

# Contents

Introduction .....	1
Prerequisites .....	1
Restrictions and guidelines .....	1
Example: Configuring cross-subnet portal authentication .....	1
Network configuration .....	1
Analysis .....	2
Applicable hardware and software versions .....	2
Procedures .....	4
Configuring Device A .....	4
Configuring Device B .....	5
Configuring the RADIUS and portal server .....	6
Verifying the configuration .....	12
Configuration files .....	12
Example: Configuring extended cross-subnet portal authentication .....	13
Network configuration .....	13
Analysis .....	14
Applicable hardware and software versions .....	14
Procedures .....	16
Configuring Device A .....	16
Configuring Device B .....	17
Configuring the RADIUS, portal, and security policy server .....	18
Verifying the configuration .....	19
Configuration files .....	20
Example: Configuring direct portal authentication .....	21
Network configuration .....	21
Analysis .....	22
Applicable hardware and software versions .....	22
Procedures .....	24
Configuring the device .....	24
Configuring the RADIUS and portal server .....	25
Verifying the configuration .....	25
Configuration files .....	26

# Introduction

This document provides examples for configuring the following portal authentications:

- **Cross-subnet authentication**—Applies to networks where Layer 3 forwarding devices exist between the authentication client and the access device. After a user passes authentication on an interface, the access device generates an ACL for the user based on the user's IP address to permit packets from the user on the interface.
- **Direct authentication**—Applies to networks where no layer 3 forwarding devices exist between the authentication client and the access device. In such a network, the access device can learn MAC addresses of users. The access device can use both ACLs and MAC addresses to enhance control on user packet forwarding.

## Prerequisites

The configuration examples in this document were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

This document assumes that you have basic knowledge of portal.

## Restrictions and guidelines

When you configure direct or cross-subnet portal authentication, follow these restrictions and guidelines:

- Only the RADIUS server can perform authentication, authorization, and accounting for portal users.
- On the RADIUS server, configure routes to reach the authentication interfaces and user networks.
- The INC server uses session control packets to send disconnection requests to the access device. If you use the INC server as the RADIUS server, execute the **radius session-control enable** command on the access device. Otherwise, the access device cannot receive portal user logout requests from the RADIUS server.
- When the access device runs Portal 2.0, configure the BAS-IP attribute for portal packets sent to the portal authentication server. Make sure the BAS-IP is the same as the **IP Address** configured on the portal authentication server. Otherwise, the portal authentication server will drop unsolicited portal packets (such as logout notifications) from the access device.

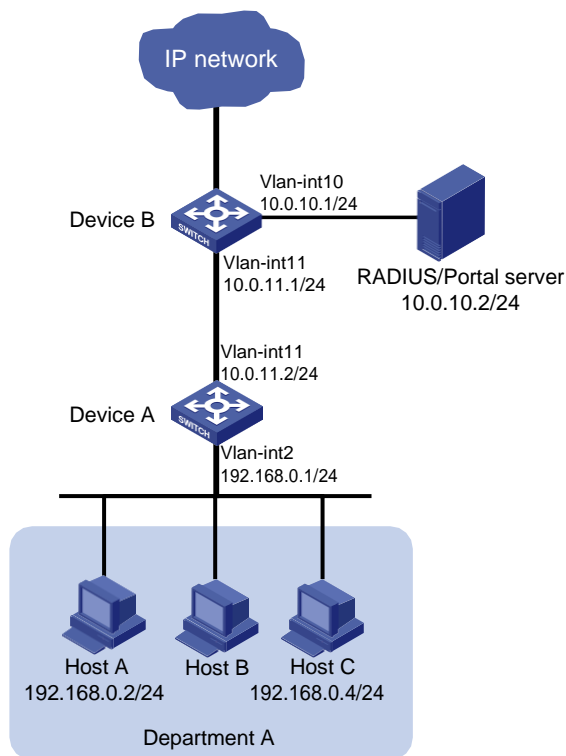
## Example: Configuring cross-subnet portal authentication

### Network configuration

As shown in [Figure 1](#), Device B supports portal authentication. An INC server acts as a portal authentication server, a portal Web server, and a RADIUS server. The RADIUS server is used to perform AAA on portal users. In this example, the INC server runs INC PLAT 7.0 (E0202) and INC UAM 7.0 (E0202).

Configure cross-subnet portal authentication. Before passing authentication, a host can access only the portal server. After passing authentication, the host can access resources in the IP network.

**Figure 1 Network diagram**



## Analysis

To enable Device B to perform cross-subnet portal authentication through RADIUS, you must complete the following tasks:

- Configure the portal authentication and Web server, and enable cross-subnet portal authentication.
- Configure the RADIUS scheme. Specify the AAA server for the scheme and apply the scheme to the portal authentication domain.

## Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
SC 3570 switch series	Release 11xx
SC 5525 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
SC 5520 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
SC 3170 switch series	Release 11xx
SC 3130 switch series	Release 63xx

# Procedures

## Configuring Device A

# Configure VLAN-interface 2 and VLAN-interface 11, and assign them IP addresses.

```
<DeviceA> system-view
[DeviceA] vlan 2
[DeviceA-vlan2] quit
[DeviceA] vlan 11
[DeviceA-vlan11] quit
[DeviceA] interface vlan-interface 2
[DeviceA-Vlan-interface2] ip address 192.168.0.1 24
[DeviceA-Vlan-interface2] quit
[DeviceA] interface vlan-interface 11
[DeviceA-Vlan-interfacell] ip address 10.0.11.2 24
[DeviceA-Vlan-interfacell] quit
```

# Assign the corresponding physical interfaces to the VLANs. (Details not shown.)

# Configure a static route to the RADIUS server.

```
[DeviceA] ip route-static 10.0.10.0 255.255.255.0 10.0.11.1
```

## Configuring Device B

# Configure VLAN-interface 10 and VLAN-interface 11, and assign them IP addresses.

```
<DeviceB> system-view
[DeviceB] vlan 10
[DeviceB-vlan10] quit
[DeviceB] vlan 11
[DeviceB-vlan11] quit
[DeviceB] interface vlan-interface 11
[DeviceB-Vlan-interface11] ip address 10.0.11.1 24
[DeviceB-Vlan-interface11] quit
[DeviceB] interface vlan-interface 10
[DeviceB-Vlan-interface10] ip address 10.0.10.1 24
[DeviceB-Vlan-interface10] quit
```

# Configure portal authentication server **newpt**.

```
[DeviceB] portal server newpt
[DeviceB-portal-server-newpt] ip 10.0.10.2 key simple portal
[DeviceB-portal-server-newpt] port 50100
[DeviceB-portal-server-newpt] quit
```

# Configure portal Web server **newpt**. The URL must be the same as the URL configured for the portal page on the portal Web server.

```
[DeviceB] portal web-server newpt
[DeviceB-portal-websvr-newpt] url http://10.0.10.2:8080/portal
[DeviceB-portal-websvr-newpt] quit
```

# Enable cross-subnet authentication on VLAN-interface 11, the interface connected to Device A.

```
[DeviceB] interface Vlan-interface 11
[DeviceB-Vlan-interface11] portal enable method layer3
```

# Configure the BAS-IP as 10.0.11.1 for portal packets sent from VLAN-interface 11 to the portal authentication server.

```
[DeviceB-Vlan-interface11] portal bas-ip 10.0.11.1
```

# Specify portal Web server **newpt** on VLAN-interface 11.

```
[DeviceB-Vlan-interface11] portal apply web-server newpt
[DeviceB-Vlan-interface11] quit
```

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

```
[DeviceB] radius scheme iNC
```

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

```
[DeviceB-radius-iNC] primary authentication 10.0.10.2
[DeviceB-radius-iNC] primary accounting 10.0.10.2
[DeviceB-radius-iNC] key authentication simple expert
```

```
[DeviceB-radius-iNC] key accounting simple expert
# Exclude the ISP domain name from the username sent to the RADIUS server.
[DeviceB-radius-iNC] user-name-format without-domain
[DeviceB-radius-iNC] quit
# Enable the RADIUS session-control feature.
[DeviceB] radius session-control enable
# Create an ISP domain named portal.com and enter its view.
[DeviceB] domain portal.com
# Configure AAA methods for the ISP domain.
[DeviceB-isp-portal.com] authentication portal radius-scheme iNC
[DeviceB-isp-portal.com] authorization portal radius-scheme iNC
[DeviceB-isp-portal.com] accounting portal radius-scheme iNC
[DeviceB-isp-portal.com] quit
# Specify domain portal.com as the default ISP domain. If a user enters the username without the
ISP domain name at login, the AAA methods of the default domain are used for the user.
[DeviceB] domain default enable portal.com
# Configure a static route to Department A.
[DeviceB] ip route-static 192.168.0.0 255.255.255.0 10.0.11.2
```

## Configuring the RADIUS and portal server

### Adding an access device

1. Log in to INC, and click the **User** tab.
2. From the navigation tree, select **User Access Manager > Access Device Management > Access Device**.
3. Click **Add**.  
The **Add Access Device** page appears.
4. In the **Access Configuration** area, configure the following parameters:
  - Enter **expert** in the **Shared Key** and **Confirm Shared Key** fields.
  - Enter **1812** in the **Authentication Port** field and **1813** in the **Accounting Port** field.
  - Select **LAN Access Service** from the **Service Type** list.
  - Select **INTELBRAS(General)** from the **Access Device Type** list.
5. In the **Device List** area, click **Add Manually**.
6. On the page that appears, enter IP address **10.0.10.1** in the **Start IP** field, and click **OK**.
7. Click **OK**.

**Figure 2 Adding an access device**

User > User Access Policy > Access Device Management > Access Device > Add Access Device ? Help

**Access Configuration**

Authentication Port \* 1812 Accounting Port \* 1813  
RADIUS Accounting Fully Supported Service Type LAN Access Service  
Access Device Type H3C(General) Access Device Group --  
Shared Key \* \*\*\*\*\* Confirm Shared Key \* \*\*\*\*\*  
Service Group Ungrouped

**Device List**

Select Add Manually Clear All

Device Name	Device IP	Device Model	Comments	Delete
	10.0.10.1			

Total Items: 1.

OK Cancel

## Adding an access policy

1. Click the **User** tab.
2. From the navigation tree, select **User Access Manager > Access Policy**.
3. Click **Add**.
4. On the page that appears, enter **portal** in the **Access Policy Name** field. Use the default settings for other parameters.
5. Click **OK**.

**Figure 3 Adding an access policy**

User > User Access Policy > Access Policy > Add Access Policy

**Basic Information**

Access Policy Name \* portal  
Service Group \* Ungrouped  
Description

**Authorization Information**

Access Period None ? Allocate IP \* No  
Downstream Rate(Kbps) Upstream Rate(Kbps)  
Priority RSA Authentication  
Certificate Authentication ☒ None ☐ EAP  
Certificate Type EAP-TLS AuthN  
Deploy VLAN  
☐ Deploy User Profile Deploy User Group ?  
☐ Deploy ACL

## Adding an access service

1. Click the **User** tab.
2. From the navigation tree, select **User Access Manager > Access Service**.

3. Click **Add**.
4. On the page that appears, configure the following parameters:
  - o Enter **Portal-auth** in the **Service Name** field.
  - o Select **portal** from the **Default Access Policy** list.
  - o Use the default settings for other parameters.
5. Click **OK**.

**Figure 4 Adding an access service**

User > User Access Policy > Access Service > Add Access Service

**Basic Information**

Service Name \*  Service Suffix

Service Group \*  Default Access Policy \*

Default Proprietary Attribute Assignment Policy \*  Default BYOD Page \*

Description

☒ Available ☐ Transparent Authentication on Portal Endpoints

**Access Scenario List**

Access Scenario	Access Policy	Proprietary Attribute Assignment Policy	BYOD Page	Priority	Modify	Delete
No match found.						

OK Cancel

## Configuring an access user

1. Click the **User** tab.
2. From the navigation tree, select **Access User> All Access Users**.
3. Click **Add**.  
The **Add Access User** page appears.
4. In the **Access Information** area, click the **Add User** button for the **User Name** field.
5. On the page that appears, configure the following parameters:
  - o Enter **hello** in the **User Name** field.
  - o Enter **111111** in the **Identity Number** field.
  - o Use the default settings for other parameters.
  - o Click **OK**.

**Figure 5 Adding a user**

User > All Access Users > Add Access User

**Access account**

**Access Information**

User Name \*

**Basic Information**

User Name \*  Identity Number \*

Contact Address  Telephone

Email  User Group \*

OK Cancel



6. In the **Access Information** area, enter **portal** in the **Account Name** field and configure the password as **123456** for the account.
7. In the **Access Service** area, select the access service named **Portal-auth**.
8. Use the default settings for other parameters.
9. Click **OK**.

**Figure 6 Configuring an access user**

User > All Access Users > Add Access User

Access account

Access Information

User Name \*

hello

Select

Add User

Account Name \*

portal

☐ Trial Account

☐ Default BYOD User

☐ Computer User

☐ Fast Access User

Password \*

\*\*\*\*\*

Confirm Password \*

\*\*\*\*\*

☒ Allow User to Change Password

☐ Enable Password Strategy

☐ Modify Password at Next Login

Inspiration Time

Expiration Time

Max. Idle Time(Minutes)

Max. Concurrent Logins

1

Max. Smart Device Bindings for Portal

1

Login Message

Access Service

Service Name	Service Suffix	Status	Allocate IP
<input type="checkbox"/> 802.1x		Available	
<input checked="" type="checkbox"/> Portal-auth		Available	

## Configuring a portal page

1. Click the **User** tab.
2. From the navigation tree, select **User Access Policy > Portal Service > Server**.
3. Use the default settings for all parameters.
4. Click **OK**.

**Figure 7 Configuring a portal page**

User > User Access Policy > Portal Service > Server

Portal Server

Basic Information

Log Level \*

Info

Portal Server

Request Timeout(Seconds) \*

4

Server Heartbeat Interval(Seconds) \*

20

User Heartbeat Interval(Minutes) \*

5

Portal Web

Request Timeout(Seconds) \*

15

Packet Code

Verify Endpoint Requests

Yes

Use Cache

Yes

HTTP Heartbeat Display

New Page

HTTPS Heartbeat Display

Original Page


Portal Page

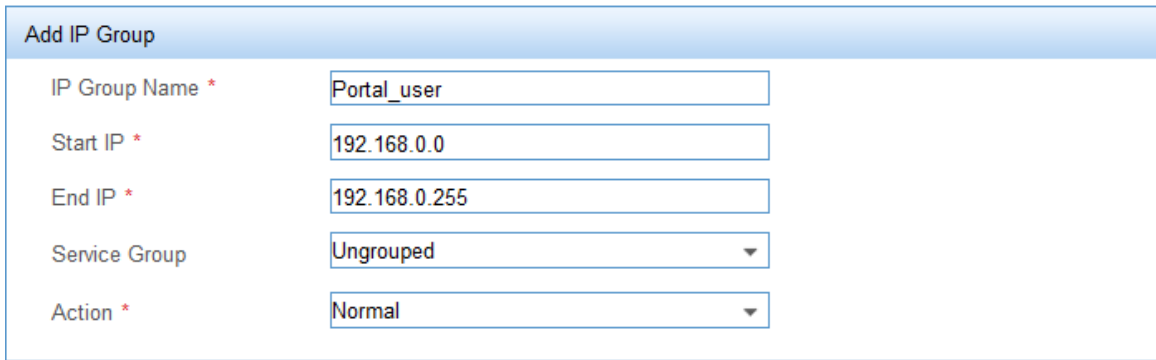
http://10.0.10.2:8080/portal/

## Adding an IP group for portal authentication

1. Click the **User** tab.
2. From the navigation tree, select **User Access Policy > Portal Service > IP Group**.
3. Click **Add**.
4. On the page that appears, configure the following parameters:
  - o Enter **Portal\_user** in the **IP Group Name** field.
  - o Enter **192.168.0.0** in the **Start IP** field and **192.168.0.255** in the **End IP** field.
  - o Use the default settings for other parameters.
5. Click **OK**.

**Figure 8 Adding an IP group**

 User > User Access Policy > Portal Service > IP Group > Add IP Group



Add IP Group	
IP Group Name *	Portal_user
Start IP *	192.168.0.0
End IP *	192.168.0.255
Service Group	Ungrouped
Action *	Normal

OK Cancel

## Configuring an access device for portal authentication

1. Click the **User** tab.
2. From the navigation tree, select **User Access Policy > Portal Service > Device**.
3. Click **Add**.
4. On the **Add Device** page, configure the following parameters:
  - o Enter **NAS** in the **Device Name** field.
  - o Enter **10.0.11.1** in the **IP Address** field.
  - o Enter **portal** in the **Key** and **Confirm Key** fields.

The key must be the same as that for the portal authentication server configured on Device B.
  - o Select **Layer 3** from the **Access Method** list.
  - o Use the default settings for other parameters.
5. Click **OK**.

**Figure 9 Adding an access device**

User > User Access Policy > Portal Service > Device > Add Device

Add Device

Device Information

Device Name \*

NAS

Version \*

Portal 2.0

Listening Port \*

2000

Authentication Retries \*

0

Support Server Heartbeat \*

No

Key \*

.....

Access Method \*

Layer 3

Device Description

Service Group \*

Ungrouped

IP Address \*

10.0.11.1

Local Challenge \*

No

Logout Retries \*

1

Support User Heartbeat \*

No

Confirm Key \*

.....

OK

Cancel

## Configuring a port group for portal authentication

1. On the **Device** page, click the **Port Group** icon.

**Figure 10 Accessing the Device page**

User > User Access Policy > Portal Service > Device Add to My Favorites ? Help

Query Devices

Device Name

Version




Deploy Result

Service Group

Query

Reset

Add

Device Name	Version	Service Group	IP Address	Last Deployed at	Deploy Result	Operation
NAS	Portal 2.0	Ungrouped	10.0.11.1		Not Deployed	  

1-1 of 1. Page 1 of 1.

2. On the **Configure Port Group** page, click **Add**.
3. On the **Add Port Group** page, configure the following parameters:
  - o Enter **portal** in the **Port Group Name** field.
  - o Select **Portal\_user** from the **IP Group** list.
  - o Use the default settings for other parameters.
4. Click **OK**.

**Figure 11 Adding a port group**

User > User Access Policy > Portal Service > Device > Configure Port Group > Add Port Group

Add Port Group

Port Group Name \*

portal

Start Port \*

0

Protocol \*

HTTP

NAT or Not \*

No

Authentication Type \*

CHAP

Heartbeat Interval(Minutes) \*

10

User Domain

Transparent Authentication

Not Supported

User Attribute Type

Language \*

English

End Port \*

777777

Quick Authentication \*

No

Error Transparent Transmission \*

Yes

IP Group \*

Portal\_user

Heartbeat Timeout(Minutes) \*

30

Port Group Description

Client Protection Against Cracks \*

No

Default Authentication Page

OK

Cancel

# Verifying the configuration

A user can perform portal authentication by using the INTELBRAS iNode client or through a Web page. This example triggers portal authentication by accessing a Web page.

# Access a Web page through a Web browser on a host. You are redirected to the authentication page **http://10.0.10.2:8080/portal**. Enter the username **portal** and the password **123456** to log in. After passing the authentication, you are redirected to the authentication success page.

# Execute the **display portal user** command on Device B to display the portal user information.

```
[DeviceB] display portal user interface vlan-interface 11
Total portal users: 1
Username: portal
  Portal server: newpt
  State: Online
  VPN instance: N/A
  MAC              IP              Vlan   Interface
  0015-e9a6-7cfe   192.168.0.2    11     Vlan-interface11
Authorization information:
  DHCP IP pool: N/A
  User profile: N/A
  Session group profile: N/A
  ACL number: N/A
  Inbound CAR: N/A
  Outbound CAR: N/A
```

## Configuration files

- Device A:

```
#
vlan 2
#
vlan 11
#
interface Vlan-interface2
 ip address 192.168.0.1 255.255.255.0
#
interface Vlan-interface11
 ip address 10.0.11.2 255.255.255.0
#
ip route-static 10.0.10.0 24 10.0.11.1
#
```
- Device B:

```
#
vlan 10 to 11
#
interface Vlan-interface10
 ip address 10.0.10.1 255.255.255.0
```

```

#
interface Vlan-interface11
 ip address 10.0.11.1 255.255.255.0
 portal enable method layer3
 portal bas-ip 10.0.11.1
 portal apply web-server newpt
#
ip route-static 192.168.0.0 24 10.0.11.2
#
radius session-control enable
#
radius scheme iNC
primary authentication 10.0.10.2
primary accounting 10.0.10.2
key authentication cipher $c$3$M30nGDQxiOCAxe2AJ9yEZdk8kjoWag==
key accounting cipher $c$3$M23dGDQxiOCAxe2BJ9yEZdk8kjoWag==
user-name-format without-domain
#
domain portal.com
 authentication portal radius-scheme iNC
 authorization portal radius-scheme iNC
 accounting portal radius-scheme iNC
#
domain default enable portal.com
#
portal web-server newpt
 url http://10.0.10.2:8080/portal
#
portal server newpt
 ip 10.0.10.2 key cipher $c$3$r0VxoIiBrpzju9h2akP4TxyknX8VTuYKfA==
#

```

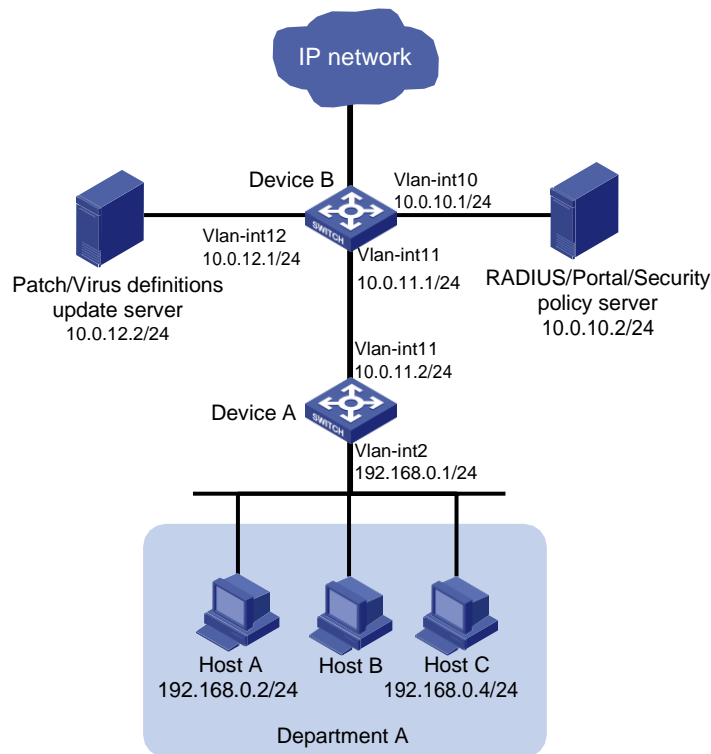
## Example: Configuring extended cross-subnet portal authentication

### Network configuration

As shown in [Figure 12](#), Device B supports portal authentication. An INC server acts as a portal authentication server, a portal Web server, a RADIUS server, and a security policy server. The RADIUS server is used to perform AAA on portal users. The security policy server is deployed to perform security check on portal-authenticated users. In this example, the INC server runs INC PLAT 7.0 (E0202) and INC UAM 7.0 (E0202).

Configure extended cross-subnet portal authentication. Before passing portal authentication, a host can access only the portal Web server. After the host passes authentication, the security policy server performs a security check on the host. If the host fails the security check, the host is permitted to access only the Patch/Virus definitions update server. After passing the security check, the host can access resources in the IP network.

**Figure 12 Network diagram**



## Analysis

To enable Device B to perform cross-subnet portal authentication through RADIUS, you must complete the following tasks:

- Configure the portal authentication and Web server, and enable cross-subnet portal authentication.
- Configure the RADIUS scheme. Specify the AAA server for the scheme and apply the scheme to the portal authentication domain.

To perform security check on authenticated users, you must complete the following tasks:

- On Device B, create an ACL (ACL 3000 in this example) for users who fail security checks, and an ACL (ACL 3001 in this example) for users who pass security checks.
- On the security policy server, specify ACL 3000 as the isolation ACL and ACL 3001 as the security ACL.

## Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
SC 3570 switch series	Release 11xx
SC 5525 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
SC 5520 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
SC 3170 switch series	Release 11xx
SC 3130 switch series	Release 63xx
SC 3570 switch series	Release 11xx

# Procedures

## Configuring Device A

# Configure VLAN-interface 2 and VLAN-interface 11, and assign them IP addresses.

```
<DeviceA> system-view
[DeviceA] vlan 2
[DeviceA-vlan2] quit
[DeviceA] vlan 11
[DeviceA-vlan11] quit
[DeviceA] interface vlan-interface 2
[DeviceA-Vlan-interface2] ip address 192.168.0.1 24
[DeviceA-Vlan-interface2] quit
[DeviceA] interface vlan-interface 11
[DeviceA-Vlan-interfacell] ip address 10.0.11.2 24
[DeviceA-Vlan-interfacell] quit
```

# Assign the corresponding physical interfaces to the VLANs. (Details not shown.)

# Configure a static route to the RADIUS, portal, and security policy server.

```
[DeviceA] ip route-static 10.0.10.0 255.255.255.0 10.0.11.1
```

# Configure a static route to the patch and virus definitions update server.

```
[DeviceA] ip route-static 10.0.12.0 255.255.255.0 10.0.11.1
```

## Configuring Device B

# Configure VLAN-interface 10, VLAN-interface 11, and VLAN-interface 12, and assign them IP addresses.

```
<DeviceB> system-view
[DeviceB] vlan 10
[DeviceB-vlan10] quit
[DeviceB] vlan 11
[DeviceB-vlan11] quit
[DeviceB] vlan 12
[DeviceB-vlan12] quit
[DeviceB] interface vlan-interface 11
[DeviceB-Vlan-interface11] ip address 10.0.11.1 24
[DeviceB-Vlan-interface11] quit
[DeviceB] interface vlan-interface 10
[DeviceB-Vlan-interface10] ip address 10.0.10.1 24
[DeviceB-Vlan-interface10] quit
[DeviceB] interface vlan-interface 12
[DeviceB-Vlan-interface12] ip address 10.0.12.1 24
[DeviceB-Vlan-interface12] quit
```

# Configure the portal authentication server **newpt**.

```
[DeviceB] portal server newpt
[DeviceB-portal-server-newpt] ip 10.0.10.2 key simple portal
[DeviceB-portal-server-newpt] port 50100
[DeviceB-portal-server-newpt] quit
```

# Configure portal Web server **newpt**. The URL must be the same as the URL configured for the portal page on the portal Web server.

```
[DeviceB] portal web-server newpt
[DeviceB-portal-websvr-newpt] url http://10.0.10.2:8080/portal
[DeviceB-portal-websvr-newpt] quit
```

# Enable cross-subnet authentication on VLAN-interface 11, the interface connected to Device A.

```
[DeviceB] interface Vlan-interface 11
[DeviceB-Vlan-interface11] portal enable method layer3
```

# Configure the BAS-IP as 10.0.11.1 for portal packets sent from VLAN-interface 11 to the portal authentication server.

```
[DeviceB-Vlan-interface11] portal bas-ip 10.0.11.1
```

# Specify portal Web server **newpt** on VLAN-interface 11.



```

[DeviceB-Vlan-interface11] portal apply web-server newpt
[DeviceB-Vlan-interface11] quit

# Create a static route to Department A.
[DeviceB] ip route-static 192.168.0.0 255.255.255.0 10.0.11.2

# Create RADIUS scheme named iNC and enter its view.
[DeviceB] radius scheme iNC

# Specify the primary authentication server and primary accounting server, and configure the keys
for communication with the server.
[DeviceB-radius-iNC] primary authentication 10.0.10.2
[DeviceB-radius-iNC] primary accounting 10.0.10.2
[DeviceB-radius-iNC] key authentication simple expert
[DeviceB-radius-iNC] key accounting simple expert

# Exclude the ISP domain name from the username sent to the RADIUS server.
[DeviceB-radius-iNC] user-name-format without-domain
[DeviceB-radius-iNC] quit

# Enable RADIUS session control.
[DeviceB] radius session-control enable

# Create an ISP domain named portal.com and enter its view.
[DeviceB] domain portal.com

# Configure AAA methods for the ISP domain.
[DeviceB-isp-portal.com] authentication portal radius-scheme iNC
[DeviceB-isp-portal.com] authorization portal radius-scheme iNC
[DeviceB-isp-portal.com] accounting portal radius-scheme iNC
[DeviceB-isp-portal.com] quit

# Specify domain portal.com as the default ISP domain. If a user enters the username without the
ISP domain name at login, the AAA methods of the default domain are used for the user.
[DeviceB] domain default enable portal.com

# Configure ACL 3000 to permit access only to the Patch/Virus definitions update server and ACL
3001 to permit access to any IP address.
[DeviceB] acl number 3000
[DeviceB-acl-adv-3000] rule permit ip destination 10.0.12.2 0
[DeviceB-acl-adv-3000] rule deny ip
[DeviceB-acl-adv-3000] quit
[DeviceB] acl number 3001
[DeviceB-acl-adv-3001] rule permit ip
[DeviceB-acl-adv-3001] quit

```

## Configuring the RADIUS, portal, and security policy server

# Configure the RADIUS server and portal server. For more information, see "[Configuring the RADIUS and portal server](#)."

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

# Verifying the configuration

A user can perform the extended cross-subnet authentication only by using the INTELBRAS iNode client.

# Open the iNode client on a host, and create a portal connection. Enter the username and password and click **Connect**. The user passes the portal authentication.

# On the iNode client, check security check information. The user failed to pass the security check.

# Display portal user information on Device B to verify that ACL 3000 has been deployed to the user.

```
[DeviceB] display portal user all
Total portal users: 1
Username: portal
  Portal server: newpt
  State: Online
  VPN instance: N/A
  MAC          IP          VLAN   Interface
  0015-e9a6-7cfe 192.168.0.2    11     Vlan-interface11
Authorization information:
  DHCP IP pool: N/A
  User profile: N/A
  Session group profile: N/A
  ACL number: 3000
  Inbound CAR: N/A
  Outbound CAR: N/A
```

# Update the virus database on the host to meet the security requirement.

# On the iNode client, disconnect the portal connection and then log in again. Check security check information. The iNode client displays that the host successfully passed the security check.

# Display portal user information on Device B to verify that ACL 3001 has been deployed to the portal user.

```
[DeviceB]display portal user all
Total portal users: 1
Username: portal
  Portal server: newpt
  State: Online
  Authorization ACL: 3001
  VPN instance: N/A
  MAC          IP          VLAN   Interface
  0015-e9a6-7cfe 192.168.0.2    11     Vlan-interface11
Authorization information:
  DHCP IP pool: N/A
  User profile: N/A
  Session group profile: N/A
  ACL number: 3001
  Inbound CAR: N/A
  Outbound CAR: N/A
```

# Configuration files

- **Device A:**

```
#
vlan 2
#
vlan 11
#
interface Vlan-interface2
 ip address 192.168.0.1 255.255.255.0
#
interface Vlan-interface11
 ip address 10.0.11.2 255.255.255.0
#
ip route-static 10.0.10.0 24 10.0.11.1
ip route-static 10.0.12.0 24 10.0.11.1
#
```

- **Device B:**

```
#
vlan 10 to 12
#
interface Vlan-interface10
 ip address 10.0.10.1 255.255.255.0
#
interface Vlan-interface11
 ip address 10.0.11.1 255.255.255.0
portal enable method layer3
portal bas-ip 10.0.11.1
portal apply web-server newpt
#
interface Vlan-interface12
 ip address 10.0.12.1 255.255.255.0
#
ip route-static 192.168.0.0 24 10.0.11.2
#
acl number 3000
 rule 0 permit ip destination 10.0.12.2 0
 rule 5 deny ip
#
acl number 3001
 rule 0 permit ip
#
radius session-control enable
#
radius scheme iNC
 primary authentication 10.0.10.2
 primary accounting 10.0.10.2
key authentication cipher $c$3$M30nGDQxiOCAxe2AJ9yEZdk8kjoWag==
```

```

key accounting cipher $c$3$M23dGDQxiOCAxe2BJ9yEZdk8kjoWag==
  user-name-format without-domain
#
domain portal.com
  authentication portal radius-scheme iNC
  authorization portal radius-scheme iNC
  accounting portal radius-scheme iNC
#
domain default enable portal.com
#
portal web-server newpt
  url http://10.0.10.2:8080/portal
#
portal server newpt
  ip 10.0.10.2 key cipher $c$3$r0VxoIiBrpzju9h2akP4TxyknX8VTuYKfA==
#

```

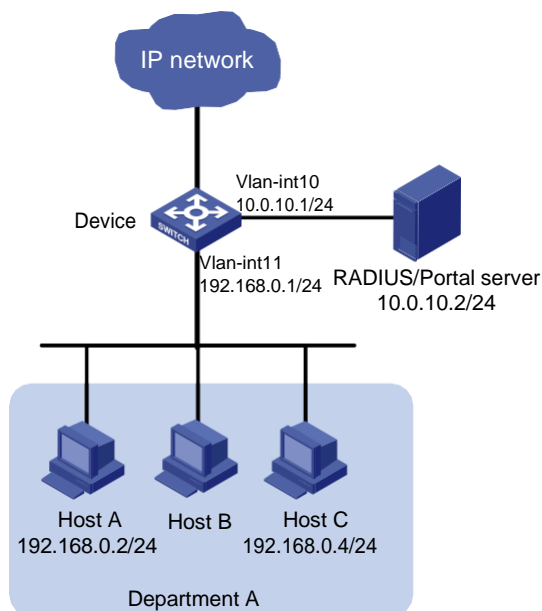
## Example: Configuring direct portal authentication

### Network configuration

As shown in [Figure 13](#), hosts in Department A are directly connected to the device. An INC server acts as a portal authentication server, a portal Web server, and a RADIUS server. The RADIUS server is used to perform AAA on portal users. In this example, the INC server runs INC PLAT 7.0 (E0202) and INC UAM 7.0 (E0202).

Configure direct portal authentication. The hosts can access only the portal server before passing authentication and can access other network resources after passing authentication.

**Figure 13 Network diagram**



# Analysis

To enable the device to perform portal authentication through RADIUS, you must complete the following tasks:

- Configure the portal authentication and Web server, and enable direct portal authentication.
- Configure the RADIUS scheme. Specify the AAA server for the scheme and apply the scheme to the portal authentication domain.

## Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
SC 3570 switch series	Release 11xx
SC 5525 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
SC 5520 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
SC 3170 switch series	Release 11xx
SC 3130 switch series	Release 63xx

## Procedures

### Configuring the device

# Configure VLAN-interface 10 and VLAN-interface 11, and assign them IP addresses.

```
<Device> system-view
[Device] vlan 10
[Device-vlan10] quit
[Device] vlan 11
[Device-vlan11] quit
[Device] interface vlan-interface 11
[Device-Vlan-interface11] ip address 192.168.0.1 24
[Device-Vlan-interface11] quit
[Device] interface vlan-interface 10
[Device-Vlan-interface10] ip address 10.0.10.1 24
[Device-Vlan-interface10] quit
```

# Configure the portal authentication server **newpt**.

```
[Device] portal server newpt
[Device-portal-server-newpt] ip 10.0.10.2 key simple portal
[Device-portal-server-newpt] port 50100
[Device-portal-server-newpt] quit
```

# Configure portal Web server **newpt**. The URL must be the same as the URL configured for the portal page on the portal Web server.

```
[Device] portal web-server newpt
[Device-portal-websvr-newpt] url http://10.0.10.2:8080/portal
```

```

[Device-portal-websvr-newpt] quit

# Enable direct portal authentication on VLAN-interface 11.
[Device] interface Vlan-interface 11
[Device-Vlan-interface11] portal enable method direct

# Configure the BAS-IP as 192.168.0.1 for portal packets sent from VLAN-interface 11 to the portal authentication server.
[Device-Vlan-interface11] portal bas-ip 192.168.0.1

# Specify portal Web server newpt on VLAN-interface 11.
[Device-Vlan-interface11] portal apply web-server newpt
[Device-Vlan-interface11] quit

# Create a RADIUS scheme named iNC and enter its view.
[Device] radius scheme iNC

# Specify the primary authentication server and primary accounting server, and configure the keys for communication with the server.
[Device-radius-iNC] primary authentication 10.0.10.2
[Device-radius-iNC] primary accounting 10.0.10.2
[Device-radius-iNC] key authentication simple expert
[Device-radius-iNC] key accounting simple expert

# Exclude the ISP domain name from the username sent to the RADIUS server.
[Device-radius-iNC] user-name-format without-domain
[Device-radius-iNC] quit

# Enable the RADIUS session-control feature.
[Device] radius session-control enable

# Create an ISP domain named portal.com and enter its view.
[Device] domain portal.com

# Configure AAA methods for the ISP domain.
[Device-isp-portal.com] authentication portal radius-scheme iNC
[Device-isp-portal.com] authorization portal radius-scheme iNC
[Device-isp-portal.com] accounting portal radius-scheme iNC
[Device-isp-portal.com] quit

# Specify ISP domain portal.com 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.
[Device] domain default enable portal.com

```

## Configuring the RADIUS and portal server

Configure the RADIUS server and portal server. For more information, see "[Configuring the RADIUS and portal server](#)."

When you configuring an access device for portal authentication (as shown in [Figure 13](#)), select **Directly Selected** from the **Access Method** list, and enter **192.168.0.1** in the **IP Address** field.

## Verifying the configuration

A user can perform portal authentication by using the INTELBRAS iNode client or through a Web page. This example uses the Web page.

# Access a Web page through a Web browser on a host. You are redirected to the authentication page **http://10.0.10.2:8080/portal**. Enter the username **portal** and the password **123456** to log in. After passing the authentication, you are redirected to the authentication success page.

# Execute the **display portal user** command to display portal user information on Device.

```
[Device] display portal user interface vlan-interface 11
Total portal users: 1
Username: portal
  Portal server: newpt
  State: Online
  VPN instance: N/A
  MAC           IP           Vlan   Interface
  0015-e9a6-7cfe 192.168.0.2 11     Vlan-interfacell
```

Authorization information:

DHCP IP pool: N/A  
User profile: N/A  
Session group profile: N/A  
ACL number: N/A  
Inbound CAR: N/A  
Outbound CAR: N/A

## Configuration files

```
#
vlan 10 to 11
#
interface Vlan-interface10
 ip address 10.0.10.1 255.255.255.0
#
interface Vlan-interface11
 ip address 192.168.0.1 255.255.255.0
 portal enable method direct
 portal bas-ip 192.168.0.1
 portal apply web-server newpt
#
radius session-control enable
#
radius scheme iNC
primary authentication 10.0.10.2
primary accounting 10.0.10.2
key authentication cipher $c$3$M30nGDQxiOCAxe2AJ9yEZdk8kjoWag==
key accounting cipher $c$3$M23dGDQxiOCAxe2BJ9yEZdk8kjoWag==
user-name-format without-domain
#
domain portal.com
 authentication portal radius-scheme iNC
 authorization portal radius-scheme iNC
 accounting portal radius-scheme iNC
#
domain default enable portal.com
#
portal web-server newpt
 url http://10.0.10.2:8080/portal
#
portal server newpt
 ip 10.0.10.2 key cipher $c$3$r0VxoIiBrpzju9h2akP4TxyknX8VTuYKfA==
#
```