."

You can specify an IPv4 portal authentication domain, an IPv6 portal authentication domain, or both on an interface.

To specify an IPv4 portal authentication domain:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter interface view.	**interface** *interface-type interface-number*	N/A
3. Specify an IPv4 portal authentication domain.	**portal domain** *domain-name*	By default, no ISP domain is specified for IPv4 portal users on the interface.

To specify an IPv6 portal authentication domain:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter interface view.	**interface** *interface-type interface-number*	N/A
3. Specify an IPv6 portal authentication domain.	**portal ipv6 domain** *domain-name*	By default, no ISP domain is specified for IPv6 portal users on the interface.

Enabling outgoing packets filtering on a portal-enabled interface

When you enable this feature on a portal-enabled interface, the device permits the interface to send the following packets:

- Packets whose destination IP addresses are IP addresses of authenticated portal users.
- Packets that match portal-free rules.

Other outgoing packets on the interface are dropped.

To enable outgoing packets filtering on a portal-enabled interface:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter interface view.	**interface** *interface-type interface-number*	N/A
3. Enable outgoing packets filtering.	**portal** [**ipv6**] **outbound-filter enable**	By default, outgoing packets filtering is disabled. The interface can send any packets.

Configuring portal detection features

Configuring online detection of portal users

Configure online detection to timely detect abnormal logouts of portal users.

- Configure ARP or ICMP detection for IPv4 portal users.
- Configure ND or ICMPv6 detection for IPv6 portal users.

If the device receives no packets from a portal user within the idle time, the device detects the user's online status as follows:

- **ICMP or ICMPv6 detection**—Sends ICMP or ICMPv6 requests to the user at configurable intervals to detect the user status.
  - If the device receives a reply within the maximum number of detection attempts, it considers that the user is online and stops sending detection packets. Then the device resets the idle timer and repeats the detection process when the timer expires.
  - If the device receives no reply after the maximum number of detection attempts, the device logs out the user.
- **ARP or ND detection**—Sends ARP or ND requests to the user and detects the ARP or ND entry status of the user at configurable intervals.

- ○ If the ARP or ND entry of the user is refreshed within the maximum number of detection attempts, the device considers that the user is online and stops detecting the user's ARP or ND entry. Then the device resets the idle timer and repeats the detection process when the timer expires.
- ○ If the ARP or ND entry of the user is not refreshed after the maximum number of detection attempts, the device logs out the user.

ARP and ND detections apply only to direct and re-DHCP portal authentication. ICMP detection applies to all portal authentication modes.

To configure online detection of IPv4 portal users:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter interface view.	**interface** *interface-type interface-number*	N/A
3. Configure online detection of IPv4 portal users.	**portal user-detect type** { **arp** | **icmp** } [**retry** *retries*] [**interval** *interval*] [**idle** *time*]	By default, this feature is disabled on the interface.

To configure online detection of IPv6 portal users:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter interface view.	**interface** *interface-type interface-number*	N/A
3. Configure online detection of IPv6 portal users.	**portal ipv6 user-detect type** { **icmpv6** | **nd** } [**retry** *retries*] [**interval** *interval*] [**idle** *time*]	By default, this feature is disabled on the interface.

Configuring portal authentication server detection

During portal authentication, if the communication between the access device and portal authentication server is broken, both of the following occur:

- New portal users are not able to log in.
- The online portal users are not able to log out normally.

To address this problem, the access device needs to be able to detect the reachability changes of the portal server quickly and take corresponding actions to deal with the changes.

With the portal authentication server detection feature, the device periodically detects portal packets sent by a portal authentication server to determine the reachability of the server. If the device receives a portal packet within a detection timeout (**timeout** *timeout*) and the portal packet is valid, the device considers the portal authentication server to be reachable. Otherwise, the device considers the portal authentication server to be unreachable.

You can configure the device to take the following actions when the server reachability status changes:

- Sending a log message, which contains the name, the current state, and the original state of the portal authentication server.
- Enabling portal fail-permit. When the portal authentication server is unreachable, the portal fail-permit feature on an interface allows users on the interface to have network access. When the server recovers, it resumes portal authentication on the interface. For more information, see "Configuring the portal fail-permit feature."

Portal packets include user login packets, user logout packets, and heartbeat packets. Heartbeat packets are periodically sent by a server. By detecting heartbeat packets, the device can detect the server's actual status more quickly than by detecting other portal packets.

Only the IMC portal authentication server supports sending heartbeat packets. To test server reachability by detecting heartbeat packets, you must enable the server heartbeat feature on the IMC portal authentication server.

To configure portal authentication server detection:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A-
2. Enter portal authentication server view.	**portal server** *server-name*	N/A
3. Configure portal authentication server detection.	**server-detect** [**timeout** *timeout*] **log**	By default, portal authentication server detection is disabled. This feature takes effect regardless of whether portal authentication is enabled on an interface or not.

Configuring portal Web server detection

A portal authentication process cannot complete if the communication between the access device and the portal Web server is broken. To address this problem, you can enable portal Web server detection on the access device.

With the portal Web server detection feature, the access device simulates a Web access process to initiate a TCP connection to the portal Web server. If the TCP connection can be established successfully, the access device considers the detection successful, and the portal Web server is reachable. Otherwise, it considers the detection to have failed. Portal authentication status on interfaces of the access device does not affect the portal Web server detection feature.

You can configure the following detection parameters:

- **Detection interval**—Interval at which the device detects the server reachability.
- **Maximum number of consecutive failures**—If the number of consecutive detection failures reaches this value, the access device considers that the portal Web server is unreachable.

You can configure the device to take the following actions when the server reachability status changes:

- Sending a log message, which contains the name, the current state, and the original state of the portal Web server.
- Enabling portal fail-permit. When the portal Web server is unreachable, the portal fail-permit feature on an interface allows users on the interface to have network access. When the server recovers, it resumes portal authentication on the interface. For more information, see "Configuring the portal fail-permit feature."

To configure portal Web server detection:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter portal Web server view.	**portal web-server** *server-name*	N/A

Step	Command	Remarks
3. Configure portal Web server detection.	**server-detect** [**interval** *interval*] [**retry** *retries*] **log**	By default, portal Web server detection is disabled. This feature takes effect regardless of whether portal authentication is enabled on an interface or not.

Configuring portal user synchronization

Once the access device loses communication with a portal authentication server, the portal user information on the access device and that on the portal authentication server might be inconsistent after the communication resumes. To address this problem, the device provides the portal user synchronization feature. This feature is implemented by sending and detecting portal synchronization packets, as follows:

1. The portal authentication server sends the online user information to the access device in a synchronization packet at the user heartbeat interval, which is set on the portal authentication server.
2. Upon receiving the synchronization packet, the access device compares the users carried in the packet with its own user list. If a user contained in the packet does not exist on the access device, the access device informs the portal authentication server to delete the user. The access device starts the synchronization detection timer (**timeout** *timeout*) immediately when a user logs in. If the user does not appear in any synchronization packet within a synchronization detection interval, the access device considers the user does not exist on the portal authentication server and logs the user out.

Portal user synchronization requires a portal authentication server to support the portal user heartbeat function. Only the IMC portal authentication server supports the portal user heartbeat function. To implement the portal user synchronization feature, you also need to configure the user heartbeat function on the portal authentication server. Make sure the user heartbeat interval configured on the portal authentication server is not greater than the synchronization detection timeout configured on the access device.

Deleting a portal authentication server on the access device also deletes the user synchronization configuration for the portal authentication server.

To configure portal user information synchronization:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter portal authentication server view.	**portal server** *server-name*	N/A
3. Configure portal user synchronization.	**user-sync timeout** *timeout*	By default, portal user synchronization is disabled.

Configuring the portal fail-permit feature

Perform this task to configure the portal fail-permit feature on an interface. When the access device detects that the portal authentication server or portal Web server is unreachable, it allows users on the interface to have network access without portal authentication.

If you enable fail-permit for both a portal authentication server and a portal Web server on an interface, the interface does the following:

- Disables portal authentication when either server is unreachable.
- Resumes portal authentication when both servers are reachable.

After portal authentication resumes, unauthenticated users must pass portal authentication to access the network. Users who have passed portal authentication before the fail-permit event can continue accessing the network.

To configure portal fail-permit:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter interface view.	**interface** *interface-type interface-number*	N/A
3. Enable portal fail-permit for a portal authentication server.	**portal** [**ipv6**] **fail-permit server** *server-name*	By default, portal fail-permit is disabled for a portal authentication server.
4. Enable portal fail-permit for a portal Web server.	**portal** [**ipv6**] **apply web-server** *server-name* **fail-permit**	By default, portal fail-permit is disabled for a portal Web server.

Configuring BAS-IP for portal packets sent to the portal authentication server

If the device runs Portal 2.0, the unsolicited packets sent to the portal authentication server must carry the BAS-IP attribute. If the device runs Portal 3.0, the unsolicited packets sent to the portal authentication server must carry the BAS-IP or BAS-IPv6 attribute.

If IPv4 portal authentication is enabled on an interface, you can configure the BAS-IP attribute on the interface. If IPv6 portal authentication is enabled on an interface, you can configure the BAS-IPv6 attribute on the interface.

After this attribute is configured, the source IP address for unsolicited notification portal packets the device sends to the portal authentication server is the configured BAS-IP or BAS-IPv6 address. If the attribute is not configured, the source IP address of the portal packets is the IP address of the packet output interface.

During a re-DHCP portal authentication or mandatory user logout process, the device sends portal notification packets to the portal authentication server. For the authentication or logout process to complete, make sure the BAS-IP/BAS-IPv6 attribute is the same as the device IP or IPv6 address specified on the portal authentication server.

To configure the BAS-IP attribute for portal packets sent to the portal authentication server:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter interface view.	**interface** *interface-type interface-number*	N/A

Step	Command	Remarks
3. Configure BAS-IP for IPv4 portal packets sent to the portal authentication server.	**portal bas-ip** *ipv4-address*	By default: • The BAS-IP attribute of an IPv4 portal reply packet sent to the portal authentication server is the source IPv4 address of the packet. • The BAS-IP attribute of an IPv4 portal notification packet sent to the portal authentication server is the IPv4 address of the packet's output interface.
4. Configure BAS-IPv6 for IPv6 portal packets sent to the portal authentication server.	**portal bas-ipv6** *ipv6-address*	By default: • The BAS-IPv6 attribute of an IPv6 portal reply packet sent to the portal authentication server is the source IPv6 address of the packet. • The BAS-IPv6 attribute of an IPv6 portal notification packet sent to the portal authentication server is the IPv6 address of the packet's output interface.

Applying a NAS-ID profile to an interface

By default, the device sends its device name in the NAS-Identifier attribute of any RADIUS requests.

A NAS-ID profile enables you to send different NAS-Identifier attribute strings in RADIUS requests from different VLANs. The strings can be organization names, service names, or any user categorization criteria, depending on the administrative requirements.

For example, map the NAS-ID **companyA** to all VLANs of company A. The device will send **companyA** in the NAS-Identifier attribute for the RADIUS server to identify requests from any Company A users.

You can apply a NAS-ID profile to a portal-enabled interface. If no NAS-ID profile is specified on the interface or no matching NAS-ID is found in the specified profile, the device uses the device name as the interface NAS-ID.

To apply a NAS-ID profile to an interface:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Create a NAS-ID profile and enter NAS-ID profile view.	**aaa nas-id profile** *profile-name*	For more information about this command, see *Security Commands Reference*.
3. Configure a NAS ID and VLAN binding in the profile.	**nas-id** *nas-identifier* **bind vlan** *vlan-id*	By default, no NAS ID and VLAN binding exists. For more information about this command, see *Security Commands Reference*.
4. Return to system view.	**quit**	N/A
5. Enter interface view.	**interface** *interface-type interface-number*	N/A
6. Specify the NAS-ID profile on the interface.	**portal nas-id-profile** *profile-name*	By default, no NAS-ID profile is specified on the interface.

Enabling portal roaming

Portal roaming takes effect only on portal users logging in from VLAN interfaces.

If portal roaming is enabled on a VLAN interface, an online portal user can access resources from any Layer 2 port in the VLAN without re-authentication.

If portal roaming is disabled, to access external network resources from a Layer 2 port different from the current access port in the VLAN, the user must do the following:

- First log out from the current port.
- Then re-authenticate on the new Layer 2 port.

To enable portal roaming:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enable portal roaming.	**portal roaming enable**	By default, portal roaming is disabled. You cannot enable portal roaming when login users exist on the device.

Logging out portal users

Logging out a user terminates the authentication process for the user or removes the user from the authenticated users list.

To log out users:

Step	Command
1. Enter system view.	**system-view**
2. Log out IPv4 portal users.	**portal delete-user** { *ipv4-address* | **all** | **interface** *interface-type interface-number* }
3. Log out IPv6 portal users.	**portal delete-user** { **all** | **interface** *interface-type interface-number* | **ipv6** *ipv6-address* }

Configuring the local portal Web server feature

To perform local portal authentication for users, perform the following task:

- Configure a local portal Web server.
- Configure a name for the portal Web server and specify a local IP address of the device as the server's URL.
- Enable portal authentication on the user access interface.
- Specify the portal Web server on the portal-enabled interface.

During local portal authentication, the local Web portal server pushes authentication pages to users. You must customize the authentication pages, and upload them to the device. On the device, specify an authentication page file as the default authentication page file for local portal authentication.

Customizing authentication pages

Authentication pages are HTML files. Local portal authentication requires the following authentication pages:

- Logon page
- Logon success page
- Logon failure page
- Online page
- System busy page
- Logoff success page

You must customize the authentication pages, including the page elements that the authentication pages will use, for example, **back.jpg** for authentication page **Logon.htm**.

Follow the authentication page customization rules when you edit the authentication page files.

File name rules

The names of the main authentication page files are fixed (see Table 1). You can define the names of the files other than the main authentication page files. File names and directory names are case insensitive.

Table 1 Main authentication page file names

Main authentication page	File name
Logon page	logon.htm
Logon success page	logonSuccess.htm
Logon failure page	logonFail.htm
Online page Pushed after the user gets online for online notification	online.htm
System busy page Pushed when the system is busy or the user is in the logon process	busy.htm
Logoff success page	logoffSuccess.htm

Page request rules

The local portal Web server supports only Get and Post requests.

- **Get requests**—Used to get the static files in the authentication pages and allow no recursion. For example, if file **Logon.htm** includes contents that perform Get action on file **ca.htm**, file **ca.htm** cannot include any reference to file **Logon.htm**.
- **Post requests**—Used when users submit username and password pairs, log in, and log out.

Post request attribute rules

1. Observe the following requirements when editing a form of an authentication page:
   - An authentication page can have multiple forms, but there must be one and only one form whose action is **logon.cgi**. Otherwise, user information cannot be sent to the local portal Web server.
   - The username attribute is fixed as **PtUser**. The password attribute is fixed as **PtPwd**.
   - The value of the **PtButton** attribute is either **Logon** or **Logoff**, which indicates the action that the user requests.
   - A logon Post request must contain **PtUser**, **PtPwd**, and **PtButton** attributes.
   - A logoff Post request must contain the **PtButton** attribute.

2. Authentication pages **logon.htm** and **logonFail.htm** must contain the logon Post request.

   The following example shows part of the script in page **logon.htm**.

```
<form action=logon.cgi method = post >
<p>User name:<input type="text" name = "PtUser" style="width:160px;height:22px"
maxlength=64>
<p>Password :<input type="password" name = "PtPwd" style="width:160px;height:22px"
maxlength=32>
<p><input type=SUBMIT value="Logon" name = "PtButton" style="width:60px;"
onclick="form.action=form.action+location.search;">
</form>
```

3. Authentication pages **logonSuccess.htm** and **online.htm** must contain the logoff Post request.

   The following example shows part of the script in page **online.htm**.

```
<form action=logon.cgi method = post >
<p><input type=SUBMIT value="Logoff" name="PtButton" style="width:60px;">
</form>
```

Page file compression and saving rules

You must compress the authentication pages and their page elements into a standard zip file.

- The name of a zip file can contain only letters, numbers, and underscores.
- The authentication pages must be placed in the root directory of the zip file.
- Zip files can be transferred to the device through FTP or TFTP and must be saved in the root directory of the device.

  Examples of zip files on the device:

```
<Sysname> dir
Directory of flash:
   0     -rw-      1405  Feb 28 2008 15:53:31   ssid2.zip
   1     -rw-      1405  Feb 28 2008 15:53:20   ssid1.zip
   2     -rw-      1405  Feb 28 2008 15:53:39   ssid3.zip
   3     -rw-      1405  Feb 28 2008 15:53:44   ssid4.zip
2540 KB total (1319 KB free)
```

Redirecting authenticated users to a specific webpage

To make the device automatically redirect authenticated users to a specific webpage, do the following in logon.htm and logonSuccess.htm:

1. In logon.htm, set the target attribute of Form to **_blank**.

   See the contents in gray:

```
    <form method=post action=logon.cgi target="_blank">
```

2. Add the function for page loading pt_init() to logonSucceess.htm.

   See the contents in gray:

```
    <html>
    <head>
    <title>LogonSuccessed</title>
    <script type="text/javascript" language="javascript"
src="pt_private.js"></script>
    </head>
    <body onload="pt_init();" onbeforeunload="return pt_unload();">
    ... ...
    </body>
```

```
</html>
```

Configuring a local portal Web server

After a local portal Web server is configured on the access device, the access device acts as the portal Web server and the portal authentication server. No external portal Web server and portal authentication server are needed.

Configuration prerequisites

Perform the following tasks for the local portal Web server to support HTTPS:

- Configure a PKI policy, obtain the CA certificate, and request a local certificate. For more information, see "Configuring PKI."
- Configure an SSL server policy, and specify the PKI domain configured in the PKI policy. For more information, see "Configuring SSL."

Configuration procedure

To configure a local portal Web server:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Create a local portal Web server and enter its view.	**portal local-web-server** { **http** | **https ssl-server-policy** *policy-name* [**tcp-port** *port-number*] }	By default, no local portal Web server is configured.
3. Specify the default authentication page file for the local portal Web server.	**default-logon-page** *filename*	By default, no default authentication page file is specified for the local portal Web server.
4. (Optional.) Configure the HTTP listening TCP port for the local portal Web server.	**tcp-port** *port-number*	By default, the HTTP service listening port number is 80.

Displaying and maintaining portal

Execute **display** commands in any view and the **reset** command in user view.

Task	Command
Display portal rules on an interface.	**display portal rule** { **all** | **dynamic** | **static** } **interface** *interface-type interface-number* [**slot** *slot-id*]
Display portal configuration and portal running state information on an interface.	**display portal interface** *interface-type interface-number*
Display portal authentication server information.	**display portal server** [*server-name*]
Display portal Web server information.	**display portal web-server** [*server-name*]
Display packet statistics for portal authentication servers.	**display portal packet statistics** [**server** *server-name*]
Display portal user information.	**display portal user** { **all** | **interface** *interface-type interface-number* }
Clear packet statistics for portal authentication servers.	**reset portal packet statistics** [**server** *server-name*]

Portal configuration examples

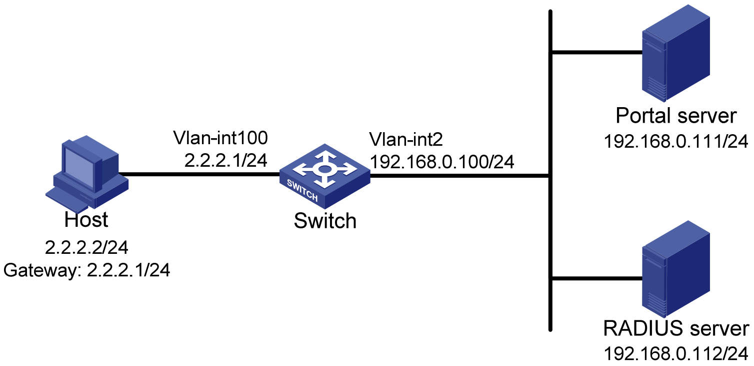
Configuring direct portal authentication

Network requirements

As shown in Figure 5, the host is directly connected to the switch (the access device). The host is assigned a public IP address either manually or through DHCP. A portal server acts as both a portal authentication server and a portal Web server. A RADIUS server acts as the authentication/accounting server.

Configure direct portal authentication, so the host can access only the portal server before passing the authentication and access other network resources after passing the authentication.

Figure 5 Network diagram



Configuration prerequisites

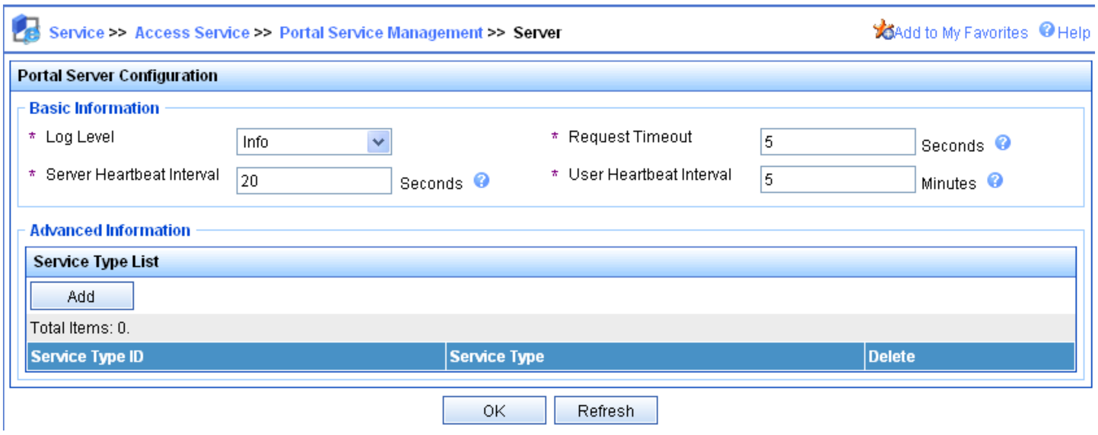
- Configure IP addresses for the host, switch, and servers as shown in Figure 5 and make sure they can reach each other.
- Configure the RADIUS server properly to provide authentication and accounting functions.

Configuring the portal authentication server on IMC PLAT 3.20

This example assumes that the portal server runs on IMC PLAT 3.20-R2602P13 and IMC UAM 3.60-E6301.

1. Configure the portal authentication server:
   a. Log in to IMC and click the **Service** tab.
   b. Select **Access Service** > **Portal Service Management** > **Server** from the navigation tree to enter the portal server configuration page, as shown in Figure 6.
   c. Configure the portal server parameters as needed.
      This example uses the default values.
   d. Click **OK**.

Figure 6 Portal authentication server configuration



Service >> Access Service >> Portal Service Management >> Server

Portal Server Configuration

Basic Information

* Log Level	Info	* Request Timeout	5 Seconds
* Server Heartbeat Interval	20 Seconds	* User Heartbeat Interval	5 Minutes

Advanced Information

Service Type List

Total Items: 0.

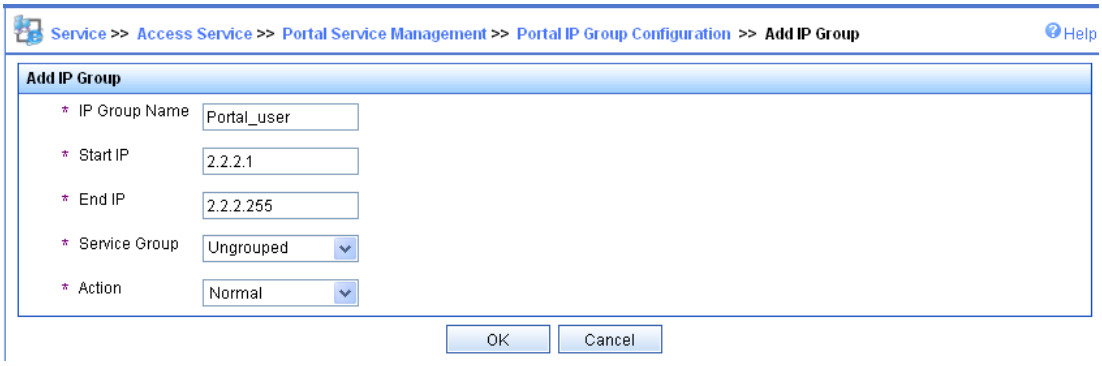
Service Type ID	Service Type	Delete

2. Configure the IP address group:
   a. Select **Access Service** > **Portal Service Management** > **IP Group** from the navigation tree to enter the portal IP address group configuration page.
   b. Click **Add** to open the page as shown in Figure 7.
   c. Enter the IP group name.
   d. Enter the start IP address and end IP address of the IP group.

      Make sure the host IP address (2.2.2.2) is in the IP group.
   e. Select a service group.

      This example uses the default group **Ungrouped**.
   f. Select **Normal** from the **Action** list.
   g. Click **OK**.

Figure 7 Adding an IP address group



Service >> Access Service >> Portal Service Management >> Portal IP Group Configuration >> Add IP Group

Add IP Group

* IP Group Name	Portal_user
* Start IP	2.2.2.1
* End IP	2.2.2.255
* Service Group	Ungrouped
* Action	Normal

3. Add a portal device:
   a. Select **Access Service** > **Portal Service Management** > **Device** from the navigation tree to enter the portal device configuration page.
   b. Click **Add** to open the page as shown in Figure 8.
   c. Enter the device name **NAS**.
   d. Enter the IP address of the switch's interface connected to the host.
   e. Enter the key, which must be the same as that configured on the switch.
   f. Set whether to enable IP address reallocation.

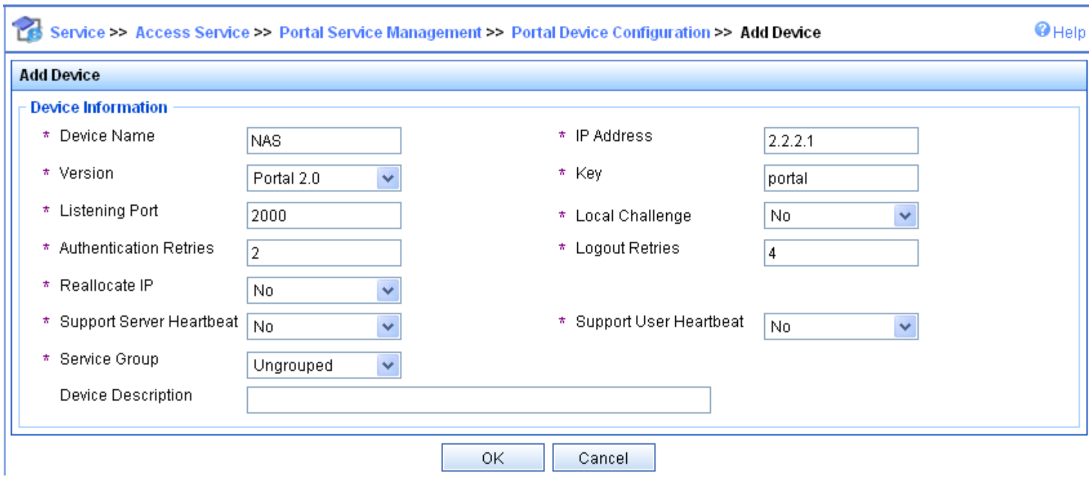
      This example uses direct portal authentication. Therefore, select **No** from the **Reallocate IP** list.

g. Set whether to support the portal server heartbeat and user heartbeat functions.

In this example, select **No** for both **Support Server Heartbeat** and **Support User Heartbeat**.

h. Click **OK**.

Figure 8 Adding a portal device



Service >> Access Service >> Portal Service Management >> Portal Device Configuration >> Add Device   Help

Add Device

Device Information

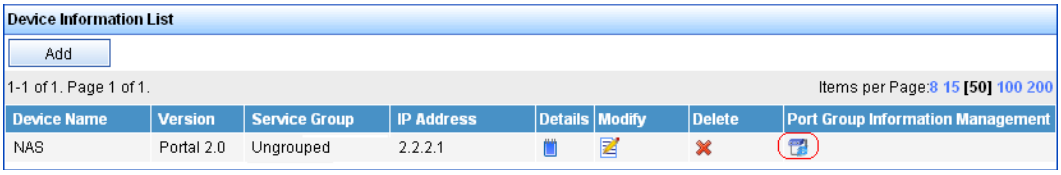
* Device Name	NAS	* IP Address	2.2.2.1
* Version	Portal 2.0	* Key	portal
* Listening Port	2000	* Local Challenge	No
* Authentication Retries	2	* Logout Retries	4
* Reallocate IP	No		
* Support Server Heartbeat	No	* Support User Heartbeat	No
* Service Group	Ungrouped		
Device Description			

OK   Cancel

4. Associate the portal device with the IP address group:

a. As shown in Figure 9, click the icon in the **Port Group Information Management** column of device **NAS** to enter the port group configuration page.

Figure 9 Device list



Device Information List

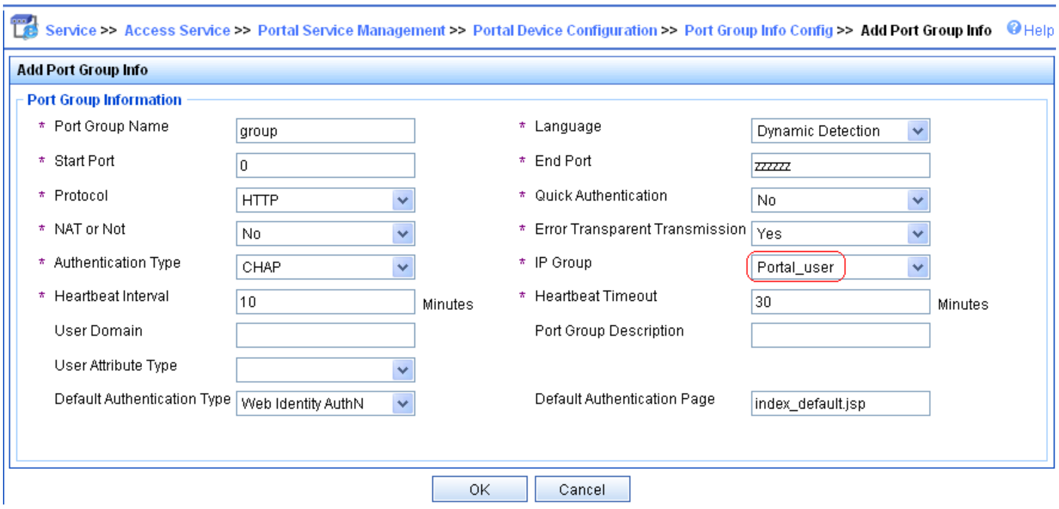
Add

1-1 of 1. Page 1 of 1.   Items per Page:8 15 [50] 100 200

Device Name	Version	Service Group	IP Address	Details	Modify	Delete	Port Group Information Management
NAS	Portal 2.0	Ungrouped	2.2.2.1			✖	

b. Click **Add** to open the page as shown in Figure 10.

Figure 10 Port group configuration



Service >> Access Service >> Portal Service Management >> Portal Device Configuration >> Port Group Info Config >> Add Port Group Info   Help

Add Port Group Info

Port Group Information

* Port Group Name	group	* Language	Dynamic Detection
* Start Port	0	* End Port	zzzzzz
* Protocol	HTTP	* Quick Authentication	No
* NAT or Not	No	* Error Transparent Transmission	Yes
* Authentication Type	CHAP	* IP Group	Portal_user
* Heartbeat Interval	10 Minutes	* Heartbeat Timeout	30 Minutes
User Domain		Port Group Description	
User Attribute Type			
Default Authentication Type	Web Identity AuthN	Default Authentication Page	index_default.jsp

OK   Cancel

c. Enter the port group name.

d. Select the configured IP address group.

The IP address used by the user to access the network must be within this IP address group.

e. Click **OK**.

5. Select **Access Service** > **Service Parameters** > **Validate System Configuration** from the navigation tree to validate the configurations.

Configuring the portal authentication server on IMC PLAT 5.0

This example assumes that the portal server runs on IMC PLAT 5.0(E0101) and IMC UAM 5.0(E0101).

1. Configure the portal authentication server:

a. Log in to IMC and click the **Service** tab.

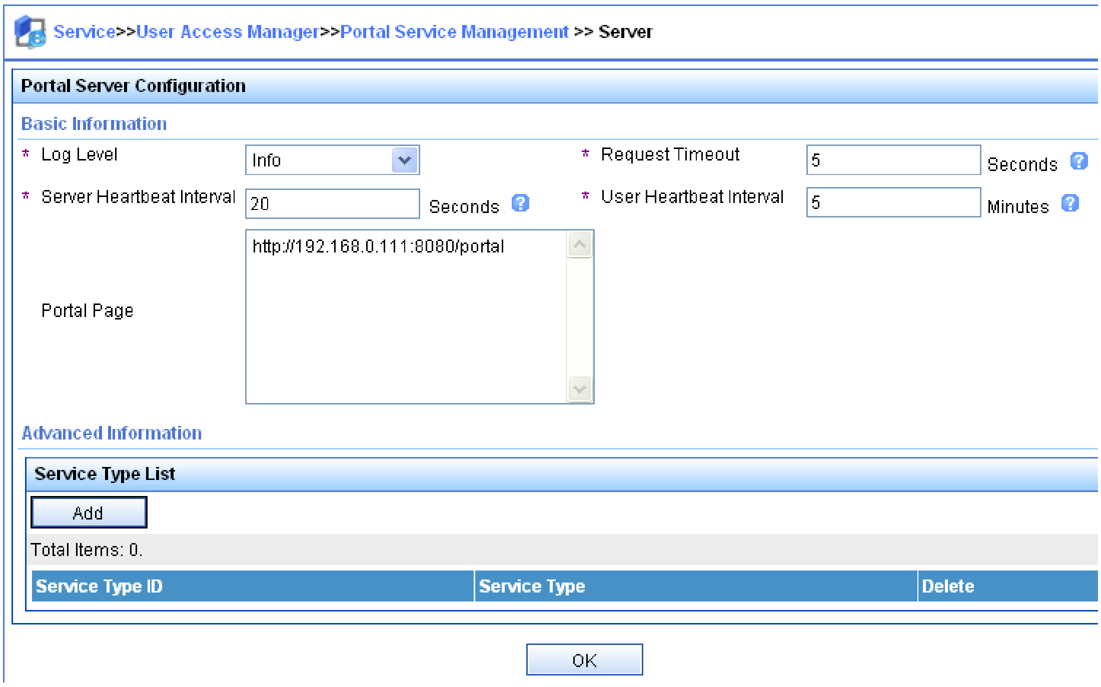
b. Select **User Access Manager** > **Portal Service Management** > **Server** from the navigation tree to enter the portal server configuration page, as shown in Figure 11.

c. Configure the portal server parameters as needed.

This example uses the default settings.

d. Click **OK**.

Figure 11 Portal server configuration



Service>>User Access Manager>>Portal Service Management >> Server

Portal Server Configuration

Basic Information

* Log Level	Info		* Request Timeout	5	Seconds
* Server Heartbeat Interval	20	Seconds	* User Heartbeat Interval	5	Minutes
Portal Page	http://192.168.0.111:8080/portal				

Advanced Information

Service Type List

Add

Total Items: 0.

Service Type ID	Service Type	Delete

OK

2. Configure the IP address group:

a. Select **User Access Manager** > **Portal Service Management** > **IP Group** from the navigation tree to enter the portal IP address group configuration page.

b. Click **Add** to open the page as shown in Figure 12.

c. Enter the IP group name.

d. Enter the start IP address and end IP address of the IP group.

Make sure the host IP address is in the IP group.

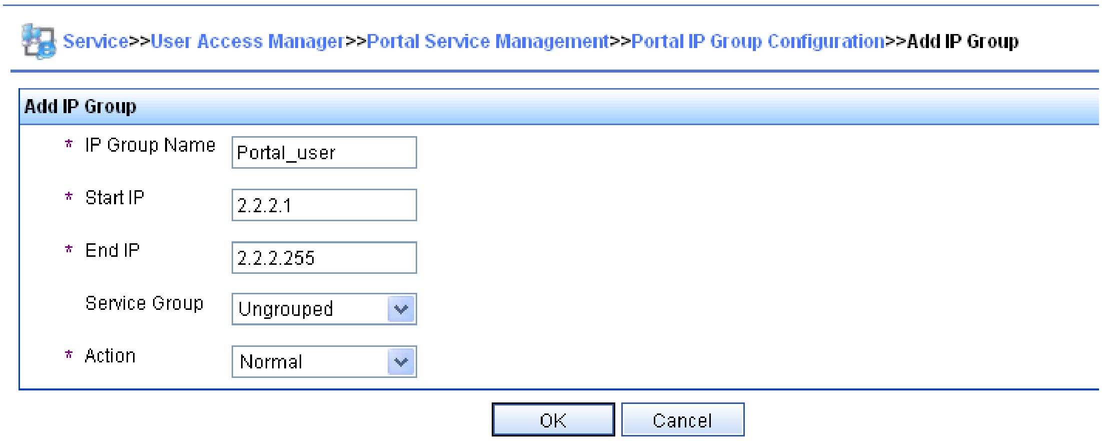
e. Select a service group.

This example uses the default group **Ungrouped**.

f. Select **Normal** from the **Action** list.

g. Click **OK**.

Figure 12 Adding an IP address group



Service>>User Access Manager>>Portal Service Management>>Portal IP Group Configuration>>Add IP Group

Add IP Group

* IP Group Name	Portal_user
* Start IP	2.2.2.1
* End IP	2.2.2.255
Service Group	Ungrouped
* Action	Normal

3. Add a portal device:

   a. Select **User Access Manager** > **Portal Service Management** > **Device** from the navigation tree to enter the portal device configuration page.

   b. Click **Add** to open the page as shown in Figure 13.

   c. Enter the device name **NAS**.

   d. Enter the IP address of the switch's interface connected to the host.

   e. Enter the key, which must be the same as that configured on the switch.

   f. Set whether to enable IP address reallocation.

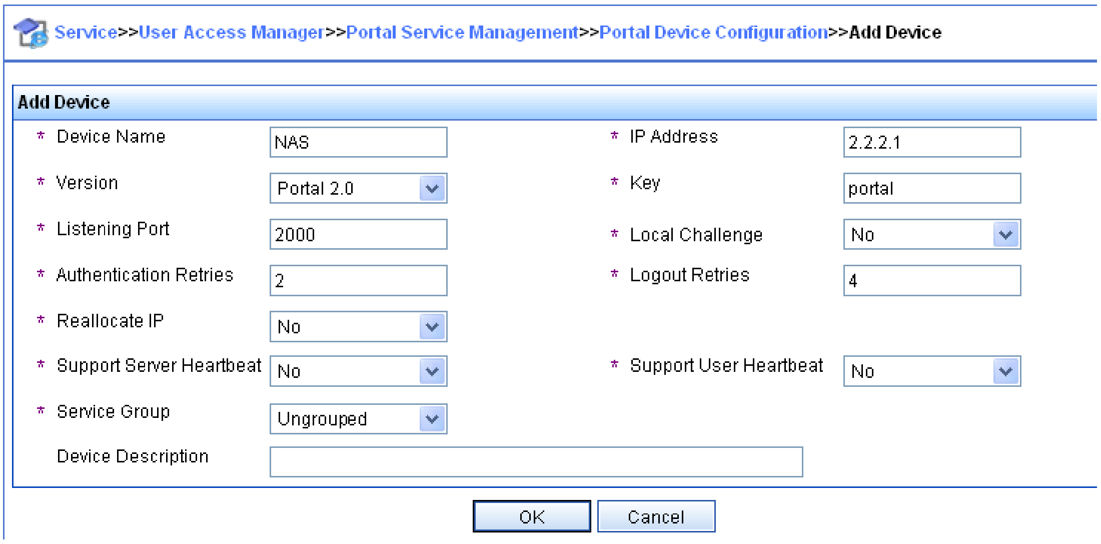
      This example uses direct portal authentication. Therefore, select **No** from the **Reallocate IP** list.

   g. Select whether to support server heartbeat and user heartbeat functions.

      In this example, select **No** for both **Support Server Heartbeat** and **Support User Heartbeat**.

   h. Click **OK**.

Figure 13 Adding a portal device



Service>>User Access Manager>>Portal Service Management>>Portal Device Configuration>>Add Device

Add Device

* Device Name	NAS	* IP Address	2.2.2.1
* Version	Portal 2.0	* Key	portal
* Listening Port	2000	* Local Challenge	No
* Authentication Retries	2	* Logout Retries	4
* Reallocate IP	No		
* Support Server Heartbeat	No	* Support User Heartbeat	No
* Service Group	Ungrouped		
Device Description			

4. Associate the portal device with the IP address group:

   a. As shown in Figure 14, click the icon in the **Port Group Information Management** column of device **NAS** to enter the port group configuration page.

b. Click **Add** to open the page as shown in Figure 15.

c. Enter the port group name.

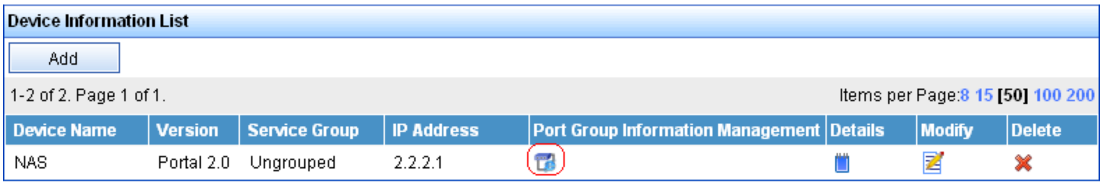
d. Select the configured IP address group.

The IP address used by the user to access the network must be within this IP address group.

e. Use the default settings for other parameters.

f. Click **OK**.

Figure 14 Device list

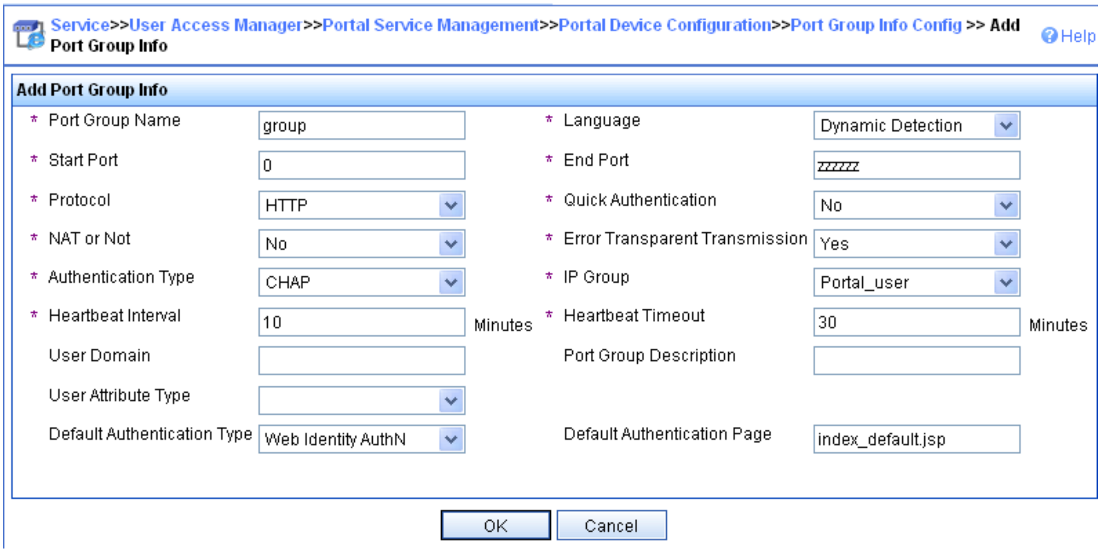


Device Information List

1-2 of 2. Page 1 of 1. Items per Page:8 15 [50] 100 200

Device Name	Version	Service Group	IP Address	Port Group Information Management	Details	Modify	Delete
NAS	Portal 2.0	Ungrouped	2.2.2.1				✗

Figure 15 Adding a port group



Service>>User Access Manager>>Portal Service Management>>Portal Device Configuration>>Port Group Info Config >> Add Port Group Info

Add Port Group Info

* Port Group Name	group		* Language	Dynamic Detection	
* Start Port	0		* End Port	zzzzzz	
* Protocol	HTTP		* Quick Authentication	No	
* NAT or Not	No		* Error Transparent Transmission	Yes	
* Authentication Type	CHAP		* IP Group	Portal_user	
* Heartbeat Interval	10	Minutes	* Heartbeat Timeout	30	Minutes
User Domain			Port Group Description		
User Attribute Type					
Default Authentication Type	Web Identity AuthN		Default Authentication Page	index_default.jsp	

5. Select **User Access Manager** > **Service Parameters** > **Validate System Configuration** from the navigation tree to validate the configurations.

Configuring the switch

1. Configure a RADIUS scheme:

# Create a RADIUS scheme named **rs1** and enter its view.

```
<Switch> system-view
[Switch] radius scheme rs1
```

# Specify the primary authentication server and primary accounting server, and configure the keys for communication with the servers.

```
[Switch-radius-rs1] primary authentication 192.168.0.112
[Switch-radius-rs1] primary accounting 192.168.0.112
[Switch-radius-rs1] key authentication simple radius
[Switch-radius-rs1] key accounting simple radius
```

# Exclude the ISP domain name from the username sent to the RADIUS server.

```
[Switch-radius-rs1] user-name-format without-domain
[Switch-radius-rs1] quit
```

# Enable RADIUS session control.

```
[Switch] radius session-control enable
```

2. Configure an authentication domain:

   # Create an ISP domain named **dm1** and enter its view.

   ```
   [Switch] domain dm1
   ```

   # Configure AAA methods for the ISP domain.

   ```
   [Switch-isp-dm1] authentication portal radius-scheme rs1
   [Switch-isp-dm1] authorization portal radius-scheme rs1
   [Switch-isp-dm1] accounting portal radius-scheme rs1
   [Switch-isp-dm1] quit
   ```

   # Configure domain **dm1** as the default ISP domain. If a user enters the username without the ISP domain name at login, the authentication and accounting methods of the default domain are used for the user.

   ```
   [Switch] domain default enable dm1
   ```

3. Configure portal authentication:

   # Configure a portal authentication server.

   ```
   [Switch] portal server newpt
   New portal server added.
   [Switch-portal-server-newpt] ip 192.168.0.111 key simple portal
   [Switch-portal-server-newpt] port 50100
   [Switch-portal-server-newpt] quit
   ```

   # Configure a portal Web server.

   ```
   [Switch] portal web-server newpt
   [Switch-portal-websvr-newpt] url http://192.168.0.111:8080/portal
   [Switch-portal-websvr-newpt] quit
   ```

   # Enable direct portal authentication on VLAN-interface 100.

   ```
   [Switch] interface vlan-interface 100
   [Switch–Vlan-interface100] portal enable method direct
   ```

   # Reference the portal Web server **newpt** on VLAN-interface 100.

   ```
   [Switch–Vlan-interface100] portal apply web-server newpt
   ```

   # Configure the BAS-IP as 2.2.2.1 for portal packets sent from VLAN-interface 100 to the portal authentication server.

   ```
   [Switch–Vlan-interface100] portal bas-ip 2.2.2.1
   [Switch–Vlan-interface100] quit
   ```

Verifying the configuration

# Verify that the portal configuration has taken effect.

```
[Switch] display portal interface vlan-interface 100
 Portal information of Vlan-interface100
     Nas id profile: Not configured
 IPv4:
     Portal status: Enabled
     Authentication type: Direct
     Portal Web server: newpt
     Authentication domain: Not configured
     Bas-ip: 2.2.2.1
     User Detection:  Not configured
     Action for server detection:
```

```
         Server type    Server name                                       Action
         --             --                                                --
     Layer3 source network:
         IP address               Mask

     Destination authenticate subnet:
         IP address               Mask
IPv6:
     Portal status: Disabled
     Authentication type: Disabled
     Portal Web server: Not configured
     Authentication domain: Not configured
     Bas-ipv6: Not configured
     User detection: Not configured
     Action for server detection:
         Server type    Server name                                       Action
         --             --                                                --
     Layer3 source network:
         IP address                                                       Prefix length

     Destination authenticate subnet:
         IP address                                                       Prefix length
```

A user can perform portal authentication by using the H3C iNode client or a Web browser. Before passing the authentication, the user can access only the authentication page **http://192.168.0.111:8080/portal** and all Web requests will be redirected to the authentication page. After passing the authentication, the user can access Internet resources.

# After the user passes authentication, use the following command to display information about the portal user.

```
[Switch] display portal user interface vlan-interface 100
 Total portal users: 1
  Username: abc
  Portal server: newpt
  State: Online
  Authorization ACL: --
  VPN instance: --
  MAC                IP                 VLAN   Interface
  0015-e9a6-7cfe     2.2.2.2            100    Vlan-interface100
```

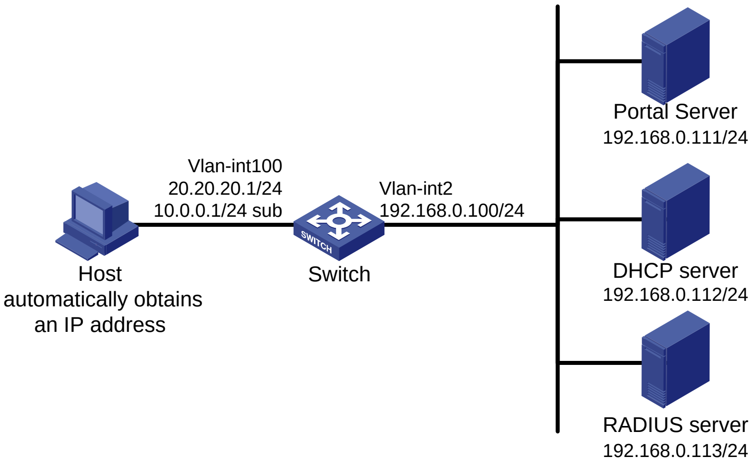
Configuring re-DHCP portal authentication

Network requirements

As shown in Figure 16, the host is directly connected to the switch (the access device). The host obtains an IP address through the DHCP server. A portal server acts as both a portal authentication server and a portal Web server. A RADIUS server acts as the authentication/accounting server.

Configure re-DHCP portal authentication. Before passing the authentication, the host is assigned a private IP address. After passing the authentication, the host gets a public IP address and can access Internet resources.

Figure 16 Network diagram



Configuration prerequisites and guidelines

- Configure IP addresses for the switch and servers as shown in Figure 16 and make sure the host, switch, and servers can reach each other.
- Configure the RADIUS server properly to provide authentication and accounting functions.
- For re-DHCP portal authentication, configure a public address pool (20.20.20.0/24) and a private address pool (10.0.0.0/24) on the DHCP server. (Details not shown.)
- For re-DHCP portal authentication:
  - The switch must be configured as a DHCP relay agent.
  - The portal-enabled interface must be configured with a primary IP address (a public IP address) and a secondary IP address (a private IP address).

  For information about DHCP relay agent configuration, see *Layer 3—IP Services Configuration Guide*.
- Make sure the IP address of the portal device added on the portal server is the public IP address (20.20.20.1) of the switch's interface connecting the host. The private IP address range for the IP address group associated with the portal device is the private subnet 10.0.0.0/24 where the host resides. The public IP address range for the IP address group is the public subnet 20.20.20.0/24.

Configuration procedure

Perform the following tasks on the switch.

1. Configure a RADIUS scheme:

# Create a RADIUS scheme named **rs1** and enter its view.

```
<Switch> system-view
[Switch] radius scheme rs1
```

# Specify the primary authentication server and primary accounting server, and configure the keys for communication with the servers.

```
[Switch-radius-rs1] primary authentication 192.168.0.113
[Switch-radius-rs1] primary accounting 192.168.0.113
[Switch-radius-rs1] key authentication simple radius
[Switch-radius-rs1] key accounting simple radius
```

# Exclude the ISP domain name from the username sent to the RADIUS server.

```
[Switch-radius-rs1] user-name-format without-domain
[Switch-radius-rs1] quit
```

# Enable RADIUS session control.

```
[Switch] radius session-control enable
```

2. Configure an authentication domain:

# Create an ISP domain named **dm1** and enter its view.

```
[Switch] domain dm1
```

# Configure AAA methods for the ISP domain.

```
[Switch-isp-dm1] authentication portal radius-scheme rs1
[Switch-isp-dm1] authorization portal radius-scheme rs1
[Switch-isp-dm1] accounting portal radius-scheme rs1
[Switch-isp-dm1] quit
```

# Configure domain **dm1** as the default ISP domain. If a user enters the username without the ISP domain name at login, the authentication and accounting methods of the default domain are used for the user.

```
[Switch] domain default enable dm1
```

3. Configure DHCP relay and authorized ARP:

# Configure DHCP relay.

```
[Switch] dhcp enable
[Switch] dhcp relay client-information record
[Switch] interface vlan-interface 100
[Switch–Vlan-interface100] ip address 20.20.20.1 255.255.255.0
[Switch–Vlan-interface100] ip address 10.0.0.1 255.255.255.0 sub
[Switch-Vlan-interface100] dhcp select relay
[Switch-Vlan-interface100] dhcp relay server-address 192.168.0.112
```

# Enable authorized ARP.

```
[Switch-Vlan-interface100] arp authorized enable
[Switch-Vlan-interface100] quit
```

4. Configure portal authentication:

# Configure a portal authentication server.

```
[Switch] portal server newpt
[Switch-portal-server-newpt] ip 192.168.0.111 key simple portal
[Switch-portal-server-newpt] port 50100
[Switch-portal-server-newpt] quit
```

# Configure a portal Web server.

```
[Switch] portal web-server newpt
[Switch-portal-websvr-newpt] url http://192.168.0.111:8080/portal
[Switch-portal-websvr-newpt] quit
```

# Enable re-DHCP portal authentication on VLAN-interface 100.

```
[Switch] interface vlan-interface 100
[Switch–Vlan-interface100] portal enable method redhcp
```

# Reference the portal Web server **newpt** on VLAN-interface 100.

```
[Switch–Vlan-interface100] portal apply web-server newpt
```

# Configure the BAS-IP as 20.20.20.1 for portal packets sent from VLAN-interface 100 to the portal authentication server.

```
[Switch–Vlan-interface100] portal bas-ip 20.20.20.1
[Switch–Vlan-interface100] quit
```

Verifying the configuration

# Verify that the portal configuration has taken effect.

```
[Switch] display portal interface vlan-interface 100
```

```
 Portal information of Vlan-interface100
     Nas id profile: Not configured
 IPv4:
     Portal status: Enabled
     Authentication type: Redhcp
     Portal Web server: newpt
     Authentication domain: Not configured
     Bas-ip: 20.20.20.1
     User Detection:  Not configured
     Action for server detection:
         Server type    Server name                        Action
         --             --                                 --
     Layer3 source network:
         IP address               Mask

     Destination authenticate subnet:
         IP address               Mask
IPv6:
     Portal status: Disabled
     Authentication type: Disabled
     Portal Web server: Not configured
     Authentication domain: Not configured
     Bas-ipv6: Not configured
     User detection: Not configured
     Action for server detection:
         Server type    Server name                        Action
         --             --                                 --
     Layer3 source network:
         IP address                                        Prefix length

     Destination authenticate subnet:
         IP address                                        Prefix length
```

A user can perform portal authentication by using the H3C iNode client or a Web browser. Before passing the authentication, the user can access only the authentication page **http://192.168.0.111:8080/portal** and all Web requests will be redirected to the authentication page. After passing the authentication, the user can access Internet resources.

# After the user passes authentication, use the following command to display information about the portal user.

```
[Switch] display portal user interface vlan-interface 100
Total portal users: 1
Username: abc
  Portal server: newpt
  State: Online
  Authorization ACL: None
  VPN instance: --
  MAC                IP                 VLAN   Interface
  0015-e9a6-7cfe     20.20.20.2         100    Vlan-interface100
```

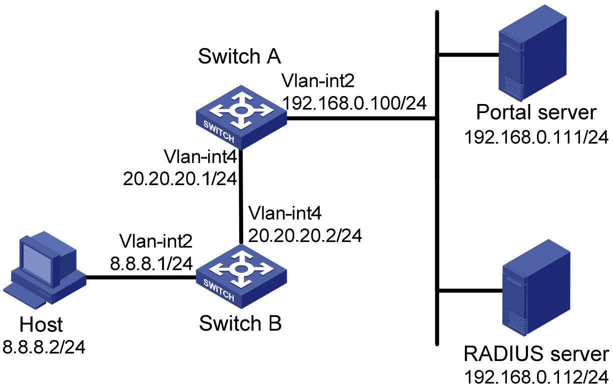
Configuring cross-subnet portal authentication

Network requirements

As shown in Figure 17, Switch A supports portal authentication. The host accesses Switch A through Switch B. A portal server acts as both a portal authentication server and a portal Web server. A RADIUS server acts as the authentication/accounting server.

Configure Switch A for cross-subnet portal authentication. Before passing the authentication, the host can access only the portal Web server. After passing the authentication, the user can access Internet resources.

Figure 17 Network diagram



Configuration prerequisites and guidelines

- Configure IP addresses for the switch and servers as shown in Figure 17 and make sure the host, switch, and servers can reach each other.
- Configure the RADIUS server properly to provide authentication and accounting functions.
- Make sure the IP address of the portal device added on the portal authentication server is the IP address (20.20.20.1) of the switch's interface connecting the host. The IP address group associated with the portal device is the subnet of the host (8.8.8.0/24).

Configuration procedure

Perform the following tasks on Switch A.

1. Configure a RADIUS scheme:

   # Create a RADIUS scheme named **rs1** and enter its view.

   ```
   <SwitchA> system-view
   [SwitchA] radius scheme rs1
   ```

   # Specify the primary authentication server and primary accounting server, and configure the keys for communication with the servers.

   ```
   [SwitchA-radius-rs1] primary authentication 192.168.0.112
   [SwitchA-radius-rs1] primary accounting 192.168.0.112
   [SwitchA-radius-rs1] key authentication simple radius
   [SwitchA-radius-rs1] key accounting simple radius
   ```

   # Exclude the ISP domain name from the username sent to the RADIUS server.

   ```
   [SwitchA-radius-rs1] user-name-format without-domain
   [SwitchA-radius-rs1] quit
   ```

   # Enable RADIUS session control.

   ```
   [SwitchA] radius session-control enable
   ```

2. Configure an authentication domain:

# Create an ISP domain named **dm1** and enter its view.

```
[SwitchA] domain dm1
```

# Configure AAA methods for the ISP domain.

```
[SwitchA-isp-dm1] authentication portal radius-scheme rs1
[SwitchA-isp-dm1] authorization portal radius-scheme rs1
[SwitchA-isp-dm1] accounting portal radius-scheme rs1
[SwitchA-isp-dm1] quit
```

# Configure domain **dm1** as the default ISP domain. If a user enters the username without the ISP domain name at login, the authentication and accounting methods of the default domain are used for the user.

```
[SwitchA] domain default enable dm1
```

3. Configure portal authentication:

   # Configure a portal authentication server.

```
[SwitchA] portal server newpt
[SwitchA-portal-server-newpt] ip 192.168.0.111 key simple portal
[SwitchA-portal-server-newpt] port 50100
[SwitchA-portal-server-newpt] quit
```

# Configure a portal Web server.

```
[SwitchA] portal web-server newpt
[SwitchA-portal-websvr-newpt] url http://192.168.0.111:8080/portal
[SwitchA-portal-websvr-newpt] quit
```

# Enable cross-subnet portal authentication on VLAN-interface 4.

```
[SwitchA] interface vlan-interface 4
[SwitchA–Vlan-interface4] portal enable method layer3
```

# Reference the portal Web server **newpt** on VLAN-interface 4.

```
[SwitchA–Vlan-interface4] portal apply web-server newpt
```

# Configure the BAS-IP as 20.20.20.1 for portal packets sent from VLAN-interface 4 to the portal authentication server.

```
[SwitchA–Vlan-interface4] portal bas-ip 20.20.20.1
[SwitchA–Vlan-interface4] quit
```

On Switch B, configure a default route to subnet 192.168.0.0/24, specifying the next hop address as 20.20.20.1. (Details not shown.)

Verifying the configuration

# Verify that the portal configuration has taken effect.

```
[SwitchA] display portal interface vlan-interface 4
 Portal information of Vlan-interface4
     Nas id profile: Not configured
 IPv4:
     Portal status: Enabled
     Authentication type: Layer3
     Portal Web server: newpt
     Authentication domain: Not configured
     Bas-ip: 20.20.20.1
     User Detection:  Not configured
     Action for server detection:
         Server type    Server name                        Action
         --             --                                 --
     Layer3 source network:
         IP address               Mask

     Destination authenticate subnet:
         IP address               Mask
IPv6:
     Portal status: Disabled
     Authentication type: Disabled
     Portal Web server: Not configured
     Authentication domain: Not configured
     Bas-ipv6: Not configured
     User detection: Not configured
     Action for server detection:
         Server type    Server name                         Action
         --             --                                  --
     Layer3 source network:
         IP address                                         Prefix length

     Destination authenticate subnet:
         IP address                                         Prefix length
```

A user can perform portal authentication by using the H3C iNode client or a Web browser. Before passing the authentication, the user can access only the authentication page **http://192.168.0.111:8080/portal** and all Web requests will be redirected to the authentication page. After passing the authentication, the user can access Internet resources.

# After the user passes authentication, use the following command to display information about the portal user.

```
[SwitchA] display portal user interface vlan-interface 4
Total portal users: 1
Username: abc
  Portal server: newpt
  State: Online
  Authorization ACL: None
  VPN instance: --
  MAC                IP                 VLAN   Interface
  0015-e9a6-7cfe     8.8.8.2            4      Vlan-interface4
```

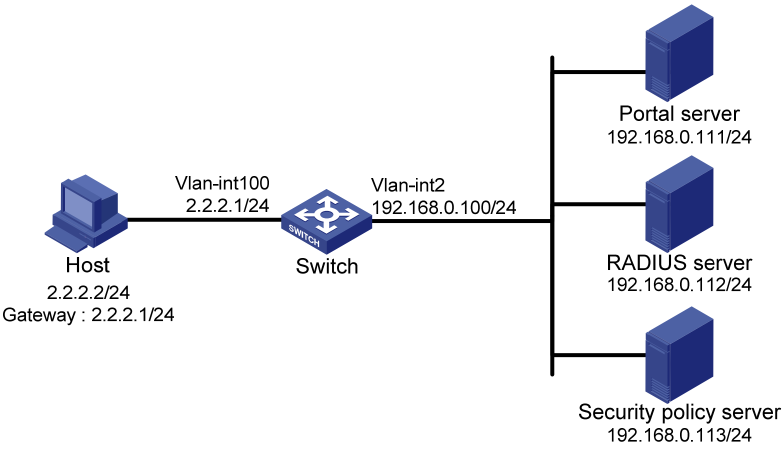
Configuring extended direct portal authentication

Network requirements

As shown in Figure 18, the host is directly connected to the switch (the access device). The host is assigned a public IP address either manually or through DHCP. A portal server acts as both a portal authentication server and a portal Web server. A RADIUS server acts as the authentication/accounting server.

Configure extended direct portal authentication. If the host fails security check after passing identity authentication, it can access only subnet 192.168.0.0/24. After passing security check, the host can access Internet resources.

Figure 18 Network diagram



Configuration prerequisites

- Configure IP addresses for the host, switch, and servers as shown in Figure 18 and make sure they can reach each other.
- Configure the RADIUS server properly to provide authentication and accounting functions.

Configuration procedure

Perform the following tasks on the switch.

1. Configure a RADIUS scheme:

   # Create a RADIUS scheme named rs1 and enter its view.

   ```
   <Switch> system-view
   [Switch] radius scheme rs1
   ```

   # Specify the primary authentication server and primary accounting server, and configure the keys for communication with the servers.

   ```
   [Switch-radius-rs1] primary authentication 192.168.0.112
   [Switch-radius-rs1] primary accounting 192.168.0.112
   [Switch-radius-rs1] key accounting simple radius
   [Switch-radius-rs1] key authentication simple radius
   [Switch-radius-rs1] user-name-format without-domain
   ```

   # Specify the security policy server.

   ```
   [Switch-radius-rs1] security-policy-server 192.168.0.113
   [Switch-radius-rs1] quit
   ```

   # Enable RADIUS session control.

   ```
   [Switch] radius session-control enable
   ```

2. Configure an authentication domain:

   # Create an ISP domain named dm1 and enter its view.

   ```
   [Switch] domain dm1
   ```

   # Configure AAA methods for the ISP domain.

   ```
   [Switch-isp-dm1] authentication portal radius-scheme rs1
   [Switch-isp-dm1] authorization portal radius-scheme rs1
   [Switch-isp-dm1] accounting portal radius-scheme rs1
   [Switch-isp-dm1] quit
   ```

   # Configure domain dm1 as the default ISP domain. If a user enters the username without the ISP domain name at login, the authentication and accounting methods of the default domain are used for the user.

```
[Switch] domain default enable dm1
```

3. Configure ACL 3000 as the isolation ACL and ACL 3001 as the security ACL:

```
[Switch] acl number 3000
[Switch-acl-adv-3000] rule permit ip destination 192.168.0.0 0.0.0.255
[Switch-acl-adv-3000] rule deny ip
[Switch-acl-adv-3000] quit
[Switch] acl number 3001
[Switch-acl-adv-3001] rule permit ip
[Switch-acl-adv-3001] quit
```

NOTE:

Make sure you specify ACL 3000 as the isolation ACL and ACL 3001 as the security ACL on the security policy server.

4. Configure portal authentication:

# Configure a portal authentication server.

```
[Switch] portal server newpt
[Switch-portal-server-newpt] ip 192.168.0.111 key simple portal
[Switch-portal-server-newpt] port 50100
[Switch-portal-server-newpt] quit
```

# Configure a portal Web server.

```
[Switch] portal web-server newpt
[Switch-portal-websvr-newpt] url http://192.168.0.111:8080/portal
[Switch-portal-websvr-newpt] quit
```

# Enable direct portal authentication on VLAN-interface 100.

```
[Switch] interface vlan-interface 100
[Switch–Vlan-interface100] portal enable method direct
```

# Reference the portal Web server **newpt** on VLAN-interface 100.

```
[Switch–Vlan-interface100] portal apply web-server newpt
```

# Configure the BAS-IP as 2.2.2.1 for portal packets sent from VLAN-interface 100 to the portal authentication server.

```
[Switch–Vlan-interface100] portal bas-ip 2.2.2.1
[Switch–Vlan-interface100] quit
```

Verifying the configuration

# Verify that the portal configuration has taken effect.

```
[Switch] display portal interface vlan-interface 100
 Portal information of Vlan-interface100
     Nas id profile: Not configured
 IPv4:
     Portal status: Enabled
     Authentication type: Direct
     Portal Web server: newpt
     Authentication domain: Not configured
     Bas-ip: 2.2.2.1
     User Detection:  Not configured
     Action for server detection:
         Server type    Server name                        Action
         --             --                                 --
     Layer3 source network:
         IP address               Mask

     Destination authenticate subnet:
         IP address               Mask
IPv6:
     Portal status: Disabled
     Authentication type: Disabled
     Portal Web server: Not configured
     Authentication domain: Not configured
     Bas-ipv6: Not configured
     User detection: Not configured
     Action for server detection:
         Server type    Server name                        Action
         --             --                                 --
     Layer3 source network:
         IP address                                        Prefix length

     Destination authenticate subnet:
         IP address                                        Prefix length
```

Before a user performs portal authentication by using the H3C iNode client, the user can access only the authentication page **http://192.168.0.111:8080/portal**. All Web requests the user initiates will be redirected to the authentication page.

- If the user passes the authentication but fails the security check, the user can access only the resources that match ACL 3000.
- After passing both the authentication and the security check, the user can access Internet resources that match ACL 3001.

# After the user passes authentication, use the following command to display information about the portal user.

```
[Switch] display portal user interface vlan-interface 100
Total portal users: 1
Username: abc
  Portal server: newpt
  State: Online
  Authorization ACL: 3001
  VPN instance: --
  MAC                IP                 VLAN   Interface
  0015-e9a6-7cfe     2.2.2.2            100    Vlan-interface100
```

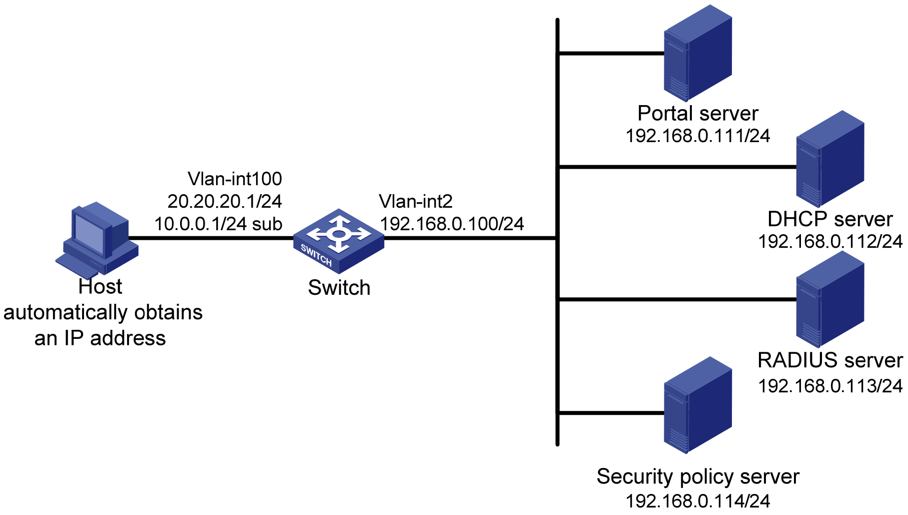
Configuring extended re-DHCP portal authentication

Network requirements

As shown in Figure 19, the host is directly connected to the switch (the access device). The host obtains an IP address through the DHCP server. A portal server acts as both a portal authentication server and a portal Web server. A RADIUS server acts as the authentication/accounting server.

Configure extended re-DHCP portal authentication. Before passing portal authentication, the host is assigned a private IP address. After passing portal identity authentication, the host obtains a public IP address and accepts security check. If the host fails the security check, it can access only subnet 192.168.0.0/24. After passing the security check, the host can access Internet resources.

Figure 19 Network diagram



Configuration prerequisites and guidelines

- Configure IP addresses for the switch and servers as shown in Figure 19 and make sure the host, switch, and servers can reach each other.
- Configure the RADIUS server properly to provide authentication and accounting functions.
- For re-DHCP portal authentication, configure a public address pool (20.20.20.0/24) and a private address pool (10.0.0.0/24) on the DHCP server. (Details not shown.)
- For re-DHCP portal authentication:
  - The switch must be configured as a DHCP relay agent.
  - The portal-enabled interface must be configured with a primary IP address (a public IP address) and a secondary IP address (a private IP address).

  For information about DHCP relay agent configuration, see *Layer 3—IP Services Configuration Guide*.
- Make sure the IP address of the portal device added on the portal server is the public IP address (20.20.20.1) of the switch's interface connecting the host. The private IP address range for the IP address group associated with the portal device is the private subnet 10.0.0.0/24 where the host resides. The public IP address range for the IP address group is the public subnet 20.20.20.0/24.

Configuration procedure

Perform the following tasks on the switch.

1. Configure a RADIUS scheme:

# Create a RADIUS scheme named **rs1** and enter its view.

```
<Switch> system-view
[Switch] radius scheme rs1
```

# Specify the primary authentication server and primary accounting server, and configure the keys for communication with the servers.

```
[Switch-radius-rs1] primary authentication 192.168.0.113
[Switch-radius-rs1] primary accounting 192.168.0.113
[Switch-radius-rs1] key accounting simple radius
[Switch-radius-rs1] key authentication simple radius
[Switch-radius-rs1] user-name-format without-domain
```

# Specify the security policy server.

```
[Switch-radius-rs1] security-policy-server 192.168.0.114
[Switch-radius-rs1] quit
```

# Enable RADIUS session control.

```
[Switch] radius session-control enable
```

2. Configure an authentication domain:

   # Create an ISP domain named **dm1** and enter its view.

   ```
   [Switch] domain dm1
   ```

   # Configure AAA methods for the ISP domain.

   ```
   [Switch-isp-dm1] authentication portal radius-scheme rs1
   [Switch-isp-dm1] authorization portal radius-scheme rs1
   [Switch-isp-dm1] accounting portal radius-scheme rs1
   [Switch-isp-dm1] quit
   ```

   # Configure domain **dm1** as the default ISP domain. If a user enters the username without the ISP domain name at login, the authentication and accounting methods of the default domain are used for the user.

   ```
   [Switch] domain default enable dm1
   ```

3. Configure ACL 3000 as the isolation ACL and ACL 3001 as the security ACL:

   ```
   [Switch] acl number 3000
   [Switch-acl-adv-3000] rule permit ip destination 192.168.0.0 0.0.0.255
   [Switch-acl-adv-3000] rule deny ip
   [Switch-acl-adv-3000] quit
   [Switch] acl number 3001
   [Switch-acl-adv-3001] rule permit ip
   [Switch-acl-adv-3001] quit
   ```

NOTE:

Make sure you specify ACL 3000 as the isolation ACL and ACL 3001 as the security ACL on the security policy server.

4. Configure DHCP relay and authorized ARP:

   # Configure DHCP relay.

   ```
   [Switch] dhcp enable
   [Switch] dhcp relay client-information record
   [Switch] interface vlan-interface 100
   [Switch–Vlan-interface100] ip address 20.20.20.1 255.255.255.0
   [Switch–Vlan-interface100] ip address 10.0.0.1 255.255.255.0 sub
   [Switch-Vlan-interface100] dhcp select relay
   [Switch-Vlan-interface100] dhcp relay server-address 192.168.0.112
   ```

   # Enable authorized ARP.

   ```
   [Switch-Vlan-interface100] arp authorized enable
   [Switch-Vlan-interface100] quit
   ```

5. Configure portal authentication:

   # Configure a portal authentication server.

   ```
   [Switch] portal server newpt
   [Switch-portal-server-newpt] ip 192.168.0.111 key simple portal
   [Switch-portal-server-newpt] port 50100
   [Switch-portal-server-newpt] quit
   ```

   # Configure a portal Web server.

```
[Switch] portal web-server newpt
[Switch-portal-websvr-newpt] url http://192.168.0.111:8080/portal
[Switch-portal-websvr-newpt] quit
```

# Enable re-DHCP portal authentication on VLAN-interface 100.

```
[Switch] interface vlan-interface 100
[Switch–Vlan-interface100] portal enable method redhcp
```

# Reference the portal Web server **newpt** on VLAN-interface 100.

```
[Switch–Vlan-interface100] portal apply web-server newpt
```

# Configure the BAS-IP as 20.20.20.1 for portal packets sent from VLAN-interface 100 to the portal authentication server.

```
[Switch–Vlan-interface100] portal bas-ip 20.20.20.1
[Switch–Vlan-interface100] quit
```

Verifying the configuration

# Verify that the portal configuration has taken effect.

```
[Switch] display portal interface vlan-interface 100
 Portal information of Vlan-interface100
     Nas id profile: Not configured
 IPv4:
     Portal status: Enabled
     Authentication type: Redhcp
     Portal Web server: newpt
     Authentication domain: Not configured
     Bas-ip: 20.20.20.1
     User Detection:  Not configured
     Action for server detection:
         Server type    Server name                        Action
         --             --                                 --
     Layer3 source network:
         IP address               Mask

     Destination authenticate subnet:
         IP address               Mask
IPv6:
     Portal status: Disabled
     Authentication type: Disabled
     Portal Web server: Not configured
     Authentication domain: Not configured
     Bas-ipv6: Not configured
     User detection: Not configured
     Action for server detection:
         Server type    Server name                        Action
         --             --                                 --
     Layer3 source network:
         IP address                                        Prefix length

     Destination authenticate subnet:
         IP address                                        Prefix length
```

Before a user performs portal authentication by using the H3C iNode client, the user can access only the authentication page **http://192.168.0.111:8080/portal**. All Web requests the user initiates will be redirected to the authentication page.

- If the user passes the authentication but fails the security check, the user can access only the resources that match ACL 3000.
- After passing both the authentication and the security check, the user can access Internet resources that match ACL 3001.

# After the user passes authentication, use the following command to display information about the portal user.

```
[Switch] display portal user interface vlan-interface 100
Total portal users: 1
Username: abc
  Portal server: newpt
  State: Online
  Authorization ACL: 3001
  VPN instance: --
  MAC                IP                  VLAN   Interface
  0015-e9a6-7cfe     20.20.20.2          100    Vlan-interface100
```

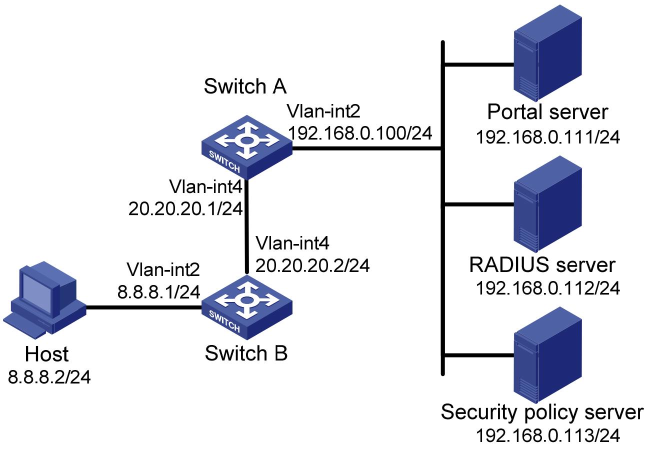
Configuring extended cross-subnet portal authentication

Network requirements

As shown in Figure 20, Switch A supports portal authentication. The host accesses Switch A through Switch B. A portal server acts as both a portal authentication server and a portal Web server. A RADIUS server acts as the authentication/accounting server.

Configure Switch A for extended cross-subnet portal authentication. Before passing portal authentication, the host can access only the portal server. After passing portal identity authentication, the host accepts security check. If the host fails the security check it can access only the subnet 192.168.0.0/24. After passing the security check, the host can access Internet resources.

Figure 20 Network diagram



Configuration prerequisites and guidelines

- Configure IP addresses for the switch and servers as shown in Figure 20 and make sure the host, switch, and servers can reach each other.
- Configure the RADIUS server properly to provide authentication and accounting functions.

- Make sure the IP address of the portal device added on the portal server is the IP address (20.20.20.1) of the switch's interface connecting the host. The IP address group associated with the portal device is the subnet of the host (8.8.8.0/24).

Configuration procedure

Perform the following tasks on Switch A.

1. Configure a RADIUS scheme:

   # Create a RADIUS scheme named **rs1** and enter its view.

   ```
   <SwitchA> system-view
   [SwitchA] radius scheme rs1
   ```

   # Specify the primary authentication server and primary accounting server, and configure the keys for communication with the servers.

   ```
   [SwitchA-radius-rs1] primary authentication 192.168.0.112
   [SwitchA-radius-rs1] primary accounting 192.168.0.112
   [SwitchA-radius-rs1] key accounting simple radius
   [SwitchA-radius-rs1] key authentication simple radius
   [SwitchA-radius-rs1] user-name-format without-domain
   ```

   # Specify the security policy server.

   ```
   [SwitchA-radius-rs1] security-policy-server 192.168.0.113
   [SwitchA-radius-rs1] quit
   ```

   # Enable RADIUS session control.

   ```
   [SwitchA] radius session-control enable
   ```

2. Configure an authentication domain:

   # Create an ISP domain named **dm1** and enter its view.

   ```
   [SwitchA] domain dm1
   ```

   # Configure AAA methods for the ISP domain.

   ```
   [SwitchA-isp-dm1] authentication portal radius-scheme rs1
   [SwitchA-isp-dm1] authorization portal radius-scheme rs1
   [SwitchA-isp-dm1] accounting portal radius-scheme rs1
   [SwitchA-isp-dm1] quit
   ```

   # Configure domain **dm1** as the default ISP domain. If a user enters the username without the ISP domain name at login, the authentication and accounting methods of the default domain are used for the user.

   ```
   [SwitchA] domain default enable dm1
   ```

3. Configure ACL 3000 as the isolation ACL and ACL 3001 as the security ACL:

   ```
   [SwitchA] acl number 3000
   [SwitchA-acl-adv-3000] rule permit ip destination 192.168.0.0 0.0.0.255
   [SwitchA-acl-adv-3000] rule deny ip
   [SwitchA-acl-adv-3000] quit
   [SwitchA] acl number 3001
   [SwitchA-acl-adv-3001] rule permit ip
   [SwitchA-acl-adv-3001] quit
   ```

   NOTE:

   Make sure you specify ACL 3000 as the isolation ACL and ACL 3001 as the security ACL on the security policy server.

4. Configure portal authentication:

   # Configure a portal authentication server.

```
[SwitchA] portal server newpt
[SwitchA-portal-server-newpt] ip 192.168.0.111 key simple portal
[SwitchA-portal-server-newpt] port 50100
[SwitchA-portal-server-newpt] quit
```

# Configure a portal Web server.

```
[SwitchA] portal web-server newpt
[SwitchA-portal-websvr-newpt] url http://192.168.0.111:8080/portal
[SwitchA-portal-websvr-newpt] quit
```

# Enable cross-subnet portal authentication on VLAN-interface 4.

```
[SwitchA] interface vlan-interface 4
[SwitchA–Vlan-interface4] portal enable method layer3
```

# Reference the portal Web server newpt on VLAN-interface 4.

```
[SwitchA–Vlan-interface4] portal apply web-server newpt
```

# Configure the BAS-IP as 20.20.20.1 for portal packets sent from VLAN-interface 4 to the portal authentication server.

```
[SwitchA–Vlan-interface4] portal bas-ip 20.20.20.1
[SwitchA–Vlan-interface4] quit
```

On Switch B, configure a default route to subnet 192.168.0.0/24, specifying the next hop address as 20.20.20.1. (Details not shown.)

Verifying the configuration

# Verify that the portal configuration has taken effect.

```
[SwitchA] display portal interface vlan-interface 4
 Portal information of Vlan-interface4
     Nas id profile: Not configured
 IPv4:
     Portal status: Enabled
     Authentication type: Layer3
     Portal Web server: newpt
     Authentication domain: Not configured
     Bas-ip: 20.20.20.1
     User Detection:  Not configured
     Action for server detection:
         Server type    Server name                        Action
         --             --                                 --
     Layer3 source network:
         IP address               Mask

     Destination authenticate subnet:
         IP address               Mask
IPv6:
     Portal status: Disabled
     Authentication type: Disabled
     Portal Web server: Not configured
     Authentication domain: Not configured
     Bas-ipv6: Not configured
     User detection: Not configured
     Action for server detection:
         Server type    Server name                        Action
```

```
        --             --                                 --
    Layer3 source network:
        IP address                                        Prefix length

    Destination authenticate subnet:
        IP address                                        Prefix length
```

Before a user performs portal authentication by using the H3C iNode client, the user can access only the authentication page **http://192.168.0.111:8080/portal**. All Web requests the user initiates will be redirected to the authentication page.

- If the user passes the authentication but fails the security check, the user can access only the resources that match ACL 3000.
- After passing both the authentication and the security check, the user can access Internet resources that match ACL 3001.

# After the user passes authentication, use the following command to display information about the portal user.

```
[SwitchA] display portal user interface vlan-interface 4
Total portal users: 1
Username: abc
  Portal server: newpt
  State: Online
  Authorization ACL: 3001
  VPN instance: --
  MAC                IP                 VLAN   Interface
  0015-e9a6-7cfe     8.8.8.2            4      Vlan-interface4
```

Configuring portal server detection and portal user synchronization

Network requirements

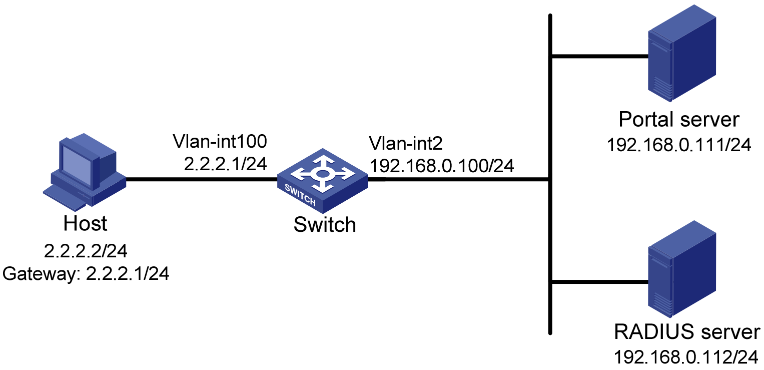
As shown in Figure 21, the host is directly connected to the switch (the access device). The host is assigned a public IP address either manually or through DHCP. A portal server acts as both a portal authentication server and a portal Web server. A RADIUS server acts as the authentication/accounting server.

Configure direct portal authentication on the switch, so the host can access only the portal server before passing the authentication and access Internet resources after passing the authentication.

Configure the switch to do the following:

- Detect the reachability state of the portal authentication server.
- Send log messages upon state changes.
- Disable portal authentication when the authentication server is unreachable.
- Synchronize portal user information with the portal server periodically.

Figure 21 Network diagram



Configuration prerequisites and guidelines

- Configure IP addresses for the switch and servers as shown in Figure 21 and make sure the host, switch, and servers can reach each other.
- Configure the RADIUS server properly to provide authentication and accounting functions.
- Configure the portal authentication server. Be sure to enable the server heartbeat function and the user heartbeat function.
- Configure the switch (access device) as follows:
    - Configure direct portal authentication on VLAN-interface 100, the interface to which the host is connected.
    - Configure portal authentication server detection, so that the switch can detect the reachability of the portal authentication server by cooperating with the portal server heartbeat function.
    - Configure portal user synchronization, so that the switch can synchronize portal user information with the portal authentication server by cooperating with the portal user heartbeat function.

Configuring the portal authentication server on IMC PLAT 3.20

This example assumes that the portal server runs on IMC PLAT 3.20-R2602P13 and IMC UAM 3.60-E6301.

1. Configure the portal authentication server:

   a. Log in to IMC and click the **Service** tab.

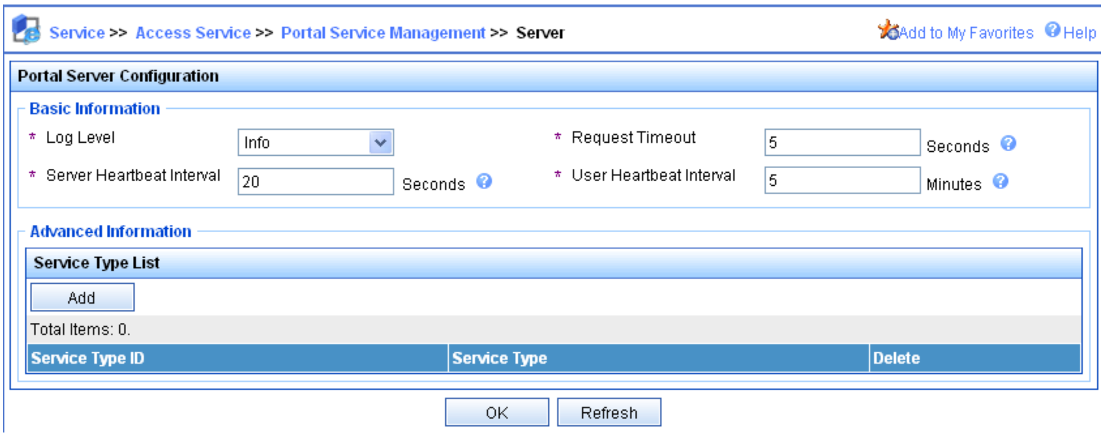
   b. Select **Access Service** > **Portal Service Management** > **Server** from the navigation tree to enter the portal server configuration page, as shown in Figure 22.

   c. Configure the portal server heartbeat interval and user heartbeat interval.

   d. Use the default settings for other parameters.

   e. Click **OK**.

Figure 22 Portal authentication server configuration



Service >> Access Service >> Portal Service Management >> Server

Add to My Favorites Help

Portal Server Configuration

Basic Information

* Log Level	Info	* Request Timeout	5 Seconds
* Server Heartbeat Interval	20 Seconds	* User Heartbeat Interval	5 Minutes

Advanced Information

Service Type List

Add

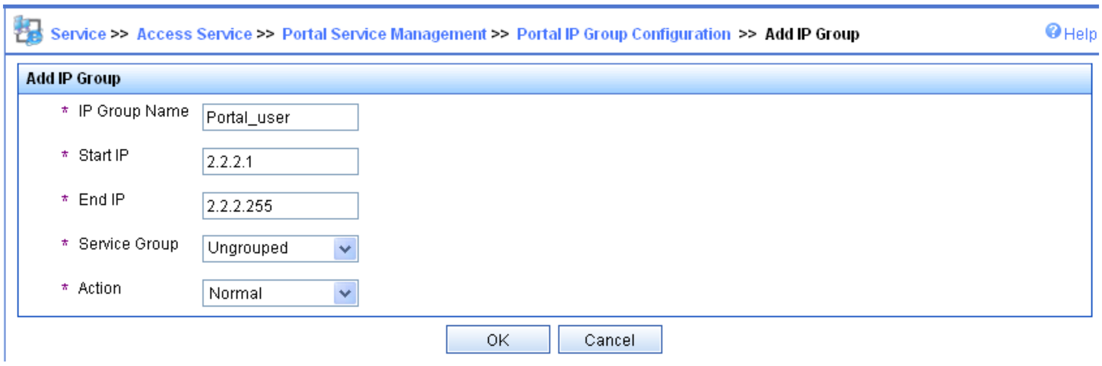
Total Items: 0.

Service Type ID	Service Type	Delete

OK Refresh

2. Configure the IP address group:
   a. Select **Access Service** > **Portal Service Management** > **IP Group** from the navigation tree to enter the portal IP address group configuration page.
   b. Click **Add** to open the page as shown in Figure 23.
   c. Enter the IP group name.
   d. Enter the start IP address and end IP address of the IP group.
      Make sure the host IP address (2.2.2.2) is in the IP group.
   e. Select a service group.
      This example uses the default group **Ungrouped**.
   f. Select **Normal** from the **Action** list.
   g. Click **OK**.

Figure 23 Adding an IP address group



Service >> Access Service >> Portal Service Management >> Portal IP Group Configuration >> Add IP Group

Help

Add IP Group

* IP Group Name	Portal_user
* Start IP	2.2.2.1
* End IP	2.2.2.255
* Service Group	Ungrouped
* Action	Normal

OK Cancel

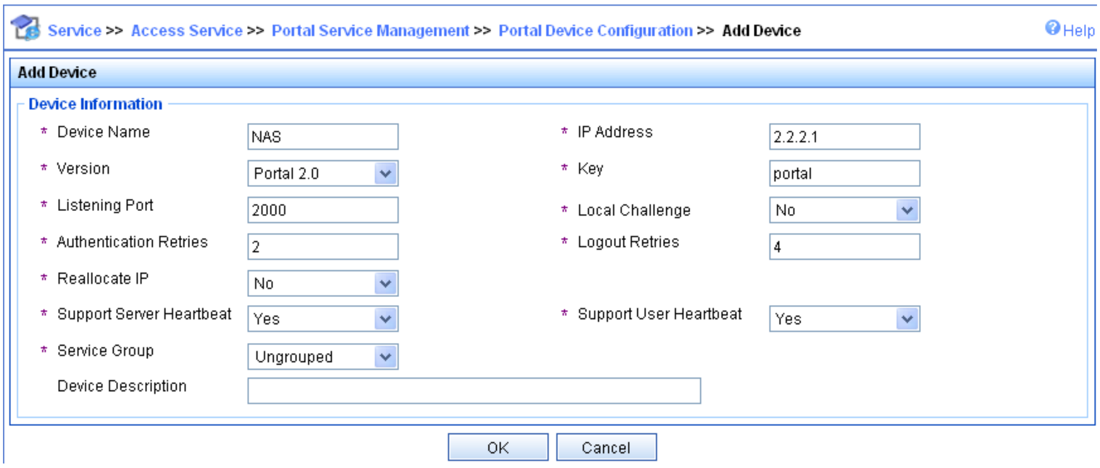
3. Add a portal device:
   a. Select **Access Service** > **Portal Service Management** > **Device** from the navigation tree to enter the portal device configuration page.
   b. Click **Add** to open the page as shown in Figure 24.
   c. Enter the device name **NAS**.
   d. Enter the IP address of the switch's interface connected to the host.
   e. Enter the key, which must be the same as that configured on the switch.
   f. Set whether to enable IP address reallocation.
      This example uses direct portal authentication. Therefore, select **No** from the **Reallocate IP** list.

g. Set whether to support the portal server heartbeat and user heartbeat functions.

   In this example, select **Yes** for both **Support Server Heartbeat** and **Support User Heartbeat**.

h. Click **OK**.

Figure 24 Adding a portal device



Service >> Access Service >> Portal Service Management >> Portal Device Configuration >> Add Device Help

Add Device

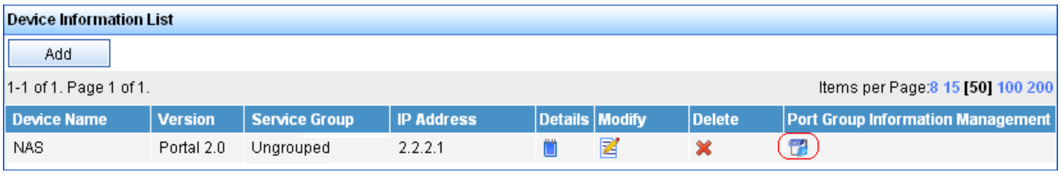
Device Information

* Device Name	NAS	* IP Address	2.2.2.1
* Version	Portal 2.0	* Key	portal
* Listening Port	2000	* Local Challenge	No
* Authentication Retries	2	* Logout Retries	4
* Reallocate IP	No		
* Support Server Heartbeat	Yes	* Support User Heartbeat	Yes
* Service Group	Ungrouped		
Device Description			

4. Associate the portal device with the IP address group:

   a. As shown in Figure 25, click the icon in the **Port Group Information Management** column of device **NAS** to enter the port group configuration page.

Figure 25 Device list



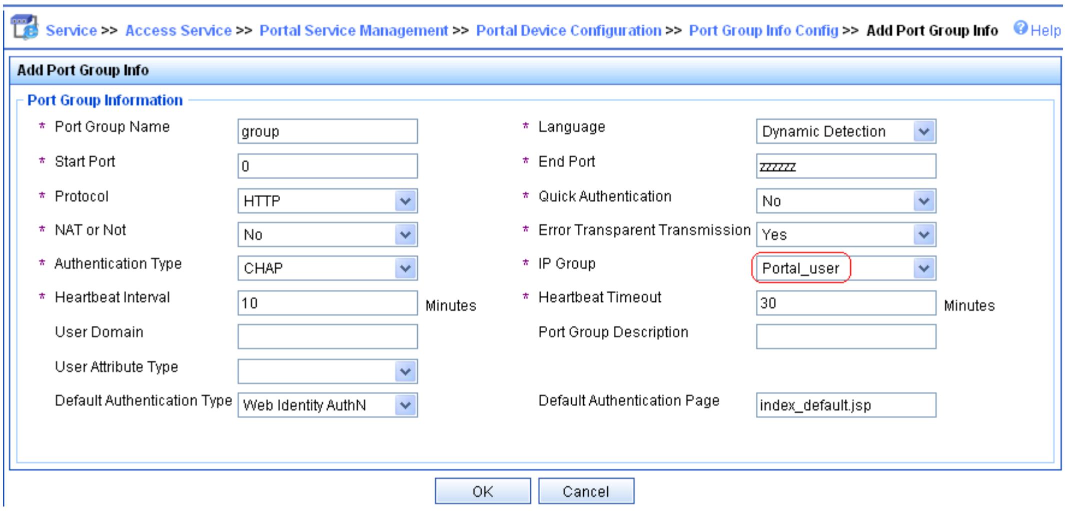
Device Information List

1-1 of 1. Page 1 of 1. Items per Page:8 15 [50] 100 200

Device Name	Version	Service Group	IP Address	Details	Modify	Delete	Port Group Information Management
NAS	Portal 2.0	Ungrouped	2.2.2.1			✗	

   b. Click **Add** to open the page as shown in Figure 26.

Figure 26 Port group configuration



Service >> Access Service >> Portal Service Management >> Portal Device Configuration >> Port Group Info Config >> Add Port Group Info Help

Add Port Group Info

Port Group Information

* Port Group Name	group	* Language	Dynamic Detection
* Start Port	0	* End Port	zzzzzz
* Protocol	HTTP	* Quick Authentication	No
* NAT or Not	No	* Error Transparent Transmission	Yes
* Authentication Type	CHAP	* IP Group	Portal_user
* Heartbeat Interval	10 Minutes	* Heartbeat Timeout	30 Minutes
User Domain		Port Group Description	
User Attribute Type			
Default Authentication Type	Web Identity AuthN	Default Authentication Page	index_default.jsp

   c. Enter the port group name.

   d. Select the configured IP address group.

The IP address used by the user to access the network must be within this IP address group.

e. User default values for other parameters.

f. Click **OK**.

5. Select **Access Service** > **Service Parameters** > **Validate System Configuration** from the navigation tree to validate the configurations.

Configuring the portal authentication server on IMC PLAT 5.0

This example assumes that the portal server runs on IMC PLAT 5.0(E0101) and IMC UAM 5.0(E0101).

1. Configure the portal authentication server:

a. Log in to IMC and click the **Service** tab.

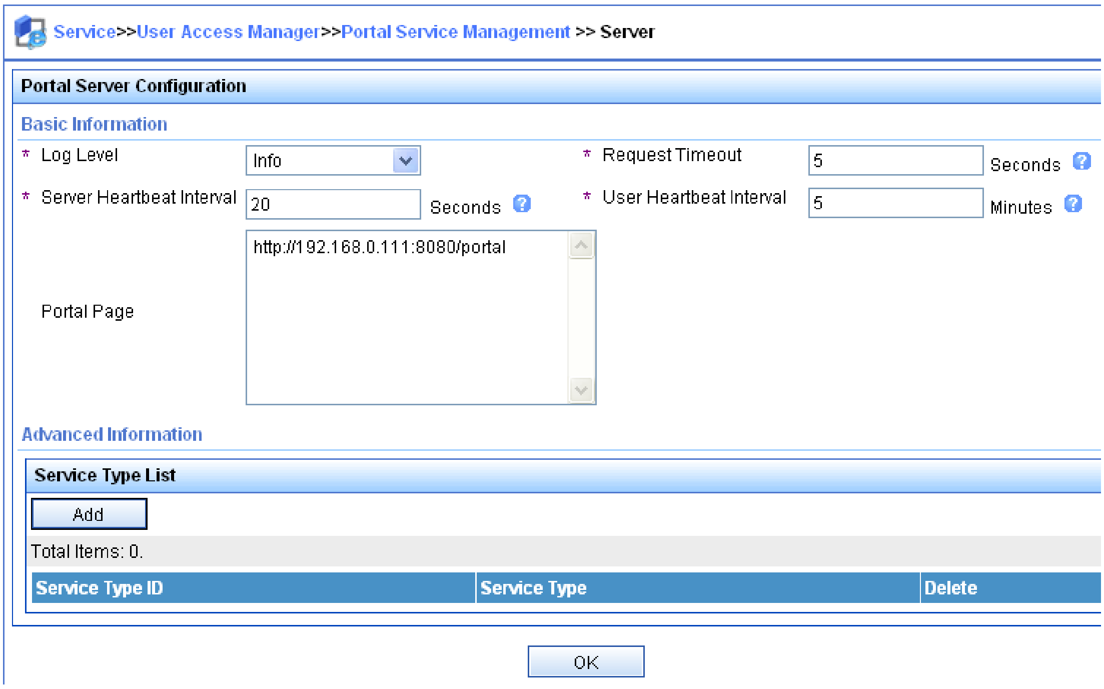
b. Select **User Access Manager** > **Portal Service Management** > **Server** from the navigation tree to enter the portal server configuration page, as shown in Figure 27.

c. Configure the portal server heartbeat interval and user heartbeat interval.

d. Use the default settings for other parameters.

e. Click **OK**.

Figure 27 Portal authentication server configuration



Service>>User Access Manager>>Portal Service Management >> Server

Portal Server Configuration

Basic Information

* Log Level: Info

* Request Timeout: 5 Seconds

* Server Heartbeat Interval: 20 Seconds

* User Heartbeat Interval: 5 Minutes

Portal Page: http://192.168.0.111:8080/portal

Advanced Information

Service Type List

Add

Total Items: 0.

Service Type ID	Service Type	Delete

OK

2. Configure the IP address group:

a. Select **User Access Manager** > **Portal Service Management** > **IP Group** from the navigation tree to enter the portal IP address group configuration page.

b. Click **Add** to open the page as shown in Figure 28.

c. Enter the IP group name.

d. Enter the start IP address and end IP address of the IP group.

Make sure the host IP address is in the IP group.

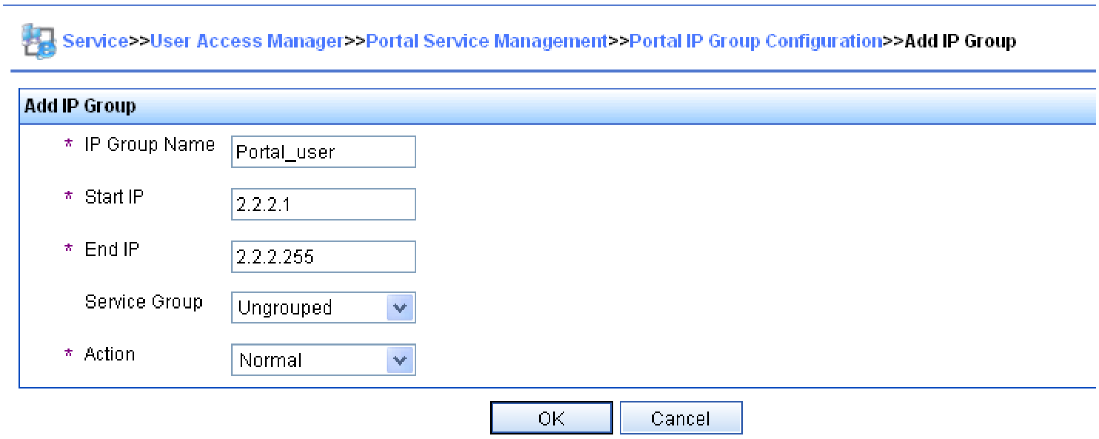
e. Select a service group.

This example uses the default group **Ungrouped**.

f. Select **Normal** from the **Action** list.

g. Click **OK**.

Figure 28 Adding an IP address group


Service>>User Access Manager>>Portal Service Management>>Portal IP Group Configuration>>Add IP Group
OK
Cancel

Add IP Group

* IP Group Name	Portal_user
* Start IP	2.2.2.1
* End IP	2.2.2.255
Service Group	Ungrouped
* Action	Normal

3. Add a portal device:

a. Select **User Access Manager** > **Portal Service Management** > **Device** from the navigation tree to enter the portal device configuration page.

b. Click **Add** to open the page as shown in Figure 29.

c. Enter the device name **NAS**.

d. Enter the IP address of the switch's interface connected to the host.

e. Enter the key, which must be the same as that configured on the switch.

f. Set whether to enable IP address reallocation.

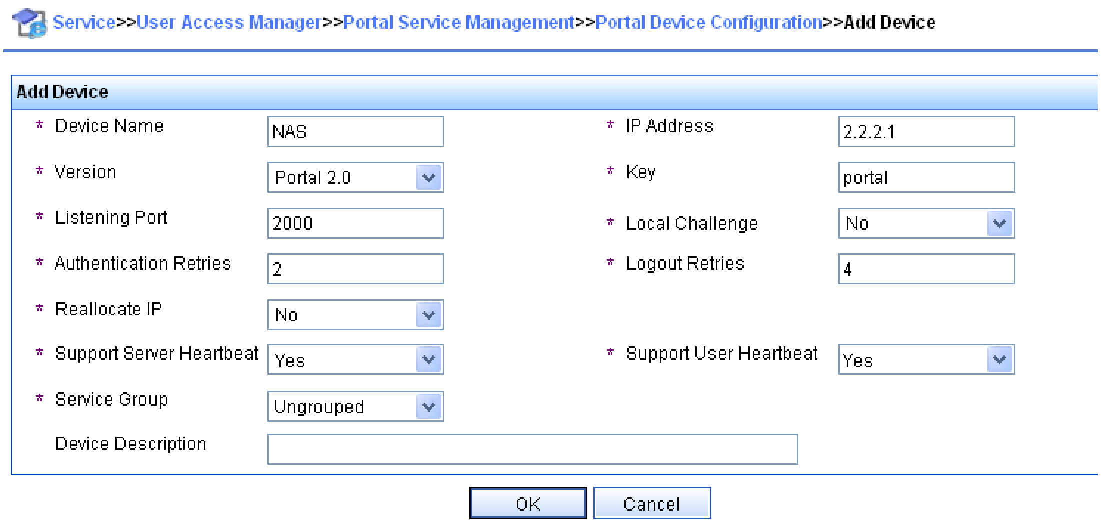
This example uses direct portal authentication. Therefore, select **No** from the **Reallocate IP** list.

g. Select whether to support server heartbeat and user heartbeat functions.

In this example, select **Yes** for both **Support Server Heartbeat** and **Support User Heartbeat**.

h. Click **OK**.

Figure 29 Adding a portal device


Service>>User Access Manager>>Portal Service Management>>Portal Device Configuration>>Add Device
OK
Cancel

Add Device

* Device Name	NAS	* IP Address	2.2.2.1
* Version	Portal 2.0	* Key	portal
* Listening Port	2000	* Local Challenge	No
* Authentication Retries	2	* Logout Retries	4
* Reallocate IP	No		
* Support Server Heartbeat	Yes	* Support User Heartbeat	Yes
* Service Group	Ungrouped		
Device Description			

4. Associate the portal device with the IP address group:

a. As shown in Figure 30, click the icon in the **Port Group Information Management** column of device **NAS** to enter the port group configuration page.

b. Click **Add** to open the page as shown in Figure 31.

c. Enter the port group name.

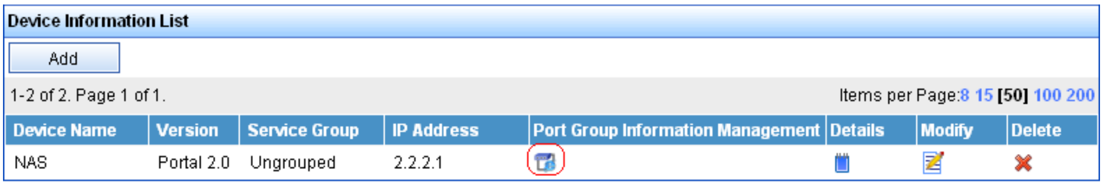
d. Select the configured IP address group.

   The IP address used by the user to access the network must be within this IP address group.

e. Use the default settings for other parameters.

f. Click **OK**.

Figure 30 Device list



Device Information List

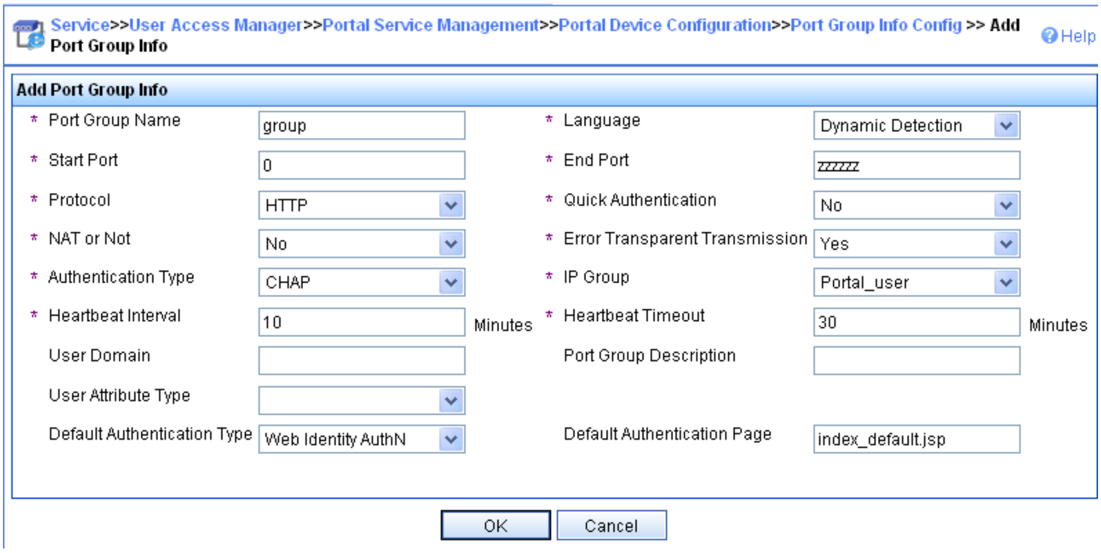
Add

1-2 of 2. Page 1 of 1.

Items per Page:8 15 [50] 100 200

Device Name	Version	Service Group	IP Address	Port Group Information Management	Details	Modify	Delete
NAS	Portal 2.0	Ungrouped	2.2.2.1				✖

Figure 31 Adding a port group



Service>>User Access Manager>>Portal Service Management>>Portal Device Configuration>>Port Group Info Config >> Add Port Group Info

Help

Add Port Group Info

* Port Group Name	group		* Language	Dynamic Detection	
* Start Port	0		* End Port	zzzzzz	
* Protocol	HTTP		* Quick Authentication	No	
* NAT or Not	No		* Error Transparent Transmission	Yes	
* Authentication Type	CHAP		* IP Group	Portal_user	
* Heartbeat Interval	10	Minutes	* Heartbeat Timeout	30	Minutes
User Domain			Port Group Description		
User Attribute Type					
Default Authentication Type	Web Identity AuthN		Default Authentication Page	index_default.jsp	

OK Cancel

5. Select **User Access Manager** > **Service Parameters** > **Validate System Configuration** from the navigation tree to validate the configurations.

Configuring the switch

1. Configure a RADIUS scheme:

   # Create a RADIUS scheme named **rs1** and enter its view.

```
<Switch> system-view
[Switch] radius scheme rs1
```

   # Specify the primary authentication server and primary accounting server, and configure the keys for communication with the servers.

```
[Switch-radius-rs1] primary authentication 192.168.0.112
[Switch-radius-rs1] primary accounting 192.168.0.112
[Switch-radius-rs1] key authentication simple radius
[Switch-radius-rs1] key accounting simple radius
```

   # Exclude the ISP domain name from the username sent to the RADIUS server.

```
[Switch-radius-rs1] user-name-format without-domain
[Switch-radius-rs1] quit
```

# Enable RADIUS session control.

```
[Switch] radius session-control enable
```

2. Configure an authentication domain:

   # Create an ISP domain named **dm1** and enter its view.

   ```
   [Switch] domain dm1
   ```

   # Configure AAA methods for the ISP domain.

   ```
   [Switch-isp-dm1] authentication portal radius-scheme rs1
   [Switch-isp-dm1] authorization portal radius-scheme rs1
   [Switch-isp-dm1] accounting portal radius-scheme rs1
   [Switch-isp-dm1] quit
   ```

   # Configure domain **dm1** as the default ISP domain. If a user enters the username without the ISP domain name at login, the authentication and accounting methods of the default domain are used for the user.

   ```
   [Switch] domain default enable dm1
   ```

3. Configure portal authentication:

   # Configure a portal authentication server.

   ```
   [Switch] portal server newpt
   [Switch-portal-server-newpt] ip 192.168.0.111 key simple portal
   [Switch-portal-server-newpt] port 50100
   ```

   # Configure reachability detection of the portal authentication server: configure the server detection interval as 40 seconds, and send log messages upon reachability status changes.

   ```
   [Switch-portal-server-newpt] server-detect timeout 40 log
   ```

   NOTE:

   The value of **timeout** must be greater than or equal to the portal server heartbeat interval.

   # Configure portal user synchronization with the portal authentication server, and configure the synchronization detection interval as 600 seconds.

   ```
   [Switch-portal-server-newpt] user-sync timeout 600
   [Switch-portal-server-newpt] quit
   ```

   NOTE:

   The value of **timeout** must be greater than or equal to the portal user heartbeat interval.

   # Configure a portal Web server.

   ```
   [Switch] portal web-server newpt
   [Switch-portal-websvr-newpt] url http://192.168.0.111:8080/portal
   [Switch-portal-websvr-newpt] quit
   ```

   # Enable direct portal authentication on VLAN-interface 100.

   ```
   [Switch] interface vlan-interface 100
   [Switch–Vlan-interface100] portal enable method direct
   ```

   # Enable portal fail-permit for the portal authentication server **newpt**.

   ```
   [Switch–Vlan-interface100] portal fail-permit server newpt
   ```

   # Reference the portal Web server **newpt** on VLAN-interface 100.

   ```
   [Switch–Vlan-interface100] portal apply web-server newpt
   ```

   # Configure the BAS-IP as 2.2.2.1 for portal packets sent from VLAN-interface 100 to the portal authentication server.

```
[Switch-Vlan-interface100] portal bas-ip 2.2.2.1
[Switch-Vlan-interface100] quit
```

Verifying the configuration

# Use the following command to display information about the portal authentication server.

```
[Switch] display portal server newpt
Portal server: newpt
  IP                     : 192.168.0.111
  VPN instance           : Not configured
  Port                   : 50100
  Server Detection       : Timeout 40s  Action: log
  User synchronization   : Timeout 600s
  Status                 : Up
```

The **Up** status of the portal authentication server indicates that the portal authentication server is reachable. If the access device detects that the portal authentication server is unreachable, the **Status** field in the command output displays **Down**. The access device generates a server unreachable log "Portal server newpt turns down from up" and disables portal authentication on the access interface, so the host can access the external network without authentication.

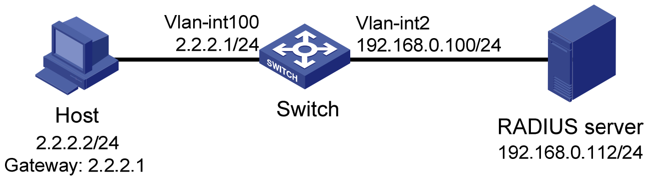
Configuring direct portal authentication using the local portal Web server

Network requirements

As shown in Figure 32, the host is directly connected to the switch (the access device). The host is assigned a public IP address either manually or through DHCP. The switch acts as both a portal authentication server and a portal Web server. A RADIUS server acts as the authentication/accounting server.

Configure direct portal authentication on the switch. Before a user passes portal authentication, the user can access only the local portal Web server. After passing portal authentication, the user can access other network resources.

Figure 32 Network diagram



Configuration prerequisites and guidelines

- Configure IP addresses for the host, switch, and server as shown in Figure 2 and make sure they can reach each other.
- Configure the RADIUS server correctly to provide authentication and accounting functions.
- Customize the authentication pages, compress them to a file, and upload the file to the root directory of the storage medium of the switch.

Configuration procedure

1. Configure a RADIUS scheme:

   # Create a RADIUS scheme named **rs1** and enter its view.

```
<Switch> system-view
[Switch] radius scheme rs1
```

# Specify the primary authentication server and primary accounting server, and configure the keys for communication with the servers.

```
[Switch-radius-rs1] primary authentication 192.168.0.112
[Switch-radius-rs1] primary accounting 192.168.0.112
[Switch-radius-rs1] key authentication simple radius
[Switch-radius-rs1] key accounting simple radius
```

# Exclude the ISP domain name from the username sent to the RADIUS server.

```
[Switch-radius-rs1] user-name-format without-domain
[Switch-radius-rs1] quit
```

# Enable RADIUS session control.

```
[Switch] radius session-control enable
```

2. Configure an authentication domain:

# Create an ISP domain named **dm1** and enter its view.

```
[Switch] domain dm1
```

# Configure AAA methods for the ISP domain.

```
[Switch-isp-dm1] authentication portal radius-scheme rs1
[Switch-isp-dm1] authorization portal radius-scheme rs1
[Switch-isp-dm1] accounting portal radius-scheme rs1
[Switch-isp-dm1] quit
```

# Configure domain **dm1** as the default ISP domain. If a user enters the username without the ISP domain name at login, the authentication and accounting methods of the default domain are used for the user.

```
[Switch] domain default enable dm1
```

3. Configure portal authentication:

# Create a local portal Web server. Use HTTP to exchange authentication information with clients.

```
[Switch] portal local-web-server http
```

# Specify file **abc.zip** as the default authentication page file for local portal authentication. (Make sure the file exist under the root directory of the switch.)

```
[Switch–portal-local-websvr-http] default-logon-page abc.zip
```

# Set the HTTP service listening port number to 2331 for the local portal Web server.

```
[Switch–portal-local-webserver-http] tcp-port 2331
[Switch–portal-local-websvr-http] quit
```

# Configure the portal Web server name as **newpt** and URL as the IP address of the portal authentication-enabled interface or a loopback interface (except 127.0.0.1).

```
[Switch] portal web-server newpt
[Switch-portal-websvr-newpt] url http://2.2.2.1:8080/portal
[Switch-portal-websvr-newpt] quit
```

# Enable direct portal authentication on VLAN-interface 100.

```
[Switch] interface vlan-interface 100
[Switch–Vlan-interface100] portal enable method direct
```

# Specify the portal Web server **newpt** on VLAN-interface 100.

```
[Switch–Vlan-interface100] portal apply web-server newpt
[Switch–Vlan-interface100] quit
```

Verifying the configuration

# Verify that the portal configuration has taken effect.

```
[Switch] display portal interface vlan-interface 100
 Portal information of Vlan-interface 100
```

```
     VSRP instance: --
     VSRP state: N/A
     Authorization                  Strict checking
     ACL                            Disabled
     User profile                   Disabled
 IPv4:
     Portal status: Enabled
     Authentication type: Direct
     Portal Web server: newpt
     Authentication domain: Not configured
     Pre-auth IP pool: Not configured
     BAS-IP: Not configured
     User Detection:  Not configured
     Action for server detection:
         Server type    Server name                        Action
         --             --                                 --
     Layer3 source network:
         IP address               Mask

     Destination authenticate subnet:
         IP address               Mask
IPv6:
     Portal status: Disabled
     Authentication type: Disabled
     Portal Web server: Not configured
     Authentication domain: Not configured
     Pre-auth IP pool: Not configured
     BAS-IPv6: Not configured
     User detection: Not configured
     Action for server detection:
         Server type    Server name                        Action
         --             --                                 --
     Layer3 source network:
         IP address                                        Prefix length

     Destination authenticate subnet:
         IP address                                        Prefix length
```

A user can perform portal authentication by using a Web browser. Before passing the authentication, the user can access only the authentication page **http://2.2.2.1:8080/portal** and all Web requests will be redirected to the authentication page. After passing the authentication, the user can access Internet resources.

# After the user passes authentication, use the following command to display information about the portal user.

```
[Switch] display portal user interface vlan-interface 100
Total portal users: 1
Username: abc
  Portal server: newpt
  State: Online
  VPN instance: --
```

```
MAC                IP                 VLAN   Interface
0015-e9a6-7cfe     2.2.2.2            --     vlan-interface 100
Authorization information:
  IP pool: N/A
  User profile: N/A
  Session group profile: N/A
  ACL: N/A
  CAR: N/A
```

Troubleshooting portal

No portal authentication page is pushed for users

Symptom

When a user is redirected to the IMC portal authentication server, no portal authentication page or error message is prompted for the user. The login page is blank.

Analysis

The key configured on the portal access device and that configured on the portal authentication server are inconsistent. As a result, packet verification fails, and the portal authentication server refuses to push the authentication page.

Solution

Use the **display portal server** command on the access device to check whether a key is configured for the portal authentication server.

- If no key is configured, configure the right key.
- If a key is configured, use the **ip** or **ipv6** command in the portal authentication server view to correct the key, or correct the key configured for the access device on the portal authentication server.

Cannot log out portal users on the access device

Symptom

You cannot use the **portal delete-user** command on the access device to log out a portal user, but the portal user can log out by clicking the **Disconnect** button on the portal authentication client.

Analysis

When you execute the **portal delete-user** command on the access device to log out a user, the access device sends an unsolicited logout notification message to the portal authentication server. The destination port number in the logout notification is the listening port number of the portal authentication server configured on the access device. If this listening port number is not the actual listening port number configured on the server, the server cannot receive the notification. As a result, the portal server does not log out the user.

When a user uses the **Disconnect** button on the authentication client to log out, the portal authentication server sends an unsolicited logout request message to the access device. The access device uses the source port in the logout request as the destination port in the logout ACK message. As a result, the portal authentication server can definitely receive the logout ACK message and log out the user.

Solution

1. Use the **display portal server** command to display the listening port of the portal authentication server configured on the access device.
2. Use the **portal server** command in system view to change the listening port number to the actual listening port of the portal authentication server.

Cannot log out portal users on the RADIUS server

Symptom

The access device uses the H3C IMC server as the RADIUS server to perform identity authentication for portal users. You cannot log out the portal users on the RADIUS server.

Analysis

The H3C IMC server uses session control packets to send disconnection requests to the access device. On the access device, the listening UDP port for session control packets is disabled by default. Therefore, the access device cannot receive the portal user logout requests from the RADIUS server.

Solution

On the access device, execute the **radius session-control enable** command in system view to enable the RADIUS session control function.

Users logged out by the access device still exist on the portal authentication server

Symptom

After you log out a portal user on the access device, the user still exists on the portal authentication server.

Analysis

When you execute the **portal delete-user** command on the access device to log out a user, the access device sends an unsolicited logout notification to the portal authentication server. If the BAS-IP or BAS-IPv6 address carried in the logout notification is different from the portal device IP address specified on the portal authentication server, the portal authentication server discards the logout notification. When sending of the logout notifications times out, the access device logs out the user. However, the portal authentication server does not receive the logout notification successfully. Therefore, it regards the user is still online.

Solution

Configure the BAS-IP or BAS-IPv6 attribute on the interface enabled with portal authentication. Make sure the attribute value is the same as the portal device IP address specified on the portal authentication server.

Re-DHCP portal authenticated users cannot log in successfully

Symptom

The device performs re-DHCP portal authentication for users. A user enters the correct username and password, and the client successfully obtains the private and public IP addresses. However, the authentication result for the user is failure.

Analysis

When the access device detects that the client IP address is changed, it sends an unsolicited portal packet to notify of the IP change to the portal authentication server. The portal authentication server notifies of the authentication success only after it receives the IP change notification from both the access device and the client.

If the BAS-IP or BAS-IPv6 address carried in the portal notification packet is different from the portal device IP address specified on the portal authentication server, the portal authentication server discards the portal notification packet. As a result, the portal authentication server considers that the user has failed the authentication.

Solution

Configure the BAS-IP or BAS-IPv6 attribute on the interface enabled with portal authentication. Make sure the attribute value is the same as the portal device IP address specified on the portal authentication server.