

INTELBRAS Access Controllers Local Portal Authentication Configuration Examples

Copyright © 2024 Intelbras S.A All rights reserved.

No part of this manual may be reproduced or transmitted in any form or by any means without prior written consent of Intelbras S.A

Except for the trademarks of Intelbras S.A, any trademarks that may be mentioned in this document are the property of their respective owners.

The information in this document is subject to change without notice.

Contents

Introduction	1
Prerequisites	1
Example: Configuring local portal authentication.....	1
Network configuration.....	1
Analysis	2
Restrictions and guidelines	2
Procedures	2
Configuring the AC.....	2
Configuring the switch	5
Configuring the RADIUS server	5
Verifying the configuration	8
Configuration files.....	9
Related documentation	10

Introduction

The following information provides an example of configuring local portal authentication on the AC.

Prerequisites

The following information applies to Comware-based access controllers and access points. Procedures and information in the examples might be slightly different depending on the software or hardware version of the access controllers and access points.

The configuration examples 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.

The following information is provided based on the assumption that you have basic knowledge of portal authentication.

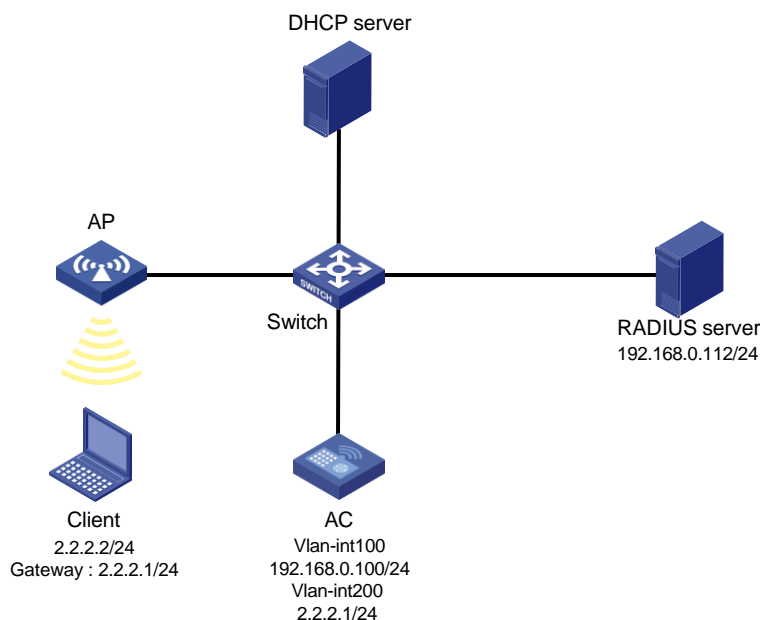
Example: Configuring local portal authentication

Network configuration

As shown in [Figure 1](#), the AP and the client obtain IP addresses from the DHCP server.

- Configure the access device AC to also act as the portal Web server and the portal authentication server.
- Use the RADIUS server as both the authentication server and the authorization server.
- Configure direct portal authentication on the AC.

Figure 1 Network diagram



Analysis

To allow an authenticated user to access network resources on any Layer 2 ports in its access VLAN without re-authentication, you must enable the portal roaming feature.

To avoid possible authentication failure caused by frequent logins and logouts of portal clients in a short time, disable the Rule ARP entry feature.

To allow the RADIUS server to modify user authorization information and log out users, enable the RADIUS session-control feature.

Restrictions and guidelines

Use the actual serial ID of an AP to uniquely identify that AP.

The portal authentication server type and portal Web server type configured on the AC must be the same as the types of the servers actually used. In this example, the server type is CMCC.

By default, the portal Web server URL redirected to users does carry parameters. You can configure the parameters to be carried in the redirection URL as needed.

To enable portal authentication on a VLAN interface, you must use the centralized forwarding mode. To enable portal authentication on a service template, you can use the centralized forwarding mode or the local forwarding mode. In this example, portal authentication is enabled on a service template.

Edit portal authentication pages, compress them to a .zip file (this example uses **abc.zip**), and then upload the file to the root directory of the storage medium of the AC. On the AC, you must specify this file as the default authentication page file.

To change the default authentication page file, you must first execute the **undo default-logon-page** command, and then specify a new default authentication page file.

Procedures

Configuring the AC

1. Configure VLANs and interfaces:

Create VLAN 100 and VLAN-interface 100. Assign the VLAN interface an IP address. The AC will use this IP address to establish a CAPWAP tunnel with the AP.

```
<AC> system-view
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 192.168.0.100 24
[AC-Vlan-interface100] quit
```

Create VLAN 200 and VLAN-interface 200. Assign the VLAN interface an IP address. This VLAN will be used for wireless client access.

```
[AC] vlan 200
[AC-vlan200] quit
[AC] interface vlan-interface 200
[AC-Vlan-interface200] ip address 2.2.2.1 24
[AC-Vlan-interface200] quit
```

Configure the interface that is connected to the switch as a trunk port, and assign the port to VLAN 100 and VLAN 200.

```
[AC] interface gigabitethernet 1/0/1
[AC-GigabitEthernet1/0/1] port link-type trunk
[AC-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[AC-GigabitEthernet1/0/1] quit
```

Configure routing to make sure the client, servers, and AC can reach one another. (Details not shown.)

2. Configure the wireless service:

Create a service template named **st1** and enter its view.

```
[AC] wlan service-template st1
```

Configure the SSID of the service template as **service**.

```
[AC-wlan-st-st1] ssid service
```

Assign clients coming online through the service template to VLAN 200.

```
[AC-wlan-st-st1] vlan 200
```

Specify the AKM mode as PSK, and configure the preshared key as 12345678 in plain text.

```
[AC-wlan-st-st1] akm mode psk
```

```
[AC-wlan-st-st1] preshared-key pass-phrase simple 12345678
```

Specify the cipher suite as CCMP and the security IE as RSN.

```
[AC-wlan-st-st1] cipher-suite ccmp
```

```
[AC-wlan-st-st1] security-ie rsn
```

Configure the AC to forward client data traffic. (Skip this step if the client data traffic forwarder is the AC by default.)

```
[AC-wlan-st-st1] client forwarding-location ac
```

Configure the authentication domain for portal users as **dm1**.

```
[AC-wlan-st-st1] portal domain dm1
```

Enable the service template.

```
[AC-wlan-st-st1] service-template enable
```

```
[AC-wlan-st-st1] quit
```

3. Configure the AP:

NOTE:

In large-scale networks, configure AP groups instead of single APs as a best practice.

Create an AP named **office**. Specify the AP model and serial ID.

```
[AC] wlan ap office model AP 3620
```

```
[AC-wlan-ap-office] serial-id 219801A28N819CE0002T
```

```
[AC-wlan-ap-office] quit
```

Create AP group **group1** and add AP **office** to AP group **group1**.

```
[AC] wlan ap-group group1
```

```
[AC-wlan-ap-group-group1] ap office
```

Bind service template **st1** to radio 2 in AP group **group1**.

```
[AC-wlan-ap-group-group1] ap-model AP 3620
```

```
[AC-wlan-ap-group-group1-ap-model-AP 3620] radio 2
```

```
[AC-wlan-ap-group-group1-ap-model-AP 3620-radio-2] service-template st1
```

Enable radio 2.

```
[AC-wlan-ap-group-group1-ap-model-AP 3620-radio-2] radio
```

```
enable [AC-wlan-ap-group-group1-ap-model-AP 3620-radio-2] quit
```

```
[AC-wlan-ap-group-group1-ap-model-AP 3620]
```

```
quit [AC-wlan-ap-group-group1] quit
```

4. Configure a RADIUS scheme:

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

```
[AC] radius scheme rs1
```

Configure the primary authentication and accounting servers and shared keys used for secure communication with the servers.

```
[AC-radius-rs1] primary authentication 192.168.0.112
```

```
[AC-radius-rs1] primary accounting 192.168.0.112
```

```
[AC-radius-rs1] key authentication simple radius
```

```
[AC-radius-rs1] key accounting simple radius
```

Configure the AC to remove the domain name from the usernames sent to the RADIUS servers.

```
[AC-radius-rs1] user-name-format without-domain
```

Specify 2.2.2.1 as the source IP address for outgoing RADIUS packets sent to the RADIUS servers.

```
[AC-radius-rs1] nas-ip 2.2.2.1
```

```
[AC-radius-rs1] quit
```

Enable the RADIUS session-control feature.

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

5. Configure the authentication domain:

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

```
[AC] domain dm1
```

Configure the authentication, authorization, and accounting methods as RADIUS for portal users in the ISP domain.

```
[AC-isp-dm1] authentication portal radius-scheme rs1
```

```
[AC-isp-dm1] authorization portal radius-scheme rs1
```

```
[AC-isp-dm1] accounting portal radius-scheme rs1
```

Configure the idle cut feature for users. Log out a user if the user's traffic is less than 1024 bytes in 15 minutes.

```
[AC-isp-dm1] authorization-attribute idle-cut 15 1024
```

```
[AC-isp-dm1] quit
```

6. Configure portal authentication:

Create a portal Web server named **newpt** and specify the server's URL as **http://2.2.2.1/portal**.

```
[AC] portal web-server newpt
```

```
[AC-portal-websvr-newpt] url http://2.2.2.1/portal
```

Configure the portal redirection URL to carry the **wlanuserip** parameter and the parameter value is the user's IP address.

```
[AC-portal-websvr-newpt] url-parameter wlanuserip source-address
```

Configure the portal Web server type as CMCC.

```
[AC-portal-websvr-newpt] server-type cmcc
```

```
[AC-portal-websvr-newpt] quit
```

Configure two destination-based portal-free rules to permit the traffic destined for the DNS server.

```
[AC] portal free-rule 1 destination ip any udp 53
```

```
[AC] portal free-rule 2 destination ip any tcp 53
```

Enable direct portal authentication on service template **st1**.

```
[AC] wlan service-template st1
```

```
[AC-wlan-st-st1] portal enable method direct
```

Specify portal Web server **newpt** on service template **st1**.

```
[AC-wlan-st-st1] portal apply web-server newpt
[AC-wlan-st-st1] quit
```

Enable the local portal service and enter HTTP-based local portal Web service view.

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

Specify the default authentication page file as **abc.zip**. (The file must already exist in the root directory of the storage medium of the AC.)

```
[AC-portal-local-websvr-http] default-logon-page abc.zip
[AC-portal-local-websvr-http] quit
```

Enable the portal roaming feature.

```
[AC] portal roaming enable
```

Disable the Rule ARP entry feature for portal clients.

```
[AC] undo portal refresh arp enable
```

Enable the wireless client validity check feature.

```
[AC] portal host-check enable
```

Configuring the switch

Create VLAN 100. The switch will use this VLAN to forward traffic on the CAPWAP tunnel between the AC and the AP.

```
<Switch> system-view
[Switch] vlan 100
[Switch-vlan100] quit
```

Create VLAN 200. The switch will use this VLAN to forward traffic of wireless clients.

```
[Switch] vlan 200
[Switch-vlan200] quit
```

Configure GigabitEthernet 1/0/1 (the port connected to the AC) as a trunk port. Assign the trunk port to VLAN 100 and VLAN 200.

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[Switch-GigabitEthernet1/0/1] quit
```

Configure GigabitEthernet 1/0/2 (the port connected to the AP) as an access port. Assign the access port to VLAN 100.

```
[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] port link-type access
[Switch-GigabitEthernet1/0/2] port access vlan 100
```

Enable PoE on the access port.

```
[Switch-GigabitEthernet1/0/2] poe enable
[Switch-GigabitEthernet1/0/2] quit
```

Configuring the RADIUS server

This example uses the INC server to describe the RADIUS server configuration. The INC server runs on INC PLAT 7.1(E0303p13), INC INC - EIA 7.1(F0302p08), and INC EIP 7.1(F0302p08).

1. Add an access device:

a. Log in to INC and click the **User** tab.

- b. From the navigation tree, select **User Access Policy > Access Device Management > Access Device**.
- c. Click **Add** to open the **Add Access Device** page.
- d. Configure the shared key as **radius**.
The shared key must be the same as that configured for the RADIUS server on the AC.
- e. In the **Device List** area, click **Add Manually** to open the **Add Access Device Manually** page. Enter the start IP address **2.2.2.1** and click **OK**.
- f. Use the default settings for other parameters on the **Add Access Device** page.
- g. Click **OK**.

Figure 2 Adding an access device

[User](#) > [User Access Policy](#) > [Access Device Management](#) > [Access Device](#) > Add Access Device

Access Configuration

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

Device List

Device Name	Device IP	Device Model	Comments	Delete
	2.2.2.1			

Total Items: 1.

2. Add an access policy:
 - a. From the navigation tree, select **User Access Policy > Access Policy**.
 - b. Click **Add** to open the **Add Access Policy** page.
 - c. Enter the policy name, select the service group, and use the default settings for other parameters.
 - d. Click **OK**.

Figure 3 Adding an access policy

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

Basic Information

Access Policy Name *

Service Group *

Description

Authorization Information

Access Period

Allocate IP *

Downstream Rate(Kbps)

Upstream Rate(Kbps)

Priority

☐ RSA Authentication

Certificate Authentication ☒ None ☐ EAP

Certificate Type

Deploy VLAN

☐ Deploy User Profile

Deploy User Group

☐ Deploy ACL

3. Add an access service:
 - a. From the navigation tree, select **User Access Policy > Access Service**.
 - b. Click **Add** to open the **Add Access Service** page.
 - c. Enter the service name.
 - d. Select the access policy configured in the previous step as the default access policy.
 - e. Use the default settings for other parameters.
 - f. Click **OK**.

Figure 4 Adding an access service

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

Basic Information

Service Name *

Service Suffix

Service Group *

Default Access Policy *

Default Proprietary Attribute Assignment Policy *

Default Max. Number of Bound Endpoints *

Default Max. Number of Online Endpoints *

Description

☒ Available ? ☐ Transparent Authentication on Portal Endpoints ?

Access Scenario List

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

4. Add an access user:
 - a. From the navigation tree, select **Access User > All Access Users**.
 - b. Click **Add** to open the **Add Access User** page.
 - c. Click **Select** to select an existing user or click **Add User** to add a new user.

- d. Enter the account name.
- e. Enter and confirm the password.
- f. In the **Access Service** area, select the access service configured in the previous step.
- g. Use the default settings for other parameters.
- h. Click **OK**.

Figure 5 Adding an access user

Verifying the configuration

Use the configured username and password to perform portal authentication through a Web browser on the client. Before passing authentication, all Web accesses are redirected to the portal authentication page (**http://2.2.2.1/portal**). After passing authentication, you can access other network resources.

Display the online portal user information on the AC.

```
[AC] display portal user all
```

```
Total portal users: 1
```

```
Username: Client
```

```
AP name: office
```

```
Radio ID: 2
```

```
SSID: service
```

```
Portal server:newpt
```

```
State: Online
```

```
VPN instance: N/A
```

MAC	IP	VLAN	Interface
0024-d705-c686	2.2.2.2	200	WLAN-BSS1/0/2

```
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

- AC:

```
#
vlan 100
#
vlan 200
#
wlan service-template st1
  ssid service
  vlan 200
  client forwarding-location ac
  akm mode psk
  preshared-key pass-phrase cipher $c$3$9tIUHskAUVqCH9/EPrL26ldkcEQnngexUEFj
  cipher-suite ccmp
  security-ie rsn
  portal enable method direct
  portal domain dm1
  portal apply web-server newpt
  service-template enable
#
interface Vlan-interface100
  ip address 192.168.0.100 255.255.255.0

#
interface Vlan-interface200
  ip address 2.2.2.1 255.255.255.0
#
interface GigabitEthernet1/0/1
  port link-type trunk
  port trunk permit vlan 1 100 200
#
  radius session-control enable
#
radius scheme rs1
  primary authentication 192.168.0.112
  primary accounting 192.168.0.112
  key authentication cipher $c$3$Sggqz7lDs4XPnethmAgyAKVlke7qwEkYbQ==
  key accounting cipher $c$3$4J/JBRGwqB4F213furJmKB6JWYXBFjWE6g==
  user-name-format without-domain
  nas-ip 2.2.2.1
#
domain dm1
  authorization-attribute idle-cut 15 1024
  authentication portal radius-scheme rs1
  authorization portal radius-scheme rs1
  accounting portal radius-scheme rs1
#
```

```

portal host-check enable
portal free-rule 1 destination ip any udp 53
portal free-rule 2 destination ip any tcp 53
#
portal roaming enable
undo portal refresh arp enable
#
portal web-server newpt
url http://2.2.2.1/portal
server-type cmcc
url-parameter wlanuserip source-address
#
portal local-web-server http
default-logon-page abc.zip
#
wlan ap-group group1
ap office
ap-model AP 3620
radio 1
radio 2
radio enable
service-template st1
#
wlan ap office model AP 3620
serial-id 219801A28N819CE0002T
#

```

- **Switch:**

```

#
vlan 100
#
vlan 200
#
interface GigabitEthernet1/0/1
port link-type trunk
port trunk permit vlan 1 100 200
#
interface GigabitEthernet1/0/2
port link-type access
port access vlan 100
poe enable

```

Related documentation

- *User Access and Authentication Command Reference in INTELBRAS Access Controllers Command References*
- *User Access and Authentication Configuration Guide in INTELBRAS Access Controllers Configuration Guides*
- *WLAN Access Command Reference in INTELBRAS Access Controllers Command References*

- *WLAN Access Configuration Guide in INTELBRAS Access Controllers Configuration Guides*

INTELBRAS Access Controllers

HTTPS-Based Local Portal

Authentication Configuration Examples

Copyright © 2024 Intelbras S.A All rights reserved.

No part of this manual may be reproduced or transmitted in any form or by any means without prior written consent of Intelbras S.A

Except for the trademarks of Intelbras S.A, any trademarks that may be mentioned in this document are the property of their respective owners.

The information in this document is subject to change without notice.

Contents

Introduction	1
Prerequisites	1
Example: Configuring HTTPS-based local portal authentication	1
Network configuration	1
Restrictions and guidelines	1
Procedures	1
Verifying the configuration	4
Configuration files	8
Related documentation	10

Introduction

The following information provides an example of configuring HTTP-based local portal authentication.

Prerequisites

This document applies to Comware-based access controllers and access points. Procedures and information in the examples might be slightly different depending on the software or hardware version of the access controllers and access points.

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 SSL, portal authentication, and PKI.

Example: Configuring HTTPS-based local portal authentication

Network configuration

As shown in [Figure 1](#), the wireless client needs to access the network resources.

Configure HTTPS-based local portal authentication on the AC to allow the client to access network resources only after the client passes portal authentication.

Configure PKI and SSL on the AC to perform digital certificate-based authentication on the client but not to display the message of unavailable security certificate revocation information when the client performs portal authentication.

Figure 1 Network diagram



Restrictions and guidelines

Before configuring HTTPS-based local portal authentication, make sure the devices can reach each other.

Use the actual serial ID of an AP to uniquely identify that AP.

Make sure the AC has a valid CA certificate and a valid local certificate.

Procedures

Configuring certificates

Create a PKI domain named **domain1**.

```
<AC> system-view
```

```
[AC] pki domain domain1
```

Disable CRL checking.

```
[AC-pki-domain-domain1] undo crl check enable
```

```
[AC-pki-domain-domain1] quit
```

Import CA certificate file **certnew.cer in DER format to PKI domain **domain1**. The certificate file contains the root certificate.**

```
[AC] pki import domain domain1 der ca filename certnew.cer
```

The trusted CA's finger print is:

```
MD5 fingerprint:98D8 2B98 6D35 1DE7 A13A C362 DA33 2F38
```

```
SHA1 fingerprint:5817 1C1E D81F 1B5F 525D 5183 C196 37B8 73C7 46E5
```

Is the finger print correct?(Y/N):y

Import local certificate file **QQ.pfx in PKCS12 format to PKI domain **domain1**. The certificate file contains a key pair.**

```
[AC] pki import domain domain1 p12 local filename QQ.pfx
```

Please input the password:

Configuring an SSL server policy

Create an SSL server policy named **myssl.**

```
[AC] ssl server-policy myssl
```

Specify PKI domain **domain1 for SSL server policy **myssl**.**

```
[AC-ssl-server-policy-myssl] pki-domain domain1
```

Enable mandatory SSL client authentication.

```
[AC-ssl-server-policy-myssl] client-verify enable
```

```
[AC-ssl-server-policy-myssl] quit
```

Configuring AAA

Add network access user named **user1, and assign the portal service to the user.**

```
[AC] local-user user1 class network
```

```
[AC-luser-network-user1] password simple user1
```

```
[AC-luser-network-user1] service-type portal
```

```
[AC-luser-network-user1] quit
```

Create an ISP domain named **dm1, and configure local authentication, authorization, and accounting for portal users in the domain.**

```
[AC] domain dm1
```

```
[AC-isp-dm1] authentication portal local
```

```
[AC-isp-dm1] authorization portal local
```

```
[AC-isp-dm1] accounting portal local
```

```
[AC-isp-dm1] quit
```

Specify ISP domain **dm1 as the default ISP domain.**

```
[AC] domain default enable dm1
```

Configuring the wireless service and HTTPS-based portal authentication

Create a portal Web server named **newpt.**

```
[AC] portal web-server newpt
```

Specify **https://84.7.0.3/portal as the URL of the portal Web server.**

```
[AC-portal-websvr-newpt] url https://84.7.0.3/portal
```

```
[AC-portal-websvr-newpt] quit
```

```

# Enable validity check on wireless portal clients.
[AC] portal host-check enable

# Configure two destination-based portal-free rules to permit the traffic destined for the DNS server.
[AC] portal free-rule 1 destination ip any udp 53
[AC] portal free-rule 2 destination ip any tcp 53

# Create a service template named service1.
[AC] wlan service-template service1

# Set the SSID of the service template.
[AC-wlan-st-service1] ssid service1

# Specify the AKM mode as PSK, and configure the preshared key as 12345678 in plain text.
[AC-wlan-st-service1] akm mode psk
[AC-wlan-st-service1] preshared-key pass-phrase simple 12345678

# Specify the cipher suite as CCMP and the security IE as RSN.
[AC-wlan-st-service1] cipher-suite ccmp
[AC-wlan-st-service1] security-ie rsn

# Configure the AC to forward client data traffic. (Skip this step if the client data traffic forwarder is the AC by default.)
[AC-wlan-st-service1] client forwarding-location ac

# Enable direct portal authentication on the service template.
[AC-wlan-st-service1] portal enable method direct

# Specify portal Web server newpt on the service template.
[AC-wlan-st-service1] portal apply web-server newpt

# Enable the service template.
[AC-wlan-st-service1] service-template enable
[AC-wlan-st-service1] quit

# Set the HTTPS service port number to 8080. Make sure this port number is not used by the local portal Web service.
[AC] ip https port 8080

# Create an HTTPS-based local portal Web service and specify SSL server policy myssl for the service.
[AC] portal local-web-server https ssl-server-policy myssl

# Specify file defaultfile.zip as the default authentication page file for the local portal Web service.
[AC-portal-local-websvr-https] default-logon-page defaultfile.zip
[AC-portal-local-websvr-https] quit

```

Configuring the AP

NOTE:

In large-scale networks, configure AP groups instead of single APs as a best practice.

```

# Create VLAN 200. This VLAN will be used for wireless client access.
[AC] vlan 200
[AC-vlan200] quit

# Create an AP named ap1 with model AP 3620, and specify the serial ID of the AP.
[AC] wlan ap ap1 model AP 3620
[AC-wlan-ap-ap1] serial-id 219801A28N819CE0002T

```

```

[AC-wlan-ap-ap1] quit
# Create AP group group1 and add AP 1 to AP group group1.
[AC] wlan ap-group group1
[AC-wlan-ap-group-group1] ap ap1
# Bind service template service1 to radio 2 in AP group group1.
[AC-wlan-ap-group-group1] ap-model AP 3620
[AC-wlan-ap-group-group1-ap-model-AP 3620] radio 2
[AC-wlan-ap-group-group1-ap-model-AP 3620-radio-2] service-template service1 vlan 200
# Enable radio 2.
[AC-wlan-ap-group-group1-ap-model-AP 3620-radio-2] radio
enable [AC-wlan-ap-group-group1-ap-model-AP 3620-radio-2] quit
[AC-wlan-ap-group-group1-ap-model-AP 3620]
quit [AC-wlan-ap-group-group1] quit

```

Verifying the configuration

Verifying certificate import

Display information about the CA certificate in PKI domain **domain1** to verify that the CA certificate has been imported to the PKI domain.

```

[AC] display pki certificate domain domain1 ca
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number:
      27:ef:22:2e:cc:63:9e:9c:4c:f7:2b:ba:81:d2:8e:a9
    Signature Algorithm: sha1WithRSAEncryption
    Issuer: C=BR, ST=brasilia, L=haidian, O=intelbras, OU=wireless/emailAddress=kf2
576@intelbras.com/description=kf2576, CN=wlan
    Validity
      Not Before: Jul 12 05:16:08 2017 GMT
      Not After : Jul 12 05:24:51 2517 GMT
    Subject: C=BR, ST=brasilia, L=haidian, O=intelbras, OU=wireless/emailAddress=kf
2576@intelbras.com/description=kf2576, CN=wlan
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      Public-Key: (512 bit)
      Modulus:
        00:cb:7e:d0:dd:38:f7:e8:20:00:2d:ba:f0:b7:37:
        33:f6:cb:7a:1b:6b:74:56:63:5f:34:94:e3:06:4b:
        06:36:e5:3e:22:ab:96:c5:52:d3:57:98:b0:b4:72:
        6e:1f:0b:ed:40:50:0c:db:7d:c6:5e:15:34:a1:89:
        e7:de:ec:84:07
      Exponent: 65537 (0x10001)
  X509v3 extensions:
    X509v3 Key Usage:
      Digital Signature, Certificate Sign, CRL Sign
    X509v3 Basic Constraints: critical

```

```

    CA:TRUE
X509v3 Subject Key Identifier:
    96:BB:A7:8D:70:C7:E9:46:C3:B7:EE:F4:E8:1A:D8:6F:16:B8:15:73
X509v3 CRL Distribution Points:

    Full Name:
        URI:http://cal/CertEnroll/wlan.crl
        URI:file://\\cal\CertEnroll\wlan.crl

1.3.6.1.4.1.311.21.1:
...
Signature Algorithm: sha1WithRSAEncryption
    60:76:1a:52:bf:f0:79:45:22:04:7c:91:13:8a:9c:be:d9:18:
    20:14:5d:55:5c:31:22:49:ba:40:bc:ec:c2:ba:08:ac:11:0e:
    d5:d8:23:18:f4:5c:6a:c9:10:5e:d4:92:4c:d7:b8:cf:dc:92:
    41:24:db:93:3e:7a:14:3b:ad:b0

# Display information about the local certificate in PKI domain domain1 to verify that the local
certificate has been imported to the PKI domain.
[AC] display pki certificate domain domain1 local
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            3b:1a:30:5e:00:00:00:00:00:1d
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=BR, ST=brasil, L=haidian, O=intelbras, OU=wireless/emailAddress=kf2
576@intelbras.com/description=kf2576, CN=wlan
        Validity
            Not Before: Dec 27 12:01:47 2017 GMT
            Not After : Dec 27 12:11:47 2273 GMT
        Subject: C=CN, CN=QQ
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            Public-Key: (1024 bit)
            Modulus:
                00:c4:bf:a1:86:3b:ba:53:8b:aa:c7:43:1a:1a:be:
                18:4e:fa:d1:5e:9a:49:b3:bb:b9:92:be:64:6b:97:
                06:f6:bd:c0:d9:36:20:50:c6:eb:5c:4f:89:1c:6d:
                c6:62:65:1f:a0:06:50:9e:ee:23:b7:ad:73:58:dc:
                e9:62:1a:5f:87:8b:fd:da:2f:43:58:0f:45:06:b8:
                7f:d5:43:52:e6:ed:fe:ce:7e:fa:20:6d:bc:67:c6:
                e5:dd:06:35:bd:fb:a2:04:85:34:b9:dd:ff:3c:f8:
                78:9e:92:ad:4c:86:7d:33:04:09:90:ce:ab:a8:30:
                f3:87:f5:4b:c7:9c:a5:4d:8b
            Exponent: 65537 (0x10001)
X509v3 extensions:
    X509v3 Key Usage: critical
        Digital Signature, Non Repudiation, Key Encipherment, Data Encip

```

```

herment
    S/MIME Capabilities:
.....0...+....0050...*.H..
..*.H..
    X509v3 Subject Key Identifier:
        73:9E:F6:85:15:4F:FE:1B:CC:C3:1C:48:99:41:E7:DA:8E:89:B8:74
    X509v3 Extended Key Usage:
        TLS Web Server Authentication
    X509v3 Authority Key Identifier:
        keyid:96:BB:A7:8D:70:C7:E9:46:C3:B7:EE:F4:E8:1A:D8:6F:16:B8:15:7

3

    X509v3 CRL Distribution Points:

        Full Name:
            URI:ldap:///CN=wlan,CN=cal,CN=CDP,CN=Public%20Key%20Services,C
N=Services,DC=UnavailableConfigDN?certificateRevocationList?base?objectClass=cRL
DistributionPoint
            URI:http://cal/CertEnroll/wlan.crl
            URI:file:///\\cal\CertEnroll\wlan.crl

        Authority Information Access:
            CA Issuers - URI:http://cal/CertEnroll/cal_wlan.crt
            CA Issuers - URI:file:///\\cal\CertEnroll\cal_wlan.crt

    Signature Algorithm: sha1WithRSAEncryption
        0b:f8:f8:53:ef:b2:f9:01:07:4e:89:cf:b7:5b:e2:72:a6:38:
        fa:af:99:30:0c:57:3f:36:25:f9:ed:02:7b:df:4b:a8:bd:92:
        63:b8:d8:ae:ae:72:9a:4d:1f:ea:fa:8a:1f:dc:5a:ad:ec:31:
        2a:15:65:ea:74:bc:95:c1:21:a9

```

Verifying SSL server policy configuration

Display information about SSL server policy myssl.

```
[AC] display ssl server-policy myssl
```

```
SSL server policy: myssl
```

```
Version-info:
```

```
SSL3.0: Enabled
```

```
TLS1.0: Enabled
```

```
TLS1.1: Enabled
```

```
TLS1.2: Enabled
```

```
PKI domain: user2
```

```
Ciphersuites:
```

```
RSA_AES_128_CBC_SHA
```

```
RSA_DES_CBC_SHA
```

```
RSA_RC4_128_MD5
```

```
RSA_RC4_128_SHA
```

```
RSA_3DES_CBC_SHA
```

```
RSA_AES_256_CBC_SHA
```

```
EXP_RSA_RC4_MD5
```

```
RSA_RC2_CBC_MD5
EXP_RSA_DES_CBC_SHA
DHE_RSA_AES_128_CBC_SHA
DHE_RSA_AES_256_CBC_SHA
RSA_AES_128_CBC_SHA256
RSA_AES_256_CBC_SHA256
DHE_RSA_AES_128_CBC_SHA256
DHE_RSA_AES_256_CBC_SHA256
ECDHE_RSA_AES_128_CBC_SHA256
ECDHE_RSA_AES_256_CBC_SHA384
ECDHE_RSA_AES_128_GCM_SHA256
ECDHE_RSA_AES_256_GCM_SHA384
ECDHE_ECDSA_AES_128_CBC_SHA256
ECDHE_ECDSA_AES_256_CBC_SHA384
ECDHE_ECDSA_AES_128_GCM_SHA256
ECDHE_ECDSA_AES_256_GCM_SHA384
Session cache size: 500
Caching timeout: 3600 seconds
Client-verify: Enabled
```

Verifying portal authentication

Display information about portal Web server **newpt**.

```
[AC] display portal web-server newpt
```

Portal Web server: newpt

```
Type: INC
URL: https://84.7.0.3/portal
URL parameters: Not configured
VPN instance: Not configured
Server detection: Not configured
IPv4 status: Up
IPv6 status: N/A
Captive-bypass: Disabled
If-match: Not configured
```

On a mobile phone that has connected to the wireless network, access **<https://84.7.0.3/portal>** (the URL of portal Web server **newpt**). The portal authentication page opens, as shown in [Figure 2](#). Enter the username and password of user **user1** on the portal authentication page.

Figure 2 Portal authentication page on a mobile phone

! 欢迎登录H3C PORTAL认证页面

H3C

账户

密码

登录

第三方账号登录

Display information about online portal users on the AC to verify that the user has come online.

```
[AC] display portal user all
Total portal users: 1
Username: user1
  AP name: ap1
  Radio ID: 2
  SSID: service1
  Portal server: N/A
  State: Online
  VPN instance: N/A
  MAC          IP          VLAN    Interface
  145f-94aa-d323 84.7.0.12    200     WLAN-BSS1/0/5
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 200
#
wlan service-template service1
  ssid service1
  client forwarding-location ac
  akm mode psk
  preshared-key pass-phrase cipher $c$3$9tIUH$kaUVqCH9/EPrL26ldkcEQnngexUEFj
```



```

cipher-suite ccmp
security-ie rsn
portal enable method direct
portal apply web-server newpt
service-template enable
#
domain dml
authentication portal local
authorization portal local
accounting portal local
#
domain default enable dml
#
local-user user1 class network
password cipher $c$3$iN3qo9XCWBRXSHA5q0sqlhkblSu/MCul
service-type portal
authorization-attribute user-role network-operator
#
pki domain domain1
undo crl check enable
#
ssl server-policy myssl
pki-domain domain1
client-verify enable
#
portal host-check enable
portal free-rule 1 destination ip any udp 53
portal free-rule 2 destination ip any tcp 53
#
portal web-server newpt
url https://84.7.0.3/portal
#
portal local-web-server https ssl-server-policy myssl
default-logon-page defaultfile.zip
#
ip https port 8080
ip http enable
ip https enable
#
wlan ap-group group1
ap ap1
ap-model AP 3620
radio 1
radio 2
radio enable
service-template service1 vlan 200
#

```

```
wlan ap ap1 model AP 3620  
serial-id 219801A28N819CE0002T  
#
```

Related documentation

- *Security Command Reference in INTELBRAS Access Controllers Command Reference*
- *Security Configuration Guide in INTELBRAS Access Controllers Configuration Guide*
- *WLAN Access Command Reference in INTELBRAS Access Controllers Command Reference*
- *WLAN Access Configuration Guide in INTELBRAS Access Controllers Configuration Guide*

INTELBRAS Access Controllers Remote Portal Authentication Configuration Examples

Copyright © 2024 Intelbras S.A All rights reserved.

No part of this manual may be reproduced or transmitted in any form or by any means without prior written consent of Intelbras S.A

Except for the trademarks of Intelbras S.A, any trademarks that may be mentioned in this document are the property of their respective owners.

The information in this document is subject to change without notice.

Contents

Introduction	1
Prerequisites	1
Example: Configuring remote portal authentication	1
Network configuration	1
Analysis	2
Restrictions and guidelines	2
Procedures	2
Configuring INC	2
Configuring the AC	7
Configuring the switch	10
Verifying the configuration	11
Configuration files	12
Related documentation	14

Introduction

The following information provides an example of configuring remote portal authentication.

Prerequisites

The following information applies to Comware-based access controllers and access points. Procedures and information in the examples might be slightly different depending on the software or hardware version of the access controllers and access points.

The configuration examples 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.

The following information is provided based on the assumption that you have basic knowledge of AAA, portal, and WLAN.

Example: Configuring remote portal authentication

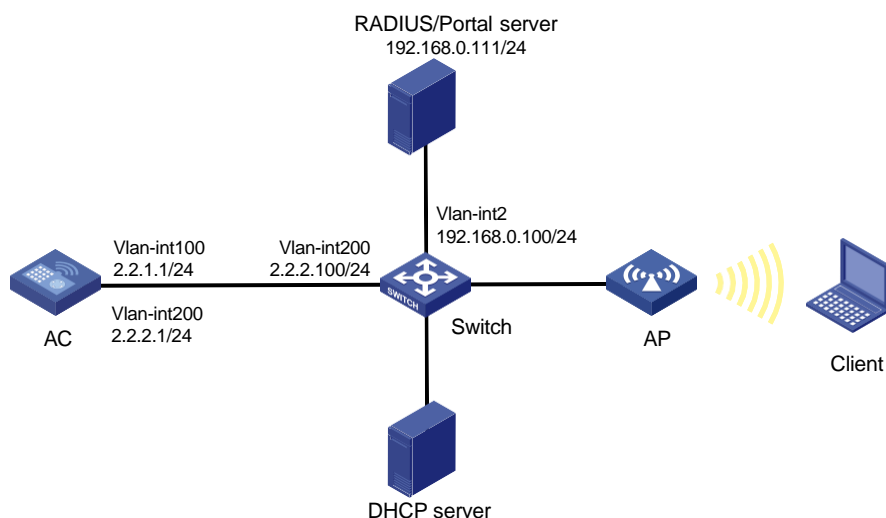
Network configuration

As shown in [Figure 1](#), the AP and the client obtain IP addresses from the DHCP server.

To implement remote portal authentication, perform the following tasks:

- Configure direct portal authentication.
- Configure a portal authentication server and a portal Web server on INC.
- Configure a RADIUS server as the authentication server and accounting server.

Figure 1 Network diagram



Analysis

To allow an authenticated user to access network resources on any Layer 2 ports in its access VLAN without re-authentication, enable portal roaming.

To avoid possible authentication failure caused by frequent logins and logouts of portal clients in a short time, disable the Rule ARP entry feature for portal clients.

For the RADIUS server to dynamically change user authorization information or forcibly disconnect users, enable the RADIUS session-control feature.

Restrictions and guidelines

Use the serial ID labeled on the AP's rear panel to specify an AP.

Make sure the types of the portal authentication server and portal Web server specified on the AC are the same as those actually used. (This example uses CMCC servers.)

By default, the portal Web server URL redirected to users does not carry parameters. You can configure the parameters to be carried in the redirection URL as needed.

Procedures

Configuring INC

In this example, the INC server runs INC PLAT 7.1 (E0303p13), INC INC - EIA 7.1 (F0302p08), and INC EIP 7.1 (F0302p08).

Configuring the RADIUS server

1. Add an access device.
 - a. Log in to INC and click the **User** tab.
 - b. From the navigation tree, select **User Access Policy > Access Device Management > Access Device**.
 - c. Click **Add** to open the page as shown in [Figure 2](#).
 - d. In the **Device List** area, click **Add Manually** to open the **Add Access Device Manually** page. Enter **2.2.2.1** in the **Start IP** field and then click **OK**.
 - e. In the **Access Configuration** area, set the shared key to **radius**, which must be the same as that configured on the AC.
 - f. Use the default settings for other parameters.
 - g. Click **OK**.

Figure 2 Adding an access device

User > User Access Policy > Access Device Management > Access Device > Add Access Device

Access Configuration

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

Device List

Select Add Manually Clear All

Device Name	Device IP	Device Model	Comments	Delete
	2.2.2.1			

Total Items: 1.

OK Cancel

2. Add an access policy.
 - a. From the navigation tree, select **User Access Policy > Access Policy**.
 - b. Click **Add** to open the page as shown in [Figure 3](#).
 - c. Enter the access policy name.
 - d. Select a service group. This example uses the default setting (**Ungrouped**).
 - e. Use the default settings for other parameters.
 - f. Click **OK**.

Figure 3 Adding an access policy

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

Basic Information

Access Policy Name *	AccessPolicy
Service Group *	Ungrouped
Description	

Authorization Information

Access Period	None	Allocate IP *	No
Downstream Rate(Kbps)		Upstream Rate(Kbps)	
Priority		<input type="checkbox"/> RSA Authentication	
Certificate Authentication	<input checked="" type="radio"/> None <input type="radio"/> EAP		
Certificate Type	EAP-TLS Authf		
Deploy VLAN			
<input type="checkbox"/> Deploy User Profile		Deploy User Group	
<input type="checkbox"/> Deploy ACL			

3. Add an access service.
 - a. From the navigation tree, select **User Access Policy > Access Service**.

- b. Click **Add** to open the page as shown in [Figure 4](#).
- c. Enter the service name.
- d. Use the default settings for other parameters.
- e. Click **OK**.

Figure 4 Adding an access service

4. Add an access user.
 - a. From the navigation tree, select **Access User > All Access Users**.
 - b. Click **Add** to open the page as shown in [Figure 5](#).
 - c. Select an existing access user or click **Add User** to add a new access user.
 - d. Set the password.
 - e. In the **Access Service** area, select the configured access service.
 - f. Use the default settings for other parameters.
 - g. Click **OK**.

Figure 5 Adding an access user

Configuring the portal server

1. Configure the portal authentication service:
 - a. From the navigation tree, select **User Access Policy > Portal Service > Server** to open the portal server configuration page, as shown in [Figure 6](#).

- b. Configure the portal server parameters as needed.
This example uses the default settings.
- c. Click **OK**.

Figure 6 Configuring the portal server

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 ? LB Device Address

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://192.168.0.111:8080/portal/

192.168.0.111

2. Configure the IP address group:
 - a. From the navigation tree, select **User Access Policy > Portal Service > IP Group**.
 - 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 client 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 7 Adding an IP address group

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

OK Cancel

3. Add a portal device:
 - a. From the navigation tree, select **User Access Policy > Portal Service > Device**.
 - b. Click **Add** to open the page as shown in [Figure 8](#).
 - c. Enter the device name.
 - d. Select **CMCC 1.0** from the **Version** list.
 - e. Enter the IP address of the AC's interface connected to the client.
 - f. 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**.
 - g. Enter the key, which must be the same as that configured on the AC.
 - h. Select **Directly Connected** for **Access Method**.
 - i. Use the default settings for other parameters.
 - j. Click **OK**.

Figure 8 Adding a portal device

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

Add Device

Device Information

Device Name *	NAS	Service Group *	Ungrouped ▼
Version *	CMCC 1.0 ▼	IP Address *	2.2.2.1
Listening Port *	2000	Local Challenge *	No ▼
Authentication Retries *	0	Logout Retries *	1
Support Server Heartbeat *	No ▼	Support User Heartbeat *	No ▼
Key *	*****	Confirm Key *	*****
Access Method *	Directly Connected ▼		
Device Description			

OK Cancel

4. Associate the portal device with the IP address group:
 - a. Click the **Port Group** icon in the **Operation** field of device **NAS**, as shown in [Figure 9](#).

Figure 9 Device list

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	CMCC 1.0	Ungrouped	2.2.2.1		Not Deployed	<div> <div>Port Group</div> <div></div> <div></div> <div></div> </div>

1-1 of 1. Page 1 of 1.

« < 1 > » 50

- b. Click **Add** to open the page as shown in [Figure 10](#).
 - 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 10 Adding a port group

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

Add Port Group

Port Group Name *	Group	Language *	English
Start Port *	0	End Port *	zzzzzz
Protocol *	HTTP	Quick Authentication *	No
NAT or Not *	No	Error Transparent Transmission *	Yes
Authentication Type *	CHAP	IP Group *	Porta_user
Heartbeat Interval(Minutes) *	0	Heartbeat Timeout(Minutes) *	0
User Domain		Port Group Description	
Transparent Authentication	Not Supported	Client Protection Against Cracks *	No
Page Push Policy		Default Authentication Page	

OK Cancel

Configuring the AC

1. Configure interfaces on the AC:

Create VLAN 100 and VLAN-interface 100. Assign an IP address to the VLAN interface. The AC will use this IP address to establish CAPWAP data and control tunnels with the AP.

```
<AC> system-view
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 2.2.1.1 24
[AC-Vlan-interface100] quit
```

Create VLAN 200 and VLAN-interface 200. Assign an IP address to the VLAN interface. The AC will use VLAN 200 for client access.

```
[AC] vlan 200
[AC-vlan200] quit
[AC] interface vlan-interface 200
[AC-Vlan-interface200] ip address 2.2.2.1 24
[AC-Vlan-interface200] quit
```

Configure the interface that is connected to the switch as a trunk port, and assign the port to VLAN 100 and VLAN 200.

```
[AC] interface gigabitEthernet 1/0/1
[AC-GigabitEthernet1/0/1] port link-type trunk
[AC-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[AC-GigabitEthernet1/0/1] quit
```

2. Configure a static route to reach the INC server:

```
[AC] ip route-static 192.168.0.0 255.255.0.0 2.2.2.100
```

3. Configure a wireless service:

Create a service template named **st1** and enter its view.

```
[AC] wlan service-template st1
```

Set the SSID of service template **st1** to **service**.

```
[AC-wlan-st-st1] ssid service
```

Assign clients coming online through service template **st1** to VLAN 200.

```
[AC-wlan-st-service] vlan 200
```

Specify the AKM mode as PSK, and configure the preshared key as 12345678 in plain text.

```
[AC-wlan-st-st1] akm mode psk
```

```
[AC-wlan-st-st1] preshared-key pass-phrase simple 12345678
```

Specify the cipher suite as CCMP and the security IE as RSN.

```
[AC-wlan-st-st1] cipher-suite ccmp
```

```
[AC-wlan-st-st1] security-ie rsn
```

Configure the AC to forward client data traffic. (Skip this step if the client data traffic forwarder is the AC by default.)

```
[AC-wlan-st-st1] client forwarding-location ac
```

Specify ISP domain **dm1** as the authentication domain for portal users on service template **st1**.

```
[AC-wlan-st-st1] portal domain dm1
```

Enable service template **st1**.

```
[AC-wlan-st-st1] service-template enable
```

```
[AC-wlan-st-st1] quit
```

4. Configure the AP:

NOTE:

In large-scale networks, configure AP groups instead of single APs as a best practice.

Create an AP named **office** with model **AP 3620** and set its serial ID to **219801A28N819CE0002T**.

```
[AC] wlan ap office model AP 3620
```

```
[AC-wlan-ap-office] serial-id 219801A28N819CE0002T
```

```
[AC-wlan-ap-office] quit
```

Create AP group **group1** and add AP **office** to AP group **group1**.

```
[AC] wlan ap-group group1
```

```
[AC-wlan-ap-group-group1] ap office
```

Bind service template **st1** to radio 2 in AP group **group1**.

```
[AC-wlan-ap-group-group1] ap-model AP 3620
```

```
[AC-wlan-ap-group-group1-ap-model-AP 3620] radio 2
```

```
[AC-wlan-ap-group-group1-ap-model-AP 3620-radio-2] service-template st1
```

Enable radio 2.

```
[AC-wlan-ap-group-group1-ap-model-AP 3620-radio-2] radio
```

```
enable [AC-wlan-ap-group-group1-ap-model-AP 3620-radio-2] quit
```

```
[AC-wlan-ap-group-group1-ap-model-AP 3620]
```

```
quit [AC-wlan-ap-group-group1] quit
```

5. Configure a RADIUS scheme:

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

```
[AC] radius scheme rs1
```

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

```
[AC-radius-rs1] primary authentication 192.168.0.111
[AC-radius-rs1] primary accounting 192.168.0.111
[AC-radius-rs1] key authentication simple radius
[AC-radius-rs1] key accounting simple radius
```

Configure the AC to remove the domain name from the usernames sent to the RADIUS servers.

```
[AC-radius-rs1] user-name-format without-domain
```

Specify 2.2.2.1 as the source IP address for outgoing RADIUS packets sent to the RADIUS servers.

```
[AC-radius-rs1] nas-ip 2.2.2.1
[AC-radius-rs1] quit
```

Enable the RADIUS session-control feature.

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

6. Configure an authentication domain:

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

```
[AC] domain dm1
```

Configure the authentication, authorization, and authorization methods as RADIUS for portal users in the ISP domain.

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

Configure the idle cut feature for users in the ISP domain. Log out a user if the user's traffic is less than 1024 bytes in 15 minutes.

```
[AC-isp-dm1] authorization-attribute idle-cut 15 1024
[AC-isp-dm1] quit
```

7. Configure portal authentication:

Create a portal authentication server named **newpt**, specify IP address 192.168.0.111 as the IP address of the authentication server, and specify 50100 as the portal service port number.

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

Specify CMCC as the type of portal authentication server **newpt**.

```
[AC-portal-server-newpt] server-type cmcc
[AC-portal-server-newpt] quit
```

Create a portal Web server named **newpt** and specify **http://192.168.0.111:8080/portal** as the URL of the server.

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

Add parameters **ssid**, **wlanuserip**, and **wlanacname** to the URL of portal Web server **newpt**. Specify the AP's SSID, the IP address of the client, and the AC's name as the values for the parameters, respectively. (The parameters are required to be carried in the URL of a portal Web server of the CMCC type.)

```
[AC-portal-websvr-newpt] url-parameter ssid ssid
[AC-portal-websvr-newpt] url-parameter wlanuserip source-address
[AC-portal-websvr-newpt] url-parameter wlanacname value AC
```

Specify CMCC as the type of portal Web server **newpt**.

```
[AC-portal-websvr-newpt] server-type cmcc
```

```

[AC-portal-websvr-newpt] quit
# Configure a destination-based portal-free rule numbered 0 to permit traffic destined for IP
address 192.168.0.111 (the portal Web server).
[AC] portal free-rule 0 destination ip 192.168.0.111 24
# Configure two destination-based portal-free rules to permit the traffic destined for the DNS
server.
[AC] portal free-rule 1 destination ip any udp 53
[AC] portal free-rule 2 destination ip any tcp 53
# Enable portal roaming.
[AC] portal roaming enable
# Enable validity check on wireless portal clients.
[AC] portal host-check enable
# Disable the Rule ARP entry feature for portal clients.
[AC] undo portal refresh arp enable
# Enable direct portal authentication on service template st1.
[AC] wlan service-template st1
[AC-wlan-st-st1] portal enable method direct
# Specify ISP domain dm1 as the portal authentication domain.
[AC-wlan-st-st1] portal domain dm1
# Specify portal Web server newpt on service template st1 for portal authentication.
[AC-wlan-st-st1] portal apply web-server newpt
# Configure the BAS-IP attribute as 2.2.2.2 for portal packets sent to portal authentication
server newpt.
[AC-wlan-st-st1] portal bas-ip 2.2.2.1
[AC-wlan-st-st1] quit

```

Configuring the switch

Create VLAN 100. The switch will use this VLAN to forward traffic on the CAPWAP tunnel between the AC and the AP.

```

<Switch> system-view
[Switch] vlan 100
[Switch-vlan100] quit

```

Create VLAN 200. The switch will use this VLAN to forward client traffic.

```

[Switch] vlan 200
[Switch-vlan200] quit

```

Create VLAN 2.

```

[Switch] vlan 2
[Switch-vlan2] quit

```

Configure GigabitEthernet 1/0/1 (the port connected to the AC) as a trunk port and assign the trunk port to VLAN 100 and VLAN 200.

```

[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[Switch-GigabitEthernet1/0/1] quit

```

Configure GigabitEthernet 1/0/2 (the port connected to the AP) as an access port and assign the access port to VLAN 100.

```

[Switch] interface gigabitethernet 1/0/2

```

```
[Switch-GigabitEthernet1/0/2] port link-type access
[Switch-GigabitEthernet1/0/2] port access vlan 100

# Enable PoE on the access port.
[Switch-GigabitEthernet1/0/2] poe enable
[Switch-GigabitEthernet1/0/2] quit

# Configure GigabitEthernet 1/0/3 (the port connected to the INC) as an access port. Assign the
access port to VLAN 2.
[Switch] interface gigabitethernet 1/0/3
[Switch-GigabitEthernet1/0/3] port link-type access
[Switch-GigabitEthernet1/0/3] port access vlan 2
[Switch-GigabitEthernet1/0/3] quit

# Create VLAN-interface 200 and assign an IP address to the VLAN interface.
[Switch] interface vlan-interface 200
[Switch-Vlan-interface200] ip address 2.2.2.100 255.255.255.0
[Switch-Vlan-interface200] quit

# Create VLAN-interface 2 and assign an IP address to the VLAN interface.
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] ip address 192.168.0.100 255.255.255.0
[Switch-Vlan-interface2] quit
```

Verifying the configuration

Use the configured username and password to perform portal authentication through a Web browser on the client. Before passing portal authentication, the user can access only the authentication page **http://192.168.0.111:8080/portal**. All Web requests from the user will be redirected to the authentication page. After passing portal authentication, the user can access other network resources.

Display information about all portal users.

```
[AC] display portal user all
Total portal users: 1
Username: Client
  AP name: office
  Radio ID: 2
  SSID: service
  Portal server: newpt
  State: Online
  VPN instance: N/A
  MAC          IP          VLAN    Interface
  0021-6330-0933 2.2.2.2    200     WLAN-BSS1/0/2
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

- AC:

```
#
vlan 100
#
vlan 200
#
wlan service-template st1
    ssid service
    vlan 200
client forwarding-location ac
    akm mode psk
    preshared-key pass-phrase cipher $c$3$9tIUHskAUVqCH9/EPrL26ldkcEQnngeXUEFj
    cipher-suite ccmp
    security-ie rsn
    portal enable method direct
    portal domain dm1
    portal bas-ip 2.2.2.1
    portal apply web-server newpt
    service-template enable
#
interface Vlan-interface100
    ip address 2.2.1.1 255.255.255.0
#
interface Vlan-interface200
    ip address 2.2.2.1 255.255.255.0
#
interface GigabitEthernet1/0/1
    port link-type trunk
    port trunk permit vlan 1 100 200
#
    ip route-static 192.168.0.0 16 2.2.2.100
#
    radius session-control enable
#
radius scheme rs1
    primary authentication 192.168.0.111
    primary accounting 192.168.0.111
    key authentication cipher $c$3$Sqqgz7lDs4XPnethmAgyAKVlke7qwEkYbQ==
    key accounting cipher $c$3$4J/JBRGwqB4F213furJmKB6JWYXBFjWE6g==
    user-name-format without-domain
    nas-ip 2.2.2.1
#
domain dm1
authorization-attribute idle-cut 15 1024
authentication portal radius-scheme rs1
authorization portal radius-scheme rs1
```

```

    accounting portal radius-scheme rs1
#
portal host-check enable
portal free-rule 0 destination ip 192.168.0.0 255.255.255.0
portal free-rule 1 destination ip any udp 53
portal free-rule 2 destination ip any tcp 53
#
    portal roaming enable
    undo portal refresh arp enable
#
portal web-server newpt
    url http://192.168.0.111:8080/portal
    server-type cmcc
    url-parameter ssid ssid
    url-parameter wlanacname value AC
    url-parameter wlanuserip source-address
#
portal server newpt
    ip 192.168.0.111 key cipher $c$3$Q82T/9AHq5HT7uFX7nho8K0Y6jziycoJTw==
    server-type cmcc
#
wlan ap-group group1
    ap office
    ap-model AP 3620
        radio 1
        radio 2
            radio enable
            service-template st1
#
wlan ap office model AP 3620
    serial-id 219801A28N819CE0002T
#

```

- **Switch:**

```

#
vlan 100
#
vlan 200
#
interface Vlan-interface2
    ip address 192.168.0.100 255.255.255.0
#
interface Vlan-interface200
    ip address 2.2.2.100 255.255.255.0
#
interface GigabitEthernet1/0/1
    port link-type trunk
    port trunk permit vlan 1 100 200
#

```

```
interface GigabitEthernet1/0/2
  port link-type access
  port access vlan 100
  poe enable
#
interface GigabitEthernet1/0/3
  port link-type access
  port access vlan 2
#
```

Related documentation

- *User Access and Authentication Command Reference in INTELBRAS Access Controllers Command References*
- *User Access and Authentication Configuration Guide in INTELBRAS Access Controllers Configuration Guides*
- *WLAN Access Command Reference in INTELBRAS Access Controllers Command References*
- *WLAN Access Configuration Guide in INTELBRAS Access Controllers Configuration Guides*

INTELBRAS Access Controllers

Local Portal Authentication Through the LDAP Server

Configuration Examples

Copyright © 2024 Intelbras S.A All rights reserved.

No part of this manual may be reproduced or transmitted in any form or by any means without prior written consent of Intelbras S.A

Except for the trademarks of Intelbras S.A, any trademarks that may be mentioned in this document are the property of their respective owners.

The information in this document is subject to change without notice.

Contents

Introduction	1
Prerequisites	1
Example: Configuring local portal authentication through the LDAP server	1
Network configuration	1
Restrictions and guidelines	2
Procedures	2
Configuring the AC	2
Configuring the switch	4
Configuring the LDAP server	5
Verifying the configuration	8
Configuration files	8
Related documentation	10

Introduction

The following information provides an example of configuring the local portal service on the AC to send wireless user information to the LDAP server for authentication.

Prerequisites

The following information applies to Comware-based access controllers and access points. Procedures and information in the examples might be slightly different depending on the software or hardware version of the access controllers and access points.

The configuration examples 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.

The following information is provided based on the assumption that you have basic knowledge of AAA, portal, and WLAN.

Example: Configuring local portal authentication through the LDAP server

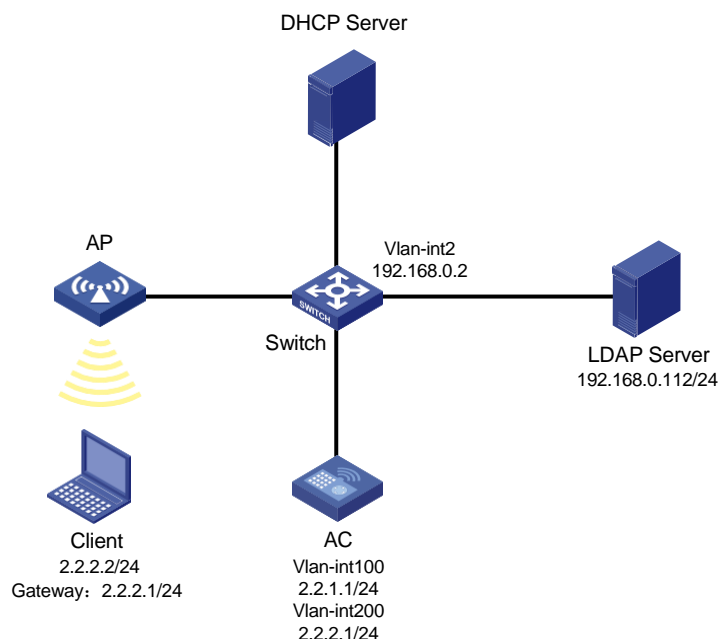
Network configuration

As shown in [Figure 1](#), the AP and the client obtain IP addresses from the DHCP server.

Configuration requirements are as follows:

- Configure the local portal service on the AC to provide authentication pages for clients.
- Use the LDAP server to authenticate the clients.

Figure 1 Network diagram



Restrictions and guidelines

Configure routing to make sure the devices can reach one another.

Use the actual serial ID of an AP to uniquely identify that AP.

Edit the authentication pages, compress them to a .zip file (this example uses **abc.zip**), and then upload the file to the root directory of the storage medium of the AC. On the AC, you must specify this file as the default authentication page file.

To change the default authentication page file, you must first execute the **undo default-logon-page** command, and then specify a new default authentication page file.

Procedures

Configuring the AC

1. Configuring VLANs and interfaces:

Create VLAN 100 and VLAN-interface 100. Assign the VLAN interface an IP address. The AC will use this IP address to establish a CAPWAP tunnel with the AP.

```
<AC> system-view
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 2.2.1.1 24
[AC-Vlan-interface100] quit
```

Create VLAN 200 and VLAN-interface 200. Assign the VLAN interface an IP address. This VLAN will be used for wireless client access.

```
[AC] vlan 200
[AC-vlan200] quit
[AC] interface vlan-interface 200
[AC-Vlan-interface200] ip address 2.2.2.1 24
[AC-Vlan-interface200] quit
```

Configure GigabitEthernet 1/0/1 (the port connected to the switch) as a trunk port. Assign the port to VLAN 100 and VLAN 200.

```
[AC] interface gigabitethernet 1/0/1
[AC-GigabitEthernet1/0/1] port link-type trunk
[AC-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[AC-GigabitEthernet1/0/1] quit
```

2. Configure the LDAP scheme:

Create an LDAP server named **ldap** and enter its view.

```
[AC] ldap server ldap
```

Specify the administrator DN.

```
[AC-ldap-server-ldap] login-dn cn=administrator,cn=users,dc=ldap,dc=com
```

Specify the base DN for user search.

```
[AC-ldap-server-ldap] search-base-dn dc=ldap,dc=com
```

Specify the IP address of the LDAP server.

```
[AC-ldap-server-ldap] ip 192.168.0.112
```

Specify the administrator password.

```
[AC-ldap-server-ldap] login-password simple 123456
```

```
[AC-ldap-server-ldap] quit
```

Create an LDAP scheme named **ldap** and enter its view.

```
[AC] ldap scheme ldap
```

Specify **ldap** as the LDAP authentication server.

```
[AC-ldap-ldap] authentication-server ldap
```

```
[AC-ldap-ldap] quit
```

Create an ISP domain named **ldap** and enter its view.

```
[AC] domain ldap
```

Configure the authentication method as LDAP and the authentication and accounting methods as none for portal users in ISP domain **ldap**.

```
[AC-isp-ldap] authentication portal ldap-scheme ldap
```

```
[AC-isp-ldap] authorization portal none
```

```
[AC-isp-ldap] accounting portal none
```

Configure the idle cut feature for users in ISP domain **ldap**. Log out a user if the user's traffic is less than 1024 bytes in 15 minutes.

```
[AC-isp-ldap] authorization-attribute idle-cut 15 1024
```

```
[AC-isp-ldap] quit
```

3. Configure portal authentication:

Create a portal Web server named **newpt** and specify **http://2.2.2.1/portal** as the server's URL.

```
[AC] portal web-server newpt
```

```
[AC-portal-websvr-newpt] url http://2.2.2.1/portal
```

```
[AC-portal-websvr-newpt] quit
```

Create an HTTP-based local portal Web service.

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

Specify file **abc.zip** as the default authentication page file. (The file must already exist in the root directory of the storage medium of the AC.)

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

```
[AC-portal-local-websvr-http] quit
```

Configure two destination-based portal-free rules to permit the traffic destined for the DNS server.

```
[AC] portal free-rule 1 destination ip any udp 53
```

```
[AC] portal free-rule 2 destination ip any tcp 53
```

4. Configure the wireless service:

Create a service template named **st1** and enter its view.

```
[AC] wlan service-template st1
```

Set the SSID of the service template to **service**.

```
[AC-wlan-st-st1] ssid service
```

Assign clients coming online through the service template to VLAN 200.

```
[AC-wlan-st-st1] vlan 200
```

Enable direct portal authentication on the service template.

```
[AC-wlan-st-st1] portal enable method direct
```

Specify ISP domain **ldap** as the portal authentication domain.

```
[AC-wlan-st-st1] portal domain ldap
```

Specify portal Web server **newpt** on the service template.

```
[AC-wlan-st-st1] portal apply web-server newpt
```

Configure the AC to forward client data traffic. (Skip this step if the client data traffic forwarder is the AC by default.)


```
[AC-wlan-st-st1] client forwarding-location ac
# Specify the AKM mode as PSK, and configure the preshared key as 12345678 in plain text.
[AC-wlan-st-st1] akm mode psk
[AC-wlan-st-st1] preshared-key pass-phrase simple 12345678
# Specify the cipher suite as CCMP and the security IE as RSN.
[AC-wlan-st-st1] cipher-suite ccmp
[AC-wlan-st-st1] security-ie rsn
# Enable the service template.
[AC-wlan-st-st1] service-template enable
[AC-wlan-st-st1] quit
```

5. Configure the AP:

NOTE:

In large-scale networks, configure AP groups instead of single APs as a best practice.

Create an AP named **ap1** with model **AP 3620**, and specify the AP model and serial ID.

```
[AC] wlan ap ap1 model AP 3620
[AC-wlan-ap-ap1] serial-id 219801A28N819CE0002T
```

Create AP group **group1** and add AP **ap1** to AP group **group1**.

```
[AC] wlan ap-group group1
[AC-wlan-ap-group-group1] ap ap1
```

Bind service template **st1** to radio 2 in AP group **group1**.

```
[AC-wlan-ap-group-group1] ap-model AP 3620
[AC-wlan-ap-group-group1-ap-model-AP 3620] radio 2
[AC-wlan-ap-group-group1-ap-model-AP 3620-radio-2] service-template st1
```

Enable radio 2.

```
[AC-wlan-ap-group-group1-ap-model-AP 3620-radio-2] radio
enable [AC-wlan-ap-group-group1-ap-model-AP 3620-radio-2]
return
```

Configuring the switch

Create VLAN 100. The switch will use this VLAN to forward traffic on the CAPWAP tunnel between the AC and AP.

```
<Switch> system-view
[Switch] vlan 100
[Switch-vlan100] quit
```

Create VLAN 200. The switch will use this VLAN to forward traffic of wireless clients.

```
[Switch] vlan 200
[Switch-vlan200] quit
```

Create VLAN 2. The switch will use this VLAN to connect to the LDAP server.

```
[Switch] vlan 2
[Switch-vlan2] quit
```

Assign VLAN-interface 2 (the interface connected to the LDAP server) to VLAN 2. (Details not shown.)

Assign the VLAN interface an IP address.

```
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] ip address 192.168.0.2 255.255.255.0
```

```
[Switch-Vlan-interface2] quit
```

Configure GigabitEthernet 1/0/1 (the port connected to the AC) as a trunk port. Assign the trunk port to VLAN 100 and VLAN 200.

```
[Switch] interface gigabitethernet1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[Switch-GigabitEthernet1/0/1] quit
```

Configure GigabitEthernet 1/0/2 (the port connected to the AP) as an access port. Assign the access port to VLAN 100.

```
[Switch] interface gigabitethernet1/0/2
[Switch-GigabitEthernet1/0/2] port link-type access
[Switch-GigabitEthernet1/0/2] port access vlan 100
```

Enable PoE on the access port.

```
[Switch-GigabitEthernet1/0/2] poe enable
[Switch-GigabitEthernet1/0/2] quit
```

Configuring the LDAP server

This example uses Microsoft Windows 2003 Server Active Directory to illustrate the configuration on the LDAP server.

1. Add a user named **aaa**.
 - a. On the LDAP server, select **Start > Control Panel > Administrative Tools**.
 - b. Double-click **Active Directory Users and Computers**.


The **Active Directory Users and Computers** window opens.
 - c. From the navigation tree, click **Users** under the **ldap.com** node.
 - d. Select **Action > New > User** from the menu to open the dialog box for adding a user.
 - e. Enter logon name **aaa** and click **Next**.

Figure 2 Adding user aaa

The screenshot shows the 'New Object - User' dialog box. The 'Create in' field is set to 'ldap.com/Users'. The 'First name' field contains 'aaa', 'Initials' is empty, 'Last name' is empty, and 'Full name' contains 'aaa'. The 'User logon name' field contains 'aaa' and the domain dropdown shows '@ldap.com'. The 'User logon name (pre-Windows 2000)' field contains 'LDAP\' and 'aaa'. At the bottom are '< Back', 'Next >', and 'Cancel' buttons.

- f. In the dialog box, enter password **123456**, select options as needed, and click **Next**.

New Object - User [X]

 Create in: ldap.com/Users

Password:

Confirm password:

☒ User must change password at next login

☐ User cannot change password

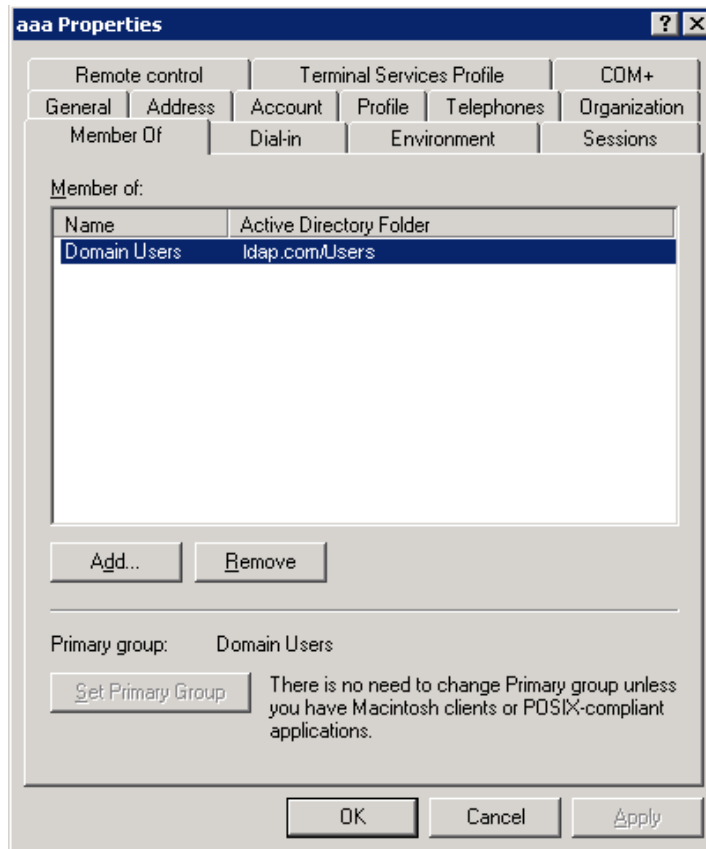
☐ Password never expires

☐ Account is disabled

< Back Next > Cancel

- 6

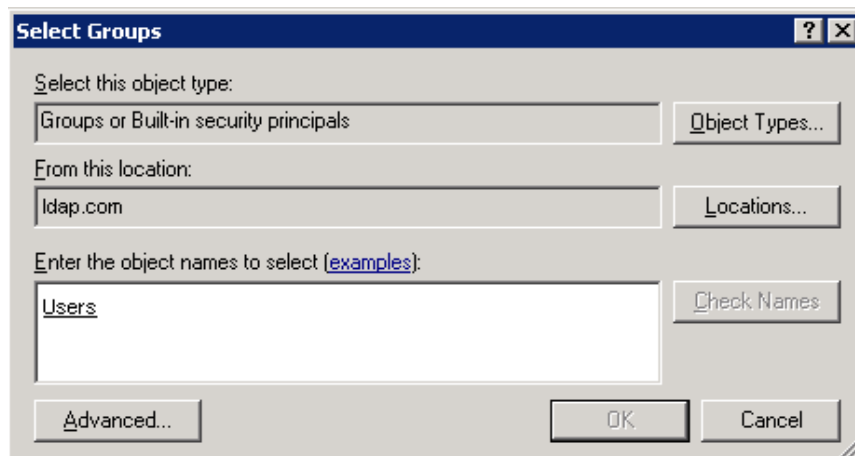
Figure 4 Modifying user properties



- d. In the **Select Groups** dialog box, enter **Users** in the **Enter the object names to select** field, and click **OK**.

User **aaa** is added to group **Users**.

Figure 5 Adding user aaa to group Users



3. Configure the administrator password:
- In the right pane, right-click user **Administrator** and select **Set Password**.
 - In the dialog box, enter the administrator password. (Details not shown.)

Verifying the configuration

Open a Web browser such as IE on the wireless client. Type an IP address in the address bar and press **Enter**. The portal authentication page opens. Enter username **aaa** and password **123456** and then click **Logon**. User **aaa** passes authentication successfully.

Display online portal users on the AC.

```
<AC> display portal user all
Index:17
State:ONLINE
SubState:NONE
ACL:3777
Work-mode:stand-alone
MAC                IP                Vlan      Interface
-----
2477-0341-f118     2.2.2.2          200       WLAN-BSS1/0/16
Total 1 user(s) matched, 1 listed.
```

Configuration files

- AC:

```
#
vlan 100
#
vlan 200
#
wlan service-template st1
  client forwarding-location ac
  akm mode psk
  preshared-key pass-phrase simple 12345678
  cipher-suite ccmp
  security-ie rsn
  ssid service
  vlan 200
  portal enable method direct
  portal domain ldap
  portal apply web-server newpt
  service-template enable
#
interface Vlan-interface100
  ip address 2.2.1.1 255.255.255.0
#
interface Vlan-interface200
  ip address 2.2.2.1 255.255.255.0
#
interface GigabitEthernet1/0/1
  port link-type trunk
  port trunk permit vlan 100 200
#
```

```

ldap server ldap
  login-dn cn=administrator,cn=users,dc=ldap,dc=com
  search-base-dn dc=ldap,dc=com
  ip 192.168.0.112
  login-password cipher $c$3$CEz2vKCnA2/51D8rFc/+nTNtOx8Gan+81Q==
#
ldap scheme ldap
  authentication-server ldap
#
domain ldap
  authorization-attribute idle-cut 15 1024
  authentication portal ldap-scheme ldap
  authorization portal none
  accounting portal none
#
portal host-check enable
portal free-rule 1 destination ip any udp 53
portal free-rule 2 destination ip any tcp 53
#
portal web-server newpt
  url http://2.2.2.1/portal
#
portal local-web-server http
  default-logon-page abc.zip
#
wlan ap ap1 model AP 3620
  serial-id 219801A28N819CE0002T
#
wlan ap-group group1
  ap ap1
  ap-model AP 3620
  radio 2
  radio enable
  service-template st1
#

```

- **Switch:**

```

#
vlan 100
#
vlan 200
#
vlan 2
#
interface Vlan-interface2
  ip address 192.168.0.2 255.255.255.0
#
interface GigabitEthernet1/0/1
  port link-mode bridge

```

```
port link-type trunk
port trunk permit vlan 100 200
#
interface GigabitEthernet1/0/2
port link-mode bridge
port access vlan 100
poe enable
#
```

Related documentation

- *User Access and Authentication Command Reference in INTELBRAS Access Controllers Command References*
- *User Access and Authentication Configuration Guide in INTELBRAS Access Controllers Configuration Guides*
- *WLAN Access Command Reference in INTELBRAS Access Controllers Command References*
- *WLAN Access Configuration Guide in INTELBRAS Access Controllers Configuration Guides*

INTELBRAS Access Controllers

Local Portal Authentication and SSID-based Authentication Page Pushing

Configuration Examples

Copyright © 2024 Intelbras S.A All rights reserved.

No part of this manual may be reproduced or transmitted in any form or by any means without prior written consent of Intelbras S.A

Except for the trademarks of Intelbras S.A, any trademarks that may be mentioned in this document are the property of their respective owners.

The information in this document is subject to change without notice.

Contents

Introduction	1
Prerequisites	1
Example: Configuring local portal authentication and SSID-based authentication page pushing	1
Network configuration	1
Analysis	2
Restrictions and guidelines	2
Procedures	2
Configuring the AC	2
Configuring the switch	6
Verifying the configuration	7
Configuration files	7
Related documentation	10

Introduction

The following information provides examples for configuring local portal authentication and SSID-based authentication page pushing on the AC.

Prerequisites

The following information applies to Comware-based access controllers and access points. Procedures and information in the examples might be slightly different depending on the software or hardware version of the access controllers and access points.

The configuration examples 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.

The following information is provided based on the assumption that you have basic knowledge of portal authentication.

Example: Configuring local portal authentication and SSID-based authentication page pushing

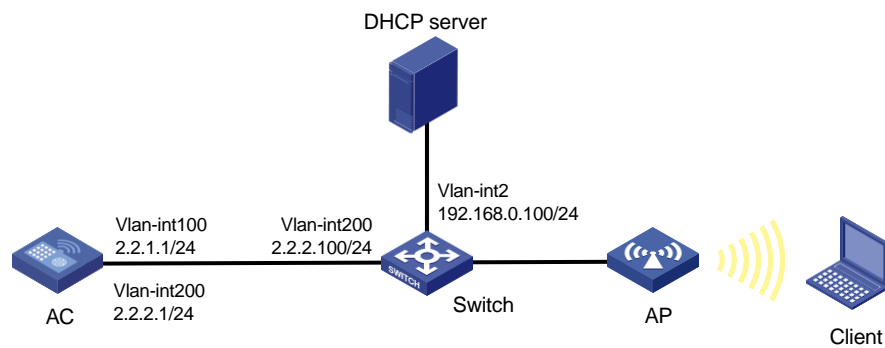
Network configuration

As shown in [Figure 1](#), the AP and the client obtain IP addresses from the DHCP server. The access device AC acts as the portal Web server and the portal authentication server.

Configure the devices to meet the following requirements:

- The AC provides direct portal authentication for the client. Before passing the authentication, the client can access only the portal Web server. After passing the authentication, the client can access other network resources.
- The client can access network resources through any Layer 2 ports in its access VLAN without re-authentication.

Figure 1 Network diagram



Analysis

To allow an authenticated user to access network resources on any Layer 2 ports in its access VLAN without re-authentication, you must enable the portal roaming feature.

In wireless networks where the AP forwards client traffic, the AC does not have ARP entries for clients. Therefore, the AC cannot check the validity of portal clients by using ARP entries. To ensure that valid users can perform portal authentication, you must enable wireless client validity check on the AC.

To avoid possible authentication failure caused by frequent logins and logouts of portal clients in a short time, disable the Rule ARP entry feature.

Restrictions and guidelines

Use the actual serial ID of an AP to uniquely identify that AP.

By default, the portal Web server URL redirected to users does carry parameters. You can configure the parameters to be carried in the redirection URL as needed.

Procedures

Configuring the AC

1. Configuring VLANs and interfaces:

Create VLAN 100 and VLAN-interface 100. Assign the VLAN interface an IP address. The AC will use this IP address to establish a CAPWAP tunnel with the AP.

```
<AC> system-view
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface 100
```

```
[AC-Vlan-interface100] ip address 2.2.1.1 24
[AC-Vlan-interface100] quit
```

Create VLAN 200 and VLAN-interface 200. Assign the VLAN interface an IP address. This VLAN will be used for wireless client access.

```
[AC] vlan 200
[AC-vlan200] quit
[AC] interface vlan-interface 200
[AC-Vlan-interface200] ip address 2.2.2.1 24
[AC-Vlan-interface200] quit
```

Configure the interface connected to the switch (GigabitEthernet 1/0/1) as a trunk port, and add the port to VLAN 100 and VLAN 200.

```
[AC] interface gigabitethernet 1/0/1
[AC-GigabitEthernet1/0/1] port link-type trunk
[AC-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[AC-GigabitEthernet1/0/1] quit
```

2. Configure the wireless service:

Create a service template named **st1 and enter its view.**

```
[AC] wlan service-template st1
```

Configure the SSID of the service template as **service.**

```
[AC-wlan-st-st1] ssid service
```

Assign clients coming online through the service template to VLAN 200.

```
[AC-wlan-st-st1] vlan 200
```

Configure the AC to forward client data traffic. (Skip this step if the client data traffic forwarder is the AC by default.)

```
[AC-wlan-st-st1] client forwarding-location ac
```

Specify the AKM mode as PSK, and configure the preshared key as 12345678 in plain text.

```
[AC-wlan-st-st1] akm mode psk
[AC-wlan-st-st1] preshared-key pass-phrase simple 12345678
```

Specify the cipher suite as CCMP and the security IE as RSN.

```
[AC-wlan-st-st1] cipher-suite ccmp
[AC-wlan-st-st1] security-ie rsn
[AC-wlan-st-st1] quit
```

Create a service template named **st2 and enter its view.**

```
[AC] wlan service-template st2
```

Configure the AC to forward client data traffic. (Skip this step if the client data traffic forwarder is the AC by default.)

```
[AC-wlan-st-st2] client forwarding-location ac
```

Configure the SSID of the service template as **service2.**

```
[AC-wlan-st-st2] ssid service2
```

Specify the AKM mode as PSK, and configure the preshared key as 12345678 in plain text.

```
[AC-wlan-st-st2] akm mode psk
[AC-wlan-st-st2] preshared-key pass-phrase simple 12345678
```

Specify the cipher suite as CCMP and the security IE as RSN.

```
[AC-wlan-st-st2] cipher-suite ccmp
[AC-wlan-st-st2] security-ie rsn
```

Assign clients coming online through the service template to VLAN 200.

```
[AC-wlan-st-st2] vlan 200
[AC-wlan-st-st2] quit
```

3. Configure the AP:

NOTE:

In large-scale networks, configure AP groups instead of single APs as a best practice.

Create an AP named **ap1. Specify the AP model and serial ID.**

```
[AC] wlan ap ap1 model AP 3620
[AC-wlan-ap-ap1] serial-id 219801A28N819CE0002T
```

Create AP group **group1 and add AP **ap1** to AP group **group1**.**

```
[AC] wlan ap-group group1
[AC-wlan-ap-group-group1] ap ap1
```

Bind service templates **st1 and **st2** to radio 2 in AP group **group1**.**

```
[AC-wlan-ap-group-group1] ap-model AP 3620
[AC-wlan-ap-group-group1-ap-model-AP 3620] radio 2
[AC-wlan-ap-group-group1-ap-model-AP 3620-radio-2] service-template
st1 [AC-wlan-ap-group-group1-ap-model-AP 3620-radio-2] service-
template st2 # Enable radio 2.
```

```
[AC-wlan-ap-group-group1-ap-model-AP 3620-radio-2] radio
enable [AC-wlan-ap-group-group1-ap-model-AP 3620-radio-2]
return
```

4. Configure the authentication domain:

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

```
<AC> system-view
[AC] domain dm1
```

Configure the authentication method as local, and authorization and accounting methods as none for portal users.

```
[AC-isp-dm1] authentication portal local
[AC-isp-dm1] authorization portal none
[AC-isp-dm1] accounting portal none
```

Configure the idle cut feature for users. Log out a user if the user's traffic is less than 1024 bytes in 15 minutes.

```
[AC-isp-dm1] authorization-attribute idle-cut 15 1024
[AC-isp-dm1] quit
```

5. Configure portal authentication:

Create a portal Web server named **newpt and specify the server's URL as **http://2.2.2.1/portal**.**

```
[AC] portal web-server newpt
[AC-portal-websvr-newpt] url http://2.2.2.1/portal
```

Configure the portal redirection URL to carry the **wlanuserip** parameter and the parameter value is the user's IP address.

```
[AC-portal-websvr-newpt] url-parameter wlanuserip source-address
[AC-portal-websvr-newpt] quit
```

Create an HTTP-based local portal Web service and enter its view.

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

Configure SSID **service** to use authentication page file **abc.zip** and SSID **service2** to use authentication page file **http.zip**. (The files must already exist in the root directory of the storage medium of the AC.)

```
[AC-portal-local-websvr-http] default-logon-page abc.zip
[AC-portal-local-websvr-http] logon-page bind ssid service2 file http.zip
[AC-portal-local-websvr-http] quit
```

Configure a local user for local portal authentication.

```
[AC] local-user 123 class network
[AC-luser-network-123] password simple 123
[AC-luser-network-123] service-type portal
[AC-luser-network-123] quit
```

Enable the portal roaming feature.

```
[AC] portal roaming enable
```

Disable the Rule ARP entry feature for portal clients.

```
[AC] undo portal refresh arp enable
```

Enable the wireless client validity check feature.

```
[AC] portal host-check enable
```

6. Configure service template **st1**:

Enable direct portal authentication on service template **st1**.

```
[AC] wlan service-template st1
[AC-wlan-st-st1] portal enable method direct
```

Configure the authentication domain for portal users as **dm1**.

```
[AC-wlan-st-st1] portal domain dml
```

Specify portal Web server **newpt** on service template **st1**.

```
[AC-wlan-st-st1] portal apply web-server newpt
[AC-wlan-st-st1] quit
```

Enable service template **st1**.

```
[AC-wlan-st-st1] service-template enable
[AC-wlan-st-st1] quit
```

7. Configure service template **st2**:

Enable direct portal authentication on service template **st2**.

```
[AC] wlan service-template st2
[AC-wlan-st-st2] portal enable method direct
```

Configure the authentication domain for portal users as **dm1**.

```
[AC-wlan-st-st2] portal domain dml
```

Specify portal Web server **newpt** on service template **st2**.

```
[AC-wlan-st-st2] portal apply web-server newpt
[AC-wlan-st-st2] quit

# Enable service template st2.

[AC-wlan-st-st2] service-template enable
[AC-wlan-st-st2] quit
```

Configuring the switch

Create VLAN 100. The switch will use this VLAN to forward traffic on the CAPWAP tunnel between the AC and the AP.

```
<Switch> system-view
[Switch] vlan 100
[Switch-vlan100] quit
```

Create VLAN 200. The switch will use this VLAN to forward traffic of wireless clients.

```
[Switch] vlan 200
[Switch-vlan200] quit
```

Create VLAN 2.

```
[Switch] vlan 2
[Switch-vlan2] quit
```

Configure GigabitEthernet 1/0/1 (the port connected to the AC) as a trunk port. Assign the trunk port to VLAN 100 and VLAN 200.

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[Switch-GigabitEthernet1/0/1] quit
```

Configure GigabitEthernet 1/0/2 (the port connected to the AP) as an access port. Assign the access port to VLAN 100.

```
[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] port link-type access
[Switch-GigabitEthernet1/0/2] port access vlan 100
```

Enable PoE on the access port.

```
[Switch-GigabitEthernet1/0/2] poe enable
[Switch-GigabitEthernet1/0/2] quit
```

Configure GigabitEthernet 1/0/3 (the port connected to the DHCP server) as an access port. Assign the access port to VLAN 2.

```
[Switch] interface gigabitethernet 1/0/3
[Switch-GigabitEthernet1/0/3] port link-type access
[Switch-GigabitEthernet1/0/3] port access vlan 2
[Switch-GigabitEthernet1/0/3] quit
```

Assign an IP address to VLAN interface 200.

```
[Switch] interface vlan-interface 200
[Switch-Vlan-interface200] ip address 2.2.2.100 255.255.255.0
[Switch-Vlan-interface200] quit
```

Assign an IP address to VLAN interface 2.

```
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] ip address 192.168.0.100 255.255.255.0
[Switch-Vlan-interface2] quit
```

Verifying the configuration

Use the configured username and password to perform portal authentication through a Web browser on the client. Before passing authentication, all Web accesses are redirected to the portal authentication page (**http://2.2.2.1/portal**). After passing authentication, you can access other network resources.

Display the online portal user information on the AC.

```
[AC] display portal user all
Total portal users: 1
Username: 123
  AP name: ap1
  Radio ID: 2
  SSID: service
  Portal server: newpt
  State: Online
  VPN instance: N/A
  MAC          IP          VLAN    Interface
  0021-6330-0933 2.2.2.2    200     WLAN-BSS1/0/1
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

- AC:

```
#
vlan 100
#
vlan 200
#
wlan service-template st1
  ssid service
client forwarding-location ac
  akm mode psk
  preshared-key pass-phrase simple 12345678
  cipher-suite ccmp
```



```

security-ie rsn
vlan 200
portal enable method direct
portal domain dml
portal apply web-server newpt
service-template enable
#
wlan service-template st2
ssid service2
client forwarding-location ac
akm mode psk
preshared-key pass-phrase simple 12345678
cipher-suite ccmp
security-ie rsn
vlan 200
portal enable method direct
portal domain dml
portal apply web-server newpt
service-template enable
#
interface Vlan-interface100
ip address 2.2.1.1 255.255.255.0
#
interface Vlan-interface200
ip address 2.2.2.1 255.255.255.0
#
interface GigabitEthernet1/0/1
port link-mode bridge
port link-type trunk
port trunk permit vlan 1 100 200
#
domain dml
authorization-attribute idle-cut 15 1024
authentication portal local
authorization portal none
accounting portal none
#
local-user 123 class network
password cipher $c$3$evSrJBp3lwOqEZw7KdwPugEfvJ5M/w==
service-type portal
#
portal host-check enable
#
portal roaming enable
undo portal refresh arp enable
#
portal web-server newpt
url http://2.2.2.1/portal

```

```

url-parameter wlanuserip source-address
#
portal local-web-server http
default-logon-page abc.zip
logon-page bind ssid service2 file http.zip
#
wlan ap ap1 model AP 3620
serial-id 219801A28N819CE0002T
#
wlan ap-group group1
ap ap1
ap-model AP 3620
radio 1
radio 2
radio enable
service-template st1
service-template st2
#
• Switch:
#
vlan 2
#
vlan 100
#
vlan 200
#
interface Vlan-interface2
ip address 192.168.0.100 255.255.255.0
#
interface Vlan-interface200
ip address 2.2.2.100 255.255.255.0
#
interface GigabitEthernet1/0/1
port link-type trunk
port trunk permit vlan 1 100 200
#
interface GigabitEthernet1/0/2
port link-type access
port access vlan 100
poe enable
#
interface GigabitEthernet1/0/3
port link-type access
port access vlan 2
#

```

Related documentation

- *AP and WT Management Command Reference in INTELBRAS Access Controllers Command References*
- *AP and WT Management Configuration Guide in INTELBRAS Access Controllers Configuration Guides*
- *User Access and Authentication Command Reference in INTELBRAS Access Controllers Command References*
- *User Access and Authentication Configuration Guide in INTELBRAS Access Controllers Configuration Guides*
- *WLAN Access Command Reference in INTELBRAS Access Controllers Command References*
- *WLAN Access Configuration Guide in INTELBRAS Access Controllers Configuration Guides*

INTELBRAS Access Controllers

Local Portal MAC-Trigger Authentication

Configuration Examples

Copyright © 2024 Intelbras S.A All rights reserved.

No part of this manual may be reproduced or transmitted in any form or by any means without prior written consent of Intelbras S.A

Except for the trademarks of Intelbras S.A, any trademarks that may be mentioned in this document are the property of their respective owners.

The information in this document is subject to change without notice.

Contents

Introduction	1
Prerequisites	1
Example: Configuring local portal MAC-trigger authentication	1
Network configuration	1
Analysis	2
Restrictions and guidelines	2
Procedures	2
Configuring the AC	2
Configuring the switch	5
Verifying the configuration	5
Configuration files	6
Related documentation	8

Introduction

The following information provides an example of configuring local portal MAC-trigger authentication.

Prerequisites

The following information applies to Comware-based access controllers and access points. Procedures and information in the examples might be slightly different depending on the software or hardware version of the access controllers and access points.

The configuration examples 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.

The following information is provided based on the assumption that you have basic knowledge of AAA, portal, and WLAN.

Example: Configuring local portal MAC-trigger authentication

Network configuration

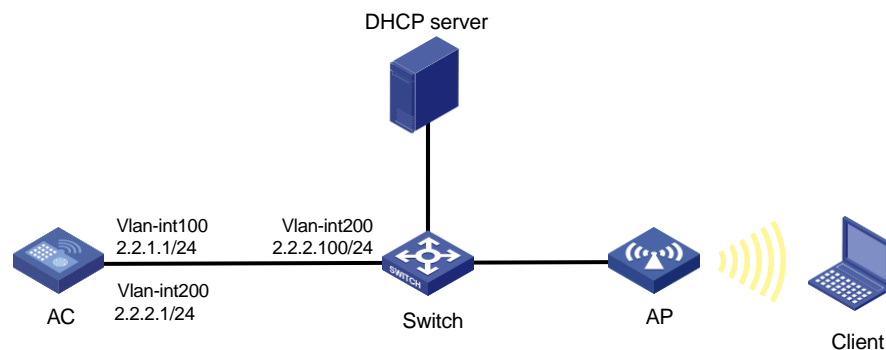
As shown in [Figure 1](#):

- The AP and the client obtain IP addresses from the DHCP server.
- The AC acts as the portal authentication server, portal Web server, and MAC binding server.

Configure the devices to meet the following requirements:

- The AC performs local portal MAC-trigger authentication on the wireless client. The client can access only the portal Web server before passing portal authentication and can access other network resources after passing portal authentication.
- The client can access the network resources through any Layer 2 ports in its access VLAN without re-authentication.

Figure 1 Network diagram



Analysis

For the client to access network resources through any Layer 2 ports in its access VLAN without re-authentication, enable portal roaming.

Restrictions and guidelines

Use the actual serial ID of an AP to uniquely identify that AP.

By default, the URL of the portal Web server to which the AC redirects portal users does not carry any parameters. You can add parameters to be carried in the URL as needed.

To avoid portal authentication failure caused by frequent logins and logouts in a short time, disable the Rule ARP entry feature.

Some types of endpoints use random MAC by default, which might cause failure of the MAC-trigger authentication. As a best practice, disable the random MAC feature on the endpoints.

Procedures

Configuring the AC

1. Configure interfaces on the AC:

Create VLAN 100 and VLAN-interface 100, and assign an IP address to the VLAN interface. The AC will use this IP address to establish CAPWAP data and control tunnels with the AP.

```
<AC> system-view
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 2.2.1.1 24
[AC-Vlan-interface100] quit
```

Create VLAN 200 and VLAN-interface 200, and assign an IP address to the VLAN interface. The AC will use VLAN 200 for client access.

```
[AC] vlan 200
[AC-vlan200] quit
[AC] interface vlan-interface 200
[AC-Vlan-interface200] ip address 2.2.2.1 24
[AC-Vlan-interface200] quit
```

Configure the interface that is connected to the switch as a trunk port, and assign the port to VLAN 100 and VLAN 200.

```
[AC] interface gigabitethernet 1/0/1
[AC-GigabitEthernet1/0/1] port link-type trunk
[AC-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[AC-GigabitEthernet1/0/1] quit
```

2. Configure an ISP domain:

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

```
[AC] domain dm1
```

Configure the AC to perform local authentication and not to perform authorization or accounting on portal users in the ISP domain.

```
[AC-isp-dm1] authentication portal local
```

```
[AC-isp-dm1] authorization portal none
```

```
[AC-isp-dm1] accounting portal none
```

Set the idle timeout period to 15 minutes and the minimum traffic that must be generated in the idle timeout period to 1024 bytes.

```
[AC-isp-dm1] authorization-attribute idle-cut 15 1024
```

```
[AC-isp-dm1] quit
```

3. Configure portal authentication:

Create a portal Web server named **newpt** and specify **http://2.2.2.1:8080/portal** as the URL of portal Web server **newpt**.

```
[AC] portal web-server newpt
```

```
[AC-portal-websvr-newpt] url http://2.2.2.1:8080/portal
```

Add the **wlanuserip** parameter to the URL of the portal Web server and specify the user IP address as the parameter value.

```
[AC-portal-websvr-newpt] url-parameter wlanuserip source-address
```

```
[AC-portal-websvr-newpt] quit
```

Configure two destination-based portal-free rules to permit the traffic destined for the DNS server.

```
[AC] portal free-rule 1 destination ip any udp 53
```

```
[AC] portal free-rule 2 destination ip any tcp 53
```

Create an HTTP-based local portal Web service.

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

Specify file **abc.zip** as the default authentication page file and 8080 as the service port number for the local portal Web service. (Make sure the file already exists under the root directory of the device storage media.)

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

```
[AC-portal-local-websvr-http] tcp-port 8080
```

```
[AC-portal-local-websvr-http] quit
```

Add a local network access user named **portaluser**, set the password of the user, and assign the portal service to the user.

```
[AC] local-user portaluser class network
```

```
[AC-luser-network-portaluser] password simple abc123
```

```
[AC-luser-network-portaluser] service-type portal
```

```
[AC-luser-network-portaluser] quit
```

Enable portal roaming.

```
[AC] portal roaming enable
```

Disable the Rule ARP entry feature for portal clients.

```
[AC] undo portal refresh arp enable
```

Enable validity check on wireless portal clients.

```
[AC] portal host-check enable
```

4. Configure portal MAC-trigger authentication:

Create a MAC binding server named **mts** and enter its view.

```
[AC] portal mac-trigger-server mts
```

Specify 2.2.2.1 as the IP address of MAC binding server **mts**.

```
[AC-portal-mac-trigger-server-mts] ip 2.2.2.1
```

Enable local portal MAC-trigger authentication, and set the aging time for local MAC-account binding entries to 60 minutes.

```
[AC-portal-mac-trigger-server-mts] local-binding enable
```

```
[AC-portal-mac-trigger-server-mts] local-binding aging-time 60
```



```

# Create a service template named st1.
[AC] wlan service-template st1
# Set the SSID of service template st1.
[AC-wlan-st-st1] ssid service
# Specify VLAN 200 for service template st1.
[AC-wlan-st-st1] vlan 200
# Enable direct portal authentication on service template st1.
[AC-wlan-st-st1] portal enable method direct
# Specify ISP domain dm1 as the authentication domain for portal users on service template st1.
[AC-wlan-st-st1] portal domain dml
# Specify portal Web server newpt on service template st1.
[AC-wlan-st-st1] portal apply web-server newpt
# Specify MAC binding server mts on service template st1.
[AC] wlan service-template st1
[AC-wlan-st-st1] portal apply mac-trigger-server mts
# Configure the AC to forward client data traffic. (Skip this step if the client data traffic forwarder is the AC by default.)
[AC-wlan-st-st1] client forwarding-location ac
# Specify the AKM mode as PSK, and configure the preshared key as 12345678 in plain text.
[AC-wlan-st-st1] akm mode psk
[AC-wlan-st-st1] preshared-key pass-phrase simple 12345678
# Specify the cipher suite as CCMP and the security IE as RSN.
[AC-wlan-st-st1] cipher-suite ccmp
[AC-wlan-st-st1] security-ie rsn
# Enable service template st1.
[AC-wlan-st-service1] service-template enable
[AC-wlan-st-st1] quit

```

5. Configure the AP:

NOTE:

In large-scale networks, configure AP groups instead of single APs as a best practice.

```

# Create an AP named ap1 with model AP 3620, and specify the serial ID of the AP.
[AC] wlan ap ap1 model AP 3620
[AC-wlan-ap-ap1] serial-id 219801A28N819CE0002T
# Create AP group group1 and add AP ap1 to AP group group1.
[AC] wlan ap-group group1
[AC-wlan-ap-group-group1] ap ap1
# Bind service template st1 to radio 2 in AP group group1.
[AC-wlan-ap-group-group1] ap-model AP 3620
[AC-wlan-ap-group-group1-ap-model-AP 3620] radio 2
[AC-wlan-ap-group-group1-ap-model-AP 3620-radio-2] service-template st1
# Enable radio 2.
[AC-wlan-ap-group-group1-ap-model-AP 3620-radio-2] radio
enable [AC-wlan-ap-group-group1-ap-model-AP 3620-radio-2]
return

```

Configuring the switch

Create VLAN 100. The switch will use this VLAN to forward traffic on the CAPWAP tunnel between the AC and the AP.

```
<Switch> system-view
[Switch] vlan 100
[Switch-vlan100] quit
```

Create VLAN 200. The switch will use this VLAN to forward client traffic.

```
[Switch] vlan 200
[Switch-vlan200] quit
```

Configure GigabitEthernet 1/0/1 (the port connected to the AC) as a trunk port and assign the port to VLAN 100 and VLAN 200.

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[Switch-GigabitEthernet1/0/1] quit
```

Configure GigabitEthernet 1/0/2 (the port connected to the AP) as an access port and assign it to VLAN 100.

```
[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] port link-type access
[Switch-GigabitEthernet1/0/2] port access vlan 100
```

Enable PoE on GigabitEthernet 1/0/2.

```
[Switch-GigabitEthernet1/0/2] poe enable
[Switch-GigabitEthernet1/0/2] quit
```

Assign an IP address to VLAN-interface 200.

```
[Switch] interface vlan-interface 200
[Switch-Vlan-interface200] ip address 2.2.2.100 255.255.255.0
[Switch-Vlan-interface200] quit
```

Verifying the configuration

Display information about MAC binding server mts.

```
[AC] display portal mac-trigger-server name mts
Portal mac trigger server name: mts
  Version           : 1.0
  Server type       : INC
  IP                 : 2.2.2.1
  Port              : 50100
  VPN instance      : Not configured
  Aging time        : 300 seconds
  Free-traffic threshold : 0 bytes
  NAS-Port-Type     : Not configured
  Binding retry times   : 3
  Binding retry interval : 1 seconds
  Authentication timeout : 3 minutes
  Local-binding       : Enabled
  Local-binding aging-time : 60 minutes
```

```

aaa-fail nobinding      : Disabled
Excluded attribute list : Not configured
Cloud-binding           : Disabled
Cloud-server URL        : Not configured

```

Use the configured user account to perform portal authentication through a Web browser. Before passing portal authentication, the user can access only the authentication page **http://2.2.2.1:8080/portal**. All Web requests from the user will be redirected to the authentication page. After passing portal authentication, the user can access other network resources. (Details not shown.)

Display information about all portal users.

```

[AC] display portal user all
Total portal users: 1
Username: portaluser
  Portal server: newpt
  State: Online
  VPN instance: N/A
  MAC           IP           VLAN   Interface
  0021-6330-0933 2.2.2.2   200    WLAN-BSS1/0/16
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

```

The output shows that the user has passed portal authentication.

Log out the user and then get the user to come online again to verify that the user can directly access network resources without entering the username and password.

Configuration files

- AC:


```

#
vlan 100
#
vlan 200
#
wlan service-template st1
  ssid service
  client forwarding-location ac
  akm mode psk
  preshared-key pass-phrase simple 12345678
  cipher-suite ccmp
  security-ie rsn
vlan 200
portal enable method direct
portal domain dm1
portal apply web-server newpt

```

```

portal apply mac-trigger-server mts
service-template enable
#
interface Vlan-interface100
ip address 2.2.1.1 255.255.255.0
#
interface Vlan-interface200
ip address 2.2.2.1 255.255.255.0
#
interface GigabitEthernet1/0/1
port link-mode bridge
port link-type trunk
port trunk permit vlan 1 100 200
#
domain dml
authorization-attribute idle-cut 15 1024
authentication portal local
authorization portal none
accounting portal none
#
portal host-check enable
portal free-rule 1 destination ip any udp 53
portal free-rule 2 destination ip any tcp 53
#
portal roaming enable
undo portal refresh arp enable
#
portal web-server newpt
url http://2.2.2.1:8080/portal
url-parameter wlanuserip source-address
#
portal local-web-server http
default-logon-page abc.zip
tcp-port 8080
#
local-user portaluser class network
password simple abc123
service-type portal
#
portal mac-trigger-server mts
ip 2.2.2.1
server-type iNC
#
wlan ap ap1 model AP 3620
serial-id 219801A28N819CE0002T
#
wlan ap-group group1
ap ap1

```

- ```
ap-model AP 3620
radio 1
radio 2
 radio enable
 service-template st1
#
```
- **Switch:**

```
#
vlan 100
#
vlan 200
#
interface Vlan-interface200
 ip address 2.2.2.100 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 1 100 200
#
interface GigabitEthernet1/0/2
 port link-type access
 port access vlan 100
 poe enable
```

## Related documentation

- *User Access and Authentication Command Reference in INTELBRAS Access Controllers Command References*
- *User Access and Authentication Configuration Guide in INTELBRAS Access Controllers Configuration Guides*
- *WLAN Access Command Reference in INTELBRAS Access Controllers Command References*
- *WLAN Access Configuration Guide in INTELBRAS Access Controllers Configuration Guides*

# INTELBRAS Access Controllers

## Portal MAC-Trigger Authentication

### Configuration Examples

---

Copyright © 2024 Intelbras S.A All rights reserved.

No part of this manual may be reproduced or transmitted in any form or by any means without prior written consent of Intelbras S.A

Except for the trademarks of Intelbras S.A, any trademarks that may be mentioned in this document are the property of their respective owners.

The information in this document is subject to change without notice.

# Contents

|                                                              |    |
|--------------------------------------------------------------|----|
| Introduction .....                                           | 1  |
| Prerequisites .....                                          | 1  |
| Example: Configuring portal MAC-trigger authentication ..... | 1  |
| Network configuration .....                                  | 1  |
| Analysis .....                                               | 2  |
| Restrictions and guidelines .....                            | 2  |
| Procedures .....                                             | 3  |
| Configuring INC .....                                        | 3  |
| Editing a configuration file for the AP .....                | 9  |
| Configuring the AC .....                                     | 9  |
| Configuring the switch .....                                 | 12 |
| Verifying the configuration .....                            | 13 |
| Configuration files .....                                    | 14 |
| Related documentation .....                                  | 16 |

# Introduction

The following information provides an example of configuring MAC-trigger authentication (MAC-based quick portal authentication).

## Prerequisites

The following information applies to Comware-based access controllers and access points. Procedures and information in the examples might be slightly different depending on the software or hardware version of the access controllers and access points.

The configuration examples 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.

The following information is provided based on the assumption that you have basic knowledge of AAA, portal, and WLAN.

## Example: Configuring portal MAC-trigger authentication

### Network configuration

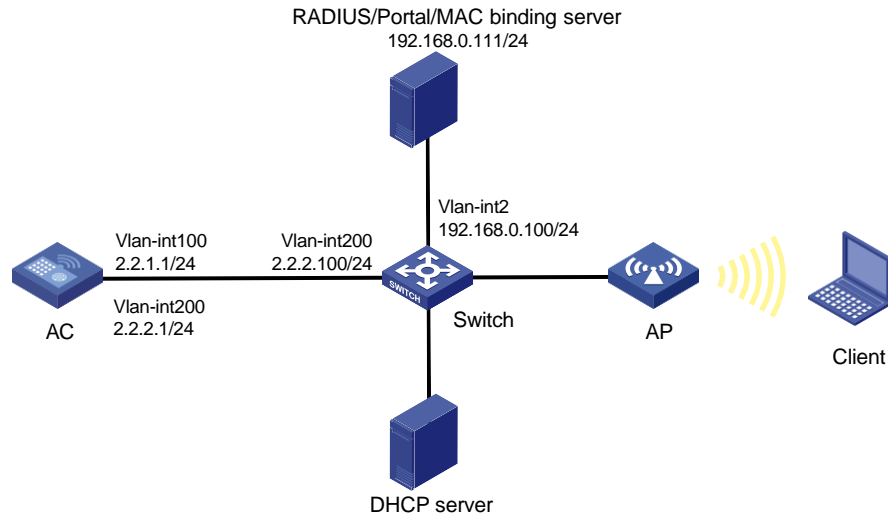
As shown in [Figure 1](#), the AP and the client obtain IP addresses from the DHCP server. The INC server acts as a portal authentication server, a portal Web server, a MAC binding server, and a RADIUS server.

Configure direct portal authentication and MAC-trigger authentication to meet the following requirements:

- The client can access only the portal Web server before passing portal authentication and can access other network resources after passing portal authentication.
- The client can access the network resources through any Layer 2 ports in its access VLAN without re-authentication.
- The RADIUS server can dynamically change the user authorization information or forcibly disconnect users.



**Figure 1 Network diagram**



## Analysis

For the client to access network resources through any Layer 2 ports in its access VLAN without re-authentication, enable portal roaming.

For the RADIUS server to dynamically change the user authorization information or forcibly disconnect users, enable the RADIUS session-control feature.

To use GigabitEthernet 1/0/1 on the AP to forward client traffic, edit a .txt configuration file and upload the file to the AC.

To ensure that dynamic user authorization information can be correctly assigned to users after they come online, enable the RADIUS DAS feature.

## Restrictions and guidelines

Use the serial ID labeled on the AP's rear panel to specify an AP.

Make sure the types of the portal authentication server, portal Web server, and MAC binding server specified on the AC are the same as those actually used. (This example uses CMCC servers.)

By default, the URL of the portal Web server to which the AC redirects portal users does not carry any parameters. You can add parameters to be carried in the URL as needed.

If portal authentication is enabled on a VLAN interface, the AC can forward client traffic. If portal authentication is enabled on a service template, both the AC and the AP can forward client traffic. (In this example, portal authentication is enabled on a service template.)

In wireless networks where the AP forwards client traffic, the AC does not have ARP entries for clients. Therefore, the AC cannot check the validity of portal clients by using ARP entries. To ensure that valid users can perform portal authentication, enable wireless client validity check on the AC.

To avoid possible authentication failure caused by frequent logins and logouts of portal clients in a short time, disable the Rule ARP entry feature.

Some types of endpoints use random MAC by default, which might cause failure of the MAC-trigger authentication. As a best practice, disable the random MAC feature on the endpoints.

# Procedures

## Configuring INC

This example uses the INC server to describe the RADIUS server and portal server configuration. The INC server runs INC PLAT 7.1 (E0303p13), INC INC - EIA 7.1 (F0302p08), and INC EIP 7.1 (F0302p08).

### Configuring the RADIUS server

Add the AC to INC as an access device:

1. Log in to INC and click the **User** tab.
2. From the navigation tree, select **User Access Policy > Access Device Management > Access Device**.
3. Click **Add** to open the page as shown in [Figure 2](#).
4. In the **Access Configuration** area, configure the parameters as follows:
  - Set the shared key to **radius**, which must be the same as that on the AC.
  - Use the default values for other parameters.
5. In the **Device List** area, click **Add Manually** to open the **Add Access Device Manually** page. Enter **2.2.2.1** in the **Start IP** field and then click **OK**.
6. Click **OK**.

**Figure 2 Adding the AC as an access device**

Access Configuration

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

Device List

Select Add Manually Clear All

| Device Name | Device IP | Device Model | Comments | Delete |
|-------------|-----------|--------------|----------|--------|
|             | 2.2.2.1   |              |          |        |

Total Items: 1.

OK Cancel

### Configuring the portal server

1. Configure the portal authentication service:
  - a. Click the **User** tab.
  - b. From the navigation tree, select **User Access Policy > Portal Service > Server** to open the portal server configuration page, as shown in [Figure 3](#).
  - c. Configure the portal server parameters as needed.  
This example uses the default values.
  - d. Click **OK**.

**Figure 3 Portal authentication server configuration**

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 LB Device Address

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://192.168.0.111:8080/portal/

192.168.0.111

2. Configure an IP address group:
  - a. From the navigation tree, select **User Access Policy > Portal Service > IP Group**.
  - b. Click **Add** to open the page as shown in [Figure 4](#).
  - c. Enter the IP group name.
  - d. Enter the start IP address and end IP address of the IP group.  
Make sure the client IP address is in the IP group.
  - e. Select a service group.  
This example uses the default value **Ungrouped**.
  - f. From the **Action** list, select **Normal**.
  - g. Click **OK**.

**Figure 4 Adding an IP address group**

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

OK Cancel

3. Add a portal device:
  - a. From the navigation tree, select **User Access Policy > Portal Service > Device**.
  - b. Click **Add** to open the page as shown in [Figure 5](#).

- c. Enter the device name.
- d. Select **CMCC 1.0** for **Version**.
- e. Enter the IP address of the AC's interface connected to the client.
- f. 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**.
- g. Enter the key, which must be the same as that configured on the AC.
- h. Select **Directly Connected** from the **Access Method** list.
- i. Use the default settings for other parameters.
- j. Click **OK**.

**Figure 5 Adding a portal device**

4. Associate the portal device with the IP address group:
  - a. As shown in Figure 6, click the **Port Group** icon  in the **Operation** field for device **NAS** to open the port group configuration page.

**Figure 6 Device list**

- b. Click **Add** to open the page as shown in Figure 7.
- 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. Select **Supported** for **Transparent Authentication**.
- f. Use the default settings for other parameters.
- g. Click **OK**.

**Figure 7 Adding a port group**

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

### Add Port Group

|                               |           |                                    |             |
|-------------------------------|-----------|------------------------------------|-------------|
| Port Group Name *             | group     | Language *                         | English     |
| 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(Minutes) * | 10        | Heartbeat Timeout(Minutes) *       | 30          |
| User Domain                   |           | Port Group Description             |             |
| Transparent Authentication    | Supported | Client Protection Against Cracks * | No          |
| Page Push Policy              |           | Default Authentication Page        |             |

OK Cancel

5. From the navigation tree, select **User Access Policy > Service Parameters > Validate System Configuration** to validate the configuration.

## Configuring the MAC binding server

1. Add an access policy:
  - a. From the navigation tree, select **User Access Policy > Access Policy**.
  - b. Click **Add** to open the page as shown in [Figure 8](#).
  - c. Enter the access policy name.
  - d. Select a service group.
 

This example uses the default value **Ungrouped**.
  - e. Use the default settings for other parameters.
  - f. Click **OK**.

**Figure 8 Adding an access policy**

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

---

**Basic Information**

Access Policy Name \*

Service Group \*

Description

---

**Authorization Information**

Access Period

Allocate IP \*

Downstream Rate(Kbps)

Upstream Rate(Kbps)

Priority

☐ RSA Authentication

Certificate Authentication ☒ None ☐ EAP

Certificate Type

Deploy VLAN

☐ Deploy User Profile

Deploy User Group

☐ Deploy ACL

2. Add an access service:
  - a. From the navigation tree, select **User Access Policy > Access Service**.
  - b. Click **Add** to open the page as shown in [Figure 9](#).
  - c. Enter the service name.
  - d. Select the **Transparent Authentication on Portal Endpoints** option.
  - e. Use the default settings for other parameters.
  - f. Click **OK**.

**Figure 9 Adding an access service**

User > User Access Policy > Access Service > Modify Access Service ? Help

---

**Basic Information**

Service Name \*

Service Suffix

Service Group \*

Default Access Policy \*

Default Proprietary Attribute Assignment Policy \*

Default Max. Number of Bound Endpoints \*

Default Max. Number of Online Endpoints \*

Description

☒ Available ☒ Transparent Authentication on Portal Endpoints

3. Add an access user:
  - a. From the navigation tree, select **Access User > All Access Users**.
  - b. Click **Add** to open the page as shown in [Figure 10](#).
  - c. Select an existing access user or click **Add User** to add a new access user.
  - d. Enter the account name.
  - e. Set the password.
  - f. In the **Access Service** area, select the access policy configured in a previous step.
  - g. Use the default settings for other parameters.
  - h. Click **OK**.

**Figure 10 Adding an access user**

User > All Access Users > Add Access User

Access Information

User Name \* client1 Select Add User

Account Name \* client ?

☐ Trial Account ☐ Default BYOD User ☐ MAC Authentication User ☐ Computer User ☐ Fast Access User

Password \* \*\*\*\*\* Confirm Password \* \*\*\*\*\*

☒ Allow User to Change Password ☐ Enable Password Strategy ☐ Modify Password at Next Login

Start Time [ ] End Time [ ]

Max. Idle Time (Minutes) [ ] Max. Concurrent Logins 1

Login Message [ ]

Access Service

| Service Name                                   | Service Suffix | Status    | Allocate IP |
|------------------------------------------------|----------------|-----------|-------------|
| <input type="checkbox"/> 802-IX-CAC1           |                | Available |             |
| <input type="checkbox"/> dot1x                 |                | Available |             |
| <input checked="" type="checkbox"/> MAC_server |                | Available |             |
| <input type="checkbox"/> office_mac            |                | Available |             |

Binding Information

OK OK & Print Cancel

4. Configure system parameters:
  - a. From the navigation tree, select **User Access Policy > Service Parameters > System Settings**.
  - b. Click the **Configure** icon for **User Endpoint Settings** to open the page as shown in [Figure 11](#).
  - c. Select whether to enable transparent portal authentication on non-smart devices.  
In this example, select **Enable** for **Non-Terminal Authentication**.
  - d. Click **OK**.

**Figure 11 Configuring user endpoint settings**

User > User Access Policy > Service Parameters > System Settings > User Endpoint Settings

User Endpoint Settings

Transparent MAC Authentication Disable Max. Device for Single Account \* 10

Non-Terminal Authentication Enable ? Log off User with Endpoint Conflict No

OK Cancel

- e. Click the **Configure** icon for **Endpoint Aging Time** to open the page as shown in [Figure 12](#).
  - f. Set the endpoint aging time as needed.  
This example uses the default value.
  - g. Click **OK**.

**Figure 12 Setting the endpoint aging time**

User > User Access Policy > Service Parameters > System Settings > Endpoint Aging Time > Modify Endpoint Aging Time

Modify Endpoint Aging Time

Endpoint Aging Time(Days) \* 7 ?

OK Cancel

5. From the navigation tree, select **User Access Policy > Service Parameters**. Then, click **Validate** to make the configuration take effect.

## Editing a configuration file for the AP

# Create a .txt configuration file named **map.txt**.

# Enter the following content in the file.

```
System-view
vlan 200
interface gigabitethernet1/0/1
port link-type trunk
port trunk permit vlan 200
```

# Upload the file to the AC.

## Configuring the AC

1. Configure interfaces on the AC:

# Create VLAN 100 and VLAN-interface 100, and assign an IP address to the VLAN interface. The AC will use this IP address to establish a CAPWAP tunnel with the AP.

```
<AC> system-view
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 2.2.1.1 24
[AC-Vlan-interface100] quit
```

# Create VLAN 200 and VLAN-interface 200, and assign an IP address to the VLAN interface. The AC will use VLAN 200 for client access.

```
[AC] vlan 200
[AC-vlan200] quit
[AC] interface vlan-interface 200
[AC-Vlan-interface200] ip address 2.2.2.1 24
[AC-Vlan-interface200] quit
```

# Configure the interface that is connected to the switch as a trunk port, and assign the port to VLAN 100 and VLAN 200.

```
[AC] interface gigabitethernet 1/0/1
[AC-GigabitEthernet1/0/1] port link-type trunk
[AC-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[AC-GigabitEthernet1/0/1] quit
```

2. Configure a static route to the INC server:

```
[AC] ip route-static 192.168.0.0 255.255.0.0 2.2.2.100
```

3. Configure a WLAN service:

# Create a service template named **st1** and enter its view.

```
[AC] wlan service-template st1
```

# Set the SSID of service template **st1** to **service**.

```
[AC-wlan-st-st1] ssid service
```

# Assign clients coming online through service template **st1** to VLAN 200.

```
[AC-wlan-st-st1] vlan 200
```

# Configure the AP to forward client data traffic from all VLANs.



```
[AC-wlan-st-st1] client forwarding-location ap
[AC-wlan-st-st1] quit

Specify the AKM mode as PSK, and configure the preshared key as 12345678 in plain text.
[AC-wlan-st-st1] akm mode psk
[AC-wlan-st-st1] preshared-key pass-phrase simple 12345678

Specify the cipher suite as CCMP and the security IE as RSN.
[AC-wlan-st-st1] cipher-suite ccmp
[AC-wlan-st-st1] security-ie rsn
[AC-wlan-st-st1] quit
```

#### 4. Configure the AP:

---

##### NOTE:

In large-scale networks, configure AP groups instead of single APs as a best practice.

---

**# Create an AP named `ap1` with model `AP 3620` and set its serial ID to `219801A28N819CE0002T`.**

```
[AC] wlan ap ap1 model AP 3620
[AC-wlan-ap-ap1] serial-id 219801A28N819CE0002T
```

**# Create AP group `group1` and add AP `ap1` to AP group `group1`.**

```
[AC] wlan ap-group group1
[AC-wlan-ap-group-group1] ap ap1
```

**# Enter the view of AP model `AP 3620` and deploy configuration file `map.txt` to the AP.**

```
[AC-wlan-ap-group-group1] ap-model AP 3620
[AC-wlan-ap-group-group1-ap-model-AP 3620] map-configuration map.txt
```

**# Bind service template `st1` to radio 2 in AP group `group1`.**

```
[AC-wlan-ap-group-group1-ap-model-AP 3620] radio 2
[AC-wlan-ap-group-group1-ap-model-AP 3620-radio-2] service-template st1
```

**# Enable radio 2.**

```
[AC-wlan-ap-group-group1-ap-model-AP 3620-radio-2] radio
enable [AC-wlan-ap-group-group1-ap-model-AP 3620-radio-2]
return
```

#### 5. Configure a RADIUS scheme:

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

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

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

```
[AC-radius-rs1] primary authentication 192.168.0.111
[AC-radius-rs1] primary accounting 192.168.0.111
[AC-radius-rs1] key authentication simple radius
[AC-radius-rs1] key accounting simple radius
```

**# Configure the AC to remove the domain name from the usernames sent to the RADIUS servers.**

```
[AC-radius-rs1] user-name-format without-domain
[AC-radius-rs1] nas-ip 2.2.2.1
[AC-radius-rs1] quit
```

**# Enable RADIUS session-control.**

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

**# Enable the RADIUS DAS feature and enter RADIUS DAS view.**

```
[AC] radius dynamic-author server
```

# Specify a session-control client with IP address 192.168.0.111 and shared key **radius** in plaintext form.

```
[AC-radius-da-server] client ip 192.168.0.111 key simple radius
```

```
[AC-radius-da-server] quit
```

## 6. Configure an authentication domain:

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

```
[AC] domain dm1
```

# Configure the authentication and authorization methods as RADIUS and the accounting method as none in the ISP domain.

```
[AC-isp-dm1] authentication portal radius-scheme rs1
```

```
[AC-isp-dm1] authorization portal radius-scheme rs1
```

```
[AC-isp-dm1] accounting portal radius-scheme rs1
```

# Set the idle timeout period to 15 minutes and the minimum traffic that must be generated in the idle timeout period to 1024 bytes.

```
[AC-isp-dm1] authorization-attribute idle-cut 15 1024
```

```
[AC-isp-dm1] quit
```

## 7. Configure portal authentication:

# Create a portal authentication server named **newpt**, specify IP address 192.168.0.111 for the authentication server, and specify 50100 as the port number for listening portal packets.

```
[AC] portal server newpt
```

```
[AC-portal-server-newpt] ip 192.168.0.111 key simple 123456
```

```
[AC-portal-server-newpt] port 50100
```

# Specify CMCC as the type of portal authentication server **newpt**.

```
[AC-portal-server-newpt] server-type cmcc
```

```
[AC-portal-server-newpt] quit
```

# Specify **http://192.168.0.111:8080/portal** as the URL of portal Web server **newpt**.

```
[AC] portal web-server newpt
```

```
[AC-portal-websvr-newpt] url http://192.168.0.111:8080/portal
```

# Add parameters **ssid**, **wlanuserip**, and **wlanacname** to the URL of portal Web server **newpt**, and specify the AP SSID, user IP address, and AC name as the values of the parameters. (These parameters are required to be carried in the URL of a CMCC-type portal Web server).

```
[AC-portal-websvr-newpt] url-parameter ssid ssid
```

```
[AC-portal-websvr-newpt] url-parameter wlanuserip source-address
```

```
[AC-portal-websvr-newpt] url-parameter wlanacname value AC
```

# Specify CMCC as the type of portal Web server **newpt**.

```
[AC-portal-websvr-newpt] server-type cmcc
```

```
[AC-portal-websvr-newpt] quit
```

# Configure portal-free rule 0 to allow portal users to access the portal Web server (whose IP address is 192.168.0.111) without authentication. Configure port-free rule 1 to permit the traffic sourced from the aggregate interface.

```
[AC] portal free-rule 0 destination ip 192.168.0.111 24
```

```
[AC] portal free-rule 1 source interface Bridge-Aggregation 1
```

# Configure two destination-based portal-free rules to permit the traffic destined for the DNS server.

```
[AC] portal free-rule 2 destination ip any udp 53
```

```
[AC] portal free-rule 3 destination ip any tcp 53
```

# Enable portal roaming.

```
[AC] portal roaming enable
```

```

Disable the Rule ARP entry feature for portal clients.
[AC] undo portal refresh arp enable

Enable validity check on wireless portal clients.
[AC] portal host-check enable

Enable direct portal authentication on service template st1.
[AC] wlan service-template st1
[AC-wlan-st-st1] portal enable method direct

Specify ISP domain dm1 as the portal authentication domain.
[AC-wlan-st-st1] portal domain dm1

Specify portal Web server newpt on service template st1 for portal authentication.
[AC-wlan-st-st1] portal apply web-server newpt
[AC-wlan-st-st1] quit

8. Configure portal MAC-trigger authentication:

Create a MAC binding server named mts and enter its view.
[AC] portal mac-trigger-server mts

Specify 192.168.0.111 as the IP address of MAC binding server mts.
[AC-portal-mac-trigger-server-mts] ip 192.168.0.111

Specify CMCC as the type of MAC binding server mts.
[AC-portal-mac-trigger-server-mts] server-type cmcc
[AC-portal-mac-trigger-server-mts] quit

Specify MAC binding server mts on service template st1.
[AC] wlan service-template st1
[AC-wlan-st-st1] portal apply mac-trigger-server mts
[AC-wlan-st-st1] portal bas-ip 2.2.2.1

Enable service template st1.
[AC-wlan-st-service1] service-template enable
[AC-wlan-st-st1] quit

```

## Configuring the switch

```

Create VLAN 100. The switch will use this VLAN to forward traffic on the CAPWAP tunnel between
the AC and the AP.
<Switch> system-view
[Switch] vlan 100
[Switch-vlan100] quit

Create VLAN 200. The switch will use this VLAN to forward client traffic.
[Switch] vlan 200
[Switch-vlan200] quit

Create VLAN 2. This VLAN will be used for communication with the INC server.
[Switch] vlan 2
[Switch-vlan2] quit

Add the port connected to the INC server to VLAN 2. (Details not shown.)

Configure the interface that is connected to the AC as a trunk port and assign the port to VLAN 100
and VLAN 200.
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100 200

```

```
[Switch-GigabitEthernet1/0/1] quit
```

**# Configure the interface that is connected to the AP as a trunk port, and assign the port to VLAN 100 and VLAN 200.**

```
[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] port link-type trunk
[Switch-GigabitEthernet1/0/2] port trunk permit vlan 100 200
[Switch-GigabitEthernet1/0/2] port trunk pvid vlan 100
```

**# Enable PoE.**

```
[Switch-GigabitEthernet1/0/2] poe enable
[Switch-GigabitEthernet1/0/2] quit
```

**# Assign an IP address to VLAN-interface 200.**

```
[Switch] interface vlan-interface 200
[Switch-Vlan-interface200] ip address 2.2.2.100 255.255.255.0
[Switch-Vlan-interface200] quit
```

**# Assign an IP address to VLAN-interface 2.**

```
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] ip address 192.168.0.100 255.255.255.0
[Switch-Vlan-interface2] quit
```

## Verifying the configuration

**# Display information about MAC binding server mts.**

```
[AC] display portal mac-trigger-server name mts
Portal mac trigger server name: mts
 Version : 1.0
 Server type : CMCC
 IP : 192.168.0.111
 Port : 50100
 VPN instance : Not configured
 Aging time : 300 seconds
 Free-traffic threshold : 0 bytes
 NAS-Port-Type : Not configured
 Binding retry times : 3
 Binding retry interval : 1 seconds
 Authentication timeout : 3 minutes
```

A user can perform portal authentication through a Web browser. Before passing portal authentication, the user can access only the authentication page **<http://192.168.0.111:8080/portal>**. All Web requests from the user will be redirected to the authentication page. After passing portal authentication, the user can access other network resources.

For the first portal authentication, the user is required to enter the username and password. When the user goes offline and then accesses the network again, the user does not need to enter the authentication username and password.

**# Display information about all portal users.**

```
[AC] display portal user all
Total portal users: 1
Username: portal
 Portal server: newpt
```

```

State: Online
VPN instance: N/A
MAC IP VLAN Interface
0021-6330-0933 2.2.2.2 200 WLAN-BSS1/0/1
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

- AC:
 

```

#
vlan 100
#
vlan 200
#
wlan service-template st1
 ssid service
 akm mode psk
 preshared-key pass-phrase simple 12345678
 cipher-suite ccmp
 security-ie rsn
 vlan 200
client forwarding-location ap
 portal enable method direct
portal domain ldap
portal bas-ip 2.2.2.1
portal apply web-server newpt
 portal apply mac-trigger-server mts
 service-template enable
#
interface Vlan-interface100
 ip address 2.2.1.1 255.255.255.0
#
interface Vlan-interface200
 ip address 2.2.2.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 100 200
#
ip route-static 192.168.0.0 16 2.2.2.100
#

```

```

radius session-control enable
#
radius scheme rs1
primary authentication 192.168.0.111
primary accounting 192.168.0.111
key authentication cipher c3$Sqqqz7lDs4XPnethmAgyAKVlke7qwEkYbQ==
key accounting cipher c3$4J/JBRGwqB4F213furJmKB6JWYXBFjWE6g==
user-name-format without-domain
nas-ip 2.2.2.1
#
radius dynamic-author server
client ip 192.168.0.111 key cipher c3$AkTEB7OgMYnCqsfDeplhoAgXUek/rVrLZw==
#
domain dml
authorization-attribute idle-cut 15 1024
authentication portal radius-scheme rs1
authorization portal radius-scheme rs1
accounting portal radius-scheme rs1
#
portal host-check enable
portal free-rule 0 destination ip 192.168.0.0 255.255.255.0
portal free-rule 1 source interface Bridge-Aggregation 1
portal free-rule 2 destination ip any udp 53
portal free-rule 3 destination ip any tcp 53
#
portal roaming enable
undo portal refresh arp enable
#
portal web-server newpt
url http://192.168.0.111:8080/portal
server-type cmcc
url-parameter ssid ssid
url-parameter wlanacname value AC
url-parameter wlanuserip source-address
#
portal server newpt
ip 192.168.0.111 key cipher c3$AkTEB7OgMYnCqsfDeplhoAgXUek/rVrLZw==
server-type cmcc
#
portal mac-trigger-server mts
ip 192.168.0.111
server-type cmcc
#
wlan ap ap1 model AP 3620
serial-id 219801A28N819CE0002T
#
wlan ap-group group1
ap ap1

```

```

ap-model AP 3620
map-configuration flash:/map.txt
radio 1
radio 2
 radio enable
 service-template st1
#

```

- **Switch:**

```

#
vlan 2
#
vlan 100
#
vlan 200
#
interface Vlan-interface2
 ip address 192.168.0.100 255.255.255.0
#
interface Vlan-interface200
 ip address 2.2.2.100 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 1 100 200
#
interface GigabitEthernet1/0/2
 port link-type trunk
 port trunk vlan 100 200
 port trunk pvid vlan 100
 poe enable

```

## Related documentation

- *User Access and Authentication Command Reference in INTELBRAS Access Controllers Command References*
- *User Access and Authentication Configuration Guide in INTELBRAS Access Controllers Configuration Guides*
- *WLAN Access Command Reference in INTELBRAS Access Controllers Command References*
- *WLAN Access Configuration Guide in INTELBRAS Access Controllers Configuration Guides*

# INTELBRAS Access Controllers

## Local Forwarding Mode and Local Portal

## MAC-Trigger Authentication

## Configuration Examples

---

Copyright © 2024 Intelbras S.A All rights reserved.

No part of this manual may be reproduced or transmitted in any form or by any means without prior written consent of Intelbras S.A

Except for the trademarks of Intelbras S.A, any trademarks that may be mentioned in this document are the property of their respective owners.

The information in this document is subject to change without notice.



# Contents

|                                                                                              |   |
|----------------------------------------------------------------------------------------------|---|
| Introduction .....                                                                           | 1 |
| Prerequisites .....                                                                          | 1 |
| Example: Configuring local forwarding mode and local portal MAC-trigger authentication ..... | 1 |
| Network configuration .....                                                                  | 1 |
| Analysis .....                                                                               | 2 |
| Restrictions and guidelines .....                                                            | 2 |
| Procedures .....                                                                             | 2 |
| Editing the AP configuration file .....                                                      | 2 |
| Configuring the AC .....                                                                     | 2 |
| Configuring the switch .....                                                                 | 5 |
| Verifying the configuration .....                                                            | 6 |
| Configuration files .....                                                                    | 7 |
| Related documentation .....                                                                  | 9 |

# Introduction

The following information provides an example of configuring local portal MAC-trigger authentication for clients on a wireless network where APs forward client traffic locally.

## Prerequisites

The following information applies to Comware-based access controllers and access points. Procedures and information in the examples might be slightly different depending on the software or hardware version of the access controllers and access points.

The configuration examples 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.

The following information is provided based on the assumption that you have basic knowledge of AAA, portal, and WLAN.

## Example: Configuring local forwarding mode and local portal MAC-trigger authentication

### Network configuration

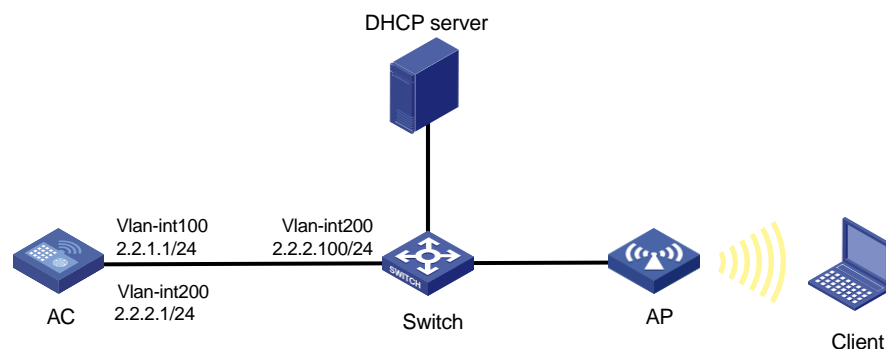
As shown in [Figure 1](#):

- The AP and the client obtain IP addresses from the DHCP server.
- The AC acts as the portal authentication server, portal Web server, and MAC binding server.

Configure the devices to meet the following requirements:

- The AC performs local portal MAC-trigger authentication on the wireless client. The client can access only the portal Web server before passing portal authentication and can access other network resources after passing portal authentication.
- The AP forwards the client traffic locally.
- The client can access the network resources through any Layer 2 ports in its access VLAN without re-authentication.

**Figure 1 Network diagram**



# Analysis

For the client to access network resources through any Layer 2 ports in its access VLAN without re-authentication, enable portal roaming.

To use GigabitEthernet 1/0/1 on the AP to forward client traffic, edit a .txt configuration file and upload the file to the AC.

## Restrictions and guidelines

Use the actual serial ID of an AP to uniquely identify that AP.

By default, the URL of the portal Web server to which the AC redirects portal users does not carry any parameters. You can add parameters to be carried in the URL as needed.

To avoid portal authentication failure caused by frequent logins and logouts in a short time, disable the Rule ARP entry feature.

Some types of endpoints use random MAC by default, which might cause failure of the MAC-trigger authentication. As a best practice, disable the random MAC feature on the endpoints.

## Procedures

### Editing the AP configuration file

# Use a text editor to edit the AP's configuration file. Name the configuration file **map.txt**, and then upload the file to the storage medium of the AC.

The content of the configuration file is as follows:

```
System-view
vlan 200
interface gigabitethernet1/0/1
port link-type trunk
port trunk permit vlan 200
```

### Configuring the AC

#### 1. Configure interfaces on the AC:

# Create VLAN 100 and VLAN-interface 100, and assign an IP address to the VLAN interface. The AC will use this IP address to establish CAPWAP data and control tunnels with the AP.

```
<AC> system-view
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 2.2.1.1 24
[AC-Vlan-interface100] quit
```

# Create VLAN 200 and VLAN-interface 200, and assign an IP address to the VLAN interface. The AC will use VLAN 200 for client access.

```
[AC] vlan 200
[AC-vlan200] quit
[AC] interface vlan-interface 200
[AC-Vlan-interface200] ip address 2.2.2.1 24
```

```
[AC-Vlan-interface200] quit
```

# Configure the interface that is connected to the switch as a trunk port, and assign the port to VLAN 100 and VLAN 200.

```
[AC] interface gigabitethernet 1/0/1
```

```
[AC-GigabitEthernet1/0/1] port link-type trunk
```

```
[AC-GigabitEthernet1/0/1] port trunk permit vlan 100 200
```

```
[AC-GigabitEthernet1/0/1] quit
```

## 2. Configure a wireless service:

# Create a service template named **st1** and enter its view.

```
[AC] wlan service-template st1
```

# Set the SSID of service template **st1** to **service**.

```
[AC-wlan-st-st1] ssid service
```

# Assign clients coming online through service template **st1** to VLAN 200.

```
[AC-wlan-st-st1] vlan 200
```

# Specify the AKM mode as PSK, and configure the preshared key as 12345678 in plain text.

```
[AC-wlan-st-st1] akm mode psk
```

```
[AC-wlan-st-st1] preshared-key pass-phrase simple 12345678
```

# Specify the cipher suite as CCMP and the security IE as RSN.

```
[AC-wlan-st-st1] cipher-suite ccmp
```

```
[AC-wlan-st-st1] security-ie rsn
```

# Configure the AP to forward client data traffic from all VLANs. (Skip this configuration if the default client data traffic forwarder is the AP.)

```
[AC-wlan-st-st1] client forwarding-location ap
```

```
[AC-wlan-st-st1] quit
```

## 3. Configure the AP:

---

### NOTE:

In large-scale networks, configure AP groups instead of single APs as a best practice.

---

# Create an AP named **office** with model **AP 3620** and specify its serial ID of the AP.

```
[AC] wlan ap office model AP 3620
```

```
[AC-wlan-ap-office] serial-id 219801A28N819CE0002T
```

```
[AC-wlan-ap-office] quit
```

# Create AP group **group1** and add AP **office** to AP group **group1**.

```
[AC] wlan ap-group group1
```

```
[AC-wlan-ap-group-group1] ap office
```

# Enter the view of AP model **AP 3620** and deploy configuration file **map.txt** to the AP.

```
[AC-wlan-ap-group-group1] ap-model AP 3620
```

```
[AC-wlan-ap-group-group1-ap-model-AP 3620] map-configuration map.txt
```

# Bind service template **st1** to radio 2 in AP group **group1**.

```
[AC-wlan-ap-group-group1-ap-model-AP 3620] radio 2
```

```
[AC-wlan-ap-group-group1-ap-model-AP 3620-radio-2] service-template st1
```

# Enable radio 2.

```
[AC-wlan-ap-group-group1-ap-model-AP 3620-radio-2] radio
```

```
enable [AC-wlan-ap-group-group1-ap-model-AP 3620-radio-2] quit
```

```
[AC-wlan-ap-group-group1-ap-model-AP 3620]
```

```
quit [AC-wlan-ap-group-group1] quit
```

## 4. Configure an ISP domain:

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

```
[AC] domain dm1
```

# Configure the AC to perform local authentication and not to perform authorization or accounting on portal users in the ISP domain.

```
[AC-isp-dm1] authentication portal local
```

```
[AC-isp-dm1] authorization portal none
```

```
[AC-isp-dm1] accounting portal none
```

# Set the idle timeout period to 15 minutes and the minimum traffic that must be generated in the idle timeout period to 1024 bytes.

```
[AC-isp-dm1] authorization-attribute idle-cut 15 1024
```

```
[AC-isp-dm1] quit
```

5. Configure portal authentication:

# Create a portal Web server named **newpt** and specify **http://2.2.2.1:8080/portal** as the URL of portal Web server **newpt**.

```
[AC] portal web-server newpt
```

```
[AC-portal-websvr-newpt] url http://2.2.2.1:8080/portal
```

# Add the **wlanuserip** parameter to the URL of the portal Web server and specify the user IP address as the parameter value.

```
[AC-portal-websvr-newpt] url-parameter wlanuserip source-address
```

```
[AC-portal-websvr-newpt] quit
```

# Configure two destination-based portal-free rules to permit the traffic destined for the DNS server.

```
[AC] portal free-rule 1 destination ip any udp 53
```

```
[AC] portal free-rule 2 destination ip any tcp 53
```

# Create an HTTP-based local portal Web service.

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

# Specify file **abc.zip** as the default authentication page file and 8080 as the service port number for the local portal Web service. (Make sure the file already exists under the root directory of the device storage media.)

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

```
[AC-portal-local-websvr-http] tcp-port 8080
```

```
[AC-portal-local-websvr-http] quit
```

# Add a local network access user named **portaluser**, set the password of the user, and assign the portal service to the user.

```
[AC] local-user portaluser class network
```

```
[AC-luser-network-portaluser] password simple abc123
```

```
[AC-luser-network-portaluser] service-type portal
```

```
[AC-luser-network-portaluser] quit
```

# Enable portal roaming.

```
[AC] portal roaming enable
```

# Disable the Rule ARP entry feature for portal clients.

```
[AC] undo portal refresh arp enable
```

# Enable validity check on wireless portal clients.

```
[AC] portal host-check enable
```

6. Configure portal MAC-trigger authentication:

# Create a MAC binding server named **mts** and enter its view.

```
[AC] portal mac-trigger-server mts
```

# Specify 2.2.2.1 as the IP address of MAC binding server **mts**.

```
[AC-portal-mac-trigger-server-mts] ip 2.2.2.1
Enable local portal MAC-trigger authentication, and set the aging time for local MAC-account
binding entries to 60 minutes.
[AC-portal-mac-trigger-server-mts] local-binding enable
[AC-portal-mac-trigger-server-mts] local-binding aging-time 60
[AC-portal-mac-trigger-server-mts] quit
Enable direct portal authentication on service template st1.
[AC] wlan service-template st1
[AC-wlan-st-st1] portal enable method direct
Specify ISP domain dm1 as the authentication domain for portal users on service template
st1.
[AC-wlan-st-st1] portal domain dm1
Specify portal Web server newpt on service template st1.
[AC-wlan-st-st1] portal apply web-server newpt
Specify MAC binding server mts on service template st1.
[AC] wlan service-template st1
[AC-wlan-st-st1] portal apply mac-trigger-server mts
Enable service template st1.
[AC-wlan-st-service1] service-template enable
[AC-wlan-st-st1] quit
```

## Configuring the switch

# Create VLAN 100. The switch will use this VLAN to forward traffic on the CAPWAP tunnel between the AC and the AP.

```
<Switch> system-view
[Switch] vlan 100
[Switch-vlan100] quit
```

# Create VLAN 200. The switch will use this VLAN to forward client traffic.

```
[Switch] vlan 200
[Switch-vlan200] quit
```

# Configure GigabitEthernet 1/0/1 (the port connected to the AC) as a trunk port and assign the port to VLAN 100 and VLAN 200.

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[Switch-GigabitEthernet1/0/1] quit
```

# Configure GigabitEthernet 1/0/2 (the port connected to the AP) as a trunk port, assign the port to VLAN 100 and VLAN 200, and set the PVID to VLAN 100.

```
[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] port link-type trunk
[Switch-GigabitEthernet1/0/2] port trunk permit vlan 100 200
[Switch-GigabitEthernet1/0/2] port trunk pvid vlan 100
```

# Enable PoE on GigabitEthernet 1/0/2.

```
[Switch-GigabitEthernet1/0/2] poe enable
[Switch-GigabitEthernet1/0/2] quit
```

# Assign an IP address to VLAN-interface 200.

```
[Switch] interface vlan-interface 200
[Switch-Vlan-interface200] ip address 2.2.2.100 255.255.255.0
[Switch-Vlan-interface200] quit
```

## Verifying the configuration

### # Display information about MAC binding server **mts**.

```
[AC] display portal mac-trigger-server name mts
[AC] display portal mac-trigger-server name mts
Portal mac trigger server name: mts
```

```
Version : 1.0
Server type : INC
IP : 2.2.2.1
Port : 50100
VPN instance : Not configured
Aging time : 300 seconds
Free-traffic threshold : 0 bytes
NAS-Port-Type : Not configured
Binding retry times : 3
Binding retry interval : 1 seconds
Authentication timeout : 3 minutes
Local-binding : Enabled
Local-binding aging-time : 60 minutes
aaa-fail nobinding : Disabled
Excluded attribute list : Not configured
Cloud-binding : Disabled
Cloud-server URL : Not configured
```

# Use the configured user account to perform portal authentication through a Web browser. Before passing portal authentication, the user can access only the authentication page **<http://2.2.2.1:8080/portal>**. All Web requests from the user will be redirected to the authentication page. After passing portal authentication, the user can access other network resources. (Details not shown.)

### # Display information about all portal users.

```
[AC] display portal user all
```

Total portal users: 1

Username: portaluser

AP name: office

Radio ID: 2

SSID: service

Portal server: newpt

State: Online

VPN instance: N/A

| MAC            | IP      | VLAN | Interface     |
|----------------|---------|------|---------------|
| 0021-6330-0933 | 2.2.2.2 | 200  | WLAN-BSS1/0/2 |

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

The output shows that the user has passed portal authentication.

# Log out the user and then get the user to come online again to verify that the user can directly access network resources without entering the username and password.

## Configuration files

- AC:

```
#
vlan 100
#
vlan 200
#
wlan service-template st1
 ssid service
 vlan 200
client forwarding-location ap
 akm mode psk
 preshared-key pass-phrase cipher c3$0Lf6p0Z6bxrf25nodjOJKYEfnZ6g6ErccHyQ
 cipher-suite ccmp
 security-ie rsn
portal enable method direct
 portal domain dml
 portal apply web-server newpt
 portal apply mac-trigger-server mts
 service-template enable
#
interface Vlan-interface100
 ip address 2.2.1.1 255.255.255.0
#
interface Vlan-interface200
 ip address 2.2.2.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 1 100 200
#
domain dml
 authorization-attribute idle-cut 15 1024
 authentication portal local
 authorization portal none
 accounting portal none
#
portal host-check enable
portal free-rule 1 destination ip any udp 53
portal free-rule 2 destination ip any tcp 53
```



```

#
portal roaming enable
undo portal refresh arp enable
#
portal web-server newpt
url http://2.2.2.1:8080/portal
server-type iNC
url-parameter wlanuserip source-address
#
portal local-web-server http
default-logon-page abc.zip
tcp-port 8080
#
portal mac-trigger-server mts
ip 2.2.2.1
server-type iNC
#
wlan ap-group group1
ap office
ap-model AP 3620
map-configuration flash:/map.txt
radio 1
radio 2
radio enable
service-template st1
#
wlan ap office model AP 3620
serial-id 219801A28N819CE0002T
#

```

- **Switch:**

```

#
vlan 100
#
vlan 200
#
interface Vlan-interface200
ip address 2.2.2.100 255.255.255.0
#
interface GigabitEthernet1/0/1
port link-type trunk
port trunk permit vlan 1 100 200
#
interface GigabitEthernet1/0/2
port link-type trunk
port trunk permit vlan 1 100 200
port trunk pvid vlan 100
poe enable

```

# Related documentation

- *User Access and Authentication Command Reference in INTELBRAS Access Controllers Command References*
- *User Access and Authentication Configuration Guide in INTELBRAS Access Controllers Configuration Guides*
- *WLAN Access Command Reference in INTELBRAS Access Controllers Command References*
- *WLAN Access Configuration Guide in INTELBRAS Access Controllers Configuration Guides*
- *AP Management Command Reference in INTELBRAS Access Controllers Command References*
- *AP Management Configuration Guide in INTELBRAS Access Controllers Configuration Guides*

# INTELBRAS Access Controllers

## Local Portal Authentication (IPv6)

### Configuration Examples

---

Copyright © 2024 Intelbras S.A All rights reserved.

No part of this manual may be reproduced or transmitted in any form or by any means without prior written consent of Intelbras S.A

Except for the trademarks of Intelbras S.A, any trademarks that may be mentioned in this document are the property of their respective owners.

The information in this document is subject to change without notice.

# Contents

|                                                             |    |
|-------------------------------------------------------------|----|
| Introduction .....                                          | 1  |
| Prerequisites .....                                         | 1  |
| Example: Configuring local IPv6 portal authentication ..... | 1  |
| Network configuration .....                                 | 1  |
| Analysis .....                                              | 2  |
| Restrictions and guidelines .....                           | 2  |
| Procedures .....                                            | 3  |
| Configuring the AC .....                                    | 3  |
| Configuring the switch .....                                | 7  |
| Configuring the RADIUS server .....                         | 10 |
| Verifying the configuration .....                           | 12 |
| Configuration files .....                                   | 13 |
| Related documentation .....                                 | 17 |

# Introduction

The following information provides examples for configuring local IPv6 portal authentication on the AC.

## Prerequisites

The following information applies to Comware-based access controllers and access points. Procedures and information in the examples might be slightly different depending on the software or hardware version of the access controllers and access points.

The configuration examples 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.

The following information is provided based on the assumption that you have basic knowledge of AAA, portal, and WLAN.

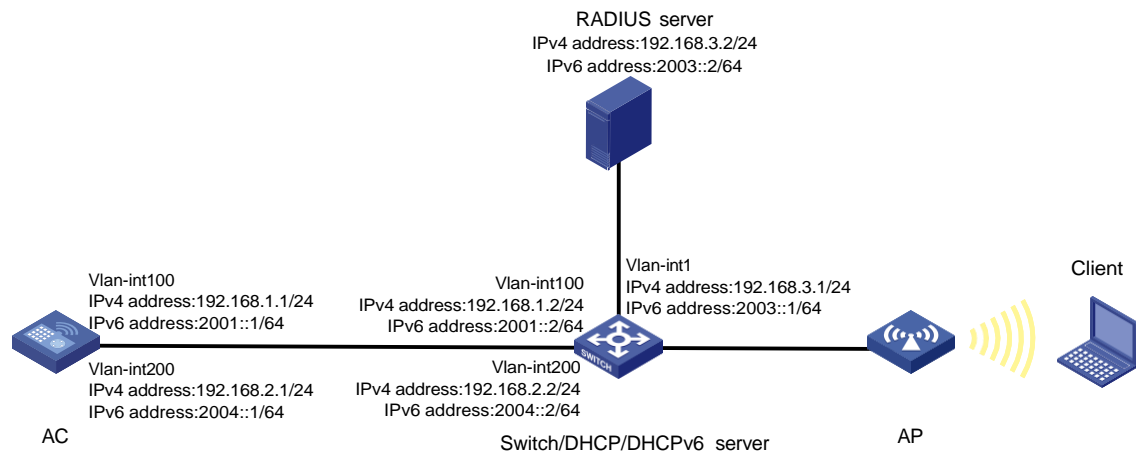
## Example: Configuring local IPv6 portal authentication

### Network configuration

As shown in [Figure 1](#), the switch acts as the DHCP server and the DHCPv6 server. The AP and the client obtain IPv4 addresses and IPv6 addresses from the switch.

- Configure the access device AC to also act as the portal Web server and the portal authentication server.
- Use the RADIUS server as both the authentication server and the authorization server.
- Configure direct portal authentication on the AC.

**Figure 1 Network diagram**



## Analysis

To allow an authenticated user to access network resources on any Layer 2 ports in its access VLAN without re-authentication, you must enable the portal roaming feature.

To avoid possible authentication failure caused by frequent logins and logouts of portal clients in a short time, disable the Rule ARP entry feature.

To allow the RADIUS server to modify user authorization information and log out users, enable the RADIUS session-control feature.

## Restrictions and guidelines

Use the actual serial ID of an AP to uniquely identify that AP.

By default, the portal Web server URL redirected to users does carry parameters. You can configure the parameters to be carried in the redirection URL as needed.

To enable portal authentication on a VLAN interface, you must use the centralized forwarding mode. To enable portal authentication on a service template, you can use the centralized forwarding mode or the local forwarding mode. In this example, portal authentication is enabled on a service template.

Edit portal authentication pages, compress them to a .zip file (this example uses **abc.zip**), and then upload the file to the root directory of the storage medium of the AC. On the AC, you must specify this file as the default authentication page file.

To change the default authentication page file, you must first execute the **undo default-logon-page** command, and then specify a new default authentication page file.

# Procedures

## Configuring the AC

### 1. Configuring VLANs and interfaces:

# Create VLAN 100 and VLAN-interface 100. Assign an IPv4 address and an IPv6 address to the VLAN interface. The AC will establish a CAPWAP tunnel with the AP in this VLAN.

```
<AC> system-view
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 192.168.1.1 24
[AC-Vlan-interface100] ipv6 address 2001::1 64
[AC-Vlan-interface100] quit
```

# Create VLAN 200 and VLAN-interface 200. Assign an IPv4 address and an IPv6 address to the VLAN interface. This VLAN will be used for wireless client access.

```
[AC] vlan 200
[AC-vlan200] quit
[AC] interface vlan-interface 200
[AC-Vlan-interface200] ip address 192.168.2.1 24
[AC-Vlan-interface200] ipv6 address 2004::1 64
[AC-Vlan-interface200] quit
```

# Configure GigabitEthernet1/0/1 (the port connected to the switch) as a trunk port, and assign the port to VLAN 1, VLAN 100, and VLAN 200.

```
[AC] interface gigabitethernet 1/0/1
[AC-GigabitEthernet1/0/1] port link-type trunk
[AC-GigabitEthernet1/0/1] port trunk permit vlan 1 100 200
[AC-GigabitEthernet1/0/1] quit
```

### 2. Configure a static IPv4 route and a static IPv6 route to the INC server.

```
[AC] ip route-static 192.168.3.0 255.255.255.0 192.168.2.2
[AC] ipv6 route-static 2003:: 64 2004::2
```

### 3. Configure the wireless service:

# Create a service template named **st1** and enter its view.

```
[AC] wlan service-template st1
```

# Configure the SSID of the service template as **service**.

```
[AC-wlan-st-st1] ssid service
```

# Assign clients coming online through the service template to VLAN 200.

```
[AC-wlan-st-st1] vlan 200
```

# Specify the AKM mode as PSK, and configure the preshared key as 12345678 in plain text.

```
[AC-wlan-st-st1] akm mode psk
[AC-wlan-st-st1] preshared-key pass-phrase simple 12345678
```

# Specify the cipher suite as CCMP and the security IE as RSN.

```
[AC-wlan-st-st1] cipher-suite ccmp
[AC-wlan-st-st1] security-ie rsn
```

# Configure the AC to forward client data traffic. (Skip this step if the client data traffic forwarder is the AC by default.)

```
[AC-wlan-st-st1] client forwarding-location ac
```

# Enable snooping ND packets on the service template.

```
[AC-wlan-st-st1] client ipv6-snooping nd-learning enable
```

# Enable snooping DHCPv6 packets on the service template.

```
[AC-wlan-st-st1] client ipv6-snooping dhcpv6-learning enable
```

# Enable the service template.

```
[AC-wlan-st-st1] service-template enable
[AC-wlan-st-st1] quit
```

#### 4. Configure the AP:

---

##### NOTE:

In large-scale networks, configure AP groups instead of single APs as a best practice.

---

# Create an AP named **office** with model **AP 3620**, and set the serial ID to **219801A28N819CE0002T**.

```
[AC] wlan ap office model AP 3620
[AC-wlan-ap-office] serial-id 219801A28N819CE0002T
[AC-wlan-ap-office] quit
```

# Create AP group **group1** and add AP **office** to AP group **group1**.

```
[AC] wlan ap-group group1
[AC-wlan-ap-group-group1] ap office
```

# Bind service template **st1** to radio 2 in AP group **group1**.

```
[AC-wlan-ap-group-group1] ap-model AP 3620
[AC-wlan-ap-group-group1-ap-model-AP 3620] radio 2
[AC-wlan-ap-group-group1-ap-model-AP 3620-radio-2] service-template st1
```

# Enable radio 2.

```
[AC-wlan-ap-group-group1-ap-model-AP 3620-radio-2] radio
enable [AC-wlan-ap-group-group1-ap-model-AP 3620-radio-2] quit
[AC-wlan-ap-group-group1-ap-model-AP 3620]
quit [AC-wlan-ap-group-group1] quit
```

#### 5. Configure an IPv4 RADIUS scheme:

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

```
[AC] radius scheme rs1
```

# Configure the primary authentication and accounting servers and shared keys used for secure communication with the servers.

```
[AC-radius-rs1] primary authentication 192.168.3.2
[AC-radius-rs1] primary accounting 192.168.3.2
[AC-radius-rs1] key authentication simple radius
[AC-radius-rs1] key accounting simple radius
```



# Configure the AC to remove the domain name from the usernames sent to the RADIUS servers.

```
[AC-radius-rs1] user-name-format without-domain
```

# Configure the BAS-IP attribute as 192.168.1.1.

```
[AC-radius-rs1] nas-ip 192.168.1.1
```

```
[AC-radius-rs1] quit
```

## 6. Configure an IPv6 RADIUS scheme:

# Create a RADIUS scheme named **rs2** and enter its view.

```
[AC] radius scheme rs2
```

# Configure the primary authentication and accounting servers and shared keys used for secure communication with the servers.

```
[AC-radius-rs2] primary authentication ipv6 2003::2
```

```
[AC-radius-rs2] primary accounting ipv6 2003::2
```

```
[AC-radius-rs2] key authentication simple radius
```

```
[AC-radius-rs2] key accounting simple radius
```

# Configure the AC to remove the domain name from the usernames sent to the RADIUS servers.

```
[AC-radius-rs2] user-name-format without-domain
```

# Configure the BAS-IPv6 attribute as 2001::1.

```
[AC-radius-rs2] nas-ip ipv6 2001::1
```

```
[AC-radius-rs2] quit
```

# Enable the RADIUS session-control feature.

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

# Enable the RADIUS DAS feature and enter RADIUS DAS view.

```
[AC] radius dynamic-author server
```

# Specify a session-control client at IPv4 address 192.168.3.2 and shared key **radius** in plaintext form.

```
[AC-radius-da-server] client ip 192.168.3.2 key simple radius
```

# Specify a session-control client at IPv6 address 2003::2 and shared key **radius** in plaintext form.

```
[AC-radius-da-server] client ipv6 2003::2 key simple radius
```

```
[AC-radius-da-server] quit
```

## 7. Configure an IPv4 authentication domain:

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

```
[AC] domain dm1
```

# Configure the authentication and authorization methods as RADIUS and the accounting method as none for portal users.

```
[AC-isp-dm1] authentication portal radius-scheme rs1
```

```
[AC-isp-dm1] authorization portal radius-scheme rs1
```

```
[AC-isp-dm1] accounting portal none
```

# Configure the idle cut feature for users in the ISP domain. Log out a user if the user's traffic is less than 1024 bytes in 15 minutes.

```
[AC-isp-dm1] authorization-attribute idle-cut 15 1024
[AC-isp-dm1] quit
```

**8. Configure an IPv6 authentication domain:**

**# Create an ISP domain named **dm2** and enter its view.**

```
[AC] domain dm2
```

**# Configure the authentication and authorization methods as RADIUS and the accounting method as none for portal users.**

```
[AC-isp-dm2] authentication portal radius-scheme rs2
[AC-isp-dm2] authorization portal radius-scheme rs2
[AC-isp-dm2] accounting portal none
```

**# Configure the idle cut feature for users in the ISP domain. Log out a user if the user's traffic is less than 1024 bytes in 15 minutes.**

```
[AC-isp-dm2] authorization-attribute idle-cut 15 1024
[AC-isp-dm2] quit
```

**9. Configure portal authentication:**

**# Create an IPv4 portal Web server named **newptv4** and specify the server's URL as **http://192.168.2.1/portal**.**

```
[AC] portal web-server newptv4
[AC-portal-websvr-newptv4] url http://192.168.2.1/portal
```

**# Configure the portal redirection URL to carry the **wlanuserip** parameter and the parameter value is the user's IP address.**

```
[AC-portal-websvr-newptv4] url-parameter wlanuserip source-address
[AC-portal-websvr-newptv4] quit
```

**# Create an IPv6 portal Web server named **newptv6** and specify the server's URL as **http://[2004::1]/portal**.**

```
[AC] portal web-server newptv6
[AC-portal-websvr-newptv6] url http://[2004::1]/portal
```

**# Configure the portal redirection URL to carry the **wlanuserip** parameter and the parameter value is the user's IP address.**

```
[AC-portal-websvr-newptv6] url-parameter wlanuserip source-address
[AC-portal-websvr-newptv6] quit
```

**# Enable direct IPv4 portal authentication and direct IPv6 portal authentication on service template **st1**.**

```
[AC] wlan service-template st1
[AC-wlan-st-st1] portal enable method direct [AC-
wlan-st-st1] portal ipv6 enable method direct
```

**# Specify ISP domain **dm1** as the authentication domain for IPv4 portal users on service template **st1**.**

```
[AC-wlan-st-st1] portal domain dm1
```

**# Specify ISP domain **dm2** as the authentication domain for IPv6 portal users on service template **st1**.**

```
[AC-wlan-st-st1] portal ipv6 domain dm2
```

# Specify IPv4 portal Web server **newptv4** on service template **st1**.

```
[AC-wlan-st-st1] portal apply web-server newptv4
```

# Specify IPv6 portal Web server **newptv6** on service template **st1**.

```
[AC-wlan-st-st1] portal ipv6 apply web-server newptv6
```

# Enable portal to support IPv4/IPv6 dual stack on service template **st1**.

```
[AC-wlan-st-st1] portal dual-stack enable
```

```
[AC-wlan-st-st1] quit
```

# Create an HTTP-based local portal service and enter its view.

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

# Specify the default authentication page file as **defaultfile.zip**. (The file must already exist in the root directory of the storage medium of the AC.)

```
[AC-portal-local-websvr-http] default-logon-page defaultfile.zip
```

```
[AC-portal-local-websvr-http] quit
```

# Enable the portal roaming feature.

```
[AC] portal roaming enable
```

# Disable the Rule ARP entry feature for portal clients.

```
[AC] undo portal refresh arp enable
```

# Enable the wireless client validity check feature.

```
[AC] portal host-check enable
```

# Configure two destination-based portal-free rules to permit the traffic destined for the DNS server.

```
[AC] portal free-rule 1 destination ip any udp 53
```

```
[AC] portal free-rule 2 destination ip any tcp 53
```

# Configure a source-based portal-free rule. Set the rule number to 3 and the source interface to aggregate interface 1. This rule allows the portal user on the aggregate interface to access network resources without authentication.

```
[AC] portal free-rule 3 source interface Bridge-Aggregation1
```

## Configuring the switch

### 1. Configure VLANs and interfaces:

# Create VLAN 100. The switch will use this VLAN to forward traffic on the CAPWAP tunnel between the AC and the AP.

```
<Switch> system-view
```

```
[Switch] vlan 100
```

```
[Switch-vlan100] quit
```

# Create VLAN 200. The switch will use this VLAN to forward traffic of wireless clients.

```
[Switch] vlan 200
```

```
[Switch-vlan200] quit
```

# Configure GigabitEthernet 1/0/1 (the port connected to the AC) as a trunk port. Assign the trunk port to VLAN 1, VLAN 100, and VLAN 200.

```
[Switch] interface gigabitethernet 1/0/1
```

```
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 1 100 200
[Switch-GigabitEthernet1/0/1] quit
```

**# Configure GigabitEthernet 1/0/2 (the port connected to the AP) as an access port. Assign the access port to VLAN 100.**

```
[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] port link-type access
[Switch-GigabitEthernet1/0/2] port access vlan 100
```

**# Enable PoE on the access port.**

```
[Switch-GigabitEthernet1/0/2] poe enable
[Switch-GigabitEthernet1/0/2] quit
```

**# Create VLAN-interface 1 and assign an IPv4 address and an IPv6 address to the VLAN interface.**

```
[Switch] interface vlan-interface 1
[Switch-Vlan-interface1] ip address 192.168.3.1 255.255.255.0
[Switch-Vlan-interface1] ipv6 address 2003::1 64
[Switch-Vlan-interface1] quit
```

**# Create VLAN-interface 100 and assign an IPv4 address and an IPv6 address to the VLAN interface.**

```
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ip address 192.168.1.2 255.255.255.0
[Switch-Vlan-interface100] ipv6 address 2001::2 64
[Switch-Vlan-interface100] quit
```

**# Create VLAN-interface 200 and assign an IPv4 address and an IPv6 address to the VLAN interface.**

```
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ip address 192.168.1.2 255.255.255.0
[Switch-Vlan-interface100] ipv6 address 2001::2 64
[Switch-Vlan-interface100] quit
```

## **2. Configure the DHCP server:**

**# Enable DHCP.**

```
[Switch] dhcp enable
```

**# Configure DHCP address pool named 100 and specify subnet 192.168.1.0/24 and gateway address 192.168.1.1 for the DHCP address pool. The switch will assign an IPv4 address in this address pool to the AP.**

```
[Switch] dhcp server ip-pool 100
[Switch-dhcp-pool-100] network 192.168.1.0 mask 255.255.255.0
[Switch-dhcp-pool-100] gateway-list 192.168.1.1
```

**# Configure Option 43 that specifies the AC's IPv6 address in hexadecimal notation in DHCP address pool 100.**

```
[Switch-dhcp-pool-100] option 43 hex 8007000001c0a80101
[Switch-dhcp-pool-100] quit
```

**# Configure DHCP address pool named 200 and specify subnet 192.168.2.0/24, gateway address 192.168.2.2, and the DNS server address of the wireless client (the same as the**

gateway address in this example) for the DHCP address pool. The switch will assign an IPv4 address in this address pool to the client.

```
[Switch] dhcp server ip-pool 200
[Switch-dhcp-pool-200] network 192.168.2.0 mask 255.255.255.0
[Switch-dhcp-pool-200] gateway-list 192.168.2.2
[Switch-dhcp-pool-200] dns-list 192.168.2.2
[Switch-dhcp-pool-200] quit
```

### 3. Configure the DHCPv6 server:

**# Configure DHCPv6 address pool named 1 and specify subnet 2001::/64 for the DHCPv6 address pool. The switch will assign an IPv6 address in this address pool to the AP.**

```
[Switch] ipv6 dhcp pool 1
[Switch-dhcp6-pool-1] network 2001::/64
```

**# Configure Option 52 that specifies the AC's IPv6 address in DHCPv6 address pool 1.**

```
[Switch-dhcp6-pool-1] option 52 hex 20010000000000000000000000000001
[Switch-dhcp6-pool-1] quit
[Switch] ipv6 dhcp server forbidden-address 2001::1
```

**# Apply DHCPv6 address pool 1 to VLAN-interface 100, and enable the DHCPv6 server on the VLAN interface.**

```
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ipv6 dhcp server apply pool 1
[Switch-Vlan-interface100] ipv6 dhcp select server
```

**# Set the M flag to 1 and the O flag to 1 in RA advertisements to be sent on VLAN-interface 100.**

```
[Switch-Vlan-interface100] ipv6 nd autoconfig managed-address-flag
[Switch-Vlan-interface100] ipv6 nd autoconfig other-flag
```

**# Disable RA message suppression.**

```
[Switch-Vlan-interface100] undo ipv6 nd ra halt
[Switch-Vlan-interface100] quit
```

**# Configure DHCPv6 address pool named 2 and specify subnet 2004::/64 for the DHCPv6 address pool. The switch will assign an IPv6 address in this address pool to the client.**

```
[Switch] ipv6 dhcp pool 2
[Switch-dhcp6-pool-2] network 2004::/64
[Switch-dhcp6-pool-2] quit
```

**# Exclude IPv6 address 2004::1 in the DHCPv6 address pool from dynamic allocation.**

```
[Switch] ipv6 dhcp server forbidden-address 2004::1
```

**# Apply DHCPv6 address pool 2 to VLAN-interface 200, and enable the DHCPv6 server on the VLAN interface.**

```
[Switch] interface Vlan-interface 200
[Switch-Vlan-interface200] ipv6 dhcp server apply pool 2
[Switch-Vlan-interface200] ipv6 dhcp select server
```

**# Set the M flag to 1 and the O flag to 1 in RA advertisements to be sent on VLAN-interface 200.**

```
[Switch-Vlan-interface200] ipv6 nd autoconfig managed-address-flag
[Switch-Vlan-interface200] ipv6 nd autoconfig other-flag
```

**# Disable RA message suppression.**

```
[Switch-Vlan-interface200] undo ipv6 nd ra halt
[Switch-Vlan-interface200] quit
```

## Configuring the RADIUS server

This example uses the INC server to describe the RADIUS server configuration. The INC server runs on INC PLAT 7.1, INC INC - EIA 7.1, and INC EIP 7.1.

**1. Add an access device:**

- a. Log in to INC and click the **User** tab.
- b. From the navigation tree, select **User Access Policy > Access Device Management > Access Device**.
- c. Click **Add**.

The **Add Access Device** page opens.

- d. In the **Access Configuration** area, set the shared key to **radius**

The shared key must be the same as that configured for the RADIUS server on the AC.

- e. In the **Device List** area, perform the following actions:

- Click **Add Manually** to open the **Add Access Device Manually** page. Enter the start IPv4 address **2.2.2.1** and click **OK**.
- Click **Add IPv6 Dev** to open the **Add Access Device Manually** page. Enter the start IPv6 address **2001::1** and click **OK**.

- f. Use the default settings for other parameters.

- g. Click **OK**.

**Figure 2 Adding an access device**

The screenshot shows the 'Add Access Device' page in the INC management interface. The breadcrumb navigation at the top reads: User > User Access Policy > Access Device Management > Access Device > Add Access Device. There is a 'Help' icon on the right.

**Access Configuration**

|                            |                                                                 |                      |           |
|----------------------------|-----------------------------------------------------------------|----------------------|-----------|
| Authentication Port *      | 1812                                                            | Accounting Port *    | 1813      |
| Service Type               | LAN Access Service                                              |                      |           |
| Access Device Type         | H3C(General)                                                    | Service Group        | Ungrouped |
| Shared Key *               | *****                                                           | Confirm Shared Key * | *****     |
| Access Device Group        | --                                                              |                      |           |
| Certificate Authentication | <input checked="" type="radio"/> None <input type="radio"/> EAP |                      |           |
| Certificate Type           | EAP-TLS Authn                                                   |                      |           |

**Device List**

Buttons: Select, Add Manually, Add IPv6 Dev, Clear All

| Device Name     | Device IP | Device Model | Comments | Delete |
|-----------------|-----------|--------------|----------|--------|
| No match found. |           |              |          |        |
| Total Items: 0. |           |              |          |        |

**2. Add an access policy:**

- a. From the navigation tree, select **User Access Policy > Access Policy**.

**b. Click Add.**

The **Add Access Policy** page opens.

**c. Enter the policy name.**

**d. Select a service group.**

**e. Use the default settings for other parameters.**

**f. Click OK.**

**Figure 3 Adding an access policy**

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

Basic Information

Access Policy Name \* AccessPolicy

Service Group \* Ungrouped

Description

Authorization Information

Access Period None Allocate IP \* No

Downstream Rate(Kbps) Upstream Rate(Kbps)

Priority

Deploy VLAN

☐ Deploy User Profile

☐ Deploy ACL

Deploy User Group

**3. Add an access service:**

**a. From the navigation tree, select User Access Policy > Access Service.**

**b. Click Add.**

The **Add Access Service** page opens.

**c. Enter the service name.**

**d. Select the access policy configured in the previous step as the default access policy.**

**e. Use the default settings for other parameters.**

**f. Click OK.**

**Figure 4 Adding an access service**

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

Basic Information

Service Name \* RadiusServer

Service Group \* Ungrouped

Default Proprietary Attribute Assignment Policy \* Do not use

Default Max. Number of Bound Endpoints \* 0

Description

☒ Available

Service Suffix

Default Access Policy \* AccessPolicy

Default Max. Number of Online Endpoints \* 0

☒ Transparent Authentication

Access Scenario List

Add

| Access Scenario | Access Policy | Proprietary Attribute Assignment Policy | Priority | Modify | Delete |
|-----------------|---------------|-----------------------------------------|----------|--------|--------|
| No match found. |               |                                         |          |        |        |

OK Cancel

**4. Add an access user:**

**a. From the navigation tree, select Access User > All Access Users.**

- b. Click **Add**.  
The **Add Access User** page opens.
- c. Click **Select** to select an existing user or click **Add User** to add a new user.
- d. Enter the account name.
- e. Enter and confirm the password.
- f. Select the access service configured in the previous step.
- g. Use the default settings for other parameters.
- h. Click **OK**.

**Figure 5 Adding an access user**

User > All Access Users > Add Access User

Access Information

User Name \* Client1 **Select** **Add User**

Account Name \* Client

☐ Trial Account ☐ Default BYOD User ☐ MAC Authentication User ☐ Computer User ☐ Fast Access User

Password \* \*\*\*\*\* Confirm Password \* \*\*\*\*\*

☒ Allow User to Change Password ☐ Enable Password Strategy ☐ Modify Password at Next Login

Start Time [ ] [ ] End Time [ ] [ ]

Max. Idle Time (Minutes) [ ] Max. Concurrent Logins 1

Login Message [ ]

Access Service

| Service Name                                     | Service Suffix | Status    | Allocate IP |
|--------------------------------------------------|----------------|-----------|-------------|
| <input checked="" type="checkbox"/> RadiusServer |                | Available |             |

## Verifying the configuration

1. Verify that the dual-stack client can access network resources after passing IPv4 portal authentication.
  - a. Use the configured username and password to perform IPv4 portal authentication through a Web browser on the client.
  - b. Verify that all Web accesses of the user are redirected to the portal authentication page (<http://192.168.2.1/portal>) before the client passes IPv4 portal authentication. After the user passes IPv4 portal authentication, the user can access network resources. (Details not shown.)
  - c. Display the online portal user information on the AC after the client passes IPv4 portal authentication.

```
[AC] display portal user all
Total portal users: 1
Username: client
 AP name: office
 Radio ID: 2
 SSID: service
 Portal server: N/A
```



```

State: Online
VPN instance: N/A
MAC IP VLAN Interface
3829-5a40-9589 192.168.2.3 200 WLAN-BSS1/0/2
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

```

The output shows that the client has come online.

2. Verify that the dual-stack client can access network resources after passing IPv6 portal authentication.
  - a. Use the configured username and password to perform IPv6 portal authentication through a Web browser on the client.
  - b. Verify that all Web accesses of the user are redirected to the portal authentication page ([http://\[2004::1\]/portal](http://[2004::1]/portal)) before the client passes IPv6 portal authentication. After the user passes IPv6 portal authentication, the user can access network resources. (Details not shown.)
  - c. Display the online portal user information on the AC after the client passes authentication.

```

[AC] display portal user all
Total portal users: 1
Username: client
 AP name: office
 Radio ID: 2
 SSID: service
 Portal server: N/A
 State: Online
 VPN instance: N/A
MAC IP VLAN Interface
3829-5a40-9589 2004::E97F:BBE1:832C: 200 WLAN-BSS1/0/2
3D3E
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

```

The output shows that the client has come online.

## Configuration files

- AC:

```

#
vlan 100
#
vlan 200
#
wlan service-template st1
 ssid service
 vlan 200
client forwarding-location ac
akm mode psk
 preshared-key pass-phrase cipher c3$0Lf6p0Z6bxrf25nodjOJKYEfnZ6g6ErccHyQ
 cipher-suite ccmp
 security-ie rsn
 client ipv6-snooping nd-learning enable
 client ipv6-snooping dhcpv6-learning enable
 portal enable method direct
 portal domain dm1
 portal apply web-server newptv4
 portal ipv6 enable method direct
 portal ipv6 domain dm2
 portal ipv6 apply web-server newptv6
 portal dual-stack enable
 service-template enable
#
interface Vlan-interface100
 ip address 192.168.1.1 255.255.255.0
 ipv6 address 2001::1/64
#
interface Vlan-interface200
 ip address 192.168.2.1 255.255.255.0
 ipv6 address 2004::1/64
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 100 200
#
 ip route-static 192.168.3.0 24 192.168.2.2
 ipv6 route-static 2003:: 64 2004::2
#
 radius session-control enable
#
radius scheme rs1
 primary authentication 192.168.3.2
 primary accounting 192.168.3.2
 key authentication cipher c3$2m4BXR2X65vE59L0SyyHH0tRVpkKDgym9w==
 key accounting cipher c3$4ieHsnXQVnQ7GwywFS+H0MoQdb6SEmJSRg==
 user-name-format without-domain

```

```

nas-ip 192.168.1.1
#
radius scheme rs2
primary authentication ipv6 2003::2
primary accounting ipv6 2003::2
key authentication cipher c3$8bAMsBFXCglbmynti08YCxotgTXYwzES0w==
key accounting cipher c3$QeTcfxJGTnPJ98PsCSbLnaZP6KAG6q42aQ==
user-name-format without-domain
nas-ip ipv6 2001::1
#
radius dynamic-author server
client ip 192.168.3.2 key cipher c3$19xAYe5vBJQMT0v6quHJFXtZlti404CjBg==
client ipv6 2003::2 key cipher c3$ELOjFzKgJUoRbJ/wZX0E9eVdGBFeTQzmHA==
#
domain dm1
authorization-attribute idle-cut 15 1024
authentication portal radius-scheme rs1
authorization portal radius-scheme rs1
accounting portal none
#
domain dm2
authorization-attribute idle-cut 15 1024
authentication portal radius-scheme rs2
authorization portal radius-scheme rs2
accounting portal none
#
portal host-check enable
portal free-rule 1 destination ip any udp 53
portal free-rule 2 destination ip any tcp 53
portal free-rule 3 source interface Bridge-Aggregation1
#
portal web-server newptv4
url http://192.168.2.1/portal
url-parameter wlanuserip source-address
#
portal web-server newptv6
url http://[2004::1]/portal
url-parameter wlanuserip source-address
#
portal local-web-server http
default-logon-page defaultfile.zip
#
wlan ap-group group1
ap office
ap-model AP 3620
radio 1
radio 2
radio enable

```

```

 service-template st1
#
wlan ap office model AP 3620
 serial-id 219801A28N819CE0002T
#
return

```

- **Switch:**

```

#
ipv6 dhcp server forbidden-address 2001::1
ipv6 dhcp server forbidden-address 2004::1
#
vlan 1
#
vlan 100
#
vlan 200
#
dhcp server ip-pool 100
 gateway-list 192.168.1.1
 network 192.168.1.0 mask 255.255.255.0
 option 43 hex 8007000001c0a80101
#
dhcp server ip-pool 200
 gateway-list 192.168.2.2
 network 192.168.2.0 mask 255.255.255.0
 dns-list 192.168.2.2
#
ipv6 dhcp pool 1
 network 2001::/64
 option 52 hex 20010000000000000000000000000001
#
ipv6 dhcp pool 2
 network 2004::/64
#
interface Vlan-interface1
 ip address 192.168.3.1 255.255.255.0
 ipv6 address 2003::1/64
#
interface Vlan-interface100
 ip address 192.168.1.2 255.255.255.0
 ipv6 dhcp select server
 ipv6 dhcp server apply pool 1
 ipv6 address 2001::2/64
 ipv6 nd autoconfig managed-address-flag
 ipv6 nd autoconfig other-flag
 undo ipv6 nd ra halt
#
interface Vlan-interface200

```

```
ip address 192.168.2.2 255.255.255.0
ipv6 dhcp select server
ipv6 dhcp server apply pool 2
ipv6 address 2004::2/64
ipv6 nd autoconfig managed-address-flag
ipv6 nd autoconfig other-flag
undo ipv6 nd ra halt
#
interface GigabitEthernet1/0/1
port link-type trunk
port trunk permit vlan 1 100 200
#
interface GigabitEthernet1/0/2
port access vlan 100
poe enable
#
Return
```

## Related documentation

- *AP and WT Management Command Reference in INTELBRAS Access Controllers Command References*
- *AP and WT Management Configuration Guide in INTELBRAS Access Controllers Configuration Guides*
- *User Access and Authentication Command Reference in INTELBRAS Access Controllers Command References*
- *User Access and Authentication Configuration Guide in INTELBRAS Access Controllers Configuration Guides*
- *WLAN Access Command Reference in INTELBRAS Access Controllers Command References*
- *WLAN Access Configuration Guide in INTELBRAS Access Controllers Configuration Guides*

# INTELBRAS Access Controllers

## Local Portal Authentication Through the LDAP Server (IPv6) Configuration Examples

---

Copyright © 2020 Intelbras S.A All rights reserved.

No part of this manual may be reproduced or transmitted in any form or by any means without prior written consent of Intelbras S.A

Except for the trademarks of Intelbras S.A, any trademarks that may be mentioned in this document are the property of their respective owners.

The information in this document is subject to change without notice.

# Contents

|                                                                               |    |
|-------------------------------------------------------------------------------|----|
| Introduction .....                                                            | 1  |
| Prerequisites .....                                                           | 1  |
| Example: Configuring local portal authentication through the LDAP server .... | 1  |
| Network configuration .....                                                   | 1  |
| Restrictions and guidelines .....                                             | 2  |
| Procedures .....                                                              | 2  |
| Configuring the AC .....                                                      | 2  |
| Configuring the switch .....                                                  | 5  |
| Configuring the LDAP server .....                                             | 5  |
| Verifying the configuration .....                                             | 8  |
| Configuration files .....                                                     | 8  |
| Related documentation .....                                                   | 10 |

# Introduction

The following information provides examples for configuring the local portal service on the AC to send wireless user information to the LDAP server for authentication.

## Prerequisites

The following information applies to Comware-based access controllers and access points. Procedures and information in the examples might be slightly different depending on the software or hardware version of the access controllers and access points.

The configuration examples 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.

The following information is provided based on the assumption that you have basic knowledge of AAA, portal, and WLAN.

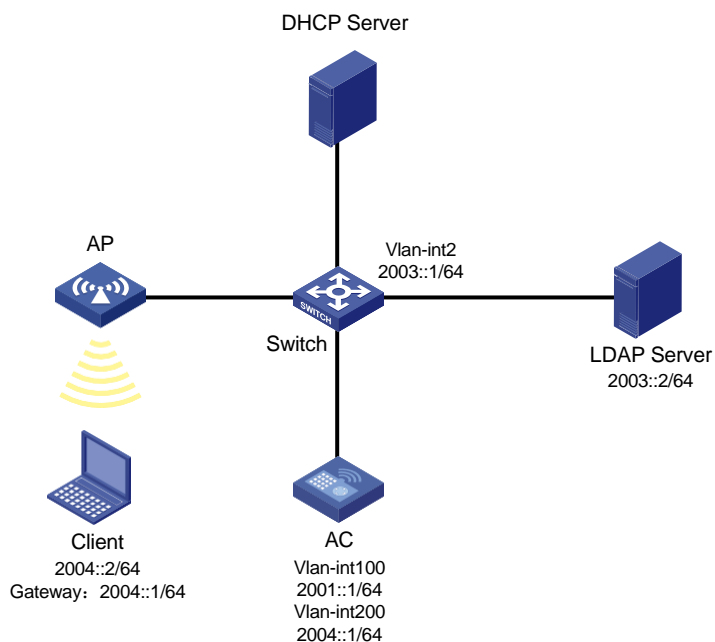
## Example: Configuring local portal authentication through the LDAP server

### Network configuration

As shown in [Figure 1](#), the AP and the client obtain IPv6 addresses from the DHCPv6 server.

Configure the local portal service on the AC to provide authentication pages for clients. Use the LDAP server to authenticate the clients.

**Figure 1 Network diagram**





# Restrictions and guidelines

When you configure local portal authentication through LDAP server, follow these restrictions and guidelines:

- Configure routing to make sure the devices can reach one another.
- Use the actual serial ID of an AP to uniquely identify that AP.
- Edit the authentication pages, compress them to a .zip file (this example uses **abc.zip**), and then upload the file to the root directory of the storage medium of the AC. On the AC, you must specify this file as the default authentication page file.
- To change the default authentication page file, you must first execute the **undo default-logon-page** command, and then specify a new default authentication page file.

## Procedures

### Configuring the AC

#### 1. Configuring VLANs and interfaces:

# Create VLAN 100 and VLAN-interface 100. Assign the VLAN interface an IPv6 address. This VLAN will be used to establish a CAPWAP tunnel with the AP.

```
<AC> system-view
```

```
[AC] vlan 100
```

```
[AC-vlan100] quit
```

```
[AC] interface vlan-interface 100
```

```
[AC-Vlan-interface100] ipv6 address 2001::1 64
```

# Disable RA message suppression.

```
[AC-Vlan-interface100] undo ipv6 nd ra halt
```

# Set the managed address configuration flag (M) to 1 in RA advertisements to be sent.

```
[AC-Vlan-interface100] ipv6 nd autoconfig managed-address-flag
```

# Set the other stateful configuration flag (O) to 1 in RA advertisements to be sent.

```
[AC-Vlan-interface100] ipv6 nd autoconfig other-flag
```

```
[AC-Vlan-interface100] quit
```

# Create VLAN 200 and VLAN-interface 200. Assign the VLAN interface an IPv6 address. This VLAN will be used for wireless client access.

```
[AC] vlan 200
```

```
[AC-vlan200] quit
```

```
[AC] interface vlan-interface 200
```

```
[AC-Vlan-interface200] ipv6 address 2004::1 64
```

# Disable RA message suppression.

```
[AC-Vlan-interface200] undo ipv6 nd ra halt
```

# Set the managed address configuration flag (M) to 1 in RA advertisements to be sent.

```
[AC-Vlan-interface200] ipv6 nd autoconfig managed-address-flag
```

# Set the other stateful configuration flag (O) to 1 in RA advertisements to be sent.

```
[AC-Vlan-interface200] ipv6 nd autoconfig other-flag
```

```
[AC-Vlan-interface200] quit
```

# Configure GigabitEthernet 1/0/1 (the port connected to the switch) as a trunk port. Assign the port to VLAN 100 and VLAN 200.

```
[AC] interface gigabitethernet 1/0/1
```

```
[AC-GigabitEthernet1/0/1] port link-type trunk
[AC-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[AC-GigabitEthernet1/0/1] quit
```

## 2. Configure the LDAP scheme:

# Create an LDAP server named **ldap** and enter its view.

```
[AC] ldap server ldap
```

# Specify the administrator DN.

```
[AC-ldap-server-ldap] login-dn cn=administrator,cn=users,dc=ldap,dc=com
```

# Specify the base DN for user search.

```
[AC-ldap-server-ldap] search-base-dn dc=ldap,dc=com
```

# Specify the IPv6 address of the LDAP server.

```
[AC-ldap-server-ldap] ipv6 2003::2
```

# Specify the administrator password.

```
[AC-ldap-server-ldap] login-password simple 123456
```

```
[AC-ldap-server-ldap] quit
```

# Create an LDAP scheme named **ldap** and enter its view.

```
[AC] ldap scheme ldap
```

# Specify **ldap** as the LDAP authentication server.

```
[AC-ldap-ldap] authentication-server ldap
```

```
[AC-ldap-ldap] quit
```

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

```
[AC] domain ldap
```

# Configure the authentication method as LDAP and the authentication and accounting methods as none for portal users in ISP domain **ldap**.

```
[AC-isp-ldap] authentication portal ldap-scheme ldap
```

```
[AC-isp-ldap] authorization portal none
```

```
[AC-isp-ldap] accounting portal none
```

# Configure the idle cut feature for users in ISP domain **ldap**. Log out a user if the user's traffic is less than 1024 bytes in 15 minutes.

```
[AC-isp-ldap] authorization-attribute idle-cut 15 1024
```

```
[AC-isp-ldap] quit
```

## 3. Configure portal authentication:

# Create a portal Web server named **newpt** and specify the server's URL as **http://[2004::1]/portal**.

```
[AC] portal web-server newpt
```

```
[AC-portal-websvr-newpt] url http://[2004::1]/portal
```

```
[AC-portal-websvr-newpt] quit
```

# Configure two destination-based portal-free rules to permit the traffic destined for the DNS server.

```
[AC] portal free-rule 1 destination ip any udp 53
```

```
[AC] portal free-rule 2 destination ip any tcp 53
```

# Enable validity check on wireless portal clients.

```
[AC] portal host-check enable
```

# Enable the local portal service and enter HTTP-based local portal Web service view.

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

# Specify the default authentication page file as **abc.zip**. (The file must already exist in the root directory of the storage medium of the AC.)

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

```
[AC-portal-local-websvr-http] quit
```

4. Configure the wireless service:

# Create a service template named **st1** and enter its view.

```
[AC] wlan service-template st1
```

# Configure the SSID of the service template as **service**.

```
[AC-wlan-st-st1] ssid service
```

# Assign clients coming online through the service template to VLAN 200.

```
[AC-wlan-st-st1] vlan 200
```

# Enable direct portal authentication.

```
[AC-wlan-st-st1] portal ipv6 enable method direct
```

# Configure the portal authentication domain as **ldap**.

```
[AC-wlan-st-st1] portal ipv6 domain ldap
```

# Specify portal Web server **newpt** on the service template.

```
[AC-wlan-st-st1] portal ipv6 apply web-server newpt
```

# Enable portal to support IPv4/IPv6 dual stack.

```
[AC-wlan-st-st1] portal dual-stack enable
```

# Configure the AC to forward client data traffic. (Skip this step if the client data traffic forwarder is the AC by default.)

```
[AC-wlan-st-st1] client forwarding-location ac
```

# Specify the AKM mode as PSK, and configure the preshared key as 12345678 in plain text.

```
[AC-wlan-st-st1] akm mode psk
```

```
[AC-wlan-st-st1] preshared-key pass-phrase simple 12345678
```

# Specify the cipher suite as CCMP and the security IE as RSN.

```
[AC-wlan-st-st1] cipher-suite ccmp
```

```
[AC-wlan-st-st1] security-ie rsn
```

# Enable the service template.

```
[AC-wlan-st-st1] service-template enable
```

```
[AC-wlan-st-st1] quit
```

5. Configure the AP:

---

**NOTE:**

In large-scale networks, configure AP groups instead of single APs as a best practice.

---

# Create an AP named **ap1**. Specify the AP model and serial ID.

```
[AC] wlan ap ap1 model AP 3620
```

```
[AC-wlan-ap-ap1] serial-id 219801A28N819CE0002T
```

# Create AP group **group1** and add AP **ap1** to AP group **group1**.

```
[AC] wlan ap-group group1
```

```
[AC-wlan-ap-group-group1] ap ap1
```

# Bind service template **st1** to radio 2 in AP group **group1**.

```
[AC-wlan-ap-group-group1] ap-model AP 3620
```

```
[AC-wlan-ap-group-group1-ap-model-AP 3620] radio 2
```

```
[AC-wlan-ap-group-group1-ap-model-AP 3620-radio-2] service-template st1
```

# Enable radio 2.

```
[AC-wlan-ap-group-group1-ap-model-AP 3620-radio-2] radio
```

```
enable [AC-wlan-ap-group-group1-ap-model-AP 3620-radio-2]
```

```
return
```

## Configuring the switch

# Create VLAN 100. The switch will use this VLAN to forward traffic on the CAPWAP tunnel between the AC and AP.

```
<Switch> system-view
[Switch] vlan 100
[Switch-vlan100] quit
```

# Create VLAN 200. The switch will use this VLAN to forward traffic of wireless clients.

```
[Switch] vlan 200
[Switch-vlan200] quit
```

# Create VLAN 2. The switch will use this VLAN to connect to the LDAP server.

```
[Switch] vlan 2
[Switch-vlan2] quit
```

# Assign VLAN-interface 2 (the interface connected to the LDAP server) to VLAN 2. (Details not shown.)

# Assign the VLAN interface an IPv6 address.

```
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] ip address 2003::1/64
[Switch-Vlan-interface2] quit
```

# Configure GigabitEthernet 1/0/1 (the port connected to the AC) as a trunk port. Assign the trunk port to VLAN 100 and VLAN 200.

```
[Switch] interface gigabitethernet1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[Switch-GigabitEthernet1/0/1] quit
```

# Configure GigabitEthernet 1/0/2 (the port connected to the AP) as an access port. Assign the access port to VLAN 100.

```
[Switch] interface gigabitethernet1/0/2
[Switch-GigabitEthernet1/0/2] port link-type access
[Switch-GigabitEthernet1/0/2] port access vlan 100
```

# Enable PoE on the access port.

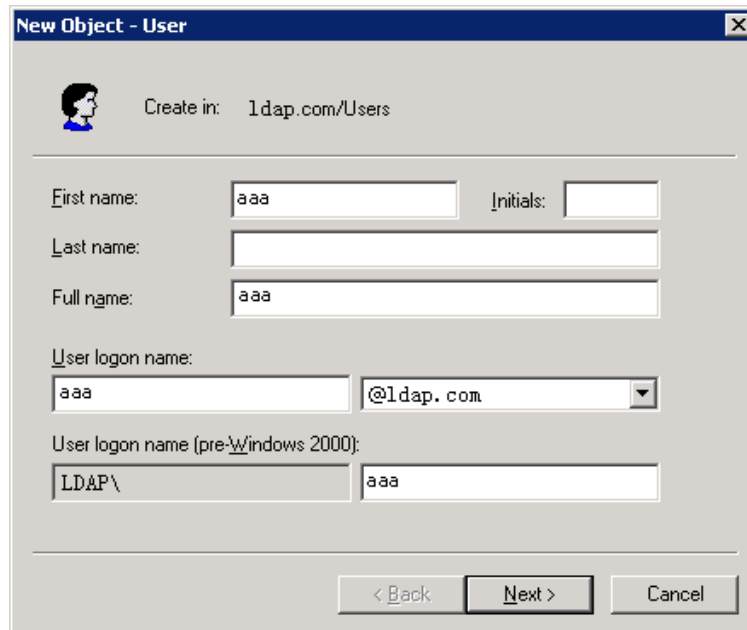
```
[Switch-GigabitEthernet1/0/2] poe enable
[Switch-GigabitEthernet1/0/2] quit
```

## Configuring the LDAP server

This example uses Microsoft Windows 2003 Server Active Directory to illustrate the configuration on the LDAP server.

1. Add a user named **aaa**.
  - a. On the LDAP server, select **Start > Control Panel > Administrative Tools**.
  - b. Double-click **Active Directory Users and Computers**.  
The **Active Directory Users and Computers** window opens.
  - c. From the navigation tree, click **Users** under the **ldap.com** node.
  - d. Select **Action > New > User** from the menu to open the dialog box for adding a user.
  - e. Enter logon name **aaa** and click **Next**.

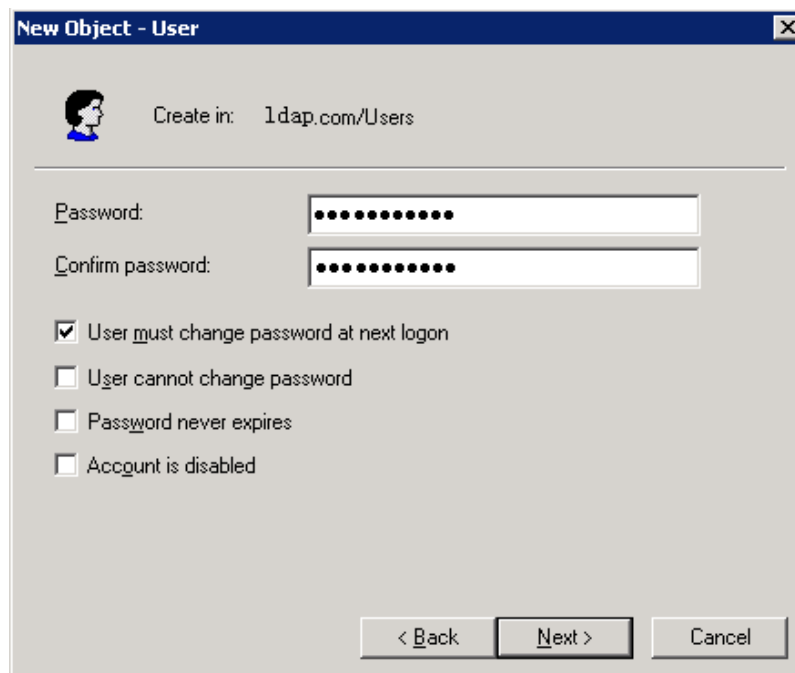
**Figure 2 Adding user aaa**



The 'New Object - User' dialog box is shown. It has a title bar with a close button. Below the title bar is a user icon and the text 'Create in: ldap.com/Users'. The main area contains several input fields: 'First name:' with 'aaa', 'Initials:' (empty), 'Last name:' (empty), 'Full name:' with 'aaa', 'User logon name:' with 'aaa' and a dropdown menu showing '@ldap.com', and 'User logon name (pre-Windows 2000):' with 'LDAP\' and 'aaa'. At the bottom are three buttons: '< Back', 'Next >', and 'Cancel'.

- f. In the dialog box, enter password **123456**, select options as needed, and click **Next**.

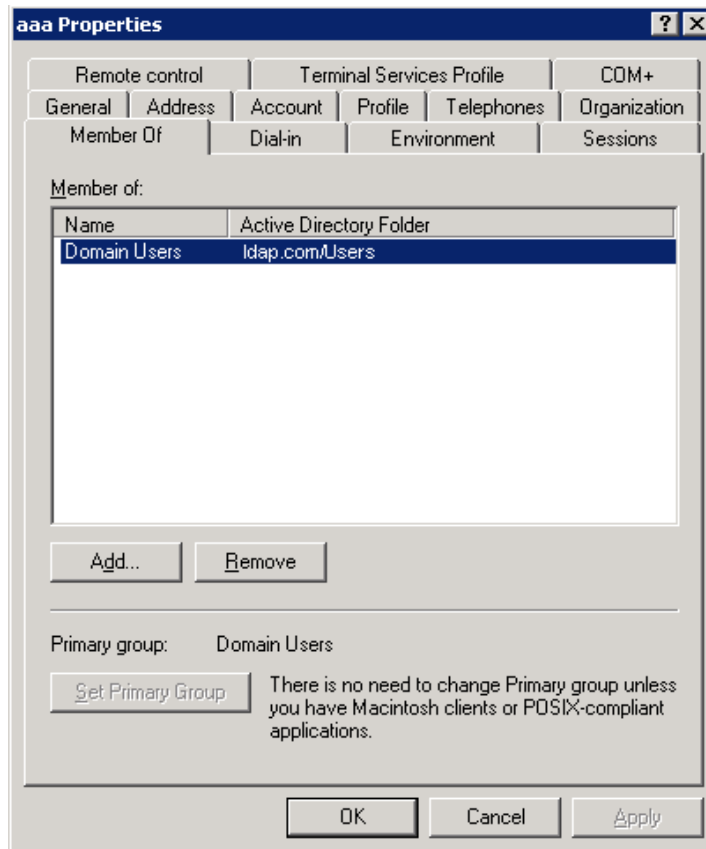
**Figure 3 Setting the user's password**



The 'New Object - User' dialog box is shown. It has a title bar with a close button. Below the title bar is a user icon and the text 'Create in: ldap.com/Users'. The main area contains two password input fields: 'Password:' and 'Confirm password:', both filled with dots. Below these are four checkboxes: 'User must change password at next logon' (checked), 'User cannot change password' (unchecked), 'Password never expires' (unchecked), and 'Account is disabled' (unchecked). At the bottom are three buttons: '< Back', 'Next >', and 'Cancel'.

- g. Click **OK**.
2. Add user **aaa** to user group **Users**:
- From the navigation tree, click **Users** under the **ldap.com** node.
  - In the right pane, right-click user **aaa** and select **Properties**.
  - In the dialog box, click the **Member Of** tab and click **Add**.

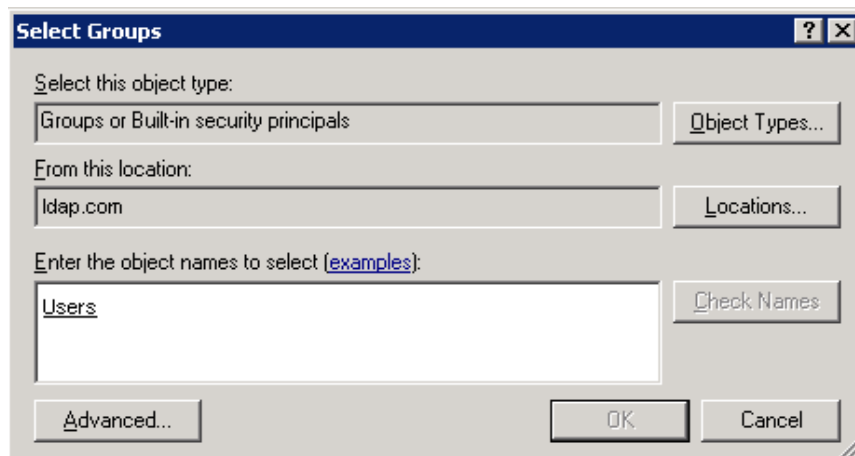
**Figure 4 Modifying user properties**



- d. In the **Select Groups** dialog box, enter **Users** in the **Enter the object names to select** field, and click **OK**.

User **aaa** is added to group **Users**.

**Figure 5 Adding user aaa to group Users**



3. Configure the administrator password:
- In the right pane, right-click user **Administrator** and select **Set Password**.
  - In the dialog box, enter the administrator password. (Details not shown.)

# Verifying the configuration

# Open a Web browser such as IE on the wireless client. Type an IPv6 address in the address bar and press **Enter**. The portal authentication page opens. Enter username **aaa** and password **123456** and then click **Logon**. User **aaa** passes authentication successfully.

# Display online portal users on the AC.

```
<AC> display portal user all
```

```
Total portal users: 1
```

```
Username: aa
```

```
AP name: ap1
```

```
Radio ID: 2
```

```
SSID: service
```

```
Portal server: N/A
```

```
State:Online
```

```
VPN instance: N/A
```

| MAC | IP | Vlan | Interface |
|-----|----|------|-----------|
|-----|----|------|-----------|

|                |         |     |                |
|----------------|---------|-----|----------------|
| 2477-0341-f118 | 2004::2 | 200 | WLAN-BSS1/0/19 |
|----------------|---------|-----|----------------|

```
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

- AC:

```
#
vlan 100
#
vlan 200
#
wlan service-template st1
 ssid service
client forwarding-location ac
 akm mode psk
 preshared-key pass-phrase simple 12345678
 cipher-suite ccmp
 security-ie rsn
vlan 200
portal ipv6 enable method direct
portal ipv6 domain ldap
portal ipv6 apply web-server newpt
portal dual-stack enable
service-template enable
#
```

```

interface Vlan-interface100
 ipv6 address 2001::1/64
 ipv6 nd autoconfig managed-address-flag
 ipv6 nd autoconfig other-flag
 undo ipv6 nd ra halt
#
interface Vlan-interface200
 ipv6 address 2004::1/64
 ipv6 nd autoconfig managed-address-flag
 ipv6 nd autoconfig other-flag
 undo ipv6 nd ra halt
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 100 200
#
ldap server ldap
 login-dn cn=administrator,cn=users,dc=ldap,dc=com
 search-base-dn dc=ldap,dc=com
 ipv6 2003::2
 login-password cipher c3$CEz2vKcNA2/51D8rFc/+nTNtOx8Gan+81Q==
#
ldap scheme ldap
 authentication-server ldap
#
domain ldap
 authorization-attribute idle-cut 15 1024
 authentication portal ldap-scheme ldap
 authorization portal none
 accounting portal none
#
portal host-check enable
portal free-rule 1 destination ip any udp 53
portal free-rule 2 destination ip any tcp 53
#
portal web-server newpt
 url http://[2004::1]/portal
#
portal local-web-server http
 default-logon-page abc.zip
#
wlan ap ap1 model AP 3620
 serial-id 219801A28N819CE0002T
#
wlan ap-group group1
ap ap1
ap-model AP 3620
radio 2

```



- ```
        radio enable
        service-template st1
#
• Switch:
#
vlan 100
#
vlan 200
#
vlan 2
#
interface Vlan-interface2
    ipv6 address 2003::1/64
#
interface GigabitEthernet1/0/1
    port link-mode bridge
    port link-type trunk
    port trunk permit vlan 100 200
#
interface GigabitEthernet1/0/2
    port link-mode bridge
    port access vlan 100
    poe enable
#
```

Related documentation

- *User Access and Authentication Command Reference in INTELBRAS Access Controllers Command References*
- *User Access and Authentication Configuration Guide in INTELBRAS Access Controllers Configuration Guides*
- *WLAN Access Command Reference in INTELBRAS Access Controllers Command References*
- *WLAN Access Configuration Guide in INTELBRAS Access Controllers Configuration Guides*

INTELBRAS Access Controllers

Remote Portal Authentication (IPv6)

Configuration Examples

Copyright © 2024 Intelbras S.A All rights reserved.

No part of this manual may be reproduced or transmitted in any form or by any means without prior written consent of Intelbras S.A

Except for the trademarks of Intelbras S.A, any trademarks that may be mentioned in this document are the property of their respective owners.

The information in this document is subject to change without notice.

Contents

Introduction	1
Prerequisites	1
Example: Configuring IPv6 remote portal authentication.....	1
Network configuration.....	1
Analysis	2
Restrictions and guidelines	2
Procedures	2
Configuring INC.....	2
Configuring the AC.....	8
Configuring the switch	13
Verifying the configuration	15
Configuration files.....	16
Related documentation	20

Introduction

The following information provides examples for configuring IPv6 remote portal authentication.

Prerequisites

The following information applies to Comware-based access controllers and access points. Procedures and information in the examples might be slightly different depending on the software or hardware version of the access controllers and access points.

The configuration examples 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.

The following information is provided based on the assumption that you have basic knowledge of AAA, portal, and WLAN.

Example: Configuring IPv6 remote portal authentication

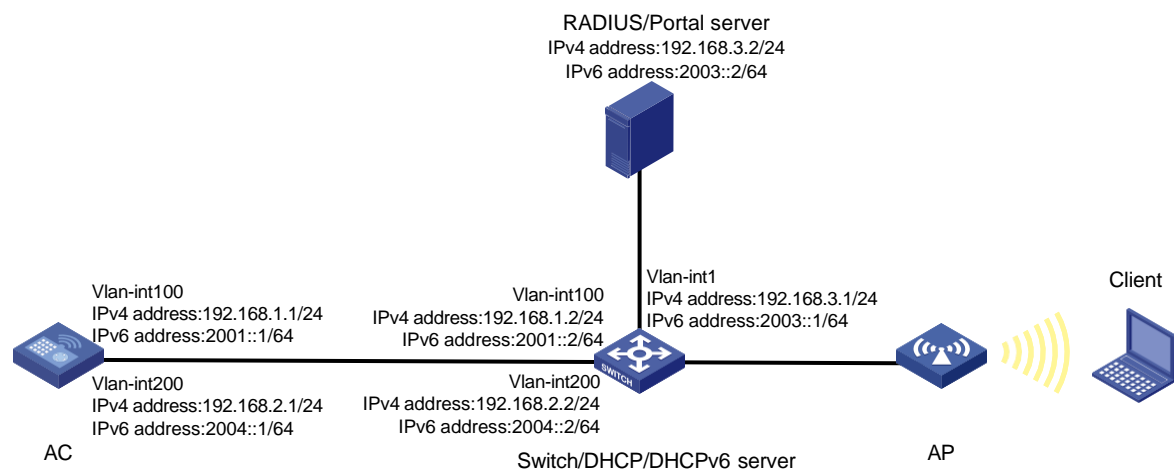
Network configuration

As shown in [Figure 1](#), the switch acts as both a DHCP server and a DHCPv6 server. The AP and the client obtain IPv4 and IPv6 addresses from the switch.

To implement remote portal authentication, perform the following tasks:

- Configure direct portal authentication.
- Configure a portal authentication server and a portal Web server on INC.
- Configure a RADIUS server as the authentication server and accounting server.

Figure 1 Network diagram



Analysis

To allow an authenticated user to access network resources on any Layer 2 ports in its access VLAN without re-authentication, enable portal roaming.

To avoid possible authentication failure caused by frequent logins and logouts of portal clients in a short time, disable the Rule ARP entry feature for portal clients.

For the RADIUS server to dynamically change user authorization information or forcibly disconnect users, enable the RADIUS session-control feature.

To allow portal users to access both IPv4 and IPv6 networks after passing one type (IPv4 or IPv6) of portal authentication, enable portal to support IPv4/IPv6 dual stack.

Restrictions and guidelines

Use the actual serial ID of an AP to uniquely identify that AP.

Make sure the types of the portal authentication server and portal Web server specified on the AC are the same as those actually used.

By default, the portal Web server URL redirected to users does not carry parameters. You can configure the parameters to be carried in the redirection URL as needed.

Procedures

Configuring INC

This example uses the INC server to describe the RADIUS server and portal server configuration. The INC server runs on INC PLAT 7.1, INC INC - EIA 7.1, and INC EIP 7.1.

Configuring the RADIUS server

1. Add an access device.
 - a. Log in to INC and click the **User** tab.
 - b. From the navigation tree, select **User Access Policy > Access Device Management > Access Device**.
 - c. Click **Add**.

The **Add Access Device** page opens.
 - d. In the **Access Configuration** area, set the shared key to **radius**, which must be the same as that configured on the AC.
 - e. In the **Device List** area, perform the following operations:
 - Click **Add Manually** to open the **Add Access Device Manually** page. Enter the start IPv4 address **192.168.1.1** and then click **OK**.
 - Click **Add IPv6 Dev** to open the **Add Access Device Manually** page. Enter the start IPv6 address **2001::1** and then click **OK**.
 - f. Use the default settings for other parameters.
 - g. Click **OK**.

Figure 2 Adding an access device

User > User Access Policy > Access Device Management > Access Device > Add Access Device

Access Configuration

Authentication Port * 1812 Accounting Port * 1813

Service Type LAN Access Service

Access Device Type H3C(General)

Shared Key * ***** Service Group Ungrouped

Confirm Shared Key * *****

Access Device Group --

Certificate Authentication ☒ None ☐ EAP

Certificate Type EAP-TLS Auth

Device List

Select Add Manually Add IPv6 Dev Clear All

Device Name	Device IP	Device Model	Comments	Delete
No match found.				
Total Items: 0.				

2. Add an access policy.
 - a. From the navigation tree, select **User Access Policy > Access Policy**.
 - b. Click **Add**.

The **Add Access Policy** page opens.
 - c. Enter the access policy name.
 - d. Select a service group. This example uses the default group (**Ungrouped**).
 - e. Use the default settings for other parameters.
 - f. Click **OK**.

Figure 3 Adding an access policy

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

Basic Information

Access Policy Name * AccessPolicy

Service Group * Ungrouped

Description

Authorization Information

Access Period None Allocate IP * No

Downstream Rate(Kbps) Upstream Rate(Kbps)

Priority

Deploy VLAN

☐ Deploy User Profile ☐ Deploy ACL

Deploy User Group

3. Add an access service.
 - a. From the navigation tree, select **User Access Policy > Access Service**.
 - b. Click **Add**.

The **Add Access Service** page opens.
 - c. Enter the service name.
 - d. Select the access policy configured in the previous step as the default access policy.
 - e. Use the default settings for other parameters.
 - f. Click **OK**.

Figure 4 Adding an access service

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

Basic Information

Service Name * RadiusServer

Service Group * Ungrouped

Default Proprietary Attribute Assignment Policy * Do not use

Default Max. Number of Bound Endpoints * 0

Description

☒ Available

Service Suffix

Default Access Policy * AccessPolicy

Default Max. Number of Online Endpoints * 0

☒ Transparent Authentication

Access Scenario List

Add

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

OK Cancel

4. Add an access user.
 - a. From the navigation tree, select **Access User > All Access Users**.
 - b. Click **Add**.

The **Add Access User** page opens.
 - c. Click **Select** to select an existing access user or click **Add User** to add a new access user.
 - d. Set the password.
 - e. Select the access service configured in the previous step.
 - f. Use the default settings for other parameters.
 - g. Click **OK**.

Figure 5 Adding an access user

User > All Access Users > Add Access User

Access Information

User Name * Client1

Account Name * Client

☐ Trial Account

☐ Default BYOD User

☐ MAC Authentication User

☐ Computer User

☐ Fast Access User

Password * *****

Confirm Password * *****

☒ Allow User to Change Password

☐ Enable Password Strategy

☐ Modify Password at Next Login

Start Time

End Time

Max. Idle Time(Minutes)

Max. Concurrent Logins 1

Login Message

Access Service

Service Name	Service Suffix	Status	Allocate IP
<input checked="" type="checkbox"/> RadiusServer		Available	

Configuring the portal server

1. Configure the portal authentication server:
 - a. From the navigation tree, select **User Access Policy > Portal Service > Server** to open the portal server configuration page, as shown in [Figure 6](#).
 - b. Configure the portal server parameters as needed.

This example uses the default settings.
 - c. Click **OK**.

Figure 6 Configuring the portal server

The screenshot shows the 'Portal Server' configuration page. The breadcrumb navigation is 'User > User Access Policy > Portal Service > Server'. The page is divided into three main sections: 'Basic Information', 'Portal Server', and 'Portal Web'.
- 'Basic Information' contains a 'Log Level' dropdown set to 'Info'.
- 'Portal Server' contains: 'Request Timeout(Seconds)' (4), 'Server Heartbeat Interval(Seconds)' (20), 'User Heartbeat Interval(Minutes)' (5), 'LB Device Address' (empty), and 'LB Device IPv6 Address' (empty).
- 'Portal Web' contains: 'Request Timeout(Seconds)' (15), 'Packet Code' (empty), 'Verify Endpoint Requests' (Yes), 'Use Cache' (Yes), 'HTTP Heartbeat Display' (New Page), and 'HTTPS Heartbeat Display' (Original Page).
At the bottom, there is a 'Portal Page' section with a text area containing four URLs: 'http://192.168.3.2:8080/portal/', 'https://192.168.3.2:8443/portal/', 'http://[2003::2]:8080/portal/', and 'https://[2003::2]:8443/portal/'.

2. Configure IP address groups:

a. From the navigation tree, select **User Access Policy > Portal Service > IP Group**.

b. Click **Add**.

The **Add IP Group** page opens.

c. Enter an IP group name.

d. Select **No** from the **IPv6** field for an IPv4 address group and **Yes** for an IPv6 address group.

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

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

f. Select a service group.

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

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

This step is required only for adding an IPv4 address group.

h. Click **OK**.

Figure 7 Adding an IPv4 address group

The screenshot shows the 'Add IP Group' page. The breadcrumb navigation is 'User > User Access Policy > Portal Service > IP Group > Add IP Group'. The page has a title 'Add IP Group' and several input fields:
- 'IP Group Name *': Portal_user4
- 'IPv6 *': No
- 'Start IP *': 192.168.2.1
- 'End IP *': 192.168.2.255
- 'Service Group': Ungrouped
- 'Action *': Normal
At the bottom right, there are 'OK' and 'Cancel' buttons.

Figure 8 Adding an IPv6 address group

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

Add IP Group

IP Group Name *	Portal_user6
IPv6 *	Yes
Start IP *	2004::1
End IP *	2004::FFFF:FFFF:FFFF:FFFF
Service Group	Ungrouped

OK Cancel

3. Add portal devices:

- a. From the navigation tree, select **User Access Policy > Portal Service > Device**.
- b. Click **Add**.

The **Add Device** page opens.

- c. Enter a device name.

- d. Select a portal version.

For adding an IPv4 portal device, select **Portal 2.0**. For adding an IPv6 portal device, select **Portal 3.0**.

- e. Enter the IP address of the AC's interface connected to the client.

- f. 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**.

- g. Enter the key, which must be the same as that configured on the AC.

- h. Select **Directly Connected** for **Access Method**.

- i. Use the default settings for other parameters.

- j. Click **OK**.

Figure 9 Adding an IPv4 portal device

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

Add Device

Device Information

Device Name *	NAS4	Service Group *	Ungrouped
Version *	Portal 2.0	IP Address *	192.168.2.1
Listening Port *	2000	Local Challenge *	No
Authentication Retries *	0	Logout Retries *	1
Support Server Heartbeat *	No	Support User Heartbeat *	No
Key *	*****	Confirm Key *	*****
Access Method *	Directly Connected		
Device Description			

OK Cancel

Figure 10 Adding an IPv6 portal device

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

Add Device

Device Information

Device Name *	NAS6	Service Group *	Ungrouped
Version *	Portal 3.0	IP Address *	2004::1
Listening Port *	2000	Local Challenge *	No
Authentication Retries *	0	Logout Retries *	1
Support Server Heartbeat *	No	Support User Heartbeat *	No
Key *	*****	Confirm Key *	*****
Access Method *	Directly Conne		
Device Description			

OK Cancel

4. Associate the portal devices with the IP address groups:
 - a. Click the **Port Group** icon in the **Operation** field of devices **NAS4** and **NAS6**, as shown in [Figure 11](#).

Figure 11 Device list

User > User Access Policy > Portal Service > Device

Query Devices

Device Name: Version:

Deploy Result: Service Group:

Query Reset

Add

Device Name	Version	Service Group	IP Address	IPv6 Address	Last Deployed at	Deploy Result	Operation
NAS6	Portal 3.0	Ungrouped		2004::1		Not Deployed	  
NAS4	Portal 2.0	Ungrouped	192.168.2.1			Not Deployed	  

- b. Click **Add** to open the **Add Port Group** page.
 - 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 12 Adding an IPv4 port group

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

Add Port Group

Port Group Name *	Group4	Language *	English
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_user4
Heartbeat Interval(Minutes) *	0	Heartbeat Timeout(Minutes) *	0
User Domain		Port Group Description	
Transparent Authentication	Not Supported	Client Protection Against Cracks *	No
Page Push Policy		Default Authentication Page	

OK Cancel

Figure 13 Adding an IPv6 port group

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

Add Port Group

Port Group Name *	Group6	Language *	English
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_user6
Heartbeat Interval(Minutes) *	0	Heartbeat Timeout(Minutes) *	0
User Domain		Port Group Description	
Transparent Authentication	Not Supported	Client Protection Against Cracks *	No
Page Push Policy		Default Authentication Page	

OK Cancel

Committing configuration changes

From the navigation tree, select **User Access Policy > Service Parameters > Validate System Configuration** to commit the configuration changes.

Configuring the AC

1. Configure interfaces on the AC:

Create VLAN 100 and VLAN-interface 100. Assign an IPv4 address and an IPv6 address to the VLAN interface. The AC will establish a CAPWAP tunnel with the AP in this VLAN.

```
<AC> system-view
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 192.168.1.1 24
[AC-Vlan-interface100] ipv6 address 2001::1 64
[AC-Vlan-interface100] quit
```

Create VLAN 200 and VLAN-interface 200. Assign an IPv4 address and an IPv6 address to the VLAN interface. The AC will use VLAN 200 for client access.

```
[AC] vlan 200
[AC-vlan200] quit
[AC] interface vlan-interface 200
[AC-Vlan-interface200] ip address 192.168.2.1 24
[AC-Vlan-interface200] ipv6 address 2004::1 64
[AC-Vlan-interface200] quit
```

Configure GigabitEthernet1/0/1 (the port connected to the switch) as a trunk port, and assign the port to VLAN 1, VLAN 100, and VLAN 200.

```
[AC] interface gigabitethernet 1/0/1
[AC-GigabitEthernet1/0/1] port link-type trunk
[AC-GigabitEthernet1/0/1] port trunk permit vlan 1 100 200
[AC-GigabitEthernet1/0/1] quit
```

2. Configure a static IPv4 route and a static IPv6 route to the INC server:

```
[AC] ip route-static 192.168.3.0 255.255.255.0 192.168.2.2
[AC] ipv6 route-static 2003:: 64 2004::2
```

3. Configure a wireless service:

Create a service template named **st1 and enter its view.**

```
[AC] wlan service-template st1
```

Set the SSID of service template **st1 to **service**.**

```
[AC-wlan-st-st1] ssid service
```

Assign clients coming online through service template **st1 to VLAN 200.**

```
[AC-wlan-st-service] vlan 200
```

Specify the AKM mode as PSK, and configure the preshared key as 12345678 in plain text.

```
[AC-wlan-st-st1] akm mode psk
```

```
[AC-wlan-st-st1] preshared-key pass-phrase simple 12345678
```

Specify the cipher suite as CCMP and the security IE as RSN.

```
[AC-wlan-st-st1] cipher-suite ccmp
```

```
[AC-wlan-st-st1] security-ie rsn
```

Configure the AC to forward client data traffic. (Skip this step if the client data traffic forwarder is the AC by default.)

```
[AC-wlan-st-st1] client forwarding-location ac
```

Enable snooping ND packets and snooping DHCPv6 packets on service template **st1.**

```
[AC-wlan-st-st1] client ipv6-snooping nd-learning enable
```

```
[AC-wlan-st-st1] client ipv6-snooping dhcpv6-learning enable
```

Enable service template **st1.**

```
[AC-wlan-st-st1] service-template enable
```

```
[AC-wlan-st-st1] quit
```

4. Configure the AP:

NOTE:

In large-scale networks, configure AP groups instead of single APs as a best practice.

Create an AP named **office with model **AP 3620** and set its serial ID to **219801A28N819CE0002T**.**

```
[AC] wlan ap office model AP 3620
```

```
[AC-wlan-ap-office] serial-id 219801A28N819CE0002T
```

```
[AC-wlan-ap-office] quit
```

Create AP group **group1 and add AP **office** to AP group **group1**.**

```
[AC] wlan ap-group group1
[AC-wlan-ap-group-group1] ap office
# Bind service template st1 to radio 2 in AP group group1.
[AC-wlan-ap-group-group1] ap-model AP 3620
[AC-wlan-ap-group-group1-ap-model-AP 3620] radio 2
[AC-wlan-ap-group-group1-ap-model-AP 3620-radio-2] service-template st1
# Enable radio 2.
[AC-wlan-ap-group-group1-ap-model-AP 3620-radio-2] radio
enable [AC-wlan-ap-group-group1-ap-model-AP 3620-radio-2] quit
[AC-wlan-ap-group-group1-ap-model-AP 3620]
quit [AC-wlan-ap-group-group1] quit
```

5. Configure an IPv4 RADIUS scheme:

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

```
[AC] radius scheme rs1
```

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

```
[AC-radius-rs1] primary authentication 192.168.3.2
[AC-radius-rs1] primary accounting 192.168.3.2
[AC-radius-rs1] key authentication simple radius
[AC-radius-rs1] key accounting simple radius
```

Configure the AC to remove the domain name from the usernames sent to the RADIUS servers.

```
[AC-radius-rs1] user-name-format without-domain
```

Specify IP address 192.168.1.1 as the source IP address for outgoing RADIUS packets.

```
[AC-radius-rs1] nas-ip 192.168.1.1
[AC-radius-rs1] quit
```

6. Configure an IPv6 RADIUS scheme:

Create a RADIUS scheme named **rs2** and enter its view.

```
[AC] radius scheme rs2
```

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

```
[AC-radius-rs2] primary authentication ipv6 2003::2
[AC-radius-rs2] primary accounting ipv6 2003::2
[AC-radius-rs2] key authentication simple radius
[AC-radius-rs2] key accounting simple radius
```

Configure the AC to remove the domain name from the usernames sent to the RADIUS servers.

```
[AC-radius-rs2] user-name-format without-domain
```

Specify IPv6 address 2001::1 as the source IP address for outgoing RADIUS packets.

```
[AC-radius-rs2] nas-ip ipv6 2001::1
[AC-radius-rs2] quit
```

Enable the RADIUS session-control feature.

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

Configure the RADIUS DAS feature:

Enable the RADIUS DAS feature and enter RADIUS DAS view.

```
[AC] radius dynamic-author server
```

Specify a session-control client at IPv4 address 192.168.3.2 and shared key **radius** in plaintext form.

```
[AC-radius-da-server] client ip 192.168.3.2 key simple radius
```

Specify a session-control client at IPv6 address 2003::2 and shared key **radius** in plaintext form.

```
[AC-radius-da-server] client ipv6 2003::2 key simple radius
```

```
[AC-radius-da-server] quit
```

7. Configure an IPv4 authentication domain:

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

```
[AC] domain dm1
```

Configure the authentication and authorization methods as RADIUS and the accounting method as none for the ISP domain.

```
[AC-isp-dm1] authentication portal radius-scheme rs1
```

```
[AC-isp-dm1] authorization portal radius-scheme rs1
```

```
[AC-isp-dm1] accounting portal none
```

Configure the idle cut feature for users in the ISP domain. Log out a user if the user's traffic is less than 1024 bytes in 15 minutes.

```
[AC-isp-dm1] authorization-attribute idle-cut 15 1024
```

```
[AC-isp-dm1] quit
```

8. Configure an IPv6 authentication domain:

Create an ISP domain named **dm2** and enter its view.

```
[AC] domain dm2
```

Configure the authentication and authorization methods as RADIUS and the accounting method as none for the ISP domain.

```
[AC-isp-dm2] authentication portal radius-scheme rs2
```

```
[AC-isp-dm2] authorization portal radius-scheme rs2
```

```
[AC-isp-dm2] accounting portal none
```

Configure the idle cut feature for users in the ISP domain. Log out a user if the user's traffic is less than 1024 bytes in 15 minutes.

```
[AC-isp-dm2] authorization-attribute idle-cut 15 1024
```

```
[AC-isp-dm2] quit
```

9. Configure portal authentication:

Create an IPv4 portal authentication server named **newptv4**, and specify IP address 192.168.3.2 for the authentication server.

```
[AC] portal server newptv4
```

```
[AC-portal-server-newptv4] ip 192.168.3.2 key simple 123456
```

```
[AC-portal-server-newptv4] quit
```

Create an IPv6 portal authentication server named **newptv6**, and specify IPv6 address 2003::2 for the authentication server.

```
[AC] portal server newptv6
```

```
[AC-portal-server-newptv6] ipv6 2003::2 key simple 123456
```

```
[AC-portal-server-newptv6] quit
```

Create an IPv4 portal Web server named **newptv4** and specify **http://192.168.3.2:8080/portal** as the URL of the server.

```
[AC] portal web-server newptv4
```

```
[AC-portal-websvr-newptv4] url http://192.168.3.2:8080/portal
```

Add parameters **ssid**, **wlanuserip**, and **wlanacname** to the redirection URL for portal Web server **newptv4**. Specify the AP's SSID, the IP address of the client, and the AC's name as the value for the **ssid**, **wlanuserip**, and **wlanacname** parameters, respectively.

```
[AC-portal-websvr-newptv4] url-parameter ssid ssid
```

```
[AC-portal-websvr-newptv4] url-parameter wlanuserip source-address
```

```
[AC-portal-websvr-newptv4] url-parameter wlanacname value AC
[AC-portal-websvr-newptv4] quit
```

Create an IPv6 portal Web server named **newptv6** and specify **http://[2003::2]:8080/portal** as the URL of the server.

```
[AC] portal web-server newptv6
[AC-portal-websvr-newptv6] url http://[2003::2]:8080/portal
```

Add parameters **ssid**, **wlanuserip**, and **wlanacname** to the redirection URL for portal Web server **newptv6**. Specify the AP's SSID, the IPv6 address of the client, and the AC's name as the value for the **ssid**, **wlanuserip**, and **wlanacname** parameters, respectively.

```
[AC-portal-websvr-newptv6] url-parameter ssid ssid
[AC-portal-websvr-newptv6] url-parameter wlanuserip source-address
[AC-portal-websvr-newptv6] url-parameter wlanacname value AC
[AC-portal-websvr-newptv6] quit
```

Enable portal roaming.

```
[AC] portal roaming enable
```

Disable the Rule ARP entry feature for portal clients.

```
[AC] undo portal refresh arp enable
```

Enable validity check on wireless portal clients.

```
[AC] portal host-check enable
```

Enable direct IPv4 portal authentication and direct IPv6 portal authentication on service template **st1**.

```
[AC] wlan service-template st1
[AC-wlan-st-st1] portal enable method direct
[AC-wlan-st-st1] portal ipv6 enable method direct
```

Specify ISP domain **dm1** as the portal authentication domain for IPv4 portal users.

```
[AC-wlan-st-st1] portal domain dm1
```

Specify ISP domain **dm2** as the portal authentication domain for IPv6 portal users.

```
[AC-wlan-st-st1] portal ipv6 domain dm2
```

Specify IPv4 portal Web server **newptv4** and IPv6 portal Web server **newptv6** on service template **st1** for portal authentication.

```
[AC-wlan-st-st1] portal apply web-server newptv4
[AC-wlan-st-st1] portal ipv6 apply web-server newptv6
```

Enable portal to support IPv4/IPv6 dual stack on service template **st1**.

```
[AC-wlan-st-st1] portal dual-stack enable
```

Configure the BAS-IP attribute as 192.168.2.1 and the BAS-IPv6 attribute as 2004::1.

```
[AC-wlan-st-st1] portal bas-ip 192.168.2.1
[AC-wlan-st-st1] portal bas-ipv6 2004::1
[AC-wlan-st-st1] quit
```

Configure two destination-based portal-free rules to permit the traffic destined for the DNS server.

```
[AC] portal free-rule 1 destination ip any udp 53
[AC] portal free-rule 2 destination ip any tcp 53
```

Configure a source-based portal-free rule. Set the rule number to 3 and the source interface to aggregate interface 1. This rule allows the portal user on the aggregate interface to access network resources without authentication.

```
[AC] portal free-rule 3 source interface Bridge-Aggregation1
```

Configuring the switch

1. Configure interfaces on the switch:

Create VLAN 100. The switch will use this VLAN to forward traffic on the CAPWAP tunnel between the AC and the AP.

```
<Switch> system-view
[Switch] vlan 100
[Switch-vlan100] quit
```

Create VLAN 200. The switch will use this VLAN to forward client traffic.

```
[Switch] vlan 200
[Switch-vlan200] quit
```

Create VLAN 2.

```
[Switch] vlan 2
[Switch-vlan2] quit
```

Configure GigabitEthernet 1/0/1 (the port connected to the AC) as a trunk port and assign the trunk port to VLAN 1, VLAN 100, and VLAN 200.

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 1 100 200
[Switch-GigabitEthernet1/0/1] quit
```

Configure GigabitEthernet 1/0/2 (the port connected to the AP) as an access port and assign the access port to VLAN 100.

```
[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] port link-type access
[Switch-GigabitEthernet1/0/2] port access vlan 100
```

Enable PoE on the access port.

```
[Switch-GigabitEthernet1/0/2] poe enable
[Switch-GigabitEthernet1/0/2] quit
```

Create VLAN-interface 1 and assign an IPv4 address and an IPv6 address to the VLAN interface.

```
[Switch] interface vlan-interface 1
[Switch-Vlan-interface1] ip address 192.168.3.1 255.255.255.0
[Switch-Vlan-interface1] ipv6 address 2003::1 64
[Switch-Vlan-interface1] quit
```

Create VLAN-interface 100 and assign an IPv4 address and an IPv6 address to the VLAN interface.

```
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ip address 192.168.1.2 255.255.255.0
[Switch-Vlan-interface100] ipv6 address 2001::2 64
[Switch-Vlan-interface100] quit
```

Create VLAN-interface 200 and assign an IPv4 address and an IPv6 address to the VLAN interface.

```
[Switch] interface vlan-interface 200
[Switch-Vlan-interface200] ip address 192.168.2.2 255.255.255.0
[Switch-Vlan-interface200] ipv6 address 2004::2 64
[Switch-Vlan-interface200] quit
```

2. Configure the DHCP server:

Enable DHCP.


```
[Switch] dhcp enable
```

Configure DHCP address pool named **100** and specify subnet 192.168.1.0/24 and gateway address 192.168.1.1 for the DHCP address pool. The switch will assign an IPv4 in this DHCP address pool to the AP.

```
[Switch] dhcp server ip-pool 100
```

```
[Switch-dhcp-pool-100] network 192.168.1.0 mask 255.255.255.0
```

```
[Switch-dhcp-pool-100] gateway-list 192.168.1.1
```

Configure Option 43 that specifies the AC's IPv4 address in hexadecimal notation in DHCP address pool **100**.

```
[Switch-dhcp-pool-100] option 43 hex 8007000001c0a80101
```

```
[Switch-dhcp-pool-100] quit
```

Configure DHCP address pool named **200** and specify subnet 192.168.2.0/24, gateway address 192.168.2.2, and the DNS server address of the wireless client (the same as the gateway address in this example) for the DHCP address pool. The switch will assign an IPv4 address in this DHCP address pool to the client.

```
[Switch] dhcp server ip-pool 200
```

```
[Switch-dhcp-pool-200] network 192.168.2.0 mask 255.255.255.0
```

```
[Switch-dhcp-pool-200] gateway-list 192.168.2.2
```

```
[Switch-dhcp-pool-200] dns-list 192.168.2.2
```

```
[Switch-dhcp-pool-200] quit
```

3. Configure the DHCPv6 server:

Create DHCPv6 address pool named **1** and specify subnet 2001::/64 for the DHCPv6 address pool. The switch will assign an IPv6 address in this DHCP address pool to the AP.

```
[Switch] ipv6 dhcp pool 1
```

```
[Switch-dhcp6-pool-1] network 2001::/64
```

Configure Option 52 that specifies the AC's IPv6 address in DHCPv6 address pool **1**.

```
[Switch-dhcp6-pool-1] option 52 hex 20010000000000000000000000000001
```

```
[Switch-dhcp6-pool-1] quit
```

```
[Switch] ipv6 dhcp server forbidden-address 2001::1
```

Apply DHCPv6 address pool **1** to VLAN-interface 100, and enable the DHCPv6 server on the VLAN interface.

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

```
[Switch-Vlan-interface100] ipv6 dhcp server apply pool 1
```

```
[Switch-Vlan-interface100] ipv6 dhcp select server
```

Set the M flag to 1 and the O flag to 1 in RA advertisements to be sent on VLAN-interface 100.

```
[Switch-Vlan-interface100] ipv6 nd autoconfig managed-address-flag
```

```
[Switch-Vlan-interface100] ipv6 nd autoconfig other-flag
```

Disable RA message suppression.

```
[Switch-Vlan-interface100] undo ipv6 nd ra halt
```

```
[Switch-Vlan-interface100] quit
```

Create DHCPv6 address pool named **2** and specify subnet 2004::/64 for the DHCPv6 address pool. The switch will assign an IPv6 address in this DHCP address pool to the client.

```
[Switch] ipv6 dhcp pool 2
```

```
[Switch-dhcp6-pool-2] network 2004::/64
```

```
[Switch-dhcp6-pool-2] quit
```

Exclude IPv6 address 2004::1 in the DHCPv6 address pool from dynamic allocation.

```
[Switch] ipv6 dhcp server forbidden-address 2004::1
```

Apply DHCPv6 address pool **2** to VLAN-interface 200, and enable the DHCPv6 server on the VLAN interface.

```
[Switch] interface Vlan-interface 200
[Switch-Vlan-interface200] ipv6 dhcp server apply pool 2
[Switch-Vlan-interface200] ipv6 dhcp select server
# Set the M flag to 1 and the O flag to 1 in RA advertisements to be sent on VLAN-interface 200.
[Switch-Vlan-interface200] ipv6 nd autoconfig managed-address-flag
[Switch-Vlan-interface200] ipv6 nd autoconfig other-flag
# Disable RA message suppression.
[Switch-Vlan-interface200] undo ipv6 nd ra halt
[Switch-Vlan-interface200] quit
```

Verifying the configuration

1. Verify that the dual-stack client can access network resources after passing IPv4 portal authentication.
 - a. Use the configured username and password to perform IPv4 portal authentication through a Web browser on the client.
 - b. Verify that all Web requests of the user will be redirected to the portal authentication page (<http://192.168.3.2:8080/portal>) before the client passes IPv4 portal authentication. After the user passes IPv4 portal authentication, the user can access network resources. (Details not shown.)
 - c. Display information about all portal users on the AC after the client passes IPv4 authentication.

```
[AC] display portal user all
Total portal users: 1
Username: client
  AP name: office
  Radio ID: 2
  SSID: service
  Portal server: newptv4
  State: Online
  VPN instance: N/A
```

MAC	IP	VLAN	Interface
3829-5a40-9589	192.168.2.3	200	WLAN-BSS1/0/2

```
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
```

The output shows that the client has come online.

2. Verify that the dual-stack client can access network resources after passing IPv6 portal authentication.
 - a. Use the configured username and password to perform IPv6 portal authentication through a Web browser on the client.
 - b. Verify that all Web accesses of the user are redirected to the portal authentication page ([http://\[2003::2\]:8080/portal](http://[2003::2]:8080/portal)) before the client passes IPv6 portal authentication. After the user passes IPv6 portal authentication, the user can access network resources. (Details not shown.)

- c. Display the online portal user information on the AC after the client passes authentication.

```
[AC] display portal user all
Total portal users: 1
Username: Client
  AP name: office
  Radio ID: 2
  SSID: service
  Portal server: newptv6
  State: Online
  VPN instance: N/A
  MAC              IP              VLAN      Interface
  3829-5a40-9589   2004::4549:7C7F:392E: 200      WLAN-BSS1/0/2
                  EE57
  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
```

The output shows that the client has come online.

Configuration files

- AC:

```
#
vlan 100
#
vlan 200
#
wlan service-template st1
  ssid service
  vlan 200
client forwarding-location ac
akm mode psk
preshared-key pass-phrase cipher $c$3$0Lf6p0Z6bxrf25nodjOJKYEfnZ6g6ErccHyQ
cipher-suite ccmp
security-ie rsn
client ipv6-snooping nd-learning enable
client ipv6-snooping dhcpv6-learning enable
portal enable method direct
portal domain dm1
portal bas-ip 192.168.2.1
portal apply web-server newptv4
portal ipv6 enable method direct
portal ipv6 domain dm2
portal bas-ipv6 2004::1
portal ipv6 apply web-server newptv6
```

```

portal dual-stack enable
service-template enable
#
interface Vlan-interface100
ip address 192.168.1.1 255.255.255.0
ipv6 address 2001::1/64
#
interface Vlan-interface200
ip address 192.168.2.1 255.255.255.0
ipv6 address 2004::1/64
#
interface GigabitEthernet1/0/1
port link-mode bridge
port link-type trunk
port trunk permit vlan 1 100 200
#
ip route-static 192.168.3.0 24 192.168.2.2
ipv6 route-static 2003:: 64 2004::2
#
radius session-control enable
#
radius scheme rs1
primary authentication 192.168.3.2
primary accounting 192.168.3.2
key authentication cipher $c$3$2m4BXR2X65vE59L0SyyHH0tRVpkKDgym9w==
key accounting cipher $c$3$4ieHsnXQVnQ7GwywFS+H0MoQdb6SEmJSRg==
user-name-format without-domain
nas-ip 192.168.1.1
#
radius scheme rs2
primary authentication ipv6 2003::2
primary accounting ipv6 2003::2
key authentication cipher $c$3$8bAMsBFXCGLbmynti08YCxotgTXYwzES0w==
key accounting cipher $c$3$QeTcfxJGTnPJ98PsCSbLnaZP6KAG6q42aQ==
user-name-format without-domain
nas-ip ipv6 2001::1
#
radius dynamic-author server
client ip 192.168.3.2 key cipher $c$3$l9xAyE5vBJQMT0v6quHJFXtZlti404CjBg==
client ipv6 2003::2 key cipher $c$3$ELOjFzKgJUoRbJ/wZX0E9eVdGBFeTQzmHA==
#
domain dm1
authorization-attribute idle-cut 15 1024
authentication portal radius-scheme rs1
authorization portal radius-scheme rs1
accounting portal none
#
domain dm2

```

```

authorization-attribute idle-cut 15 1024
authentication portal radius-scheme rs2
authorization portal radius-scheme rs2
accounting portal none
#
portal host-check enable
portal free-rule 1 destination ip any udp 53
portal free-rule 2 destination ip any tcp 53
portal free-rule 3 source interface Bridge-Aggregation1
#
portal web-server newptv4
url http://192.168.3.2:8080/portal
url-parameter ssid ssid
url-parameter wlanacname value AC
url-parameter wlanuserip source-address
#
portal web-server newptv6
url http://[2003::2]:8080/portal
url-parameter ssid ssid
url-parameter wlanacname value AC
url-parameter wlanuserip source-address
#
portal server newptv4
ip 192.168.3.2 key cipher $c$3$XkIMNqFj0It2yZOqdfPeOeasD0Jk4oJQFA==
#
portal server newptv6
ipv6 2003::2 key cipher $c$3$9MzqVffe//Ma5x4a4gJOSQKrnsBS5Es1Xg==
#
wlan ap-group group1
ap office
ap-model AP 3620
radio 1
radio 2
radio enable
service-template st1
#
wlan ap office model AP 3620
serial-id 219801A28N819CE0002T
#
return

```

- **Switch:**

```

#
ipv6 dhcp server forbidden-address 2001::1
ipv6 dhcp server forbidden-address 2004::1
#
vlan 1
#
vlan 100

```

```

#
vlan 200
#
dhcp server ip-pool 100
    gateway-list 192.168.1.1
    network 192.168.1.0 mask 255.255.255.0
    option 43 hex 8007000001c0a80101
#
dhcp server ip-pool 200
    gateway-list 192.168.2.2
    network 192.168.2.0 mask 255.255.255.0
    dns-list 192.168.2.2
#
ipv6 dhcp pool 1
    network 2001::/64
    option 52 hex 20010000000000000000000000000001
#
ipv6 dhcp pool 2
    network 2004::/64
#
interface Vlan-interface1
    ip address 192.168.3.1 255.255.255.0
    ipv6 address 2003::1/64
#
interface Vlan-interface100
    ip address 192.168.1.2 255.255.255.0
    ipv6 dhcp select server
    ipv6 dhcp server apply pool 1
    ipv6 address 2001::2/64
    ipv6 nd autoconfig managed-address-flag
    ipv6 nd autoconfig other-flag
    undo ipv6 nd ra halt
#
interface Vlan-interface200
    ip address 192.168.2.2 255.255.255.0
    ipv6 dhcp select server
    ipv6 dhcp server apply pool 2
    ipv6 address 2004::2/64
    ipv6 nd autoconfig managed-address-flag
    ipv6 nd autoconfig other-flag
    undo ipv6 nd ra halt
#
interface GigabitEthernet1/0/1
    port link-type trunk
    port trunk permit vlan 1 100 200
#
interface GigabitEthernet1/0/2
    port access vlan 100

```

```
poe enable
#
Return
```

Related documentation

- *AP and WT Management Command Reference in INTELBRAS Access Controllers Command References*
- *AP and WT Management Configuration Guide in INTELBRAS Access Controllers Configuration Guides*
- *User Access and Authentication Command Reference in INTELBRAS Access Controllers Command References*
- *User Access and Authentication Configuration Guide in INTELBRAS Access Controllers Configuration Guides*
- *WLAN Access Command Reference in INTELBRAS Access Controllers Command References*
- *WLAN Access Configuration Guide in INTELBRAS Access Controllers Configuration Guides*

INTELBRAS Access Controllers

Portal MAC-Trigger Authentication (IPv6)

Configuration Examples

Copyright © 2024 Intelbras S.A All rights reserved.

No part of this manual may be reproduced or transmitted in any form or by any means without prior written consent of Intelbras S.A

Except for the trademarks of Intelbras S.A, any trademarks that may be mentioned in this document are the property of their respective owners.

The information in this document is subject to change without notice.

Contents

Introduction	1
Prerequisites	1
Example: Configuring IPv6 portal MAC-trigger authentication	1
Network configuration	1
Analysis	2
Restrictions and guidelines	2
Procedures	3
Configuring INC	3
Editing a configuration file for the AP	11
Configuring the AC	11
Configuring the switch	16
Verifying the configuration	17
Configuration files	18
Related documentation	21

Introduction

The following information provides examples for configuring IPv6 portal MAC-trigger authentication (also called MAC-based quick portal authentication or transparent portal authentication).

Prerequisites

The following information applies to Comware-based access controllers and access points. Procedures and information in the examples might be slightly different depending on the software or hardware version of the access controllers and access points.

The configuration examples 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.

The following information is provided based on the assumption that you have basic knowledge of AAA, portal, and WLAN.

Example: Configuring IPv6 portal MAC-trigger authentication

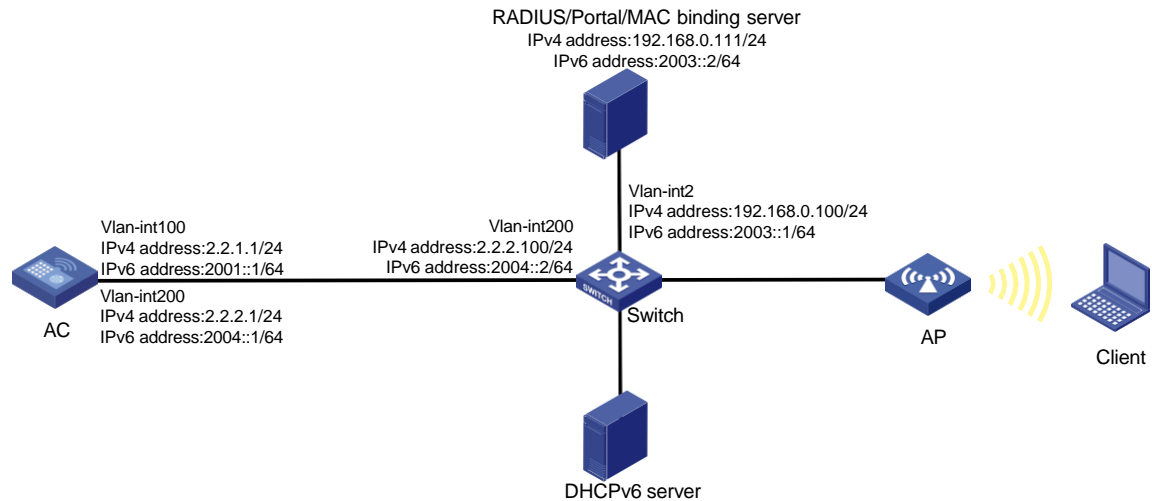
Network configuration

As shown in [Figure 1](#), the AP and the client obtain IP addresses and IPv6 addresses from the DHCP server and the DHCPv6 server, respectively. The INC server acts a portal authentication server, a portal Web server, a MAC binding server, and a RADIUS server.

Configure direct portal authentication and MAC-trigger authentication to meet the following requirements:

- The client can access only the portal Web servers before passing portal authentication and can access other network resources after passing portal authentication.
- The client can access the network resources through any Layer 2 ports in its access VLAN without re-authentication.
- The RADIUS server can dynamically change the user authorization information or forcibly disconnect users.

Figure 1 Network diagram



Analysis

To implement IPv6 portal MAC-trigger authentication, assign both IPv4 and IPv6 addresses to the AC, the client, and the INC server. Make sure both IPv4 and IPv6 routes between them are reachable.

For the client to access network resources through any Layer 2 ports in its access VLAN without re-authentication, enable portal roaming.

For the RADIUS server to dynamically change the user authorization information or forcibly disconnect users, enable the RADIUS session-control feature.

To use GigabitEthernet 1/0/1 on the AP to forward client traffic, edit a .txt configuration file and upload the file to the AC.

To ensure that dynamic user authorization information can be correctly assigned to users after they come online, enable the RADIUS DAS feature.

To allow portal users to access both IPv4 and IPv6 networks after passing one type (IPv4 or IPv6) of portal authentication, enable portal to support IPv4/IPv6 dual stack.

To view the IPv6 address of the client on the AC, enable ND snooping and DHCPv6 snooping.

Configure DNS if necessary. In this example, DNS is not required.

Restrictions and guidelines

When you configure IPv6 portal MAC-trigger authentication, follow these restrictions and guidelines:

- Use the actual serial ID of an AP to uniquely identify that AP.
- Make sure the types of the portal authentication servers, portal Web servers, and MAC binding server specified on the AC are the same as those actually used.
- By default, the URL of the portal Web server to which the AC redirects portal users does not carry any parameters. You can add parameters to be carried in the URL as needed.
- If portal authentication is enabled on a VLAN interface, only the AC can forward client traffic. If portal authentication is enabled on a service template, both the AC and the AP can forward client traffic. (In this example, portal authentication is enabled on a service template.)

- If you have set the free-traffic threshold, portal clients cannot automatically push portal authentication pages and portal users need to manually open a browser to open the pages. Do not set the free-traffic threshold if you want portal clients to automatically push portal authentication pages.
- Some types of endpoints use random MAC by default, which might cause failure of the MAC-trigger authentication. As a best practice, disable the random MAC feature on the endpoints.

Procedures

Configuring INC

This example uses the INC server to describe the RADIUS server, portal server, and MAC binding server configuration. The INC server runs on INC PLAT 7.1 (E0303), INC INC - EIA 7.1 (E0304), and INC EIP 7.1 (E0304).

Configuring the RADIUS server

Add the AC to INC as an IPv4 access device and an IPv6 access device:

1. Log in to INC and click the **User** tab.
2. From the navigation tree, select **User Access Policy > Access Device Management > Access Device**.
3. Click **Add** to open the page as shown in [Figure 2](#).
4. In the **Access Configuration** area, set the shared key to **radius**, which must be the same as that on the AC.
5. In the **Device List** area, perform the following operations:
 - a. Click **Add Manually** to open the **Add Access Device Manually** page. Enter the start IPv4 address **2.2.2.1** and then click **OK**.
 - b. Click **Add IPv6 Dev** to open the **Add Access Device Manually** page. Enter the start IPv6 address **2001::1** and then click **OK**.
6. Use the default values for other parameters.
7. Click **OK**.

Figure 2 Adding the AC as an IPv4 access device

User > User Access Policy > Access Device Management > Access Device > Add Access Device

Access Configuration

Authentication Port *	1812	Accounting Port *	1813
Service Type	LAN Access Service		
Access Device Type	H3C(General)	Service Group	Ungrouped
Shared Key *	*****	Confirm Shared Key *	*****
Access Device Group	--		
Certificate Authentication	<input checked="" type="radio"/> None <input type="radio"/> EAP		
Certificate Type	EAP-TLS Authn		

Device List

Select Add Manually Add IPv6 Dev Clear All

Device Name	Device IP	Device Model	Comments	Delete
	2.2.2.1			

Total Items: 1.

OK Cancel

Figure 3 Adding the AC as an IPv6 access device

User > User Access Policy > Access Device Management > Access Device > Add Access Device

Access Configuration

Authentication Port *	1812	Accounting Port *	1813
Service Type	LAN Access Service		
Access Device Type	H3C(General)	Service Group	Ungrouped
Shared Key *	*****	Confirm Shared Key *	*****
Access Device Group	--		
Certificate Authentication	<input checked="" type="radio"/> None <input type="radio"/> EAP		
Certificate Type	EAP-TLS Authn		

Device List

Select Add Manually Add IPv6 Dev Clear All

Device Name	Device IP	Device Model	Comments	Delete
	2001:0000:0000:0000:0000:0000:0000:0001			

Total Items: 1.

OK Cancel

Configuring the portal server

1. Configure the portal authentication service:
 - a. Click the **User** tab.
 - b. From the navigation tree, select **User Access Policy > Portal Service > Server** to open the portal server configuration page, as shown in [Figure 4](#).
 - c. Configure the portal server parameters as needed.
This example uses the default values.

d. Click **OK**.

Figure 4 Portal authentication server configuration

User > User Access Policy > Portal Service > Server

Portal Server

Basic Information

Log Level * Info

Portal Server

Request Timeout(Seconds) * 4

User Heartbeat Interval(Minutes) * 5

LB Device IP Address

Server Heartbeat Interval(Seconds) * 20

LB Device Address

Portal Web

Request Timeout(Seconds) * 15

Verify Endpoint Requests Yes

HTTP Heartbeat Display New Page

Packet Code

Use Cache Yes

HTTPS Heartbeat Display Original Page

Portal Page

Advanced Information

Service Type List

Add

Total Items: 0.

Service Type ID	Service Type	Delete
No match found.		

OK

2. Configure an IPv4 group and an IPv6 group:

a. From the navigation tree, select **User Access Policy > Portal Service > IP Group**.

b. Click **Add**.

The **Add IP Group** page opens.

c. Enter an IP group name.

d. To add an IPv4 group, select **No** from the **IPv6** field.

e. To add an IPv6 group, select **Yes** from the **IPv6** field.

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

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

g. Select a service group.

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

h. Select **Normal** from the **Action** field.

This step is required only when you add an IPv4 address group.

i. Click **OK**.

Figure 5 Adding an IPv4 group

The screenshot shows the 'Add IP Group' form in a web interface. The breadcrumb navigation at the top is 'User > User Access Policy > Portal Service > IP Group > Add IP Group'. The form title is 'Add IP Group'. The fields are as follows:

IP Group Name *	Portal_user4
IPv6 *	No
Start IP *	192.168.2.1
End IP *	192.168.2.255
Service Group	Ungrouped
Action *	Normal

At the bottom right, there are 'OK' and 'Cancel' buttons.

Figure 6 Adding an IPv6 group

The screenshot shows the 'Add IP Group' form in a web interface. The breadcrumb navigation at the top is 'User > User Access Policy > Portal Service > IP Group > Add IP Group'. The form title is 'Add IP Group'. The fields are as follows:

IP Group Name *	Portal_userv6
IPv6 *	Yes
Start IP *	2004::1
End IP *	2004::255
Service Group	Ungrouped

At the bottom right, there are 'OK' and 'Cancel' buttons.

3. Add the portal device:
 - a. From the navigation tree, select **User Access Policy > Portal Service > Device**.
 - b. Click **Add**.

The **Add Device** page opens.
 - c. Enter the device name.
 - d. Select a portal version.

For an IPv4 portal device, select **Portal 2.0**. For an IPv6 portal device, select **Portal 3.0**.
 - e. Enter the IP address of the AC's interface connected to the client.
 - f. 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**.
 - g. Enter the key, which must be the same as that configured on the AC.
 - h. Select **Directly Connected** for **Access Method**.
 - i. Use the default settings for other parameters.
 - j. Click **OK**.

Figure 7 Adding an IPv4 portal device

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

Add Device

Device Information

Device Name *	NAS	Service Group *	Ungrouped
Version *	Portal 2.0	IP Address *	2.2.2.1
Listening Port *	2000	Local Challenge *	No
Authentication Retries *	0	Logout Retries *	1
Support Server Heartbeat *	No	Support User Heartbeat *	No
Key *	*****	Confirm Key *	*****
Access Method *	Directly Conne		
Device Description			

OK Cancel

Figure 8 Adding an IPv6 portal device

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

Add Device

Device Information

Device Name *	NASv6	Service Group *	Ungrouped
Version *	Portal 3.0	IP Address *	2004::1
Listening Port *	2000	Local Challenge *	No
Authentication Retries *	0	Logout Retries *	1
Support Server Heartbeat *	No	Support User Heartbeat *	No
Key *	*****	Confirm Key *	*****
Access Method *	Directly Conne		
Device Description			

OK Cancel

4. Associate a portal device with an IP group:
 - a. In the device list page, click the **Port Group** icon  in the **Operation** field for a portal device to open the port group configuration page.

Figure 9 IPv4 device list


User > User Access Policy > Portal Service > Device

Query Devices

Device Name: Version:
Deploy Result: Service Group:

Query Reset

Add

Device Name	Version	Service Group	IP Address	IPv6 Address	Last Deployed at	Deploy Result	Operation
NAS	Portal 2.0	Ungrouped	2.2.2.1			Not Deployed	

1-1 of 1. Page 1 of 1.

Figure 10 IPv6 device list

User > User Access Policy > Portal Service > Device

Query Devices

Device Name: Version:
Deploy Result: Service Group:

Query Reset

Add

Device Name	Version	Service Group	IP Address	IPv6 Address	Last Deployed at	Deploy Result	Operation
NASv6	Portal 3.0	Ungrouped		2004::1		Not Deployed	

1-1 of 1. Page 1 of 1.

- b. Click **Add** to open the **Add Port Group** page.
 - Enter the port group name.
 - Select the configured IP group.

- The IP address used by the user to access the network must be within this IP group.
- Select **Supported** for **Transparent Authentication**.
- Use the default settings for other parameters.

c. Click **OK**.

Figure 11 Adding an IPv4 port group

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

Add Port Group

Port Group Name *	group	Language *	English
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(Minutes) *	10	Heartbeat Timeout(Minutes) *	30
User Domain		Port Group Description	
Transparent Authentication	Supported	Client Protection Against Cracks *	No
Page Push Policy		Default Authentication Page	

OK Cancel

Figure 12 Adding an IPv6 port group

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

Add Port Group

Port Group Name *	groupv6	Language *	English
Start Port *	0	End Port *	zzzzzz
Protocol *	HTTP	Quick Authentication *	No
NAT or Not *	No	Error Transparent Transmission *	Yes
Authentication Type *	PAP	IP Group *	Portal_user6
Heartbeat Interval(Minutes) *	0	Heartbeat Timeout(Minutes) *	0
User Domain		Port Group Description	
Transparent Authentication	Supported	Client Protection Against Cracks *	No
Page Push Policy		Default Authentication Page	

OK Cancel

5. From the navigation tree, select **User Access Policy > Service Parameters > Validate System Configuration** to commit the configuration changes.

Configuring the MAC binding server

1. Add an access policy:
 - a. From the navigation tree, select **User Access Policy > Access Policy**.
 - b. Click **Add** to open the page as shown in [Figure 13](#).
 - c. Enter the access policy name.
 - d. Select a service group.
This example uses the default value **Ungrouped**.
 - e. Use the default settings for other parameters.
 - f. Click **OK**.

Figure 13 Adding an access policy

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

Basic Information

Access Policy Name * AccessPolicy

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 Auth!

Deploy VLAN

☐ Deploy User Profile

Deploy User Group

☐ Deploy ACL

2. Add an access service:
 - a. From the navigation tree, select **User Access Policy > Access Service**.
 - b. Click **Add** to open the page as shown in [Figure 14](#).
 - c. Enter the service name.
 - d. Select a default access policy.
 - e. Select the **Transparent Authentication on Portal Endpoints** option.
 - f. Use the default settings for other parameters.
 - g. Click **OK**.

Figure 14 Adding an access service

User > User Access Policy > Access Service > Modify Access Service

Basic Information

Service Name * MAC_server

Service Suffix

Service Group * Ungrouped

Default Access Policy * AccessPolicy

Default Proprietary Attribute Assignment Policy * Do not use

Default Max. Number of Bound Endpoints * 0

Default Max. Number of Online Endpoints * 0

Description

☒ Available

☒ Transparent Authentication on Portal Endpoints

3. Add an access user:
 - a. From the navigation tree, select **Access User > All Access Users**.
 - b. Click **Add** to open the page as shown in [Figure 15](#).
 - c. Click **Select** to select an existing access user or click **Add User** to add a new access user.
 - d. Enter the account name.
 - e. Set the password.
 - f. Select a value from the **Max. Transparent Portal Bindings** list.
 - g. Use the default settings for other parameters.
 - h. Click **OK**.

Figure 15 Adding an access user

The screenshot shows the 'Add Access User' form. At the top, the breadcrumb is 'User > All Access Users > Add Access User'. The form is titled 'Access account' and 'Access Information'. It contains the following fields and options:

- User Name ***: Text input with 'Client1', a 'Select' button, and an 'Add User' button.
- Account Name ***: Text input with 'Client'.
- Trial Account**: ☐
- Default BYOD User**: ☐
- MAC Authentication User**: ☐
- Computer User**: ☐
- Fast Access User**: ☐
- Password ***: Password input with '.....'.
- Confirm Password ***: Password input with '.....'.
- Allow User to Change Password**: ☒
- Enable Password Strategy**: ☐
- Modify Password at Next Login**: ☐
- Inspiration Time**: Text input with a calendar icon.
- Expiration Time**: Text input with a calendar icon.
- Max. Idle Time(Minutes)**: Text input.
- Max. Concurrent Logins**: Text input with '1'.
- Max. Transparent Portal Bindings**: Dropdown menu with '1'.
- Login Message**: Text area.

4. Configure system parameters:

- From the navigation tree, select **User Access Policy > Service Parameters > System Settings**.
- Click the **Configure** icon for **User Endpoint Settings** to open the page as shown in [Figure 16](#).
- Select whether to enable transparent portal authentication on non-smart devices.
In this example, select **Enable** for **Non-Terminal Authentication**.
- Click **OK**.

Figure 16 Configuring user endpoint settings

The screenshot shows the 'User Endpoint Settings' form. The breadcrumb is 'User > User Access Policy > Service Parameters > System Settings > User Endpoint Settings'. The form contains the following fields and options:

- Transparent MAC Authentication**: Dropdown menu with 'Disable'.
- Max. Device for Single Account ***: Text input with '10'.
- Non-Terminal Authentication**: Dropdown menu with 'Enable' and a help icon.
- Log off User with Endpoint Conflict**: Dropdown menu with 'No'.

At the bottom, there are 'OK' and 'Cancel' buttons.

- Click the **Configure** icon for **Endpoint Aging Time** to open the page as shown in [Figure 17](#).
- Set the endpoint aging time as needed.
This example uses the default value.
- Click **OK**.

Figure 17 Setting the endpoint aging time

The screenshot shows the 'Modify Endpoint Aging Time' form. The breadcrumb is 'User > User Access Policy > Service Parameters > System Settings > Endpoint Aging Time > Modify Endpoint Aging Time'. The form contains the following field:

- Endpoint Aging Time(Days) ***: Text input with '7' and a help icon.

At the bottom, there are 'OK' and 'Cancel' buttons.

5. From the navigation tree, select **User Access Policy > Service Parameters > Validate System Configuration** to commit the configuration changes.

Editing a configuration file for the AP

Create a .txt configuration file named **map.txt**.

Enter the following content in the file.

```
System-view
vlan 200
interface gigabitethernet1/0/1
port link-type trunk
port trunk permit vlan 200
```

Upload the file to the AC.

Configuring the AC

1. Configure interfaces on the AC:

Create VLAN 100 and VLAN-interface 100, and assign an IPv4 address and an IPv6 address to the VLAN interface. The AC will establish a CAPWAP tunnel with the AP in this VLAN.

```
<AC> system-view
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 2.2.1.1 24
[AC-Vlan-interface100] ipv6 address 2001::1 64
```

Configure VLAN-interface 100 not to suppress RA message advertisement.

```
[AC-Vlan-interface100] undo ipv6 nd ra halt
```

Set the managed address configuration flag (M) to 1 in RA advertisements to be sent on VLAN-interface 100.

```
[AC-Vlan-interface100] ipv6 nd autoconfig managed-address-flag
```

Set the O flag to 1 in RA advertisements to be sent on VLAN-interface 100.

```
[AC-Vlan-interface100] ipv6 nd autoconfig other-flag
[AC-Vlan-interface100] quit
```

Create VLAN 200 and VLAN-interface 200, and assign an IPv4 address and an IPv6 address to the VLAN interface. The AC will use VLAN 200 for client access.

```
[AC] vlan 200
[AC-vlan200] quit
[AC] interface vlan-interface 200
[AC-Vlan-interface200] ip address 2.2.2.1 24
[AC-Vlan-interface200] ipv6 address 2004::1 64
```

Configure VLAN-interface 200 not to suppress RA message advertisement.

```
[AC-Vlan-interface200] undo ipv6 nd ra halt
```

Set the managed address configuration flag (M) to 1 in RA advertisements to be sent on VLAN-interface 200.

```
[AC-Vlan-interface200] ipv6 nd autoconfig managed-address-flag
```

Set the O flag to 1 in RA advertisements to be sent on VLAN-interface 200.

```
[AC-Vlan-interface200] ipv6 nd autoconfig other-flag
[AC-Vlan-interface200] quit
```

Configure GigabitEthernet 1/0/1 (the interface connected to the switch) as a trunk port and assign it to VLAN 100 and VLAN 200.

```
[AC] interface gigabitethernet 1/0/1
[AC-GigabitEthernet1/0/1] port link-type trunk
[AC-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[AC-GigabitEthernet1/0/1] quit
```

2. Configure a static IPv4 route and a static IPv6 route to the INC server.

```
[AC] ip route-static 192.168.0.0 255.255.0.0 2.2.2.100
[AC] ipv6 route-static 2003:: 64 2004::2
```

3. Configure a WLAN service:

Create a service template named **st1** and enter its view.

```
[AC] wlan service-template st1
```

Set the SSID of service template **st1** to **service**.

```
[AC-wlan-st-st1] ssid service
```

Assign clients coming online through service template **st1** to VLAN 200.

```
[AC-wlan-st-st1] vlan 200
```

Configure APs to forward client data traffic from all VLANs.

```
[AC-wlan-st-st1] client forwarding-location ap
[AC-wlan-st-st1] quit
```

4. Configure the AP:

NOTE:

In large-scale networks, configure AP groups instead of single APs as a best practice.

Create an AP named **ap1** with model **AP 3620** and set its serial ID to 219801A28N819CE0002T.

```
[AC] wlan ap ap1 model AP 3620
[AC-wlan-ap-ap1] serial-id 219801A28N819CE0002T
```

Create an AP group named **group1** and add AP **ap1** to the AP group.

```
[AC] wlan ap-group group1
[AC-wlan-ap-group-group1] ap ap1
```

Create an AP model named AP 3620 in AP group **group1** and then deploy configuration file **map.txt** to the AP.

```
[AC-wlan-ap-group-group1] ap-model AP 3620
[AC-wlan-ap-group-group1-ap-model-AP 3620] map-configuration
map.txt # Enter the AP group's radio 2 view, and bind service template st1
to radio 2. [AC-wlan-ap-group-group1-ap-model-AP 3620] radio 2
[AC-wlan-ap-group-group1-ap-model-AP 3620-radio-2] service-template st1
```

Enable radio 2.

```
[AC-wlan-ap-group-group1-ap-model-AP 3620-radio-2] radio
enable [AC-wlan-ap-group-group1-ap-model-AP 3620-radio-2]
return
```

5. Configure an IPv4 RADIUS scheme:

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

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

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

```
[AC-radius-rs1] primary authentication 192.168.0.111
```

```
[AC-radius-rs1] primary accounting 192.168.0.111
[AC-radius-rs1] key authentication simple radius
[AC-radius-rs1] key accounting simple radius
```

Configure the AC to remove the domain name from the usernames sent to the RADIUS servers.

```
[AC-radius-rs1] user-name-format without-domain
```

Specify IP address 2.2.2.1 as the source IP address for outgoing RADIUS packets.

```
[AC-radius-rs1] nas-ip 2.2.2.1
[AC-radius-rs1] quit
```

Enable RADIUS session-control.

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

Enable the RADIUS DAS feature and enter RADIUS DAS view.

```
[AC] radius dynamic-author server
```

Specify a session-control client with IP address 192.168.0.111 and shared key **radius in plaintext form.**

```
[AC-radius-da-server] client ip 192.168.0.111 key simple radius
[AC-radius-da-server] quit
```

6. Configure an IPv6 RADIUS scheme:

Create a RADIUS scheme named **rs2 and enter its view.**

```
[AC] radius scheme rs2
```

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

```
[AC-radius-rs2] primary authentication ipv6 2003::2
[AC-radius-rs2] primary accounting ipv6 2003::2
[AC-radius-rs2] key authentication simple radius
[AC-radius-rs2] key accounting simple radius
```

Configure the AC to remove the domain name from the usernames sent to the RADIUS servers.

```
[AC-radius-rs2] user-name-format without-domain
```

Specify IPv6 address 2004::1 as the source IPv6 address for outgoing RADIUS packets.

```
[AC-radius-rs1] nas-ip ipv6 2004::1
[AC-radius-rs2] quit
```

Enter RADIUS DAS view.

```
[AC] radius dynamic-author server
```

Specify a session-control client with IPv6 address 2003::2 and shared key **radius in plaintext form.**

```
[AC-radius-da-server] client ipv6 2003::2 key simple radius
[AC-radius-da-server] quit
```

7. Configure an IPv4 authentication domain:

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

```
[AC] domain dm1
```

Configure the authentication and authorization methods as RADIUS and the accounting method as none in the ISP domain.

```
[AC-isp-dm1] authentication portal radius-scheme rs1
[AC-isp-dm1] authorization portal radius-scheme rs1
[AC-isp-dm1] accounting portal none
```

Configure the idle cut feature for users in the ISP domain. Log out a user if the user's traffic is less than 1024 bytes in 15 minutes.

```
[AC-isp-dm1] authorization-attribute idle-cut 15 1024
[AC-isp-dm1] quit
```

8. Configure an IPv6 authentication domain:

Create an ISP domain named **dm2 and enter its view.**

```
[AC] domain dm2
```

Configure the authentication and authorization methods as RADIUS and the accounting method as none in the ISP domain.

```
[AC-isp-dm2] authentication portal radius-scheme rs2
[AC-isp-dm2] authorization portal radius-scheme rs2
[AC-isp-dm2] accounting portal none
```

Configure the idle cut feature for users in the ISP domain. Log out a user if the user's traffic is less than 1024 bytes in 15 minutes.

```
[AC-isp-dm2] authorization-attribute idle-cut 15 1024
[AC-isp-dm2] quit
```

9. Configure portal authentication:

Create an IPv4 portal authentication server named **newptv4, and specify IPv4 address 192.168.0.111 for the authentication server.**

```
[AC] portal server newptv4
[AC-portal-server-newptv4] ip 192.168.0.111 key simple 123456
[AC-portal-server-newptv4] quit
```

Create an IPv6 portal authentication server named **newptv6, and specify IPv6 address 2003::2 for the authentication server.**

```
[AC] portal server newptv6
[AC-portal-server-newptv6] ipv6 2003::2 key simple 123456
[AC-portal-server-newptv6] quit
```

Specify **http://192.168.0.111:8080/portal as the URL of IPv4 portal Web server **newptv4**.**

```
[AC] portal web-server newptv4
[AC-portal-websvr-newptv4] url http://192.168.0.111:8080/portal
```

Configure the portal redirection URL to carry the **ssid, **wlanuserip**, and **wlanacname** parameters, and their values are the AP's SSID, the user's IP address, and the AC's name.**

```
[AC-portal-websvr-newptv4] url-parameter ssid ssid
[AC-portal-websvr-newptv4] url-parameter wlanuserip source-address
[AC-portal-websvr-newptv4] url-parameter wlanacname value AC
[AC-portal-websvr-newptv4] quit
```

Specify **http://[2003::2]:8080/portal as the URL of IPv6 portal Web server **newptv6**.**

```
[AC] portal web-server newptv6
[AC-portal-websvr-newptv6] url http://[2003::2]:8080/portal
```

Configure the portal redirection URL to carry the **ssid, **wlanuserip**, and **wlanacname** parameters, and their values are the AP's SSID, the user's IP address, and the AC's name.**

```
[AC-portal-websvr-newptv6] url-parameter ssid ssid
[AC-portal-websvr-newptv6] url-parameter wlanuserip source-address
[AC-portal-websvr-newptv6] url-parameter wlanacname value AC
[AC-portal-websvr-newptv6] quit
```

Enable portal roaming.

```
[AC] portal roaming enable
```

Enable validity check on wireless portal clients.

```
[AC] portal host-check enable
```

Enable direct IPv4 portal authentication and direct IPv6 portal authentication on service template **st1**.

```
[AC] wlan service-template st1
[AC-wlan-st-st1] portal enable method direct
[AC-wlan-st-st1] portal ipv6 enable method direct
```

Enable snooping ND packets and snooping DHCPv6 packets on service template **st1**.

```
[AC-wlan-st-st1] client ipv6-snooping nd-learning enable
[AC-wlan-st-st1] client ipv6-snooping dhcpv6-learning enable
```

Specify ISP domain **dm1** as the portal authentication domain for IPv4 portal users.

```
[AC-wlan-st-st1] portal domain dm1
```

Specify ISP domain **dm2** as the portal authentication domain for IPv6 portal users.

```
[AC-wlan-st-st1] portal domain dm2
```

Specify IPv4 portal Web server **newptv4** and IPv6 portal Web server **newptv6** on service template **st1** for portal authentication.

```
[AC-wlan-st-st1] portal apply web-server newptv4
[AC-wlan-st-st1] portal ipv6 apply web-server newptv6
```

Enable portal to support IPv4/IPv6 dual stack on service template **st1**.

```
[AC-wlan-st-st1] portal dual-stack enable
```

Configure the BAS-IP attribute as 2.2.2.1 and the BAS-IPv6 attribute as 2004::1.

```
[AC-wlan-st-st1] portal bas-ip 2.2.2.1
[AC-wlan-st-st1] portal bas-ipv6 2004::1
[AC-wlan-st-st1] quit
```

Configure two destination-based portal-free rules to permit the traffic destined for the DNS server.

```
[AC] portal free-rule 1 destination ip any udp 53
[AC] portal free-rule 2 destination ip any tcp 53
```

Configure a source-based portal-free rule. Set the rule number to 3 and the source interface to aggregate interface 1. This rule allows the portal user on the aggregate interface to access network resources without authentication.

```
[AC] portal free-rule 3 source interface Bridge-Aggregation1
```

10. Configure MAC-based quick portal authentication:

Create a MAC binding server named **mts** and enter its view.

```
[AC] portal mac-trigger-server mts
```

Specify 192.168.0.111 as the IPv4 address of MAC binding server **mts**.

```
[AC-portal-mac-trigger-server-mts] ip 192.168.0.111
[AC-portal-mac-trigger-server-mts] quit
```

Specify MAC binding server **mts** on service template **st1**.

```
[AC] wlan service-template st1
[AC-wlan-st-st1] portal apply mac-trigger-server mts
```

Configure the AKM mode as PSK, and set the preshared key to 12345678 in plain text.

```
[AC-wlan-st-st1] akm mode psk
[AC-wlan-st-st1] preshared-key pass-phrase simple 12345678
```

Configure the cipher suite as CCMP and security IE as RSN.

```
[AC-wlan-st-st1] cipher-suite ccmp
[AC-wlan-st-st1] security-ie rsn
```

Enable service template **st1**.

```
[AC-wlan-st-service1] service-template enable
[AC-wlan-st-st1] quit
```


Configuring the switch

Create VLAN 100. The switch will use this VLAN to forward traffic on the CAPWAP tunnel between the AC and the AP.

```
<Switch> system-view
[Switch] vlan 100
[Switch-vlan100] quit
```

Create VLAN 200. The switch will use this VLAN to forward client traffic.

```
[Switch] vlan 200
[Switch-vlan200] quit
```

Create VLAN 2.

```
[Switch] vlan 2
[Switch-vlan2] quit
```

Configure GigabitEthernet 1/0/1 (the interface connected to the AC) as a trunk port and assign the port to VLAN 100 and VLAN 200.

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[Switch-GigabitEthernet1/0/1] quit
```

Configure GigabitEthernet 1/0/2 (the interface connected to the AP) as a trunk port and assign it to VLAN 100 and VLAN 200.

```
[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] port link-type trunk
[Switch-GigabitEthernet1/0/2] port trunk permit vlan 100 200
[Switch-GigabitEthernet1/0/2] port trunk pvid vlan 100
```

Enable PoE on GigabitEthernet 1/0/2.

```
[Switch-GigabitEthernet1/0/2] poe enable
[Switch-GigabitEthernet1/0/2] quit
```

Configure GigabitEthernet 1/0/3 (the interface connected to the RADIUS server) as an access port and assign it to VLAN 2.

```
[Switch] interface gigabitethernet 1/0/3
[Switch-GigabitEthernet1/0/3] port link-type access
[Switch-GigabitEthernet1/0/3] port access vlan 2
[Switch-GigabitEthernet1/0/3] quit
```

Assign an IPv4 address and an IPv6 address to VLAN-interface 200.

```
[Switch] interface vlan-interface 200
[Switch-Vlan-interface200] ip address 2.2.2.100 255.255.255.0
[Switch-Vlan-interface200] ipv6 address 2004::2 64
[Switch-Vlan-interface200] quit
```

Assign an IPv4 address and an IPv6 address to VLAN-interface 2.

```
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] ip address 192.168.0.100 255.255.255.0
[Switch-Vlan-interface2] ipv6 address 2003::1 64
[Switch-Vlan-interface2] quit
```

Verifying the configuration

Display information about MAC binding server mts.

```
[AC] display portal mac-trigger-server name mts
```

```
Portal mac trigger server name: mts
```

```
Version           : 1.0
Server type       : INC
IP                : 192.168.0.111
Port              : 50100
VPN instance      : Not configured
Aging time        : 300 seconds
Free-traffic threshold : 0 bytes
NAS-Port-Type     : Not configured
Binding retry times : 3
Binding retry interval : 1 seconds
Authentication timeout : 3 minutes
Local-binding     : Disabled
Local-binding aging-time : 720 minutes
aaa-fail nobinding : Disabled
Excluded attribute list : Not configured
Cloud-binding     : Disabled
Cloud-server URL  : Not configured
```

A user uses the configured username and password to perform portal authentication through a Web browser on the client. Before passing authentication, all Web accesses are redirected to the portal authentication page (**<http://192.168.0.111:8080/portal>**). After passing authentication, the user can access other network resources. (Details not shown.)

The user goes offline and then accesses the network again, the user does not need to enter the authentication username and password. (Details not shown.)

Display information about all portal users.

```
[AC] display portal user all verbose
```

```
Total portal users: 1
```

```
Basic:
```

```
AP name: ap1
Radio ID: 1
SSID: service
Current IP address: 2.2.2.13
Original IP address: 2.2.2.13
Username: 4C:49:E3:F8:CC:9D
User ID: 0x1000002d
Access interface: WLAN-BSS1/0/17
Service-VLAN/Customer-VLAN: 200/-
MAC address: 4c49-e3f8-cc9d
Authentication type: MAC-trigger
Domain name: dm
VPN instance: N/A
Status: Online
Portal server: newpt
Vendor: Xiaomi
```

```

Portal authentication method: Direct
AAA:
  Realtime accounting interval: 720s, retry times: 5
  Idle cut: N/A
  Session duration: 86400 sec, remaining: 86385 sec
  Remaining traffic: N/A
  Login time: 2018-08-10 17:13:58 Brasilia
  Online time(hh:mm:ss): 00:00:15
  DHCP IP pool: N/A
ACL&QoS&Multicast:
  Inbound CAR: N/A
  Outbound CAR: N/A
  ACL number: N/A
  User profile: N/A
  Session group profile: N/A
  Max multicast addresses: 4
Flow statistic:
  Uplink   packets/bytes: 18/5595
  Downlink packets/bytes: 18/1971
Dual stack flow statistic:
  Ipv4 address: 2.2.2.13
                uplink   packets/bytes: 18/5595
                downlink packets/bytes: 18/1971
  Ipv6 address: 2004::10
                uplink   packets/bytes: 0/0
                downlink packets/bytes: 0/0

```

The output shows that the user is online.

Configuration files

- AC:


```

#
vlan 100
#
vlan 200
#
wlan service-template st1
  ssid service
  akm mode psk
  preshared-key pass-phrase simple 12345678
  cipher-suite ccmp
  security-ie rsn
vlan 200
  client forwarding-location ap
  client ipv6-snooping nd-learning enable
  client ipv6-snooping dhcpv6-learning enable
portal enable method direct
portal domain dm1

```

```

portal bas-ip 2.2.2.1
portal apply web-server newptv4
portal apply mac-trigger-server mts
portal ipv6 enable method direct
portal ipv6 domain dm2
portal bas-ipv6 2004::1
portal ipv6 apply web-server newptv6
portal dual-stack enable
service-template enable
#
interface Vlan-interface100
ip address 2.2.1.1 255.255.255.0
ipv6 address 2001::1/64
ipv6 nd autoconfig managed-address-flag
ipv6 nd autoconfig other-flag
undo ipv6 nd ra halt
#
interface Vlan-interface200
ip address 2.2.2.1 255.255.255.0
ipv6 address 2004::1/64
ipv6 nd autoconfig managed-address-flag
ipv6 nd autoconfig other-flag
undo ipv6 nd ra halt
#
interface GigabitEthernet1/0/1
port link-mode bridge
port link-type trunk
port trunk permit vlan 100 200
#
ip route-static 192.168.0.0 16 2.2.2.100
ipv6 route-static 2003:: 64 2004::2
#
radius session-control enable
#
radius scheme rs1
primary authentication 192.168.0.111
primary accounting 192.168.0.111
key authentication cipher $c$3$Sgqz7lDs4XPnethmAgyAKVlke7qwEkYbQ==
key accounting cipher $c$3$4J/JBRGwqB4F213furJmKB6JWYXBFjWE6g==
user-name-format without-domain
nas-ip 2.2.2.1
#
radius scheme rs2
primary authentication ipv6 2003::2
primary accounting ipv6 2003::2
key authentication cipher $c$3$ZqzlvbN5klp/VDqt/prrN97yy0J4G2j8IQ==
key accounting cipher $c$3$Q6Noroq7nFDkIBYIvpIZu3qQpAZzaDUYJQ==
user-name-format without-domain

```

```

nas-ip ipv6 2004::1
#
radius dynamic-author server
  client ip 192.168.0.111 key cipher $c$3$AkTEB7OgMYnCqsfDeplhoAgXUek/rVrLZw==
  client ipv6 2003::2 key cipher $c$3$NMxmVitbKeKG6ATH6LPUIxyHrSY5fDCvzQ==
  attribute convert Hw-Server-String to Connect-Info received
#
domain dm1
  authorization-attribute idle-cut 15 1024
  authentication portal radius-scheme rs1
  authorization portal radius-scheme rs1
  accounting portal none
#
domain dm2
  authorization-attribute idle-cut 15 1024
  authentication portal radius-scheme rs2
  authorization portal radius-scheme rs2
  accounting portal none
#
portal host-check enable
portal free-rules 1 destination ip any udp 53
portal free-rule 2 destination ip any tcp 53
portal free-rule 3 source interface Bridge-Aggregation1
#
portal web-server newptv4
  url http://192.168.0.111:8080/portal
  url-parameter ssid ssid
  url-parameter wlanacname value AC
  url-parameter wlanuserip source-address
#
portal web-server newptv6
  url http://[2003::2]:8080/portal
  url-parameter ssid ssid
  url-parameter wlanacname value AC
  url-parameter wlanuserip source-address
#
portal server newptv4
  ip 192.168.0.111 key cipher $c$3$om5UnnnYF0jtLWRFaw+1+1V+47E6/lCzRg==
#
portal server newptv6
  ipv6 2003::2 key cipher $c$3$wu1Cg6I4PTcPTgPeKRF/7w9jIqIEq2xlTw==
#
portal mac-trigger-server mts
  ip 192.168.0.111
#
wlan ap ap1 model AP 3620
  serial-id 219801A28N819CE0002T
#

```

```
wlan ap-group group1
  ap ap1
  ap-model AP 3620
  map-configuration flash:/map.txt
  radio 1
  radio 2
    radio enable
    service-template st1
#
```

- **Switch:**

```
#
vlan 2
#
vlan 100
#
vlan 200
#
interface Vlan-interface2
  ip address 192.168.0.100 255.255.255.0
  ipv6 address 2003::1 64
#
interface Vlan-interface200
  ip address 2.2.2.100 255.255.255.0
  ipv6 address 2004::2 64
#
interface GigabitEthernet1/0/1
  port link-type trunk
  port trunk permit vlan 1 100 200
#
interface GigabitEthernet1/0/2
  port link-type trunk
  port access vlan 100 200
  poe enable
#
interface GigabitEthernet1/0/3
  port link-type access
  port access vlan 2
```

Related documentation

- *User Access and Authentication Command Reference in INTELBRAS Access Controllers Command References*
- *User Access and Authentication Configuration Guide in INTELBRAS Access Controllers Configuration Guides*
- *WLAN Access Command Reference in INTELBRAS Access Controllers Command References*
- *WLAN Access Configuration Guide in INTELBRAS Access Controllers Configuration Guides*

INTELBRAS Access Controllers

Remote Portal Authentication with User Profile Authorization Configuration Examples

Copyright © 2024 Intelbras S.A All rights reserved.

No part of this manual may be reproduced or transmitted in any form or by any means without prior written consent of Intelbras S.A

Except for the trademarks of Intelbras S.A, any trademarks that may be mentioned in this document are the property of their respective owners.

The information in this document is subject to change without notice.

Contents

Introduction	1
Prerequisites	1
Example: Configuring remote portal authentication and user profile authorization.....	1
Network configuration.....	1
Analysis	2
Restrictions and guidelines.....	2
Procedures	2
Editing the AP configuration file.....	2
Configuring the AC.....	3
Configuring the switch	6
Configuring the INC server.....	7
Verifying the configuration.....	13
Configuration files	14
Related documentation	16

Introduction

The following information provides an example of configuring remote portal authentication with user profile authorization.

Prerequisites

The following information applies to Comware-based access controllers and access points. Procedures and information in the examples might be slightly different depending on the software or hardware version of the access controllers and access points.

The configuration examples 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.

The following information is provided based on the assumption that you have basic knowledge of AAA, portal authentication, WLAN access, and WLAN high availability.

Example: Configuring remote portal authentication and user profile authorization

Network configuration

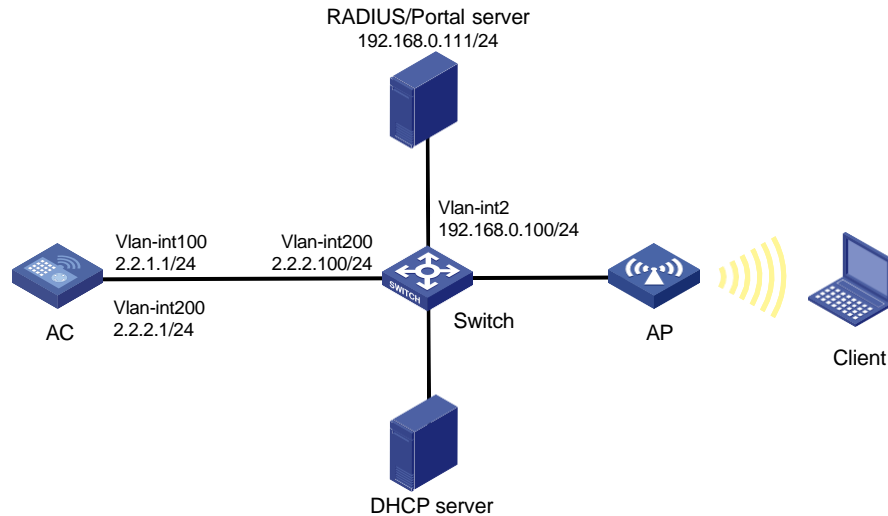
As shown in [Figure 1](#):

- The AP and the client obtain IP addresses from the DHCP server.
- The network deploys an INC server as the portal authentication server, portal Web server, and RADIUS server for portal authentication.

Configure the devices to meet the following requirements:

- The AC uses a service template to provide direct portal authentication for the client. Before passing the authentication, the client can access only the portal Web server. After passing the authentication, the client can access other network resources.
- The AP forwards the client traffic locally.
- The client can access network resources through any Layer 2 ports in its access VLAN without re-authentication.
- The RADIUS server can dynamically change user authorization information or forcibly disconnect users.

Figure 1 Network diagram



Analysis

To allow a client to access network resources through any Layer 2 ports in its access VLAN without re-authentication, enable portal roaming.

In local forwarding mode, to ensure that valid clients can perform portal authentication, enable validity check on wireless clients.

To avoid portal authentication failure caused by frequent logins and logouts in a short time, disable the Rule ARP entry feature.

For the RADIUS server to dynamically change user authorization information or forcibly disconnect users, enable the RADIUS session-control feature.

To use GigabitEthernet 1/0/1 on the AP to forward client traffic, edit a .txt configuration file and upload the file to the AC.

Restrictions and guidelines

Use the actual serial ID of an AP to uniquely identify that AP.

Make sure the type of the portal authentication server and portal Web server is the same as the type of the portal authentication server and portal Web server actually used.

By default, the portal Web server URL redirected to users does carry parameters. You can configure the parameters to be carried in the redirection URL as needed.

Procedures

Editing the AP configuration file

Use a text editor to edit the AP's configuration file. Name the configuration file **map.txt**, and then upload the file to the storage medium of the AC.

The content of the configuration file is as follows:

```
system-view
```

```

vlan 200
interface gigabitethernet1/0/1
port link-type trunk
port trunk permit vlan 200

```

Configuring the AC

1. Configure interfaces:

Create VLAN 100, create VLAN-interface 100, and assign an IP address to the VLAN interface. The AC will use this IP address to establish CAPWAP control and data tunnels with the AP.

```

<AC> system-view
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 2.2.1.1 24
[AC-Vlan-interface100] quit

```

Create VLAN 200, create VLAN-interface 200, and assign an IP address to the VLAN interface. The AC will use VLAN for wireless client access.

```

[AC] vlan 200
[AC-vlan200] quit
[AC] interface vlan-interface 200
[AC-Vlan-interface200] ip address 2.2.2.1 24
[AC-Vlan-interface200] quit

```

Configure GigabitEthernet 1/0/1 (the interface connected to the switch) as a trunk port and assign it to VLAN 100 and VLAN 200.

```

[AC] interface gigabitethernet 1/0/1
[AC-GigabitEthernet1/0/1] port link-type trunk
[AC-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[AC-GigabitEthernet1/0/1] quit

```

2. Configure a static route:

Configure a static route to the INC server.

```

[AC] ip route-static 192.168.0.0 255.255.0.0 2.2.2.100

```

3. Configure the wireless service:

Create a service template named st1.

```

[AC] wlan service-template st1

```

Set the SSID of the service template.

```

[AC-wlan-st-st1] ssid service

```

Specify VLAN 200 for the service template.

```

[AC-wlan-st-st1] vlan 200

```

Configure the AKM mode as PSK, and set the preshared key to 12345678 in plain text.

```

[AC-wlan-st-st1] akm mode psk
[AC-wlan-st-st1] preshared-key pass-phrase simple 12345678

```

Configure the cipher suite as CCMP and security IE as RSN.

```

[AC-wlan-st-st1] cipher-suite ccmp
[AC-wlan-st-st1] security-ie rsn

```

Configure APs to forward client data traffic from all VLANs. (Skip this step if the client data forwarder is APs by default.)

```
[AC-wlan-st-st1] client forwarding-location ap
[AC-wlan-st-st1] quit
```

4. Configure the AP:

NOTE:

In large-scale networks, configure AP groups instead of single APs as a best practice.

Create an AP named **office** with model **AP 3620** and set its serial ID to 219801A28N819CE0002T.

```
[AC] wlan ap office model AP 3620
[AC-wlan-ap-office] serial-id 219801A28N819CE0002T
[AC-wlan-ap-office] quit
```

Create an AP group named **group1** and add AP **office** to AP group **group1**.

```
[AC] wlan ap-group group1
[AC-wlan-ap-group-group1] ap office
```

Create an AP model named AP 3620 in AP group **group1** and then deploy configuration file **map.txt** to the AP.

```
[AC-wlan-ap-group-group1] ap-model AP 3620
[AC-wlan-ap-group-group1-ap-model-AP 3620] map-configuration
map.txt # Enter the AP group's radio 2 view, and bind service template st1
to radio 2. [AC-wlan-ap-group-group1-ap-model-AP 3620] radio 2
[AC-wlan-ap-group-group1-ap-model-AP 3620-radio-2] service-template st1
```

Enable radio 2.

```
[AC-wlan-ap-group-group1-ap-model-AP 3620-radio-2] radio
enable [AC-wlan-ap-group-group1-ap-model-AP 3620-radio-2] quit
[AC-wlan-ap-group-group1-ap-model-AP 3620]
quit [AC-wlan-ap-group-group1] quit
```

5. Configure a RADIUS scheme:

Create RADIUS scheme **rs1**.

```
[AC] radius scheme rs1
```

Configure the primary authentication and accounting servers and shared keys used for secure communication with the servers.

```
[AC-radius-rs1] primary authentication 192.168.0.111
[AC-radius-rs1] primary accounting 192.168.0.111
[AC-radius-rs1] key authentication simple radius
[AC-radius-rs1] key accounting simple radius
```

Configure the AC to remove the ISP domain name from the usernames sent to the RADIUS servers.

```
[AC-radius-rs1] user-name-format without-domain
```

Specify 2.2.2.1 as the source IP address for outgoing RADIUS packets.

```
[AC-radius-rs1] nas-ip 2.2.2.1
[AC-radius-rs1] quit
```

Enable the RADIUS session-control feature.

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

Enable the RADIUS DAS feature.

```
[AC] radius dynamic-author server
```

Specify the server at 173.18.4.100 as a DAC and set the shared key to **radius** in plaintext form for secure communication between the DAS and DAC.

```
[AC-radius-da-server] client ip 192.168.0.111 key simple radius
```

6. Configure a user profile:

Create a user profile named *intelbras*.

```
[AC] user-profile intelbras
```

Configure CAR actions in the user profile: set the CIR to 2 Mbps for incoming and outgoing packets.

```
[AC-user-profile-intelbras] qos car inbound any cir
2048 [AC-user-profile-intelbras] qos car outbound
any cir 2048 [AC-user-profile-intelbras] quit
```

7. Configure an ISP domain:

Create an ISP domain named *dm1*.

```
[AC] domain dm1
```

Configure AAA methods for portal users in the ISP domain.

```
[AC-isp-dm1] authentication portal radius-scheme rs1
[AC-isp-dm1] authorization portal radius-scheme rs1
[AC-isp-dm1] accounting portal none
```

Configure the idle cut feature so that the AC will log out a user if the user's total traffic in the idle timeout period is less than 1024 bytes.

```
[AC-isp-dm1] authorization-attribute idle-cut 15 1024
```

Assign authorization user profile *intelbras* to users in the ISP domain.

```
[AC-isp-dm1] authorization-attribute user-profile
intelbras [AC-isp-dm1] quit
```

8. Configure portal authentication:

Create portal authentication server *newpt*, specify 192.168.0.111 as the server's IP address, and specify 50100 as the portal listening port number.

```
[AC] portal server newpt
[AC-portal-server-newpt] ip 192.168.0.111
[AC-portal-server-newpt] port 50100
```

Configure the portal authentication server type as CMCC.

```
[AC-portal-server-newpt] server-type cmcc
[AC-portal-server-newpt] quit
```

Create a portal Web server named *newpt*, and specify <http://192.168.0.111:8080/portal> as the server's URL

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

Add parameters *ssid*, *wlanuserip*, and *wlanacname* to the URL of the portal Web server and specify the AP SSID, user IP address, and AC name as the values of the parameters, respectively. (You must add the parameters to the URL of a CMCC-type portal Web server.)

```
[AC-portal-websvr-newpt] url-parameter ssid ssid
[AC-portal-websvr-newpt] url-parameter wlanuserip source-address
[AC-portal-websvr-newpt] url-parameter wlanacname value AC
```

Configure the portal Web server type as CMCC.

```
[AC-portal-websvr-newpt] server-type cmcc
[AC-portal-websvr-newpt] quit
```

Configure a portal-free rule to allow users to access the portal Web server without authentication: set the rule number to 0 and the destination address to 192.168.0.111.

```
[AC] portal free-rule 0 destination ip 192.168.0.111 24
```

```

# Configure two destination-based portal-free rules to permit the traffic destined for the DNS
server.
[AC] portal free-rule 1 destination ip any udp 53
[AC] portal free-rule 2 destination ip any tcp 53

# Enable roaming for portal users.
[AC] portal roaming enable

# Disable the Rule ARP entry feature.
[AC] undo portal refresh arp enable

# Enable validity check on wireless portal clients.
[AC] portal host-check enable

# Enable direct portal authentication on service template st1.
[AC] wlan service-template st1
[AC-wlan-st-st1] portal enable method direct

# Specify ISP domain dm1 as the portal authentication domain on service template st1.
[AC-wlan-st-st1] portal domain dm1

# Specify portal Web server newpt on service template st1.
[AC-wlan-st-st1] portal apply web-server newpt

# Configure the BAS-IP as 2.2.2.1 for portal packets sent from service template st1 to the portal
authentication server.
[AC-wlan-st-st1] portal bas-ip 2.2.2.1

# Enable service template st1.
[AC-wlan-st-st1] service-template enable
[AC-wlan-st-st1] quit

```

Configuring the switch

```

# Create VLAN 100. The switch will use this VLAN to forward traffic on CAPWAP control and data
tunnels between the ACs and the AP.
<Switch> system-view
[Switch] vlan 100
[Switch-vlan100] quit

# Create VLAN 200. The switch will use this VLAN to forward packets for wireless clients.
[Switch] vlan 200
[Switch-vlan200] quit

# Create VLAN 2. The switch will use this VLAN to communicate with the INC server.
[Switch] vlan 2
[Switch-vlan2] quit

# Assign the port that connects the switch to the INC server to VLAN 2. (Details not shown.)

# Configure GigabitEthernet 1/0/1 (the port connected to the AC) as a trunk port, and assign the port
to VLAN 100 and VLAN 200.
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[Switch-GigabitEthernet1/0/1] quit

# Configure GigabitEthernet 1/0/2 (the port connected to the AP) as a trunk port, assign the port to
VLAN 100 and VLAN 200, and set the PVID to 100.
[Switch] interface gigabitethernet 1/0/2

```

```
[Switch-GigabitEthernet1/0/2] port link-type trunk
[Switch-GigabitEthernet1/0/2] port trunk permit vlan 100 200
[Switch-GigabitEthernet1/0/2] port trunk pvid vlan 100
```

Enable PoE on GigabitEthernet 1/0/2.

```
[Switch-GigabitEthernet1/0/2] poe enable
[Switch-GigabitEthernet1/0/2] quit
```

Configure GigabitEthernet 1/0/3 (the port connected to the INC server) as an access port, and assign the port to VLAN 2.

```
[Switch] interface gigabitethernet 1/0/3
[Switch-GigabitEthernet1/0/3] port link-type access
[Switch-GigabitEthernet1/0/3] port access vlan 2
[Switch-GigabitEthernet1/0/3] quit
```

Assign an IP address to VLAN-interface 200.

```
[Switch] interface vlan-interface 200
[Switch-Vlan-interface200] ip address 2.2.2.100 255.255.255.0
[Switch-Vlan-interface200] quit
```

Assign an IP address to the VLAN-interface 2.

```
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] ip address 192.168.0.100 255.255.255.0
[Switch-Vlan-interface2] quit
```

Configuring the INC server

In this example, the INC server runs INC PLAT 7.1 (E0303p13), INC INC - EIA 7.1 (F0302p08), and INC EIP 7.1 (F0302p08).

Configuring the RADIUS server

1. Add an access device:
 - a. Log in to INC and click the **User** tab.
 - b. From the navigation tree, select **User Access Policy > Access Device Management > Access Device** to open the access device page.
 - c. Click **Add** to open the **Add Access Device** page as shown in [Figure 2](#).
 - d. Configure the shared key as **radius**.

The shared key must be the same as that configured for the RADIUS server on the AC.
 - e. In the **Device List** area, click **Add Manually** to open the **Add Access Device Manually** page. Enter the start IP address **2.2.2.1** and click **OK**.
 - f. Use the default settings for other parameters on the **Add Access Device** page.
 - g. Click **OK**.

Figure 2 Adding an access device

User > User Access Policy > Access Device Management > Access Device > Add Access Device

Access Configuration

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

Device List

Select Add Manually Clear All

Device Name	Device IP	Device Model	Comments	Delete
	2.2.2.1			

Total Items: 1.

OK Cancel

2. Add an access policy:
 - a. From the navigation tree, select **User Access Policy > Access Policy** to open the access policy page.
 - b. Click **Add** to open the page as shown in [Figure 3](#).
 - c. Enter the access policy name.
 - d. Select a service group. This example uses the default setting (**ungrouped**).
 - e. Use the default settings for other parameters.
 - f. Click **OK**.

Figure 3 Adding an access policy

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

Basic Information

Access Policy Name *	AccessPolicy
Service Group *	Ungrouped
Description	

Authorization Information

Access Period	None	Allocate IP *	No
Downstream Rate(Kbps)		Upstream Rate(Kbps)	
Priority		<input type="checkbox"/> RSA Authentication	
Certificate Authentication	<input checked="" type="radio"/> None <input type="radio"/> EAP		
Certificate Type	EAP-TLS Auth?		
Deploy VLAN			
<input type="checkbox"/> Deploy User Profile		Deploy User Group	
<input type="checkbox"/> Deploy ACL			

3. Add an access service:

- a. From the navigation tree, select **User Access Policy > Access Service** to open the access service page.
- b. Click **Add** to open the page as shown in [Figure 4](#).
- c. Enter service name **RadiusServer**.
- d. Select the access policy configured in the previous step from the **Default Access Policy** list.
- e. Use the default settings for other parameters.
- f. 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 Max. Number of Bound Endpoints * Default Max. Number of Online Endpoints *

Description

☒ Available ☐ Transparent Authentication on Portal Endpoints

Access Scenario List

Add

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

OK Cancel

4. Add an access user:
 - a. From the navigation tree, select **Access User > All Access Users** to open the access user page.
 - b. Click **Add** to open the page as shown in [Figure 5](#).
 - c. Set the user: If the user already exists, click **Select** to select the user. If the user does not exist, click **Add User** to add the user.
 - d. Set the password.
 - e. Use the default settings for other parameters.
 - f. Click **OK**.

Figure 5 Adding an access user

User > All Access Users > Add Access User

Access Information

User Name * **Select Add User**

Account Name *

☐ Trial Account ☐ Default BYOD User ☐ MAC Authentication User ☐ Computer User ☐ Fast Access User

Password * Confirm Password *

☒ Allow User to Change Password ☐ Enable Password Strategy ☐ Modify Password at Next Login

Start Time End Time

Max. Idle Time(Minutes) Max. Concurrent Logins

Login Message

Access Service

Service Name	Service Suffix	Status	Allocate IP
<input checked="" type="checkbox"/> RadiusServer		Available	

OK Cancel

Configuring the portal server

1. Configure the portal service:
 - a. Log in to INC and click the **User** tab.
 - b. From the navigation tree, select **User Access Policy > Portal Service > Server** to open the portal server configuration page as shown in [Figure 6](#).
 - c. Configure the portal server parameters as needed.
This example uses the default settings.
 - d. Click **OK**.

Figure 6 Configuring the portal server

The screenshot shows the 'Portal Server' configuration page. The breadcrumb navigation at the top is 'User > User Access Policy > Portal Service > Server'. The page title is 'Portal Server'. Under the 'Basic Information' section, the 'Log Level' is set to 'Info'. The 'Portal Server' section contains four fields: 'Request Timeout(Seconds)' set to 4, 'Server Heartbeat Interval(Seconds)' set to 20, 'User Heartbeat Interval(Minutes)' set to 5, and 'LB Device Address' which is empty. The 'Portal Web' section contains five fields: 'Request Timeout(Seconds)' set to 15, 'Verify Endpoint Requests' set to 'Yes', 'HTTP Heartbeat Display' set to 'New Page', 'Packet Code' which is empty, 'Use Cache' set to 'Yes', and 'HTTPS Heartbeat Display' set to 'Original Page'. Below these fields is a 'Portal Page' text area containing the URL 'http://192.168.0.111:8080/portal/'. The IP address '192.168.0.111' is also displayed at the bottom right of the page.

2. Configure an IP address group:
 - a. From the navigation tree, select **User Access Policy > Portal Service > IP Group** to open the portal IP address group configuration page.
 - b. Click **Add** to open the **Add IP Group** 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 client 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 7 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 *	2.2.2.1
End IP *	2.2.2.255
Service Group	Ungrouped ▼
Action *	Normal ▼

OK Cancel

3. Add a portal device:
 - a. From the navigation tree, select **User Access Policy > Portal Service > Device** to open the portal device configuration page.
 - b. Click **Add** to open the page as shown in [Figure 8](#).
 - c. Enter the device name.
 - d. Select **CMCC 1.0** from the **Version** list.
 - e. Enter the IP address of the port through which the AC connects to the client in the **IP Address** field.
 - f. 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**.
 - g. Enter the key, which must be the same as that configured on the AC.
 - h. Select **Directly Connected** from the **Access Method** list.
 - i. Use the default settings for other parameters.
 - j. Click **OK**.

Figure 89 Adding a portal device

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

Add Device

Device Information

Device Name *	NAS	Service Group *	Ungrouped ▼
Version *	CMCC 1.0 ▼	IP Address *	2.2.2.1
Listening Port *	2000	Local Challenge *	No ▼
Authentication Retries *	0	Logout Retries *	1
Support Server Heartbeat *	No ▼	Support User Heartbeat *	No ▼
Key *	*****	Confirm Key *	*****
Access Method *	Directly Conne ▼		
Device Description			

OK Cancel

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


- As shown in Figure 8, click the **Port Group Information Management** icon  for the AC to open the port group configuration page.
- Click **Add** to open the page as shown in Figure 9.
- Enter the port group name.
- Select the configured IP address group.
The IP address used by the user to access the network must be within this IP address group.
- Use the default settings for other parameters.
- Click **OK**.

Figure 8 Device list




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

Query Devices

Device Name	<input type="text"/>	Version	<input type="text"/>
Deploy Result	<input type="text"/>	Service Group	<input type="text"/>

Query Reset

Add

Device Name ↕	Version ↕	Service Group ↕	IP Address	Last Deployed at ↕	Deploy Result	Operation
NAS	CMCC 1.0	Ungrouped	2.2.2.1		Not Deployed	  

1-1 of 1. Page 1 of 1. « < 1 > » 50 ▼

Figure 9 Adding a port group

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

Add Port Group

Port Group Name *	Group	Language *	English
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(Minutes) *	0	Heartbeat Timeout(Minutes) *	0
User Domain		Port Group Description	
Transparent Authentication	Not Supported	Client Protection Against Cracks *	No
Page Push Policy		Default Authentication Page	

OK Cancel

- From the navigation tree, select **User Access Policy > Service Parameters**. Then, click **Validate** to make the configuration take effect.

Verifying the configuration

Use the configured username and password to perform portal authentication through a Web browser on the client. Before passing authentication, all Web accesses are redirected to the portal authentication page (<http://192.168.0.111:8080/portal>). After passing authentication, you can access other network resources.

Display online portal user information on the AC.

```
[AC] display portal user all
Total portal users: 1
Username: Client
  AP name: office
  Radio ID: 2
  SSID: service
  Portal server: newpt
  State: Online
  VPN instance: N/A
  MAC          IP          VLAN    Interface
  bce2-659a-3232 2.2.2.2    200     WLAN-BSS1/0/4
Authorization information:
  DHCP IP pool: N/A
  User profile: intelbras
  (active, AAA) Session group
  profile: N/A
  ACL number: N/A
  Inbound CAR: N/A
  Outbound CAR: N/A
```

The output shows that the user has passed portal authentication.

Configuration files

- AC:

```
#
vlan 100
#
vlan 200
#
wlan service-template st1
    ssid service
    vlan 200
    client forwarding-location ap
    akm mode psk
    preshared-key pass-phrase cipher $c$3$0Lf6pOZ6bxrf25nodjOJKYEfnZ6g6ErccHyQ
    cipher-suite ccmp
    security-ie rsn
    portal enable method direct
portal domain dml
portal bas-ip 2.2.2.1
    portal apply web-server newpt
    service-template enable
#
interface Vlan-interface100
    ip address 2.2.1.1 255.255.255.0
#
interface Vlan-interface200
    ip address 2.2.2.1 255.255.255.0
#
interface GigabitEthernet1/0/1
    port link-type trunk
    port trunk permit vlan 1 100 200
#
ip route-static 192.168.0.0 16 2.2.2.100
#
user-profile intelbras
    qos car inbound any cir 2048 cbs 128000
    qos car outbound any cir 2048 cbs 128000
#
radius session-control enable
#
radius scheme rs1
    primary authentication 192.168.0.111
    primary accounting 192.168.0.111
    key authentication cipher $c$3$Sqqqz7lDs4XPnethmAgyAKVlke7qwEkYbQ==
    key accounting cipher $c$3$4J/JBRGwqB4F213furJMkB6JWYXBFjWE6g==
    user-name-format without-domain
nas-ip 2.2.2.1
#
```

```

radius dynamic-author server
  client ip 192.168.0.111 key cipher $c$3$AkTEB7OgMYnCqsfDeplhoAgXUek/rVrLZw==
#
domain dml
authorization-attribute idle-cut 15 1024
  authorization-attribute user-profile
intelbras authentication portal radius-
                                scheme rs1
authorization portal radius-scheme rs1
accounting portal none
#
portal host-check enable
portal free-rule 0 destination ip 192.168.0.0 255.255.255.0
portal free-rule 1 destination ip any udp 53
portal free-rule 2 destination ip any tcp 53
#
portal roaming enable
  undo portal refresh arp enable
#
portal web-server newpt
url http://192.168.0.111:8080/portal
server-type cmcc
url-parameter ssid ssid
url-parameter wlanacname value AC
url-parameter wlanuserip source-address
#
portal server newpt
ip 192.168.0.111
server-type cmcc
#
wlan ap-group group1
  ap office
  ap-model AP 3620
map-configuration flash:/map.txt
radio 1
  radio 2
  radio enable
  service-template st1
#
wlan ap office model AP 3620
  serial-id 219801A28N819CE0002T
#

```

- **Switch:**

```

#
vlan 2
#
vlan 100
#
vlan 200

```

```
#
interface Vlan-interface2
 ip address 192.168.0.100 255.255.255.0
#
interface Vlan-interface200
 ip address 2.2.2.100 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 1 100 200
#
interface GigabitEthernet1/0/2
 port link-type trunk
 port trunk permit vlan 1 100 200
 port trunk pvid vlan 100
 poe enable
#
interface GigabitEthernet1/0/3
 port link-type access
 port access vlan 2
#
```

Related documentation

- *User Access and Authentication Command Reference in INTELBRAS Access Controllers Command Reference*
- *User Access and Authentication Configuration Guide in INTELBRAS Access Controllers Configuration Guide*
- *WLAN Access Command Reference in INTELBRAS Access Controllers Command Reference*
- *WLAN Access Configuration Guide in INTELBRAS Access Controllers Configuration Guide*
- *AP Management Command Reference in INTELBRAS Access Controllers Command Reference*
- *AP Management Configuration Guide in INTELBRAS Access Controllers Configuration Guide*

INTELBRAS Access Controllers WiFiDog Portal Authentication Configuration Examples

Copyright © 2024 Intelbras S.A All rights reserved.

No part of this manual may be reproduced or transmitted in any form or by any means without prior written consent of Intelbras S.A

Except for the trademarks of Intelbras S.A, any trademarks that may be mentioned in this document are the property of their respective owners.

The information in this document is subject to change without notice.

Contents

Introduction	1
Prerequisites	1
Example: Configuring WiFiDog portal authentication	1
Network configuration	1
Analysis	1
Procedures	2
Configuring the WiFiDog server	2
Configuring the AC	2
Configuring the switch	5
Verifying the configuration	6
Configuration files	6
Related documentation	9

Introduction

The following information provides an example of configuring WiFiDog portal authentication.

Prerequisites

The following information applies to Comware-based access controllers and access points. Procedures and information in the examples might be slightly different depending on the software or hardware version of the access controllers and access points.

The configuration examples 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.

The following information is provided based on the assumption that you have basic knowledge of portal authentication and WLAN access features.

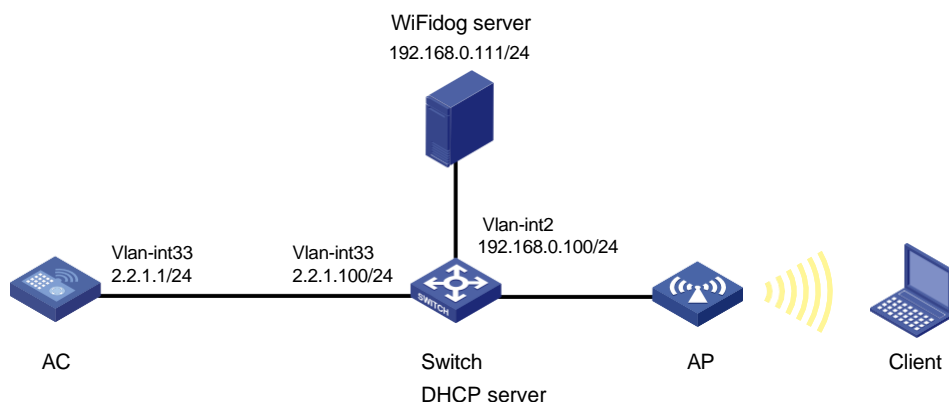
Example: Configuring WiFiDog portal authentication

Network configuration

As shown in [Figure 1](#):

- The AP and the client obtain IP addresses from the DHCP server.
- The WiFiDog server acts as the portal authentication server and the portal Web server.
- Direct portal authentication is configured for the client.
- An authenticated user can access network resources on any Layer 2 ports in its access VLAN without re-authentication.

Figure 1 Network diagram



Analysis

To allow an authenticated user to access network resources on any Layer 2 ports in its access VLAN without re-authentication, enable portal roaming.

To avoid possible authentication failure caused by frequent logins and logouts of portal clients in a short time, disable the Rule ARP entry feature for portal clients.

For portal packet exchange, configure portal-free rules to permit traffic among the portal Web server, the DNS server, and the AC.

For the client to access the portal Web server, configure a service port number on the WiFiDog server.

To use WiFiDog portal authentication, configure the AC to add the following parameters to the URL of the WiFiDog server when it redirects a portal user to the server:

- **gw_address**—IP address of the AC.
- **gw_port**—Port number of the WiFiDog service on the AC. By default, the port number is 80.
- **gw_id**—ID of the AC.
- **mac**—MAC address of the client.
- **channel_path**—Request channel. By default, the value is **intelbras**.
- **url**—URL of the original webpage that the client visits.
- **ip**—IP address of the client.

Procedures

Configuring the WiFiDog server

Restrictions and guidelines

The configuration procedure and interface vary by WiFiDog server model and software version.

Procedure

Specify the ID of the AC on the WiFiDog server. Perform this step for the WiFiDog server to identify the AC. The AC ID is user configurable and is unique in the network. In this example, configure the NAS ID of the AC as its ID on the WiFiDog server. (Details not shown.)

Configure the password used to access the WiFiDog server. (Details not shown.)

Configure a service port number on the WiFiDog server. The service port number is not fixed. In this example, the service port number is 12001. (Details not shown.)

Configuring the AC

1. Configure interfaces on the AC:

Create VLAN 33 and VLAN-interface 33, and assign an IP address to the VLAN interface. The AC will use the IP address to establish CAPWAP data and control tunnels with the AP and use VLAN 33 for client access.

```
<AC> system-view
[AC] vlan 33
[AC-vlan33] quit
[AC] interface vlan-interface 33
[AC-Vlan-interface33] ip address 2.2.1.1 24
[AC-Vlan-interface33] quit
```

Configure GigabitEthernet 1/0/2 (the port connected to the switch) as an access port and assign the port to VLAN 33.

```
[AC] interface gigabitethernet 1/0/2
[AC-GigabitEthernet1/0/2] port link-type access
```

- ```
[AC-GigabitEthernet1/0/2] port access vlan 33
[AC-GigabitEthernet1/0/2] quit
```
2. Configure a static route to reach the WiFiDog server.
 

```
[AC] ip route-static 192.168.0.0 255.255.0.0 2.2.1.100
```
  3. Configure the AC to not perform authentication, authorization, and account for portal users in ISP domain **po**.
 

```
[AC] domain po
[AC-isp-po] authentication portal none
[AC-isp-po] authorization portal none
[AC-isp-po] accounting portal none
[AC-isp-po] quit
```
  4. Create a portal authentication server named **po**. Specify the IP address of the WiFiDog server as the IP address of the authentication server, and specify the key for accessing the WiFiDog server.
 

```
[AC] portal server po
[AC-portal-server-po] ip 192.168.0.111 key simple wifitest
[AC-portal-server-po] quit
```
  5. Configure the portal Web server:
 

# Create a portal Web server named **web-po**.

```
[AC] portal web-server web-po
```

# Specify the URL of the WiFiDog as the URL of the portal Web server and set the port number to 12001.

```
[AC-portal-websvr-web-po] url http://192.168.0.111:12001/wifidog
```

# Specify WiFiDog as the type of the portal Web server.

```
[AC-portal-websvr-web-po] server-type wifidog
```

# Add parameter **channel\_path** to the URL of the portal Web server and set the parameter value to **intelbras**. The AC redirects a portal user by sending the URL with the parameter to the user.

```
[AC-portal-websvr-web-po] url-parameter channel_path value intelbras
```

# Add parameters **gw\_address**, **gw\_id**, and **gw\_port** to the URL of the portal Web server. Specify the IP address of the AC, the ID of the AC, and the WiFiDog service port number of the AC as the values for the parameters, respectively. The AC redirects a portal user by sending the URL with the parameters to the user.

```
[AC-portal-websvr-web-po] url-parameter gw_address value 2.2.1.1
[AC-portal-websvr-web-po] url-parameter gw_id nas-id
[AC-portal-websvr-web-po] url-parameter gw_port value 80
```

# Add parameters **ip**, **mac**, **ssid**, and **url** to the URL of the portal Web server. Specify the client's IP address, the client's MAC address, the AP'S SSID, and the URL of the original webpage that the client visits as the values for the parameters, respectively. The AC redirects a portal user by sending the URL with the parameters to the user.

```
[AC-portal-websvr-web-po] url-parameter ip source-address
[AC-portal-websvr-web-po] url-parameter mac source-mac
[AC-portal-websvr-web-po] url-parameter ssid ssid
[AC-portal-websvr-web-po] url-parameter url original-url
[AC-portal-websvr-web-po] quit
```
  6. Configure portal authentication rules:
 

# Configure destination-based portal-free rules to permit traffic destined for the portal Web server, the DNS server, and the AC.

```
[AC] portal free-rule 1 destination ip 8.8.8.8 255.255.255.255
[AC] portal free-rule 2 destination ip 114.114.114.114 255.255.255.255
```

```
[AC] portal free-rule 3 destination ip 2.2.1.1 255.255.255.255
[AC] portal free-rule 4 destination ip 192.168.0.111 255.255.255.255
```

# Enable validity check on wireless portal clients.

```
[AC] portal host-check enable
```

# Enable portal roaming.

```
[AC] portal roaming enable
```

# Disable the Rule ARP entry feature for portal clients.

```
[AC] undo portal refresh arp enable
```

## 7. Configure a wireless service:

# Create a service template named **po** and enter its view.

```
[AC] wlan service-template po
```

# Assign clients coming online through service template **po** to VLAN 33.

```
[AC-wlan-st-po] vlan 33
```

# Set the SSID to **service**.

```
[AC-wlan-st-po] ssid service
```

# Enable direct portal authentication in service template **po**.

```
[AC-wlan-st-po] portal enable method direct
```

# Specify ISP domain **po** as the portal authentication domain.

```
[AC-wlan-st-po] portal domain po
```

# Specify portal Web server **web-po** in service template **po** for portal authentication.

```
[AC-wlan-st-po] portal apply web-server web-po
```

# Configure the AC to forward client data traffic. (Skip this step if the client data forwarder is the AC by default.)

```
[AC-wlan-st-po] client forwarding-location ac
```

# Configure the AKM mode as PSK, and set the preshared key to 12345678 in plain text.

```
[AC-wlan-st-po] akm mode psk
```

```
[AC-wlan-st-po] preshared-key pass-phrase simple 12345678
```

# Configure the cipher suite as CCMP and security IE as RSN.

```
[AC-wlan-st-po] cipher-suite ccmp
```

```
[AC-wlan-st-po] security-ie rsn
```

# Enable the service template.

```
[AC-wlan-st-po] service-template enable
```

```
[AC-wlan-st-po] quit
```

## 8. Configure the AP:

---

### NOTE:

In large-scale networks, configure AP groups instead of single APs as a best practice.

---

# Create an AP named **ap1** with model **WA6622** and set its serial ID to 219801A24H8199E0001C.

```
[AC] wlan ap ap1 model WA6622
```

```
[AC-wlan-ap-ap1] serial-id 219801A24H8199E0001C
```

# Create an AP group named **group1** and create an AP grouping rule by AP names to add AP **ap1** to AP group **group1**.

```
[AC] wlan ap-group group1
```

```
[AC-wlan-ap-group-group1] ap ap1
```

# Enter the AP group's radio 1 view, and bind service template **po** to radio 1.

```
[AC-wlan-ap-group-group1] ap-model WA6622
```

```
[AC-wlan-ap-group-group1-ap-model-WA6622] radio 1
[AC-wlan-ap-group-group1-ap-model-WA6622-radio-1] service-template po
Enable radio 1.
[AC-wlan-ap-group-group1-ap-model-WA6622-radio-1] radio enable
[AC-wlan-ap-group-group1-ap-model-WA6622-radio-1] quit
Enter the AP group's radio 2 view, and bind service template po to radio 2.
[AC-wlan-ap-group-group1-ap-model-WA6622] radio 2
[AC-wlan-ap-group-group1-ap-model-WA6622-radio-2] service-template po
Enable radio 2.
[AC-wlan-ap-group-group1-ap-model-WA6622-radio-2] radio enable
[AC-wlan-ap-group-group1-ap-model-WA6622-radio-2] return
```

## Configuring the switch

### 1. Configure DHCP:

# Enable DHCP.

```
[Switch] dhcp enable
```

# Create a DHCP address pool named **33** for allocating IP addresses to the AP and client.

```
[Switch] dhcp server ip-pool 33
```

# Specify a gateway address, a subnet, and a DNS server address in the DHCP address pool. In this example, the gateway address is the IP address of VLAN-interface 33 on the switch. The configuration is used for communication between the client and the WiFiDog server.

```
[Switch-dhcp-pool-33] gateway-list 2.2.1.100
```

```
[Switch-dhcp-pool-33] network 2.2.1.0 mask 255.255.255.0
```

```
[Switch-dhcp-pool-33] dns-list 8.8.8.8 114.114.114.114
```

```
[Switch-dhcp-pool-33] quit
```

### 2. Configure interfaces on the switch:

# Create VLAN 33 and VLAN-interface 33, assign an IP address to the VLAN interface, and apply DHCP address pool **33** to the VLAN interface.

```
<Switch> system-view
```

```
[Switch] vlan 33
```

```
[Switch-vlan33] quit
```

```
[Switch] interface vlan-interface 33
```

```
[Switch-Vlan-interface33] ip address 2.2.1.100 255.255.0.0
```

```
[Switch-Vlan-interface33] dhcp server apply ip-pool 33
```

```
[Switch-Vlan-interface33] quit
```

# Create VLAN 2. This VLAN is used to connect the WiFiDog server.

```
[Switch] vlan 2
```

```
[Switch-vlan2] quit
```

# Create VLAN-interface 2 and assign an IP address to the VLAN interface.

```
[Switch] interface vlan-interface 2
```

```
[Switch-Vlan-interface2] ip address 192.168.0.100 255.255.255.0
```

```
[Switch-Vlan-interface2] quit
```

# Configure GigabitEthernet 1/0/8 (the port connected to the AC) as an access port, and assign the port to VLAN 33.

```
[Switch] interface gigabitethernet 1/0/8
```

```
[Switch-GigabitEthernet1/0/8] port link-type access
```

```
[Switch-GigabitEthernet1/0/8] port access vlan 33
```



```
[Switch-GigabitEthernet1/0/8] quit
Configure GigabitEthernet 1/0/10 (the port connected to the AP) as an access port, and
assign the port to VLAN 33.
[Switch] interface gigabitethernet 1/0/10
[Switch-GigabitEthernet1/0/10] port link-type access
[Switch-GigabitEthernet1/0/10] port access vlan 33
Enable PoE on GigabitEthernet 1/0/10.
[Switch-GigabitEthernet1/0/10] poe enable
[Switch-GigabitEthernet1/0/10] quit
Configure GigabitEthernet 1/0/5 (the port connected to the WiFiDog server) as an access port,
and assign the port to VLAN 2.
[Switch] interface gigabitethernet 1/0/5
[Switch-GigabitEthernet1/0/5] port link-type access
[Switch-GigabitEthernet1/0/5] port access vlan 2
[Switch-GigabitEthernet1/0/5] quit
```

## Verifying the configuration

# On the client, connect to the wireless network with SSID **service**. Before passing portal authentication, the client can access only authentication page **<http://192.168.0.111:12001/wifidog>**. All Web requests from the client will be redirected to the authentication page. After passing portal authentication, the client can access other network resources. (Details not shown.)

# On the AC, display information about all portal users to verify that a portal user has come online.

```
[AC] display portal user all
Total portal users: 1
Username: a4:c9:39:68:7d:31
 AP name: ap1
 Radio ID: 1
 SSID: service
 Portal server: N/A
 State: Online
 VPN instance: N/A
 MAC IP VLAN Interface
 a4c9-3968-7d31 2.2.1.14 33 WLAN-BSS1/0/126
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
Total number of clients: 1
```

## Configuration files

- AC:
 

```
#
vlan 33
```

```

#
ip route-static 192.168.0.0 16 2.2.1.100
#
interface Vlan-interface33
 ip address 2.2.1.1 255.255.0.0
#
interface GigabitEthernet1/0/2
 port link-type access
 port access vlan 33
#
wlan service-template po
 ssid service
 client forwarding-location ac
 akm mode psk
 preshared-key pass-phrase simple 12345678
 cipher-suite ccmp
 security-ie rsn
 vlan 33
 portal enable method direct
 portal domain po
 portal apply web-server web-po
 service-template enable
#
domain po
 authentication portal none
 authorization portal none
 accounting portal none
#
portal host-check enable
portal free-rule 1 destination ip 8.8.8.8 255.255.255.255
portal free-rule 2 destination ip 114.114.114.114 255.255.255.255
portal free-rule 3 destination ip 2.2.1.1 255.255.255.255
portal free-rule 4 destination ip 192.168.0.111 255.255.255.255
#
portal web-server web-po
 url http://192.168.0.111:12001/wifidog
 server-type wifidog
 url-parameter channel_path value
 intelbras url-parameter gw_address
 value 2.2.1.1 url-parameter gw_id nas-
 id
 url-parameter gw_port value 80
 url-parameter ip source-address
 url-parameter mac source-mac
 url-parameter ssid ssid
 url-parameter url original-url
#
portal server po
 ip 192.168.0.111 key cipher c3$IXTLQ8lWluD9vHD/OC26sera+vnHj0yEKsuT

```

```
#
wlan ap ap1 model WA6622
 serial-id 219801A24H8199E0001C
#
wlan ap-group group1
ap ap1
ap-model WA6622
radio 1
 radio enable
 service-template po
radio 2
 radio enable
 service-template po
```

- **Switch:**

```
#
 dhcp enable
#
vlan 33
#
vlan 2
#
dhcp server ip-pool 33
 gateway-list 2.2.1.100
 network 2.2.1.100 mask 255.255.255.0
 dns-list 8.8.8.8 114.114.114.114
#
interface Vlan-interface33
 ip address 2.2.1.100 255.255.0.0
 dhcp server apply ip-pool 33
#
interface Vlan-interface2
 ip address 192.168.0.100 255.255.255.0
#
interface GigabitEthernet1/0/8
 port link-type access
 port access vlan 33
#
interface GigabitEthernet1/0/10
 port link-type access
 port access vlan 33
 poe enable
#
interface GigabitEthernet1/0/5
 port link-type access
 port access vlan 2
#
```

# Related documentation

- *User Access and Authentication Configuration Guide in INTELBRAS Access Controllers Configuration Guides*
- *User Access and Authentication Command Reference in INTELBRAS Access Controllers Command References*
- *WLAN Access Configuration Guide in INTELBRAS Access Controllers Configuration Guides*
- *WLAN Access Command Reference in INTELBRAS Access Controllers Command References*

# INTELBRAS Access Controllers

## Portal Fail-Permit Configuration Examples

---

Copyright © 2024 Intelbras S.A All rights reserved.

No part of this manual may be reproduced or transmitted in any form or by any means without prior written consent of Intelbras S.A

Except for the trademarks of Intelbras S.A, any trademarks that may be mentioned in this document are the property of their respective owners.

The information in this document is subject to change without notice.

# Contents

|                                               |    |
|-----------------------------------------------|----|
| Introduction .....                            | 1  |
| Prerequisites .....                           | 1  |
| Example: Configuring portal fail-permit ..... | 1  |
| Network configuration .....                   | 1  |
| Analysis .....                                | 2  |
| Restrictions and guidelines .....             | 2  |
| Procedures .....                              | 2  |
| Configuring INC .....                         | 2  |
| Configuring the AC .....                      | 8  |
| Configuring the switch .....                  | 11 |
| Verifying the configuration .....             | 12 |
| Configuration files .....                     | 13 |
| Related documentation .....                   | 15 |

# Introduction

The following information provides an example of configuring portal fail-permit for wireless clients when the portal Web server is unreachable.

## Prerequisites

The following information applies to Comware-based access controllers and access points. Procedures and information in the examples might be slightly different depending on the software or hardware version of the access controllers and access points.

The configuration examples 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.

The following information is provided based on the assumption that you have basic knowledge of AAA, portal, and WLAN features.

## Example: Configuring portal fail-permit

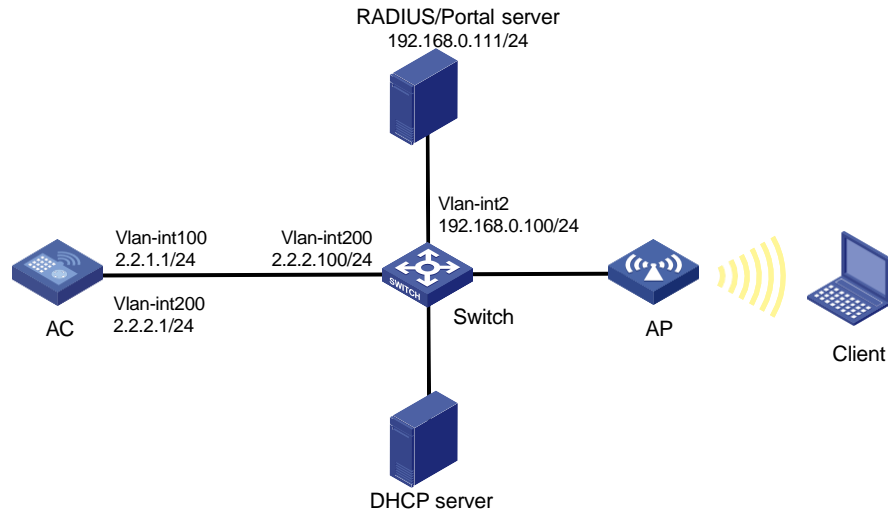
### Network configuration

As shown in [Figure 1](#), the AP and the client obtain IP addresses from the DHCP server.

To implement remote portal authentication, perform the following tasks:

- Configure direct portal authentication.
- Configure a portal authentication server and a portal Web server on INC.
- Configure a RADIUS server as the authentication server and accounting server.
- Enable the AC to detect the reachability of the portal Web server and send a log message and a trap message after server reachability status changes.
  - When the AC detects that the portal Web server is unreachable, it stops portal authentication for wireless users. The AC allows users to have network access without portal authentication.
  - After the portal Web server becomes reachable, the AC restarts portal authentication for wireless users that access the network. A user must pass portal authentication to access the network.

**Figure 1 Network diagram**



## Analysis

To allow an authenticated user to access network resources on any Layer 2 ports in its access VLAN without re-authentication, enable portal roaming.

To avoid possible authentication failure caused by frequent logins and logouts of portal clients in a short time, disable the Rule ARP entry feature for portal clients.

For the RADIUS server to dynamically change user authorization information or forcibly disconnect users, enable the RADIUS session-control feature.

## Restrictions and guidelines

Use the actual serial ID of an AP to uniquely identify that AP.

Make sure the types of the portal authentication server and portal Web server specified on the AC are the same as those actually used. (This example uses CMCC servers.)

By default, the portal Web server URL redirected to users does not include parameters. You can configure the parameters to be included in the redirection URL as needed.

## Procedures

### Configuring INC

In this example, the INC server runs INC PLAT 7.1 (E0303p13), INC INC - EIA 7.1 (F0302p08), and INC EIP 7.1 (F0302p08).

#### Configuring the RADIUS server

1. Add an access device:
  - a. Log in to INC and click the **User** tab.
  - b. From the navigation tree, select **User Access Policy > Access Device Management > Access Device**.
  - c. Click **Add** to open the page as shown in [Figure 2](#).



- d. In the **Device List** area, click **Add Manually** to open the **Add Access Device Manually** page. Enter **2.2.2.1** in the **Start IP** field and then click **OK**.
- e. In the **Access Configuration** area, set the shared key to **radius**, which must be the same as that configured on the AC.
- f. Use the default settings for other parameters.
- g. Click **OK**.

**Figure 2 Adding an access device**

User > User Access Policy > Access Device Management > Access Device > Add Access Device

Access Configuration

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

Device List

Select Add Manually Clear All

| Device Name | Device IP | Device Model | Comments | Delete |
|-------------|-----------|--------------|----------|--------|
|             | 2.2.2.1   |              |          |        |

Total Items: 1.

OK Cancel

2. Add an access policy:
  - a. From the navigation tree, select **User Access Policy > Access Policy**.
  - b. Click **Add** to open the page as shown in [Figure 3](#).
  - c. Enter the access policy name.
  - d. Select a service group. This example uses the default setting (**Ungrouped**).
  - e. Use the default settings for other parameters.
  - f. Click **OK**.

**Figure 3 Adding an access policy**

The screenshot shows the 'Add Access Policy' form. The breadcrumb navigation is 'User > User Access Policy > Access Policy > Add Access Policy'. The form is divided into two sections: 'Basic Information' and 'Authorization Information'. In the 'Basic Information' section, 'Access Policy Name' is set to 'AccessPolicy', 'Service Group' is 'Ungrouped', and 'Description' is empty. In the 'Authorization Information' section, 'Access Period' is 'None', 'Allocate IP' is 'No', 'Downstream Rate(Kbps)' and 'Upstream Rate(Kbps)' are empty, 'Priority' is empty, 'Certificate Authentication' is 'None' (selected), 'Certificate Type' is 'EAP-TLS Auth!', 'Deploy VLAN' is empty, 'Deploy User Profile' and 'Deploy ACL' are unchecked, 'RSA Authentication' is unchecked, and 'Deploy User Group' is empty with a help icon.

3. Add an access service:
  - a. From the navigation tree, select **User Access Policy > Access Service**.
  - b. Click **Add** to open the page as shown in [Figure 4](#).
  - c. Enter the service name.
  - d. Use the default settings for other parameters.
  - e. Click **OK**.

**Figure 4 Adding an access service**

The screenshot shows the 'Add Access Service' form. The breadcrumb navigation is 'User > User Access Policy > Access Service > Add Access Service'. The form is divided into two sections: 'Basic Information' and 'Access Scenario List'. In the 'Basic Information' section, 'Service Name' is 'RadiusServer', 'Service Group' is 'Ungrouped', 'Default Proprietary Attribute Assignment Policy' is 'Do not use', 'Default Max. Number of Bound Endpoints' is '0', 'Default Max. Number of Online Endpoints' is '0', 'Service Suffix' is empty, 'Default Access Policy' is 'AccessPolicy', 'Description' is empty, 'Available' is checked, and 'Transparent Authentication on Portal Endpoints' is unchecked. The 'Access Scenario List' section shows a table with columns: 'Access Scenario', 'Access Policy', 'Proprietary Attribute Assignment Policy', 'Priority', 'Modify', and 'Delete'. The table is empty, and there is an 'Add' button above it. At the bottom, there are 'OK' and 'Cancel' buttons.

4. Add an access user:
  - a. From the navigation tree, select **Access User > Access User**.
  - b. Click **Add** to open the page as shown in [Figure 5](#).
  - c. Select an existing access user or click **Add User** to add a new access user.
  - d. Set the password.

- e. In the **Access Service** area, select the configured access service.
- f. Use the default settings for other parameters.
- g. Click **OK**.

**Figure 5 Adding an access user**

User > All Access Users > Add Access User

**Access Information**

User Name \* client1 Select Add User

Account Name \* client

☐ Trial Account ☐ Default BYOD User ☐ MAC Authentication User ☐ Computer User ☐ Fast Access User

Password \* Confirm Password \*

☒ Allow User to Change Password ☐ Enable Password Strategy ☐ Modify Password at Next Login

Start Time End Time

Max. Idle Time (Minutes) Max. Concurrent Logins 1

Login Message

**Access Service**

| Service Name                                     | Service Suffix | Status    | Allocate IP |
|--------------------------------------------------|----------------|-----------|-------------|
| <input checked="" type="checkbox"/> RadiusServer |                | Available |             |

**Binding Information**

OK OK & Print Cancel

## Configuring the portal server

1. Configure the portal authentication service:
  - a. From the navigation tree, select **User Access Policy > Portal Service > Server** to open the portal server configuration page, as shown in [Figure 6](#).
  - b. Configure the portal server parameters as needed.  
This example uses the default settings.
  - c. Click **OK**.

**Figure 6 Configuring the portal server**

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 LB Device Address

**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://192.168.0.111:8080/portal/

192.168.0.111

2. Configure the IP address group:
  - a. From the navigation tree, select **User Access Policy > Portal Service > IP Group**.
  - 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 client 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 7 Adding an IP address group**

User > User Access Policy > Portal Service > IP Group > 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 ▼    |

OK Cancel

3. Add a portal device:
  - a. From the navigation tree, select **User Access Policy > Portal Service > Device**.
  - b. Click **Add** to open the page as shown in [Figure 8](#).
  - c. Enter the device name.
  - d. Select **CMCC 1.0** from the **Version** list.
  - e. Enter the IP address of the AC's interface connected to the client.
  - f. 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**.
  - g. Enter the key, which must be the same as that configured on the AC.
  - h. Select **Directly Connected** for **Access Method**.
  - i. Use the default settings for other parameters.
  - j. Click **OK**.

**Figure 8 Adding a portal device**

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

Add Device

Device Information

|                            |                  |                          |             |
|----------------------------|------------------|--------------------------|-------------|
| Device Name *              | NAS              | Service Group *          | Ungrouped ▼ |
| Version *                  | CMCC 1.0 ▼       | IP Address *             | 2.2.2.1     |
| Listening Port *           | 2000             | Local Challenge *        | No ▼        |
| Authentication Retries *   | 0                | Logout Retries *         | 1           |
| Support Server Heartbeat * | No ▼             | Support User Heartbeat * | No ▼        |
| Key *                      | *****            | Confirm Key *            | *****       |
| Access Method *            | Directly Conne ▼ |                          |             |
| Device Description         |                  |                          |             |

OK Cancel

4. Associate the portal device with the IP address group:
- a. Click the **Port Group** icon in the **Operation** field of device **NAS**, as shown in [Figure 9](#).

**Figure 9 Device list**

User > User Access Policy > Portal Service > Device





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         | CMCC 1.0 | Ungrouped     | 2.2.2.1    |                  | Not Deployed  |     |

1-1 of 1. Page 1 of 1.

<< < 1 > >> 50

- b. Click **Add** to open the page as shown in [Figure 10](#).
- 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 10 Adding a port group**

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

### Add Port Group

|                               |               |                                    |             |
|-------------------------------|---------------|------------------------------------|-------------|
| Port Group Name *             | Group         | Language *                         | English     |
| 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(Minutes) * | 0             | Heartbeat Timeout(Minutes) *       | 0           |
| User Domain                   |               | Port Group Description             |             |
| Transparent Authentication    | Not Supported | Client Protection Against Cracks * | No          |
| Page Push Policy              |               | Default Authentication Page        |             |

OK Cancel

## Configuring the AC

### 1. Configure interfaces on the AC:

# Create VLAN 100 and VLAN-interface 100. Assign an IP address to the VLAN interface. The AC will use this IP address to establish CAPWAP data and control tunnels with the AP.

```
<AC> system-view
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 2.2.1.1 24
[AC-Vlan-interface100] quit
```

# Create VLAN 200 and VLAN-interface 200. Assign an IP address to the VLAN interface. The AC will use VLAN 200 for client access.

```
[AC] vlan 200
[AC-vlan200] quit
[AC] interface vlan-interface 200
[AC-Vlan-interface200] ip address 2.2.2.1 24
[AC-Vlan-interface200] quit
```

# Configure GigabitEthernet 1/0/1 (the interface connected to the switch) as a trunk port and assign it to VLAN 100 and VLAN 200.

```
[AC] interface gigabitethernet 1/0/1
[AC-GigabitEthernet1/0/1] port link-type trunk
[AC-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[AC-GigabitEthernet1/0/1] quit
```

### 2. Configure a static route to reach the INC server.

```
[AC] ip route-static 192.168.0.0 255.255.0.0 2.2.2.100
```

### 3. Configure a wireless service:

# Create a service template named **st1** and enter its view.

```
[AC] wlan service-template st1
```

# Set the SSID of service template **st1** to **service**.

```
[AC-wlan-st-st1] ssid service
```

# Assign clients coming online through service template **st1** to VLAN 200.

```
[AC-wlan-st-st1] vlan 200
```

# Configure the AKM mode as PSK, and set the preshared key to 12345678 in plain text.

```
[AC-wlan-st-st1] akm mode psk
```

```
[AC-wlan-st-st1] preshared-key pass-phrase simple 12345678
```

# Configure the cipher suite as CCMP and security IE as RSN.

```
[AC-wlan-st-st1] cipher-suite ccmp
```

```
[AC-wlan-st-st1] security-ie rsn
```

# Configure the AC to forward client data traffic. (Skip this step if the client data forwarder is the AC by default.)

```
[AC-wlan-st-st1] client forwarding-location ac
```

```
[AC-wlan-st-st1] quit
```

#### 4. Configure the AP:

---

##### NOTE:

In large-scale networks, configure AP groups instead of single APs as a best practice.

---

# Create an AP named **office** with model AP 3620 and set its serial ID to 219801A28N819CE0002T.

```
[AC] wlan ap office model AP 3620
```

```
[AC-wlan-ap-office] serial-id 219801A28N819CE0002T
```

```
[AC-wlan-ap-office] quit
```

# Create an AP group named **group1** and add AP **office** to the AP group.

```
[AC] wlan ap-group group1
```

```
[AC-wlan-ap-group-group1] ap office
```

# Enter the AP group's radio 2 view, and bind service template **st1** to radio 2.

```
[AC-wlan-ap-group-group1] ap-model AP 3620
```

```
[AC-wlan-ap-group-group1-ap-model-AP 3620] radio 2
```

```
[AC-wlan-ap-group-group1-ap-model-AP 3620-radio-2] service-template st1
```

# Enable radio 2.

```
[AC-wlan-ap-group-group1-ap-model-AP 3620-radio-2] radio
```

```
enable [AC-wlan-ap-group-group1-ap-model-AP 3620-radio-2] quit
```

```
[AC-wlan-ap-group-group1-ap-model-AP 3620]
```

```
quit [AC-wlan-ap-group-group1] quit
```

#### 5. Configure a RADIUS scheme:

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

```
[AC] radius scheme rs1
```

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

```
[AC-radius-rs1] primary authentication 192.168.0.111
```

```
[AC-radius-rs1] primary accounting 192.168.0.111
```

```
[AC-radius-rs1] key authentication simple radius
```

```
[AC-radius-rs1] key accounting simple radius
```

# Configure the AC to remove the domain name from the usernames sent to the RADIUS servers.

```
[AC-radius-rs1] user-name-format without-domain
```

# Specify 2.2.2.1 as the source IP address for outgoing RADIUS packets sent to the RADIUS servers.

```
[AC-radius-rs1] nas-ip 2.2.2.1
[AC-radius-rs1] quit
```

# Enable the RADIUS session-control feature.

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

6. Configure an authentication domain:

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

```
[AC] domain dm1
```

# Configure the authentication, authorization, and authorization methods as RADIUS for portal users in the ISP domain, and specify RADIUS scheme **rs1**.

```
[AC-isp-dm1] authentication portal radius-scheme rs1
```

```
[AC-isp-dm1] authorization portal radius-scheme rs1
```

```
[AC-isp-dm1] accounting portal radius-scheme rs1
```

# Configure the idle cut feature for users in the ISP domain. Log out a user if the user's traffic is less than 1024 bytes in 15 minutes.

```
[AC-isp-dm1] authorization-attribute idle-cut 15 1024
```

```
[AC-isp-dm1] quit
```

7. Configure portal authentication:

# Create a portal authentication server named **newpt**, specify IP address 192.168.0.111 as the IP address of the authentication server, and specify 50100 as the portal service port number.

```
[AC] portal server newpt
```

```
[AC-portal-server-newpt] ip 192.168.0.111 key simple radius
```

```
[AC-portal-server-newpt] port 50100
```

# Specify CMCC as the type of portal authentication server **newpt**.

```
[AC-portal-server-newpt] server-type cmcc
```

```
[AC-portal-server-newpt] quit
```

# Create a portal Web server named **newpt** and specify **http://192.168.0.111:8080/portal** as the URL of the server.

```
[AC] portal web-server newpt
```

```
[AC-portal-websvr-newpt] url http://192.168.0.111:8080/portal
```

# Add parameters **ssid**, **wlanuserip**, and **wlanacname** to the URL of portal Web server **newpt**. Specify the AP's SSID, the IP address of the client, and the AC's name as the values for the parameters, respectively. (The parameters are required to be included in the URL of a portal Web server of the CMCC type.)

```
[AC-portal-websvr-newpt] url-parameter ssid ssid
```

```
[AC-portal-websvr-newpt] url-parameter wlanuserip source-address
```

```
[AC-portal-websvr-newpt] url-parameter wlanacname value AC
```

# Enable server detection for portal Web server **newpt**, set the detection interval to 60 seconds, and set the maximum number of consecutive detection failures to 2. Configure the AC to send a log message and a trap message after server reachability status changes.

```
[AC-portal-websvr-newpt] server-detect interval 60 retry 2 log
```

# Specify CMCC as the type of portal Web server **newpt**.

```
[AC-portal-websvr-newpt] server-type cmcc
```

```
[AC-portal-websvr-newpt] quit
```

# Configure a destination-based portal-free rule numbered **0** to permit traffic destined for IP address 192.168.0.111 (the portal Web server).

```
[AC] portal free-rule 0 destination ip 192.168.0.111 24
```

# Configure destination-based portal-free rules to permit traffic destined for the DNS server.

```
[AC] portal free-rule 1 destination ip any udp 53
```

```
[AC] portal free-rule 2 destination ip any tcp 53
```



```

Enable portal roaming.
[AC] portal roaming enable

Disable the Rule ARP entry feature for portal clients.
[AC] undo portal refresh arp enable

Enable validity check on wireless portal clients.
[AC] portal host-check enable

Enable direct portal authentication in service template st1.
[AC] wlan service-template st1
[AC-wlan-st-st1] portal enable method direct

Specify portal Web server newpt in service template st1 for portal authentication.
[AC-wlan-st-st1] portal apply web-server newpt

Configure the BAS-IP attribute as 2.2.2.1 for portal packets sent to portal authentication
server newpt.
[AC-wlan-st-st1] portal bas-ip 2.2.2.1

Specify ISP domain dm1 as the portal authentication domain.
[AC-wlan-st-st1] portal domain dm1

Enable portal fail-permit for the portal Web server on the service template.
[AC-wlan-st-st1] portal fail-permit web-server

Enable service template st1.
[AC-wlan-st-st1] service-template enable
[AC-wlan-st-st1] quit

```

## Configuring the switch

```

Create VLAN 100. The switch will use this VLAN to forward traffic on the CAPWAP tunnels
between the AC and the AP.
<Switch> system-view
[Switch] vlan 100
[Switch-vlan100] quit

Create VLAN 200. The switch will use this VLAN to forward client traffic.
[Switch] vlan 200
[Switch-vlan200] quit

Create VLAN 2.
[Switch] vlan 2
[Switch-vlan2] quit

Configure GigabitEthernet 1/0/1 (the port connected to the AC) as a trunk port and assign the trunk
port to VLAN 100 and VLAN 200.
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[Switch-GigabitEthernet1/0/1] quit

Configure GigabitEthernet 1/0/2 (the port connected to the AP) as an access port and assign the
access port to VLAN 100.
[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] port link-type access
[Switch-GigabitEthernet1/0/2] port access vlan 100

Enable PoE on GigabitEthernet 1/0/2.

```

```
[Switch-GigabitEthernet1/0/2] poe enable
[Switch-GigabitEthernet1/0/2] quit
```

**# Configure GigabitEthernet 1/0/3 (the port connected to the INC server) as an access port and assign the access port to VLAN 2.**

```
[Switch] interface gigabitethernet 1/0/3
[Switch-GigabitEthernet1/0/3] port link-type access
[Switch-GigabitEthernet1/0/3] port access vlan 2
[Switch-GigabitEthernet1/0/3] quit
```

**# Create VLAN-interface 200 and assign an IP address to the VLAN interface.**

```
[Switch] interface vlan-interface 200
[Switch-Vlan-interface200] ip address 2.2.2.100 255.255.255.0
[Switch-Vlan-interface200] quit
```

**# Create VLAN-interface 2 and assign an IP address to the VLAN interface.**

```
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] ip address 192.168.0.100 255.255.255.0
[Switch-Vlan-interface2] quit
```

## Verifying the configuration

**# Verify that the portal Web server is reachable. When the portal Web server is reachable, the value for the **IPv4 status** field is **Up**.**

```
[AC] display portal web-server newpt
Portal Web server: newpt
 Type: CMCC
 URL: http://192.168.0.111:8080/portal
 URL parameters:
 ssid=ssid
 wlanuserip=source-address
 wlanacname=AC
 VPN instance: Not configured
 Server detection:
 Interval: 60s
 Attempts: 2
 Action: log
 Detection URL: Not configured
 Detection type: TCP
 IPv4 status: Up
 IPv6 status: N/A
 Captive-bypass: Disabled
 If-match: Not configured
```

**# Make the portal Web server and the AC unreachable. (Details not shown.)**

**# Verify that the AC can detect the reachability status change of the portal Web server. When the portal Web server is unreachable, the value for the **IPv4 status** field is **Down**.**

```
[AC] display portal web-server newpt
Portal Web server: newpt
 Type: CMCC
 URL: http://192.168.0.111:8080/portal
```

```

URL parameters:
 ssid=ssid
 wlanuserip=source-address
 wlanacname=AC
VPN instance: Not configured
Server detection:
 Interval: 60s
 Attempts: 2
 Action: log
 Detection URL: Not configured
 Detection type: TCP
IPv4 status: Down
IPv6 status: N/A
Captive-bypass: Disabled
If-match: Not configured

```

# Verify that the AC send a log message and a trap message after server reachability status changes. (Details not shown.)

# Verify that the AC allows wireless users to have network access without portal authentication through service template **st1**. (Details not shown.)

# Make the portal Web server and the AC reachable. (Details not shown.)

# Verify that wireless users must pass portal authentication to access the network through service template **st1**. (Details not shown.)

## Configuration files

- AC:
 

```

#
vlan 100
#
vlan 200
#
wlan service-template st1
 ssid service
 vlan 200
 client forwarding-location ac
 akm mode psk
 preshared-key pass-phrase cipher c3$oLf6pOZ6bxrf25nodjOJKYEfnZ6g6ErccHyQ
 cipher-suite ccmp
 security-ie rsn
 portal enable method direct
 portal domain dm1
 portal bas-ip 2.2.2.1
 portal apply web-server newpt
 portal fail-permit web-server
 service-template enable
#
interface Vlan-interface100
ip address 2.2.1.1 255.255.255.0

```

```

#
interface Vlan-interface200
 ip address 2.2.2.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 1 100 200
#
 ip route-static 192.168.0.0 16 2.2.2.100
#
 radius session-control enable
#
radius scheme rs1
 primary authentication 192.168.0.111
 primary accounting 192.168.0.111
 key authentication cipher c3$Sqqqz7lDs4XPnethmAgyAKVlke7qwEkYbQ==
 key accounting cipher c3$4J/JBRGwqB4F2l3furJmKB6JWYXBFjWE6g==
 user-name-format without-domain
 nas-ip 2.2.2.1
#
domain dml
 authorization-attribute idle-cut 15 1024
 authentication portal radius-scheme rs1
 authorization portal radius-scheme rs1
 accounting portal radius-scheme rs1
#
portal host-check enable
portal free-rule 0 destination ip 192.168.0.0 255.255.255.0
portal free-rule 1 destination ip any udp 53
portal free-rule 2 destination ip any tcp 53
#
 portal roaming enable
 undo portal refresh arp enable
#
portal web-server newpt
 url http://192.168.0.111:8080/portal
 server-detect interval 60 retry 2 log
 server-type cmcc
 url-parameter ssid ssid
 url-parameter wlanacname value AC
 url-parameter wlanuserip source-address
#
portal server newpt
 ip 192.168.0.111 key cipher c3$Q82T/9AHq5HT7uFX7nho8K0Y6jziycoJTw==
 server-type cmcc
#
wlan ap-group group1
 ap office

```

- ```

ap-model AP 3620
  radio 1
  radio 2
  radio enable
  service-template st1
#
wlan ap office model AP 3620
  serial-id 219801A28N819CE0002T
#

```
- **Switch:**

```

#
vlan 2
#
vlan 100
#
vlan 200
#
interface Vlan-interface2
  ip address 192.168.0.100 255.255.255.0
#
interface Vlan-interface200
  ip address 2.2.2.100 255.255.255.0
#
interface GigabitEthernet1/0/1
  port link-type trunk
  port trunk permit vlan 1 100 200
#
interface GigabitEthernet1/0/2
  port link-type access
  port access vlan 100
  poe enable
#
interface GigabitEthernet1/0/3
  port link-type access
  port access vlan 2
#

```

Related documentation

- *User Access and Authentication Configuration Guide in INTELBRAS Access Controllers Configuration Guides*
- *User Access and Authentication Command Reference in INTELBRAS Access Controllers Command References*
- *WLAN Access Configuration Guide in INTELBRAS Access Controllers Configuration Guides*
- *WLAN Access Command Reference in INTELBRAS Access Controllers Command References*

INTELBRAS Access Controllers Local MAC Authentication Configuration Examples

Copyright © 2024 Intelbras S.A All rights reserved.

No part of this manual may be reproduced or transmitted in any form or by any means without prior written consent of Intelbras S.A

Except for the trademarks of Intelbras S.A, any trademarks that may be mentioned in this document are the property of their respective owners.

The information in this document is subject to change without notice.

Contents

Introduction	1
Prerequisites	1
Example: Configuring local MAC authentication for wireless clients	1
Network configuration	1
Restrictions and guidelines	1
Procedures	2
Configuring the AC	2
Configuring the switch	4
Verifying the configuration	5
Configuration files	5
Related documentation	7

Introduction

The following information provides an example for configuring local MAC authentication in WLAN.

Prerequisites

The following information applies to Comware-based access controllers and access points. Procedures and information in the examples might be slightly different depending on the software or hardware version of the access controllers and access points.

The configuration examples 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.

The following information is provided based on the assumption that you have basic knowledge of MAC authentication, WLAN authentication, and WLAN access.

Example: Configuring local MAC authentication for wireless clients

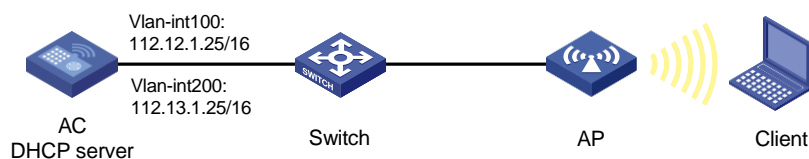
Network configuration

As shown in [Figure 1](#):

- The AC centrally forwards the client traffic.
- The AC acts as a DHCP server to provide IP addresses for the AP and the client.

Configure the AC to perform local MAC authentication to control the network access of the client. The MAC address of the client is used as the username and password for authentication. The MAC address is in hexadecimal notation without hyphens, and letters are in lower case.

Figure 1 Network diagram



Restrictions and guidelines

When you configure local MAC authentication for wireless clients, follow these restrictions and guidelines:

- Use the serial ID labeled on the AP's rear panel to specify an AP.
- Make sure the username and password configured on the AC are the same as the MAC address of the client. The username and password formats comply with the MAC authentication user account format.
- Remove the ports that connect the AC to the AP from VLAN 1 in case there are too many packets in VLAN 1.

- Some endpoints by default use random MAC addresses. To ensure successful MAC authentication for such an endpoint, disable the endpoint from using a random MAC address.

Procedures

Configuring the AC

1. Configure interfaces on the AC:

Create VLAN 100 and VLAN-interface 100, and assign an IP address to the VLAN interface. The AC will use this IP address to establish CAPWAP tunnels with the AP.

```
<AC> system-view
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 112.12.1.25 16
[AC-Vlan-interface100] quit
```

Create VLAN 200 and VLAN-interface 200, and assign an IP address to the VLAN interface. VLAN 200 will be used for client access.

```
[AC] vlan 200
[AC-vlan200] quit
[AC] interface vlan-interface 200
[AC-Vlan-interface200] ip address 112.13.1.25 16
[AC-Vlan-interface200] quit
```

Configure GigabitEthernet 1/0/1 (the port connected to the switch) as a trunk port, remove the port from VLAN 1, and assign it to VLANs 100 and 200.

```
[AC] interface gigabitEthernet 1/0/1
[AC-GigabitEthernet1/0/1] port link-type trunk
[AC-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[AC-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[AC-GigabitEthernet1/0/1] quit
```

2. Configure DHCP:

Enable DHCP.

```
[AC] dhcp enable
```

Create a DHCP address pool named **vlan100**, and specify subnet 112.12.0.0/16 and gateway IP address 112.12.1.25 in the DHCP address pool.

```
[AC] dhcp server ip-pool vlan100
[AC-dhcp-pool-vlan100] network 112.12.0.0 mask 255.255.0.0
[AC-dhcp-pool-vlan100] gateway-list 112.12.1.25
[AC-dhcp-pool-vlan100] quit
```

Create a DHCP address pool named **vlan200**, and specify subnet 112.13.0.0/16 and gateway IP address 112.13.1.25 in the DHCP address pool. In this example, the address of the DNS server is 112.13.1.25 (the gateway address). You must replace it with the actual address of the DNS server on your network.

```
[AC] dhcp server ip-pool vlan200
[AC-dhcp-pool-vlan200] network 112.13.0.0 mask 255.255.0.0
[AC-dhcp-pool-vlan200] gateway-list 112.13.1.25
[AC-dhcp-pool-vlan200] dns-list 112.13.1.25
[AC-dhcp-pool-vlan200] quit
```

3. Configure a local authentication domain:

Create an ISP domain named **local-mac** and configure the ISP domain to use local authentication for LAN access wireless clients. The AC does not perform authorization and accounting for LAN access nodes (in this example, wireless clients) in the ISP domain.

```
[AC] domain local-mac
[AC-isp-local-mac] authentication lan-access local
[AC-isp-local-mac] accounting lan-access none
[AC-isp-local-mac] authorization lan-access none
```

Configure the idle cut feature for clients in ISP domain **local-mac**.

```
[AC-isp-local-mac] authorization-attribute idle-cut 15 1024
[AC-isp-local-mac] quit
```

4. Configure a local user:

Add a network access user. Configure both the username and password as the client's MAC address **3ca9f4144c20**.

```
[AC] local-user 3ca9f4144c20 class network
[AC-luser-network-3ca9f4144c20] password simple 3ca9f4144c20
```

Set the service type to **lan-access**.

```
[AC-luser-network-3ca9f4144c20] service-type lan-access
[AC-luser-network-3ca9f4144c20] quit
```

5. Configure the AC to use the MAC address of each user as both the username and password for MAC authentication. The MAC addresses are in hexadecimal notation without hyphens and with letters in lower case. (The configuration in this step is the default configuration. This step is optional.)

```
[AC] mac-authentication user-name-format mac-address without-hyphen lowercase
```

6. Configure a wireless service:

Create a service template named **1** and enter its view.

```
[AC] wlan service-template 1
```

Configure the SSID of service template **1** as **service**.

```
[AC-wlan-st-1] ssid service
```

Assign clients coming online through the service template to VLAN 200.

```
[AC-wlan-st-1] vlan 200
```

Set the PSK AKM mode and configure simple character string of **12345678** as the PSK.

```
[AC-wlan-st-1] akm mode psk
[AC-wlan-st-1] preshared-key pass-phrase simple 12345678
```

Set the CCMP cipher suite for frame encryption and enable the RSN IE in beacon and probe responses.

```
[AC-wlan-st-1] cipher-suite ccmp
[AC-wlan-st-1] security-ie rsn
```

Enable the AC to forward client data traffic. If the AC forwards client data traffic by default, skip this step.

```
[AC-wlan-st-1] client forwarding-location ac
```

Set the authentication mode to MAC authentication.

```
[AC-wlan-st-1] client-security authentication-mode mac
```

Specify ISP domain **local-mac** for MAC authentication clients on the service template.

```
[AC-wlan-st-1] mac-authentication domain local-mac
```

Enable the service template.

```
[AC-wlan-st-1] service-template enable
[AC-wlan-st-1] quit
```

7. Configure AP settings:

❗ IMPORTANT:

In a large-scale network, configure AP groups as a best practice.

Create a manual AP named **officeap**, and specify the AP model and serial ID.

```
[AC] wlan ap officeap model AP 3620
[AC-wlan-ap-officeap] serial-id 219801A28N819CE0002T
[AC-wlan-ap-officeap] quit
```

Create AP group **group1** and create an AP grouping rule by AP names to add AP **officeap** to AP group **group1**.

```
[AC] wlan ap-group group1
[AC-wlan-ap-group-group1] ap officeap
```

Bind service template 1 to radio 2 in AP group **group1**.

```
[AC-wlan-ap-group-group1] ap-model AP 3620
[AC-wlan-ap-group-group1-ap-model-AP 3620] radio 2
[AC-wlan-ap-group-group1-ap-model-AP 3620-radio-2] service-template 1
```

Enable radio 2.

```
[AC-wlan-ap-group-group1-ap-model-AP 3620-radio-2] radio
enable [AC-wlan-ap-group-group1-ap-model-AP 3620-radio-2] quit
[AC-wlan-ap-group-group1-ap-model-AP 3620]
quit [AC-wlan-ap-group-group1] quit
```

Configuring the switch

Create VLAN 100. The switch will use this VLAN to forward the traffic on the CAPWAP tunnels between the AC and AP.

```
<Switch> system-view
[Switch] vlan 100
[Switch-vlan100] quit
```

Create VLAN 200. The switch will use this VLAN to forward packets for wireless clients.

```
[Switch] vlan 200
[Switch-vlan200] quit
```

Configure GigabitEthernet 1/0/1 (the port connected to the AC) as a trunk port, remove the port from VLAN 1, and assign the trunk port to VLAN 100.

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100
[Switch-GigabitEthernet1/0/1] quit
```

Configure GigabitEthernet 1/0/2 (the port connected to the AP) as an access port. Assign the access port to VLAN 100.

```
[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] port link-type access
[Switch-GigabitEthernet1/0/2] port access vlan 100
```

Enable PoE on GigabitEthernet 1/0/2.

```
[Switch-GigabitEthernet1/0/2] poe enable
[Switch-GigabitEthernet1/0/2] quit
```

Verifying the configuration

The client requests to access the network. On the AC, verify that the client has passed MAC authentication and come online on VLAN 200.

```
[AC] display wlan client
```

```
Total number of clients: 1
```

MAC address	User name	AP name	R IP address	VLAN
3ca9-f414-4c20	3ca9f4144c20	officeap	2 112.13.0.2	200

Configuration files

- AC:

```
#
dhcp enable
#
vlan 1
#
vlan 100
#
vlan 200
#
dhcp server ip-pool vlan100
gateway-list 112.12.1.25
network 112.12.0.0 mask 255.255.0.0
#
dhcp server ip-pool vlan200
gateway-list 112.13.1.25
network 112.13.0.0 mask 255.255.0.0
dns-list 112.13.1.25
#
wlan service-template 1
ssid service
vlan 200
client forwarding-location ac
akm mode psk
preshared-key pass-phrase cipher $c$3$9tIUHskAUVqCH9/EPrL26ldkcEQnngexUEFj
cipher-suite ccmp
security-ie rsn
client-security authentication-mode mac
mac-authentication domain local-mac
service-template enable
#
interface Vlan-interface100
ip address 112.12.1.25 255.255.0.0
#
interface Vlan-interface200
```

```

ip address 112.13.1.25 255.255.0.0
#
interface GigabitEthernet1/0/1
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 100 200
#
domain local-mac
authentication lan-access local
accounting lan-access none
authorization lan-access none
authorization-attribute idle-cut 15 1024
#
local-user 3ca9f4144c20 class network
password cipher $c$3$KWMkvq/FnQ2opPqBnpSTs3NPhVKrSOvqFPLAECsiDQ==
service-type lan-access
authorization-attribute user-role network-operator
#
wlan ap-group group1
ap officeap
ap-model AP 3620
radio 1
radio 2
radio enable
service-template 1
#
wlan ap officeap model AP 3620
serial-id 219801A28N819CE0002T
#

```

- **Switch:**

```

#
vlan 1
#
vlan 100
#
vlan 200
#
interface GigabitEthernet1/0/1
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 100
#
interface GigabitEthernet1/0/2
port access vlan 100
poe enable
#

```

Related documentation

- *AP and WT Management Configuration Guide in INTELBRAS Access Controllers Configuration Guides*
- *AP and WT Management Command Reference in INTELBRAS Access Controllers Command References*
- *Network Connectivity Configuration Guide in INTELBRAS Access Controllers Configuration Guides*
- *Network Connectivity Command Reference in INTELBRAS Access Controllers Command References*
- *User Access and Authentication Configuration Guide in INTELBRAS Access Controllers Configuration Guides*
- *User Access and Authentication Command Reference in INTELBRAS Access Controllers Command References*
- *WLAN Access Configuration Guide in INTELBRAS Access Controllers Configuration Guides*
- *WLAN Access Command Reference in INTELBRAS Access Controllers Command References*

INTELBRAS Access Controllers Remote MAC Authentication Configuration Examples

Copyright © 2024 Intelbras S.A All rights reserved.

No part of this manual may be reproduced or transmitted in any form or by any means without prior written consent of Intelbras S.A

Except for the trademarks of Intelbras S.A, any trademarks that may be mentioned in this document are the property of their respective owners.

The information in this document is subject to change without notice.

Contents

Introduction	1
Prerequisites	1
Example: Configuring remote MAC authentication	1
Network configuration	1
Restrictions and guidelines	2
Procedures	2
Configuring the AC	2
Configuring the switch	4
Configuring the RADIUS server	5
Verifying the configuration	8
Configuration files	9
Related documentation	10

Introduction

The following information provides an example for configuring remote MAC authentication in WLAN.

Prerequisites

The following information applies to Comware-based access controllers and access points. Procedures and information in the examples might be slightly different depending on the software or hardware version of the access controllers and access points.

The configuration examples 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.

The following information is provided based on the assumption that you have basic knowledge of AAA, MAC authentication, WLAN authentication, and WLAN access.

Example: Configuring remote MAC authentication

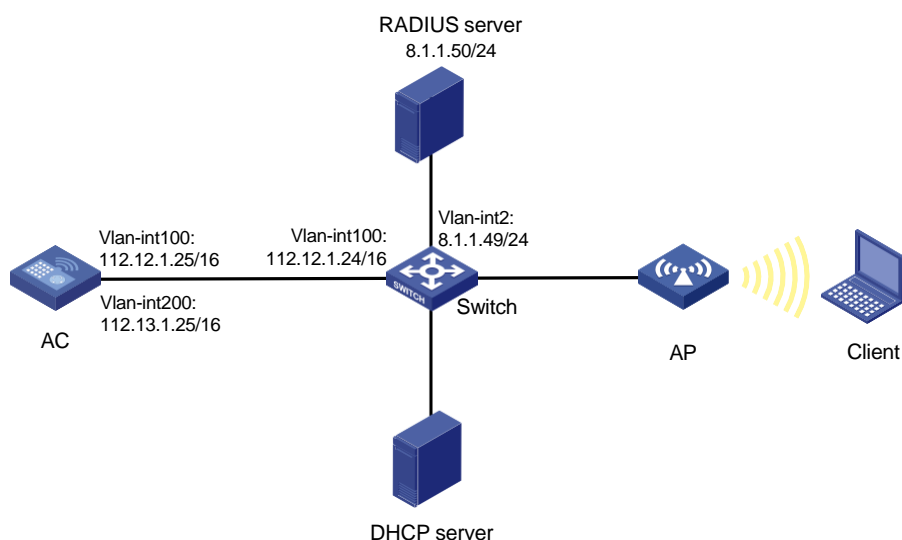
Network configuration

As shown in [Figure 1](#), the DHCP server allocates IP addresses to the AP and the client. The AC centrally forwards the client traffic.

To control the client's access to network resources, complete the following tasks:

- Configure VLAN 200 as the access VLAN of the client.
- Configure the AC to use the RADIUS server to perform MAC authentication for the client.
- Set the AKM mode to PSK to secure data transmission between the client and the AP.

Figure 1 Network diagram



Restrictions and guidelines

When you configure MAC authentication with the PSK AKM mode for wireless clients, follow these restrictions and guidelines:

- On the AC, specify the user account format for MAC authentication. In this example, the MAC address of the client is used as the username and password. Make sure the username and password configuration on the RADIUS server are consistent with the configuration on the AC.
- Use the actual serial ID of an AP to uniquely identify that AP.
- Remove the ports that connect the AC to the AP from VLAN 1 in case there are too many packets in VLAN 1.
- Some endpoints by default use random MAC addresses. To ensure successful MAC authentication for such an endpoint, disable the endpoint from using a random MAC address.

Procedures

Configuring the AC

1. Configure interfaces on the AC:

Create VLAN 100 and VLAN-interface 100, and assign an IP address to the VLAN interface. The AC will use this IP address to establish CAPWAP tunnels with the AP.

```
<AC> system-view
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 112.12.1.25 16
[AC-Vlan-interface100] quit
```

Create VLAN 200 and VLAN-interface 200, and assign an IP address to the VLAN interface. VLAN 200 will be used for client access.

```
[AC] vlan 200
[AC-vlan200] quit
[AC] interface vlan-interface 200
[AC-Vlan-interface200] ip address 112.13.1.25 16
[AC-Vlan-interface200] quit
```

Configure GigabitEthernet 1/0/1 (the port connected to the switch) as a trunk port, remove the port from VLAN 1, and assign the port to VLANs 100 and 200.

```
[AC] interface gigabitethernet 1/0/1
[AC-GigabitEthernet1/0/1] port link-type trunk
[AC-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[AC-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[AC-GigabitEthernet1/0/1] quit
```

2. Configure a static route to the INC server:

```
[AC] ip route-static 8.1.1.0 255.255.255.0 112.12.1.24
```

3. Configure RADIUS-based MAC authentication:

Create a RADIUS scheme named **office** and enter its view.

```
[AC] radius scheme office
```

Specify the IP addresses of the primary authentication and accounting RADIUS servers.

```
[AC-radius-office] primary authentication 8.1.1.50
```

```
[AC-radius-office] primary accounting 8.1.1.50
# Specify the shared keys for RADIUS authentication and accounting.
[AC-radius-office] key authentication simple 123456789
[AC-radius-office] key accounting simple 123456789
# Exclude the ISP domain names from the usernames sent to the RADIUS servers.
[AC-radius-office] user-name-format without-domain
# Specify IP address 112.12.1.25 as the source IP address for outgoing RADIUS packets.
[AC-radius-office] nas-ip 112.12.1.25
[AC-radius-office] quit
# Create an ISP domain named office1 and enter its view.
[AC] domain office1
# Apply RADIUS scheme office to ISP domain office1 for LAN user authentication,
authorization, and accounting.
[AC-isp-office1] authentication lan-access radius-scheme office
[AC-isp-office1] authorization lan-access radius-scheme office
[AC-isp-office1] accounting lan-access radius-scheme office
# Configure the idle cut feature for clients in ISP domain office1.
[AC-isp-office1] authorization-attribute idle-cut 15 1024
[AC-isp-office1] quit
# Configure the AC to use the MAC address of each user as both the username and password
for MAC authentication. The MAC addresses are in hexadecimal notation without hyphens and
with letters in lower case. (The configuration in this step is the default configuration. This step is
optional.)
[AC] mac-authentication user-name-format mac-address without-hyphen lowercase
```

4. Configure a wireless service:

```
# Create a service template named 1 and enter its view.
[AC] wlan service-template 1
# Configure the SSID of service template 1 as service.
[AC-wlan-st-1] ssid service
# Assign clients coming online through the service template to VLAN 200.
[AC-wlan-st-1] vlan 200
# Enable the AC to forward client data traffic. If the AC forwards client data traffic by default,
skip this step.
[AC-wlan-st-1] client forwarding-location ac
# Set the authentication mode to MAC authentication.
[AC-wlan-st-1] client-security authentication-mode mac
# Specify ISP domain office1 as the MAC authentication domain.
[AC-wlan-st-1] mac-authentication domain office1
```

5. Configure the AKM mode for the service template:

```
# Set the AKM mode to PSK.
[AC-wlan-st-1] akm mode psk
# Configure the plaintext string of 123456789 as the PSK.
[AC-wlan-st-1] preshared-key pass-phrase simple 123456789
# Configure CCMP as the cipher suite and enable the RSN IE in beacon and probe responses.
[AC-wlan-st-1] cipher-suite ccmp
[AC-wlan-st-1] security-ie rsn
# Enable the service template.
```

```
[AC-wlan-st-1] service-template enable
[AC-wlan-st-1] quit
```

6. Configure AP settings:

❗ IMPORTANT:

In a large-scale network, configure AP groups as a best practice.

Create a manual AP named **officeap**, and specify the AP model and serial ID.

```
[AC] wlan ap officeap model AP 3620
[AC-wlan-ap-officeap] serial-id 219801A28N819CE0002T
[AC-wlan-ap-officeap] quit
```

Create AP group **group1** and create an AP grouping rule by AP names to add AP **officeap** to AP group **group1**.

```
[AC] wlan ap-group group1
[AC-wlan-ap-group-group1] ap officeap
```

Bind service template **1** to radio **2** in AP group **group1**.

```
[AC-wlan-ap-group-group1] ap-model AP 3620
[AC-wlan-ap-group-group1-ap-model-AP 3620] radio 2
[AC-wlan-ap-group-group1-ap-model-AP 3620-radio-2] service-template 1
```

Enable radio **2**.

```
[AC-wlan-ap-group-group1-ap-model-AP 3620-radio-2] radio
enable [AC-wlan-ap-group-group1-ap-model-AP 3620-radio-2] quit
[AC-wlan-ap-group-group1-ap-model-AP 3620]
quit [AC-wlan-ap-group-group1] quit
```

Configuring the switch

Create VLAN 100. The switch will use this VLAN to forward the traffic on the CAPWAP tunnels between the AC and AP.

```
<Switch> system-view
[Switch] vlan 100
[Switch-vlan100] quit
```

Create VLAN 200. The switch will use this VLAN to forward packets for wireless clients.

```
[Switch] vlan 200
[Switch-vlan200] quit
```

Configure GigabitEthernet 1/0/1 (the port connected to the AC) as a trunk port, remove the port from VLAN 1, and assign the trunk port to VLAN 100 and VLAN 200.

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[Switch-GigabitEthernet1/0/1] quit
```

Configure GigabitEthernet 1/0/2 (the port connected to the AP) as an access port. Assign the access port to VLAN 100.

```
[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] port link-type access
[Switch-GigabitEthernet1/0/2] port access vlan 100
```

Enable PoE on GigabitEthernet 1/0/2.

```
[Switch-GigabitEthernet1/0/2] poe enable
[Switch-GigabitEthernet1/0/2] quit
```

Configure GigabitEthernet 1/0/3 (the port connected to the RADIUS server) as an access port. Assign the access port to VLAN 2.

```
[Switch] interface gigabitethernet 1/0/3
[Switch-GigabitEthernet1/0/3] port link-type access
[Switch-GigabitEthernet1/0/3] port access vlan 2
[Switch-GigabitEthernet1/0/3] quit
```

Create VLAN-interface 100 and assign an IP address to the VLAN interface.

```
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ip address 112.12.1.24 16
[Switch-Vlan-interface100] quit
```

Create VLAN-interface 2 and assign an IP address to the VLAN interface.

```
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] ip address 8.1.1.49 255.255.255.0
[Switch-Vlan-interface2] quit
```

Configuring the RADIUS server

In this example, the RADIUS server runs INC PLAT 7.1(E0303P10) and INC UAM 7.1(E0303P10).

1. Add an access device:
 - a. Log in to INC and click the **User** tab.
 - b. From the navigation tree, select **User Access Policy > Access Device Management > Access Device**.
 - c. Click **Add**.
The **Add Access Device** page opens.
 - d. In the **Device List** area, click **Add Manually** to add the device at **112.12.1.25** as an access device.
This IP address is the source IP address specified on the AC for outgoing RADIUS packets.
 - e. In the **Access Configuration** area, configure the following parameters, as shown in [Figure 2](#):
 - Enter **123456789** in the **Shared Key** and **Confirm Shared Key** fields.
The key is consistent with the shared key configured on the AC.
 - Use the default values for other parameters.
 - f. Click **OK**.

Figure 2 Adding an access device

Access Configuration

Authentication Port * 1812

Accounting Port * 1813

RADIUS Accounting Partially/Not Supported

Service Type LAN Access Service

Access Device Type H3C(General)

Service Group Ungrouped

Shared Key *

Confirm Shared Key *

Access Device Group --

Device List

Select Add Manually Clear All

Device Name	Device IP	Device Model	Comments	Delete
	112.12.1.25			

Total Items: 1.

OK Cancel

2. Add an access policy:
 - a. Click the **User** tab.
 - b. From the navigation tree, select **User Access Policy > Access Policy**.
 - c. Click **Add**.
 - d. On the **Add Access Policy** page, configure the following parameters, as shown in [Figure 3](#):
 - Enter **office** in the **Access Policy Name** field.
 - Use the default values for other parameters.
 - e. Click **OK**.

Figure 3 Adding an access policy

Basic Information

Access Policy Name * office

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 Auth?

Deploy VLAN

☐ Deploy User Profile

Deploy User Group

☐ Deploy ACL

OK Cancel

3. Add an access service:
 - a. Click the **User** tab.
 - b. From the navigation tree, select **User Access Policy > Access Service**.
 - c. Click **Add**.

- d. On the **Add Access Service** page, configure the following parameters, as shown in [Figure 4](#):
 - Enter **office_mac** in the **Service Name** field.
 - Select **office** from the **Default Access Policy** list.
 - Use the default values for other parameters.
- e. 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 Max. Number of Bound Endpoints * Default Max. Number of Online Endpoints *

Description

☒ Available ☐ Transparent Authentication on Portal Endpoints

Access Scenario List

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

4. Add an access user:
 - a. Click the **User** tab.
 - b. From the navigation tree, select **Access User > Access User**.
The access user list opens.
 - c. Click **Add**.
The **Add Access User** page opens.
 - d. In the **Access Information** area, add a user, as shown in [Figure 5](#):
 - Click **Add User**.
 - On the dialog box that opens, enter **adm_office_mac** in the **User Name** and **Identity Number** fields.
 - Click **Check Availability** to verify the validity of the username and identity number.
 - Click **OK**.
 - e. In the **Access Information** area, configure the following parameters, as shown in [Figure 6](#):
 - Enter **3891d5833b20** in the **Account Name** field.
 - Enter **3891d5833b20** in the **Password** and **Confirm Password** fields.
 - f. In the **Access Service** area, select **office_mac** from the list.
 - g. Click **OK**.

Figure 5 Adding a user

Figure 6 Adding an access user account

Verifying the configuration

The client requests to access the network.

On the AC, verify that the wireless client has passed MAC authentication and PSK authentication and come online on VLAN 200.

```
[AC] display wlan client
```

```
Total number of clients: 1
```

MAC address	User name	AP name	R IP address	VLAN
3891-d583-3b20	3891d5833b20	officeap	2 112.13.0.2	200

Configuration files

- AC:

```
#
dhcp enable
#
vlan 1
#
vlan 100
#
vlan 200
#
wlan service-template 1
  ssid service
  vlan 200
  akm mode psk
  client forwarding-location ac
  preshared-key pass-phrase cipher $c$3$heDUT35pq2/Zmsuy18nxS3vSHAeolC6kobTrDA==
  cipher-suite ccmp
  security-ie rsn
  client-security authentication-mode mac
  mac-authentication domain officel
  service-template enable
#
interface Vlan-interface100
  ip address 112.12.1.25 255.255.0.0
#
interface Vlan-interface200
  ip address 112.13.1.25 255.255.0.0
#
interface GigabitEthernet1/0/1
  port link-type trunk
  undo port trunk permit vlan 1
  port trunk permit vlan 100 200
#
ip route-static 8.1.1.0 24 112.12.1.24
#
radius scheme office
  primary authentication 8.1.1.50
  primary accounting 8.1.1.50
  key authentication cipher $c$3$o/3Ueu4pLSdJ0r1kLdAwzJU/AaBGCxnGuBXHmQ==
  key accounting cipher $c$3$oKqS/GRbPQc8AG+Vp+bJO4ZPKlk5+ceFuye/tQ==
  user-name-format without-domain
  nas-ip 112.12.1.25
#
domain officel
  authorization-attribute idle-cut 15 1024
  authentication lan-access radius-scheme office
```

```

authorization lan-access radius-scheme office
accounting lan-access radius-scheme office
#
wlan ap-group group1
  ap officeap
  ap-model AP 3620
    radio 1
    radio 2
    radio enable
    service-template 1
#
wlan ap officeap model AP 3620
  serial-id 219801A28N819CE0002T
#

```

- **Switch:**

```

#
vlan 1
#
vlan 100
#
vlan 200
#
interface Vlan-interface2
  ip address 8.1.1.49 255.255.255.0
#
interface Vlan-interface100
  ip address 112.12.1.24 255.255.0.0
#
interface GigabitEthernet1/0/1
  port link-type trunk
  undo port trunk permit vlan 1
  port trunk permit vlan 100 200
#
interface GigabitEthernet1/0/2
  port link-type access
  port access vlan 100
  poe enable
#
interface gigabitethernet 1/0/3
  port link-type access
  port access vlan 2
#

```

Related documentation

- *AP and WT Management Configuration Guide in INTELBRAS Access Controllers Configuration Guides*
- *AP and WT Management Command Reference in INTELBRAS Access Controllers Command References*

- *Network Connectivity Configuration Guide in INTELBRAS Access Controllers Configuration Guides*
- *Network Connectivity Command Reference in INTELBRAS Access Controllers Command References*
- *User Access and Authentication Configuration Guide in INTELBRAS Access Controllers Configuration Guides*
- *User Access and Authentication Command Reference in INTELBRAS Access Controllers Command References*
- *WLAN Access Configuration Guide in INTELBRAS Access Controllers Configuration Guides*
- *WLAN Access Command Reference in INTELBRAS Access Controllers Command References*

INTELBRAS Access Controllers

Transparent Authentication Through Remote MAC and Portal Authentication Configuration Examples

Copyright © 2024 Intelbras S.A All rights reserved.

No part of this manual may be reproduced or transmitted in any form or by any means without prior written consent of Intelbras S.A

Except for the trademarks of Intelbras S.A, any trademarks that may be mentioned in this document are the property of their respective owners.

The information in this document is subject to change without notice.

Contents

Introduction	1
Prerequisites	1
Example: Configuring transparent authentication through remote MAC and portal authentication	1
Network configuration	1
Analysis	2
Restrictions and guidelines	2
Procedures	3
Configuring INC	3
Configuring the AC	9
Configuring the switch	12
Verifying the configuration	13
Configuration files	14
Related documentation	17

Introduction

The following information provides examples for configuring transparent authentication through remote MAC authentication and remote portal authentication.

Prerequisites

The following information applies to Comware-based access controllers and access points. Procedures and information in the examples might be slightly different depending on the software or hardware version of the access controllers and access points.

The configuration examples 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.

The following information is provided based on the assumption that you have basic knowledge of AAA, portal, and WLAN.

Example: Configuring transparent authentication through remote MAC and portal authentication

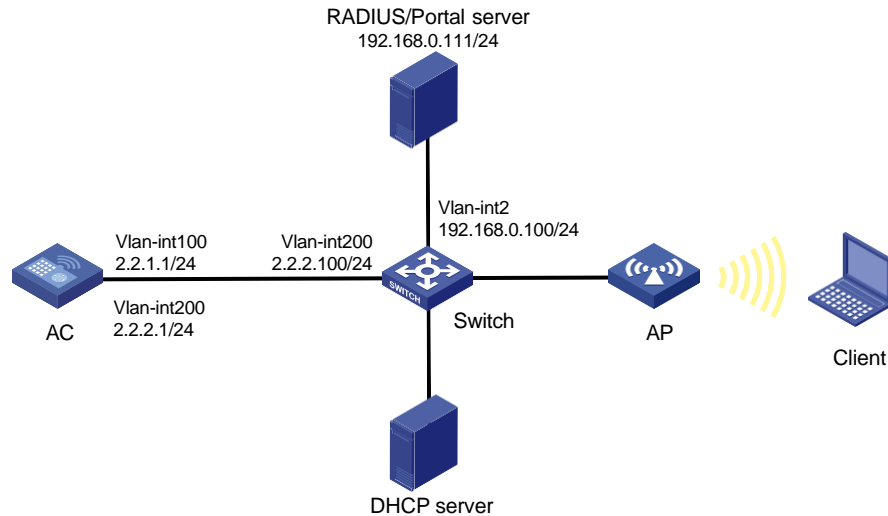
Network configuration

As shown in [Figure 1](#), the AP and the client obtain IP addresses from the DHCP server. The INC server acts as a portal authentication server, a portal Web server, and a RADIUS server.

Configure the devices to meet the following requirements:

- The AC provides remote MAC authentication and direct portal authentication for the client.
- The RADIUS server can dynamically change user authorization information or forcibly disconnect users.

Figure 1 Network diagram



Analysis

For the client to access network resources through any Layer 2 ports in its access VLAN without re-authentication, enable portal roaming.

For the RADIUS server to dynamically change the user authorization information or forcibly disconnect users, enable the RADIUS session-control feature.

To ensure that dynamic user authorization information can be correctly assigned to users after they come online, enable the RADIUS DAS feature.

Restrictions and guidelines

- Use the serial ID labeled on the AP's rear panel to specify an AP.
- By default, the URL of the portal Web server to which the AC redirects portal users does not carry any parameters. You can add parameters to be carried in the URL as needed.
- If portal authentication is enabled on a VLAN interface, the AC can forward client traffic. If portal authentication is enabled on a service template, both the AC and the AP can forward client traffic. (In this example, portal authentication is enabled on a service template.)
- In wireless networks where the AP forwards client traffic, the AC does not have ARP entries for clients. Therefore, the AC cannot check the validity of portal clients by using ARP entries. To ensure that valid users can perform portal authentication, enable wireless client validity check on the AC.
- If a portal client logs out and then tries to come online frequently in a short time, the client will fail portal authentication. To avoid this problem, disable the Rule ARP entry feature for portal clients.
- Some endpoints by default use random MAC addresses. For transparent authentication to take effect on such an endpoint, disable the endpoint from using a random MAC address.

Procedures

Configuring INC

This example uses the INC server to describe the RADIUS server and portal server configuration. The INC server runs on INC PLAT 7.1 (E0303p13), INC INC - EIA 7.1 (F0302p08), and INC EIP 7.1 (F0302p08).

Configuring the RADIUS server

1. Add the AC to INC as an access device:
 - a. Log in to INC and click the **User** tab.
 - b. From the navigation tree, select **User Access Policy > Access Device Management > Access Device**.
 - c. Click **Add** to open the page as shown in [Figure 2](#).
 - d. In the **Access Configuration** area, configure the parameters as follows:
 - Set the shared key to **radius**, which must be the same as that on the AC.
 - Use the default values for other parameters.
 - e. In the **Device List** area, click **Add Manually** to open the **Add Access Device Manually** page. Enter **2.2.2.1** in the **Start IP** field and then click **OK**.
 - f. Click **OK**.

Figure 2 Adding the AC as an access device

User > User Access Policy > Access Device Management > Access Device > Add Access Device

Access Configuration

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

Device List

Select Add Manually Clear All

Device Name	Device IP	Device Model	Comments	Delete
	2.2.2.1			

Total Items: 1.

OK Cancel

2. Add an access policy:
 - a. From the navigation tree, select **User Access Policy > Access Policy**.
 - b. Click **Add** to open the page as shown in [Figure 3](#).
 - c. Enter the access policy name.
 - d. Select a service group.

This example uses the default value **Ungrouped**.
 - e. Use the default settings for other parameters.
 - f. Click **OK**.

Figure 3 Adding an access policy

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

Basic Information

Access Policy Name * AccessPolicy

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 Auth!

Deploy VLAN

☐ Deploy User Profile

Deploy User Group ?

☐ Deploy ACL

3. Add an access service:
 - a. From the navigation tree, select **User Access Policy > Access Service**.
 - b. Click **Add** to open the page as shown in Figure 4.
 - c. Enter the service name.
 - d. Select the **Transparent Authentication on Portal Endpoints** option.
 - e. Use the default settings for other parameters.
 - f. Click **OK**.

Figure 4 Adding an access service

User > User Access Policy > Access Service > Modify Access Service

Basic Information

Service Name * MAC_server

Service Suffix

Service Group * Ungrouped

Default Access Policy * AccessPolicy

Default Proprietary Attribute Assignment Policy * Do not use

Default Max. Number of Bound Endpoints * 0

Default Max. Number of Online Endpoints * 0

Description

☒ Available

☒ Transparent Authentication on Portal Endpoints

4. Add an access user:
 - a. From the navigation tree, select **Access User > Access User**.
 - b. Click **Add** to open the page as shown in Figure 5.
 - c. Select an existing access user or click **Add User** to add a new access user.
 - d. Enter the account name.
 - e. Set the password.
 - f. Select the access service.
 - g. Use the default settings for other parameters.
 - h. Click **OK**.

Figure 5 Adding an access user

User > All Access Users > Add Access User

Access Information

User Name * Client1 Select Add User

Account Name * client

☐ Trial Account ☐ Default BYOD User ☐ MAC Authentication User ☐ Computer User ☐ Fast Access User

Password * ***** Confirm Password * *****

☒ Allow User to Change Password ☐ Enable Password Strategy ☐ Modify Password at Next Login

Start Time [] End Time []

Max. Idle Time (Minutes) [] Max. Concurrent Logins 1

Login Message []

Access Service

Service Name	Service Suffix	Status	Allocate IP
<input checked="" type="checkbox"/> MAC_server		Available	<input checked="" type="checkbox"/>

Configuring the portal server

1. Configure the portal authentication service:
 - a. Click the **User** tab.
 - b. From the navigation tree, select **User Access Policy > Portal Service > Server** to open 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

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 LB Device Address []

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://192.168.0.111:8080/portal/

2. Configure an IP address group:
 - a. From the navigation tree, select **User Access Policy > Portal Service > IP Group**.
 - 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 client IP address is in the IP group.

- e. Select a service group.
This example uses the default value **Ungrouped**.
- f. From the **Action** list, select **Normal**.
- g. Click **OK**.

Figure 7 Adding an IP address group

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

OK Cancel

3. Add a portal device:
 - a. From the navigation tree, select **User Access Policy > Portal Service > Device**.
 - b. Click **Add** to open the page as shown in [Figure 8](#).
 - c. Enter the device name.
 - d. Select **CMCC 1.0** for **Version**.
 - e. Enter the IP address of the AC's interface connected to the client.
 - f. 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**.
 - g. Enter the key, which must be the same as that configured on the AC.
 - h. Select **Directly Connected** for **Access Method**.
 - i. Use the default settings for other parameters.
 - j. Click **OK**.

Figure 8 Adding a portal device

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

Add Device

Device Information

Device Name *	NAS	Service Group *	Ungrouped ▼
Version *	CMCC 1.0 ▼	IP Address *	2.2.2.1
Listening Port *	2000	Local Challenge *	No ▼
Authentication Retries *	0	Logout Retries *	1
Support Server Heartbeat *	No ▼	Support User Heartbeat *	No ▼
Key *	*****	Confirm Key *	*****
Access Method *	Directly Conne ▼		
Device Description			

OK Cancel


4. Associate the portal device with the IP address group:
- As shown in Figure 9, click the **Port Group** icon  in the **Operation** field for device **NAS** to open the port group configuration page.

Figure 9 Device list





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

Query Devices

Device Name	<input type="text"/>	Version	<input type="text"/>
Deploy Result	<input type="text"/>	Service Group	<input type="text"/>

Query Reset

Add

Device Name	Version	Service Group	IP Address	Last Deployed at	Deploy Result	Operation
NAS	CMCC 1.0	Ungrouped	2.2.2.1		Not Deployed	   

1-1 of 1. Page 1 of 1. << < 1 > >> 50

- Click **Add** to open the page as shown in Figure 10.
- Enter the port group name.
- Select the configured IP address group.
The IP address used by the user to access the network must be within this IP address group.
- Select **Supported** for **Transparent Authentication**.
- Use the default settings for other parameters.
- Click **OK**.

Figure 10 Adding a port group

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

Add Port Group

Port Group Name *	group	Language *	English
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(Minutes) *	10	Heartbeat Timeout(Minutes) *	30
User Domain		Port Group Description	
Transparent Authentication	Supported	Client Protection Against Cracks *	No
Page Push Policy		Default Authentication Page	

OK Cancel



5. From the navigation tree, select **User Access Policy > Service Parameters > Validate System Configuration** to make the configuration take effect.
6. Configure system parameters:
 - a. From the navigation tree, select **User Access Policy > Service Parameters > System Settings**.
 - b. Click the **Configure** icon  for **User Endpoint Settings** to open the page as shown in [Figure 11](#).
 - c. Select **Enable** for **Transparent MAC Authentication**.
 - d. Select whether to enable transparent portal authentication on non-smart devices.
In this example, select **Enable** for **Non-Terminal Authentication**.
 - e. Click **OK**.

Figure 11 Configuring user endpoint settings

User > User Access Policy > Service Parameters > System Settings > User Endpoint Settings

User Endpoint Settings

Transparent MAC Authentication	Enable	Max. Device for Single Account *	10
Non-Terminal Authentication	Enable 	Log off User with Endpoint Conflict	No

OK Cancel


- f. Click the **Configure** icon  for **Endpoint Aging Time** to open the page as shown in [Figure 12](#).
 - g. Set the endpoint aging time as needed.
This example uses the default value.
 - h. Click **OK**.

Figure 12 Setting the endpoint aging time

User > User Access Policy > Service Parameters > System Settings > Endpoint Aging Time > Modify Endpoint Aging Time

Modify Endpoint Aging Time

Endpoint Aging Time(Days) * 7 ?

OK Cancel

7. From the navigation tree, select **User Access Policy > Service Parameters > Validate System Configuration** to make the configuration take effect.

Configuring the AC

1. Configure interfaces on the AC:

Create VLAN 100 and VLAN-interface 100, and assign an IP address to the VLAN interface. The AC will use this IP address to establish a CAPWAP tunnel with the AP.

```
<AC> system-view
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 2.2.1.1 24
[AC-Vlan-interface100] quit
```

Create VLAN 200 and VLAN-interface 200, and assign an IP address to the VLAN interface. The AC will use VLAN 200 for client access.

```
[AC] vlan 200
[AC-vlan200] quit
[AC] interface vlan-interface 200
[AC-Vlan-interface200] ip address 2.2.2.1 24
[AC-Vlan-interface200] quit
```

Configure GigabitEthernet 1/0/1 (the port connected to the switch) as a trunk port, and add the trunk port to VLAN 1, VLAN 100, and VLAN 200.

```
[AC] interface gigabitethernet 1/0/1
[AC-GigabitEthernet1/0/1] port link-type trunk
[AC-GigabitEthernet1/0/1] port trunk permit vlan 1 100 200
[AC-GigabitEthernet1/0/1] quit
```

2. Configure a static route to the INC server:

```
[AC] ip route-static 192.168.0.0 255.255.0.0 2.2.2.100
```

3. Configure a WLAN service:

Create a service template named **st1** and enter its view.

```
[AC] wlan service-template st1
```

Set the SSID of service template **st1** to **service**.

```
[AC-wlan-st-st1] ssid service
```

Assign clients coming online through service template **st1** to VLAN 200.

```
[AC-wlan-st-st1] vlan 200
```

Set the PSK AKM mode and configure simple character string of **12345678** as the PSK.

```
[AC-wlan-st-st1] akm mode psk
```

```
[AC-wlan-st-st1] preshared-key pass-phrase simple 12345678
```

Set the CCMP cipher suite for frame encryption and enable the RSN IE in beacon and probe responses.

```
[AC-wlan-st-st1] cipher-suite ccmp
```

```
[AC-wlan-st-st1] security-ie rsn
```

Enable the AC to forward client data traffic. If the AC forwards client data traffic by default, skip this step.

```
[AC-wlan-st-st1] client forwarding-location ac
```

```
[AC-wlan-st-st1] quit
```

4. Configure AP settings:

! IMPORTANT:

In a large-scale network, configure AP groups as a best practice.

Create an AP named **office** with model WA4320i-ACN and set its serial ID to 219801A0CNC138011454.

```
[AC] wlan ap office model AP 3620
```

```
[AC-wlan-ap-office] serial-id 219801A28N819CE0002T
```

```
[AC-wlan-ap-office] quit
```

Create AP group **group1** and create an AP grouping rule by AP names to add AP **office** to AP group **group1**.

```
[AC] wlan ap-group group1
```

```
[AC-wlan-ap-group-group1] ap office
```

Bind service template **st1** to radio 2 in AP group **group1**.

```
[AC-wlan-ap-group-group1] ap-model AP 3620
```

```
[AC-wlan-ap-group-group1-ap-model-AP 3620] radio 2
```

```
[AC-wlan-ap-group-group1-ap-model-AP 3620-radio-2] service-template st1
```

Enable radio 2.

```
[AC-wlan-ap-group-group1-ap-model-AP 3620-radio-2] radio
```

```
enable [AC-wlan-ap-group-group1-ap-model-AP 3620-radio-2] quit
```

```
[AC-wlan-ap-group-group1-ap-model-AP 3620]
```

```
quit [AC-wlan-ap-group-group1] quit
```

5. Configure a RADIUS scheme:

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

```
[AC] radius scheme rs1
```

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

```
[AC-radius-rs1] primary authentication 192.168.0.111
```

```
[AC-radius-rs1] primary accounting 192.168.0.111
```

```
[AC-radius-rs1] key authentication simple radius
```

```
[AC-radius-rs1] key accounting simple radius
```

Configure the AC to remove the domain name from the usernames sent to the RADIUS servers.

```
[AC-radius-rs1] user-name-format without-domain
```

Configure the source IP address for outgoing RADIUS packets as 2.2.2.1.

```
[AC-radius-rs1] nas-ip 2.2.2.1
```

```
[AC-radius-rs1] quit
```

Enable RADIUS session-control.

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

Enable the RADIUS DAS feature and enter RADIUS DAS view.

```
[AC] radius dynamic-author server
```

Specify a session-control client with IP address 192.168.0.111 and shared key **radius** in plaintext form.

```
[AC-radius-da-server] client ip 192.168.0.111 key simple radius
```

```
[AC-radius-da-server] quit
```

6. Configure authentication domain **dm2**:

Create an ISP domain named **dm2** and enter its view.

```
[AC] domain dm2
```

Configure the authentication, authorization, and accounting scheme RADIUS scheme **rs1** for LAN access users in the ISP domain.

```
[AC-isp-dm2] authentication lan-access radius-scheme rs1
```

```
[AC-isp-dm2] authorization lan-access radius-scheme rs1
```

```
[AC-isp-dm2] accounting lan-access radius-scheme rs1
```

```
[AC-isp-dm2] quit
```

7. Configure authentication domain **dm1**:

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

```
[AC] domain dm1
```

Configure the authentication and authorization methods as RADIUS and the accounting method as none for portal users in the ISP domain.

```
[AC-isp-dm1] authentication portal radius-scheme rs1
```

```
[AC-isp-dm1] authorization portal radius-scheme rs1
```

```
[AC-isp-dm1] accounting portal none
```

Set the idle timeout period to 15 minutes and the minimum traffic that must be generated in the idle timeout period to 1024 bytes.

```
[AC-isp-dm1] authorization-attribute idle-cut 15 1024
```

```
[AC-isp-dm1] quit
```

8. Configure portal authentication:

Create a portal authentication server.

```
[AC] portal server newpt
```

```
[AC-portal-server-newpt] ip 192.168.0.111 key simple 123456
```

```
[AC-portal-server-newpt] port 50100
```

Specify CMCC as the type of portal authentication server **newpt**.

```
[AC-portal-server-newpt] server-type cmcc
```

```
[AC-portal-server-newpt] quit
```

Specify **http://192.168.0.111:8080/portal** as the URL of portal Web server **newpt**.

```
[AC] portal web-server newpt
```

```
[AC-portal-websvr-newpt] url http://192.168.0.111:8080/portal
```

Configure the portal redirection URL to carry the **ssid**, **wlanuserip**, and **wlanacname** parameters, and their values are the wireless SSID, the user's IP address, and the AC's name (required by a CMCC portal Web server).

```
[AC-portal-websvr-newpt] url-parameter ssid ssid
```

```
[AC-portal-websvr-newpt] url-parameter wlanuserip source-address
```

```
[AC-portal-websvr-newpt] url-parameter wlanacname value AC
```

Specify CMCC as the type of portal Web server **newpt**.

```
[AC-portal-websvr-newpt] server-type cmcc
```

```
[AC-portal-websvr-newpt] quit
```

Configure a portal-free rule numbered **0** to allow portal users to access the portal Web server (whose IP address is 192.168.0.111) without authentication.


```

[AC] portal free-rule 0 destination ip 192.168.0.111 24
# Configure a portal-free rule to permit traffic from aggregate interface 1.
[AC] portal free-rule 1 source interface Bridge-Aggregation 1
# Configure destination-based portal-free rules to permit traffic destined for the DNS server.
[AC] portal free-rule 2 destination ip any udp 53
[AC] portal free-rule 3 destination ip any tcp 53
# Enable portal roaming.
[AC] portal roaming enable
# Disable the Rule ARP entry feature for portal clients.
[AC] undo portal refresh arp enable
# Enable validity check on wireless portal clients.
[AC] portal host-check enable
# Enable direct portal authentication on service template st1.
[AC] wlan service-template st1
[AC-wlan-st-st1] portal enable method direct
# Specify ISP domain dm1 as the portal authentication domain.
[AC-wlan-st-st1] portal domain dm1
# Specify portal Web server newpt on service template st1 for portal authentication.
[AC-wlan-st-st1] portal apply web-server newpt
# Configure the source IP address for outgoing portal packets as 2.2.2.1.
[AC-wlan-st-st1] portal bas-ip 2.2.2.1
[AC-wlan-st-st1] quit
9. Configure MAC authentication:
# Set the authentication mode to mac for WLAN clients on service template st1.
[AC-wlan-st-st1] client-security authentication-mode mac
# Configure the AC to ignore MAC authentication failures on service template st1.
[AC-wlan-st-st1] client-security ignore-authentication
# Specify ISP domain dm2 as the authentication domain for MAC authentication clients on
service template st1.
[AC-wlan-st-st1] mac-authentication domain dm2
# Enable service template st1.
[AC-wlan-st-st1] service-template enable
[AC-wlan-st-st1] quit

```

Configuring the switch

```

# Create VLAN 100. The switch will use this VLAN to forward traffic on the CAPWAP tunnel between
the AC and the AP.
<Switch> system-view
[Switch] vlan 100
[Switch-vlan100] quit
# Create VLAN 200. The switch will use this VLAN to forward client traffic.
[Switch] vlan 200
[Switch-vlan200] quit
# Create VLAN 2.
[Switch] vlan 2
[Switch-vlan2] quit

```

Configure GigabitEthernet 1/0/1 (the port connected to the AC) as a trunk port and assign the port to VLAN 100 and VLAN 200.

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[Switch-GigabitEthernet1/0/1] quit
```

Configure GigabitEthernet 1/0/2 (the port connected to the AP) as an access port and assign the port to VLAN 100.

```
[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] port link-type access
[Switch-GigabitEthernet1/0/2] port access vlan 100
```

Enable PoE.

```
[Switch-GigabitEthernet1/0/2] poe enable
[Switch-GigabitEthernet1/0/2] quit
```

Configure GigabitEthernet 1/0/3 (the port connected to the INC server) as an access port and assign the access port to VLAN 2.

```
[Switch] interface gigabitethernet 1/0/3
[Switch-GigabitEthernet1/0/3] port link-type access
[Switch-GigabitEthernet1/0/3] port access vlan 2
[Switch-GigabitEthernet1/0/3] quit
```

Assign an IP address to VLAN-interface 200.

```
[Switch] interface vlan-interface 200
[Switch-Vlan-interface200] ip address 2.2.2.100 255.255.255.0
[Switch-Vlan-interface200] quit
```

Assign an IP address to VLAN-interface 2.

```
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] ip address 192.168.0.100 255.255.255.0
[Switch-Vlan-interface2] quit
```

Verifying the configuration

1. Verify that the client needs to pass portal authentication when the client attempts to come online for the first time.

In this case, the RADIUS server does not have the user and its MAC address information. The AC determines that the user has failed the MAC authentication and performs portal authentication for the user.

Display information about all online portal users on the AC.

```
[AC] display portal user all
```

Total portal users: 1

Username: client

AP name: office

Radio ID: 2

SSID: service

Portal server: newpt

State: Online

VPN instance: N/A

MAC	IP	VLAN	Interface
0021-6330-0933	2.2.2.2	200	WLAN-BSS1/0/2

```
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
```

2. Log out then log in again.

After the client passes portal authentication, the RADIUS server records the user and MAC address information. When the client goes offline and then tries to access the network again, the AC determines that the client has passed MAC authentication and does not perform portal authentication for the client, either.

3. Verify that the client has passed MAC authentication.

Display information about online MAC authentication users on the AC.

```
[AC] display mac-authentication connection
User MAC address           : 0021-6330-0933
AP name                    : office
Radio ID                   : 2
SSID                      : service
BSSID                     : 70ba-efaf-ddb0
Username                   : 002163300933
Authentication domain      : dm2
Initial VLAN               : 200
Authorization VLAN         : 200
Authorization ACL number   : N/A
Authorization user profile : N/A
Termination action        : Default
Session timeout period     : 86401 s
Online from                : 2016/04/22 18:56:20
```

Configuration files

- **AC:**

```
#
vlan 100
#
vlan 200
#
wlan service-template st1
  ssid service
  vlan 200
  client forwarding-location ac
  akm mode psk
  preshared-key pass-phrase cipher $c$3$oLf6pOZ6bxrf25nodjOJKYEfnZ6g6ErccHyQ
  cipher-suite ccmp
  security-ie rsn
  client-security authentication-mode mac
  client-security ignore-authentication
```

```

mac-authentication domain dm2
portal enable method direct
portal domain dm1
portal bas-ip 2.2.2.1
portal apply web-server newpt
service-template enable
#
interface Vlan-interface100
 ip address 2.2.1.1 255.255.255.0
#
interface Vlan-interface200
 ip address 2.2.2.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 100 200
#
 ip route-static 192.168.0.0 16 2.2.2.100
#
 radius session-control enable
#
radius scheme rs1
 primary authentication 192.168.0.111
 primary accounting 192.168.0.111
 key authentication cipher $c$3$Sggqz7lDs4XPnethmAgyAKVlke7qwEkYbQ==
 key accounting cipher $c$3$4J/JBRGwqB4F213furJmKB6JWYXBFjWE6g==
 user-name-format without-domain
nas-ip 2.2.2.1
#
radius dynamic-author server
 client ip 192.168.0.111 key cipher $c$3$AkTEB7OgMYnCqsfDeplhoAgXUek/rVrLZw==
#
domain dm1
 authorization-attribute idle-cut 15 1024
 authentication portal radius-scheme rs1
 authorization portal radius-scheme rs1
 accounting portal none
#
domain dm2
 authorization-attribute idle-cut 15 1024
 authentication lan-access radius-scheme rs1
 authorization lan-access radius-scheme rs1
 accounting lan-access radius-scheme rs1
#
portal host-check enable
portal free-rule 0 destination ip 192.168.0.0 255.255.255.0
portal free-rule 1 source interface Bridge-Aggregation 1

```

```

portal free-rule 2 destination ip any udp 53
portal free-rule 3 destination ip any tcp 53
#
portal roaming enable
undo portal refresh arp enable
#
portal web-server newpt
url http://192.168.0.111:8080/portal
server-type cmcc
url-parameter ssid ssid
url-parameter wlanacname value AC
url-parameter wlanuserip source-address
#
portal server newpt
ip 192.168.0.111 key cipher $c$3$jiLQ5VIGG4TF7R3sHTT07bmv9rtiSQYBzQ==
server-type cmcc
#
wlan ap-group group1
ap office
ap-model AP 3620
radio 1
radio 2
radio enable
service-template st1
#
wlan ap office model AP 3620
serial-id 219801A28N819CE0002T
#

```

- **Switch:**

```

#
vlan 2
#
vlan 100
#
vlan 200
#
interface Vlan-interface2
ip address 192.168.0.100 255.255.255.0
#
interface Vlan-interface200
ip address 2.2.2.100 255.255.255.0
#
interface GigabitEthernet1/0/1
port link-type trunk
port trunk permit vlan 1 100 200
#
interface GigabitEthernet1/0/2
port link-type access

```

```
port access vlan 100
poe enable
#
interface GigabitEthernet1/0/3
port link-type access
port access vlan 2
#
```

Related documentation

- *AP and WT Management Command Reference in INTELBRAS Access Controllers Command References*
- *AP and WT Management Configuration Guide in INTELBRAS Access Controllers Configuration Guides*
- *User Access and Authentication Command Reference in INTELBRAS Access Controllers Command References*
- *User Access and Authentication Configuration Guide in INTELBRAS Access Controllers Configuration Guides*
- *WLAN Access Command Reference in INTELBRAS Access Controllers Command References*
- *WLAN Access Configuration Guide in INTELBRAS Access Controllers Configuration Guides*

INTELBRAS Access Controllers

Remote AP, Remote Portal, and MAC-Trigger Authentication

Configuration Examples

Copyright © 2024 Intelbras S.A All rights reserved.

No part of this manual may be reproduced or transmitted in any form or by any means without prior written consent of Intelbras S.A

Except for the trademarks of Intelbras S.A, any trademarks that may be mentioned in this document are the property of their respective owners.

The information in this document is subject to change without notice.

Contents

Introduction	1
Prerequisites	1
Example: Configuring remote AP, remote portal, and MAC-trigger authentication	1
Network configuration	1
Analysis	2
Restrictions and guidelines	2
Procedures	3
Configuring INC	3
Editing a configuration file for the AP	9
Configuring the AC	9
Configuring the switch	12
Verifying the configuration	13
Configuration files	14
Related documentation	17

Introduction

The following information provides examples for configuring remote AP, remote portal, and MAC-trigger authentication.

Prerequisites

The following information applies to Comware-based access controllers and access points. Procedures and information in the examples might be slightly different depending on the software or hardware version of the access controllers and access points.

The configuration examples 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.

The following information is provided based on the assumption that you have basic knowledge of AAA, portal, WLAN, and remote AP.

Example: Configuring remote AP, remote portal, and MAC-trigger authentication

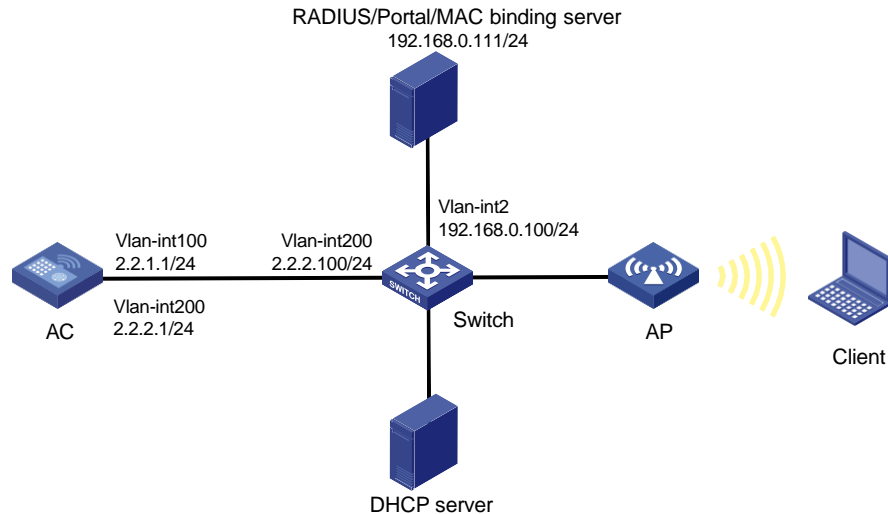
Network configuration

As shown in [Figure 1](#), the AP and the client obtain IP addresses from the DHCP server. The INC server acts as a portal authentication server, a portal Web server, a MAC binding server, and a RADIUS server.

Configure the devices to meet the following requirements:

- The AC provides direct portal authentication for the client. Before passing the authentication, the client can access only the portal Web server. After passing the authentication, the client can access other network resources. If the client goes offline and then attempts to come online again, the client does not need to enter the username and password.
- The client can access network resources through any Layer 2 ports in its access VLAN without re-authentication.
- After the AP is disconnected from the AC, the client can access the network without authentication.
- The RADIUS server can dynamically change user authorization information or forcibly disconnect users.
- The AP forwards the client traffic locally.

Figure 1 Network diagram



Analysis

For the client to access network resources through any Layer 2 ports in its access VLAN without re-authentication, enable portal roaming.

For the RADIUS server to dynamically change the user authorization information or forcibly disconnect users, enable the RADIUS session-control feature.

To use GigabitEthernet 1/0/1 on the AP to forward client traffic, edit a .txt configuration file and upload the file to the AC.

To ensure that dynamic user authorization information can be correctly assigned to users after they come online, enable the RADIUS DAS feature.

Restrictions and guidelines

- Use the actual serial ID of an AP to uniquely identify that AP.
- Make sure the types of the portal authentication server, portal Web server, and MAC binding server specified on the AC are the same as those actually used. (This example uses CMCC servers.)
- By default, the URL of the portal Web server to which the AC redirects portal users does not carry any parameters. You can add parameters to be carried in the URL as needed.
- If portal authentication is enabled on a VLAN interface, the AC can forward client traffic. If portal authentication is enabled on a service template, both the AC and the AP can forward client traffic. (In this example, portal authentication is enabled on a service template and the AP forwards client traffic locally.)
- The remote AP feature takes effect only when the AP forwards the client traffic locally.
- In wireless networks where the AP forwards client traffic, the AC does not have ARP entries for clients. Therefore, the AC cannot check the validity of portal clients by using ARP entries. To ensure that valid users can perform portal authentication, enable wireless client validity check on the AC.
- If a portal client logs out and then tries to come online frequently in a short time, the client will fail portal authentication. To avoid this problem, disable the Rule ARP entry feature for portal clients.

- Some endpoints by default use random MAC addresses. For transparent MAC authentication to take effect on such an endpoint, disable the endpoint from using a random MAC address.
- As a best practice, use the plaintext form or PSK encryption for traffic if the AP acts as both an authenticator and a forwarder.

Procedures

Configuring INC

This example uses the INC server to describe the RADIUS server, portal server, and MAC binding server configuration. The INC server runs on INC PLAT 7.1 (E0303p13), INC INC - EIA 7.1 (F0302p08), and INC EIP 7.1 (F0302p08).

Configuring the RADIUS server

Add the AC to INC as an access device:

1. Log in to INC and click the **User** tab.
2. From the navigation tree, select **User Access Policy > Access Device Management > Access Device**.
3. Click **Add** to open the page as shown in [Figure 2](#).
4. In the **Access Configuration** area, configure the parameters as follows:
 - Set the shared key to **radius**, which must be the same as that on the AC.
 - Use the default values for other parameters.
5. In the **Device List** area, click **Add Manually** to open the **Add Access Device Manually** page. Enter **2.2.2.1** in the **Start IP** field and then click **OK**.
6. Click **OK**.

Figure 2 Adding the AC as an access device

Navigation: User > User Access Policy > Access Device Management > Access Device > Add Access Device

Access Configuration

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

Device List

Device Name	Device IP	Device Model	Comments	Delete
	2.2.2.1			

Total Items: 1.

Configuring the portal server

1. Configure the portal authentication service:
 - a. Click the **User** tab.

- b. From the navigation tree, select **User Access Policy > Portal Service > Server** to open the portal server configuration page, as shown in [Figure 3](#).
- c. Configure the portal server parameters as needed.
This example uses the default values.
- d. Click **OK**.

Figure 3 Portal authentication server configuration

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 ? LB Device Address

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://192.168.0.111:8080/portal/

192.168.0.111

2. Configure an IP address group:
 - a. From the navigation tree, select **User Access Policy > Portal Service > IP Group**.
 - b. Click **Add** to open the page as shown in [Figure 4](#).
 - c. Enter the IP group name.
 - d. Enter the start IP address and end IP address of the IP group.
Make sure the client IP address is in the IP group.
 - e. Select a service group.
This example uses the default value **Ungrouped**.
 - f. From the **Action** list, select **Normal**.
 - g. Click **OK**.

Figure 4 Adding an IP address group

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

OK Cancel

3. Add a portal device:
 - a. From the navigation tree, select **User Access Policy > Portal Service > Device**.
 - b. Click **Add** to open the page as shown in Figure 5.
 - c. Enter the device name.
 - d. Select **CMCC 1.0** for **Version**.
 - e. Enter the IP address of the AC's interface connected to the client.
 - f. 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**.
 - g. Enter the key, which must be the same as that configured on the AC.
 - h. Select **Directly Connected** for **Access Method**.
 - i. Use the default settings for other parameters.
 - j. Click **OK**.

Figure 5 Adding a portal device

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

Add Device

Device Information

Device Name * NAS

Version * CMCC 1.0

Listening Port * 2000

Authentication Retries * 0

Support Server Heartbeat * No

Key * *****

Access Method * Directly Connected

Device Description

Service Group * Ungrouped

IP Address * 2.2.2.1

Local Challenge * No

Logout Retries * 1

Support User Heartbeat * No

Confirm Key * *****

OK Cancel


4. Associate the portal device with the IP address group:
 - a. As shown in Figure 6, click the **Port Group** icon  in the **Operation** field for device **NAS** to open the port group configuration page.

Figure 6 Device list

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	CMCC 1.0	Ungrouped	2.2.2.1		Not Deployed	

1-1 of 1, Page 1 of 1

- b. Click **Add** to open the page as shown in Figure 7.
- 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. Select **Supported** for **Transparent Authentication**.
- f. Use the default settings for other parameters.
- g. Click **OK**.

Figure 7 Adding a port group

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

Add Port Group

Port Group Name *

Start Port *

Protocol *

NAT or Not *

Authentication Type *

Heartbeat Interval(Minutes) *

User Domain

Transparent Authentication

Page Push Policy

Language *

End Port *

Quick Authentication *

Error Transparent Transmission *

IP Group *

Heartbeat Timeout(Minutes) *

Port Group Description

Client Protection Against Cracks *

Default Authentication Page

OK Cancel

5. From the navigation tree, select **User Access Policy > Service Parameters > Validate System Configuration** to validate the configuration.

Configuring the MAC binding server

1. Add an access policy:
 - a. From the navigation tree, select **User Access Policy > Access Policy**.
 - b. Click **Add** to open the page as shown in Figure 8.
 - c. Enter the access policy name.
 - d. Select a service group.
This example uses the default value **Ungrouped**.
 - e. Use the default settings for other parameters.
 - f. Click **OK**.

Figure 8 Adding an access policy

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

Basic Information

Access Policy Name *

Service Group *

Description

Authorization Information

Access Period

Allocate IP *

Downstream Rate(Kbps)

Upstream Rate(Kbps)

Priority

☐ RSA Authentication

Certificate Authentication ☒ None ☐ EAP

Certificate Type

Deploy VLAN

☐ Deploy User Profile

Deploy User Group

☐ Deploy ACL

2. Add an access service:
 - a. From the navigation tree, select **User Access Policy > Access Service**.
 - b. Click **Add** to open the page as shown in [Figure 9](#).
 - c. Enter the service name.
 - d. Select the **Transparent Authentication on Portal Endpoints** option.
 - e. Use the default settings for other parameters.
 - f. Click **OK**.

Figure 9 Adding an access service

User > User Access Policy > Access Service > Modify Access Service ? Help

Basic Information

Service Name *

Service Suffix

Service Group *

Default Access Policy *

Default Proprietary Attribute Assignment Policy *

Default Max. Number of Bound Endpoints *

Default Max. Number of Online Endpoints *

Description

☒ Available ☒ Transparent Authentication on Portal Endpoints

3. Add an access user:
 - a. From the navigation tree, select **Access User > Access User**.
 - b. Click **Add** to open the page as shown in [Figure 10](#).
 - c. Select an existing access user or click **Add User** to add a new access user.
 - d. Enter the account name.
 - e. Set the password.
 - f. Select access service **MAC_server**.
 - g. Use the default settings for other parameters.
 - h. Click **OK**.

Figure 10 Adding an access user

The screenshot shows the 'Add Access User' form. The breadcrumb is 'User > All Access Users > Add Access User'. The form is divided into two sections: 'Access Information' and 'Access Service'.

Access Information:

- User Name *: Client1 (with a 'Select' button and an 'Add User' button)
- Account Name *: client (with a help icon)
- Trial Account: ☐
- Default BYOD User: ☐
- MAC Authentication User: ☐
- Computer User: ☐
- Fast Access User: ☐
- Password *: *****
- Confirm Password *: *****
- Allow User to Change Password: ☒
- Enable Password Strategy: ☐
- Modify Password at Next Login: ☐
- Start Time: [empty field]
- End Time: [empty field]
- Max. Idle Time (Minutes): [empty field]
- Max. Concurrent Logins: 1
- Login Message: [empty field]

Access Service:

Service Name	Service Suffix	Status	Allocate IP
<input checked="" type="checkbox"/> MAC_server		Available	

4. Configure system parameters:
 - a. From the navigation tree, select **User Access Policy > Service Parameters > System Settings**.
 - b. Click the **Configure** icon for **User Endpoint Settings** to open the page as shown in [Figure 11](#).
 - c. Select whether to enable transparent portal authentication on non-smart devices.
In this example, select **Enable** for **Non-Terminal Authentication**.
 - d. Click **OK**.

Figure 11 Configuring user endpoint settings

The screenshot shows the 'User Endpoint Settings' form. The breadcrumb is 'User > User Access Policy > Service Parameters > System Settings > User Endpoint Settings'.

User Endpoint Settings:

- Transparent MAC Authentication: Disable (dropdown)
- Max. Device for Single Account *: 10 (text field)
- Non-Terminal Authentication: Enable (dropdown with a help icon)
- Log off User with Endpoint Conflict: No (dropdown)

Buttons: OK, Cancel

- e. Click the **Configure** icon for **Endpoint Aging Time** to open the page as shown in [Figure 12](#).
 - f. Set the endpoint aging time as needed.
This example uses the default value.
 - g. Click **OK**.

Figure 12 Setting the endpoint aging time

The screenshot shows the 'Modify Endpoint Aging Time' form. The breadcrumb is 'User > User Access Policy > Service Parameters > System Settings > Endpoint Aging Time > Modify Endpoint Aging Time'.

Modify Endpoint Aging Time:

- Endpoint Aging Time(Days) *: 7 (text field with a help icon)

Buttons: OK, Cancel

5. From the navigation tree, select **User Access Policy > Service Parameters > Validate** to make the configuration take effect.

Editing a configuration file for the AP

Create a .txt configuration file named **map.txt**.

Enter the following content in the file.

```
System-view
vlan 200
interface gigabitethernet1/0/1
port link-type trunk
port trunk permit vlan 200
```

Upload the file to the AC.

Configuring the AC

1. Configure interfaces on the AC:

Create VLAN 100 and VLAN-interface 100, and assign an IP address to the VLAN interface. The AC will use this IP address to establish a CAPWAP tunnel with the AP.

```
<AC> system-view
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 2.2.1.1 24
[AC-Vlan-interface100] quit
```

Create VLAN 200 and VLAN-interface 200, and assign an IP address to the VLAN interface. The AC will use VLAN 200 for client access.

```
[AC] vlan 200
[AC-vlan200] quit
[AC] interface vlan-interface 200
[AC-Vlan-interface200] ip address 2.2.2.1 24
[AC-Vlan-interface200] quit
```

Configure GigabitEthernet 1/0/1 (the port connected to the switch) as a trunk port and assign the port to VLANs 100 and 200.

```
[AC] interface gigabitethernet 1/0/1
[AC-GigabitEthernet1/0/1] port link-type trunk
[AC-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[AC-GigabitEthernet1/0/1] quit
```

2. Configure a static route to the INC server:

```
[AC] ip route-static 192.168.0.0 255.255.0.0 2.2.2.100
```

3. Configure a WLAN service:

Create a service template named **st1** and enter its view.

```
[AC] wlan service-template st1
```

Set the SSID of service template **st1** to **service**.

```
[AC-wlan-st-st1] ssid service
```

Assign clients coming online through service template **st1** to VLAN 200.

```
[AC-wlan-st-st1] vlan 200
```

Set the PSK AKM mode and configure simple character string of **12345678** as the PSK.

```
[AC-wlan-st-st1] akm mode psk
```

```
[AC-wlan-st-st1] preshared-key pass-phrase simple 12345678
```

Set the CCMP cipher suite for frame encryption and enable the RSN IE in beacon and probe responses.

```
[AC-wlan-st-st1] cipher-suite ccmp
```

```
[AC-wlan-st-st1] security-ie rsn
```

Use APs to forward client data traffic from VLAN 200. If APs forward client data traffic by default, skip this step.

```
[AC-wlan-st-st1] client forwarding-location ap vlan 200
```

Enable client association at APs and specify APs as authenticators to ensure that new endpoints can come online successfully.

```
[AC-wlan-st-st1] client association-location ap
```

```
[AC-wlan-st-st1] client-security authentication-location ap
```

```
[AC-wlan-st-st1] quit
```

4. Configure AP settings:

! IMPORTANT:

In a large-scale network, configure AP groups as a best practice.

Create an AP named **office** with model AP 3620 and set its serial ID to 219801A28N819CE0002T.

```
[AC] wlan ap office model AP 3620
```

```
[AC-wlan-ap-office] serial-id 219801A28N819CE0002T
```

```
[AC-wlan-ap-office] quit
```

Create AP group **group1** and create an AP grouping rule by AP names to add AP **office** to AP group **group1**.

```
[AC] wlan ap-group group1
```

```
[AC-wlan-ap-group-group1] ap office
```

Enable remote AP.

```
[AC-wlan-ap-group-group1] hybrid-remote-ap enable
```

Deploy configuration file **map.txt** to APs with model WA632 in AP group **group1**.

```
[AC-wlan-ap-group-group1] ap-model AP 3620
```

```
[AC-wlan-ap-group-group1-ap-model-AP 3620] map-configuration map.txt
```

Bind service template **st1** to radio 2 in AP group **group1**.

```
[AC-wlan-ap-group-group1-ap-model-AP 3620] radio 2
```

```
[AC-wlan-ap-group-group1-ap-model-AP 3620-radio-2] service-template st1
```

Enable radio 2.

```
[AC-wlan-ap-group-group1-ap-model-AP 3620-radio-2] radio
```

```
enable [AC-wlan-ap-group-group1-ap-model-AP 3620-radio-2] quit
```

```
[AC-wlan-ap-group-group1-ap-model-AP 3620]
```

```
quit [AC-wlan-ap-group-group1] quit
```

5. Configure a RADIUS scheme:

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

```
[AC] radius scheme rs1
```

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

```
[AC-radius-rs1] primary authentication 192.168.0.111
```

```
[AC-radius-rs1] primary accounting 192.168.0.111
```

```
[AC-radius-rs1] key authentication simple radius
```

```
[AC-radius-rs1] key accounting simple radius
```

Configure the AC to remove the domain name from the usernames sent to the RADIUS servers.

```
[AC-radius-rs1] user-name-format without-domain
```

Configure the source IP address for outgoing RADIUS packets as 2.2.2.1.

```
[AC-radius-rs1] nas-ip 2.2.2.1
```

```
[AC-radius-rs1] quit
```

Enable RADIUS session-control.

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

Enable the RADIUS DAS feature and enter RADIUS DAS view.

```
[AC] radius dynamic-author server
```

Specify a session-control client with IP address 192.168.0.111 and shared key **radius** in plaintext form.

```
[AC-radius-da-server] client ip 192.168.0.111 key simple radius
```

```
[AC-radius-da-server] quit
```

6. Configure an authentication domain:

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

```
[AC] domain dm1
```

Configure the authentication and authorization methods as RADIUS and the accounting method as none in the ISP domain.

```
[AC-isp-dm1] authentication portal radius-scheme rs1
```

```
[AC-isp-dm1] authorization portal radius-scheme rs1
```

```
[AC-isp-dm1] accounting portal none
```

Set the idle timeout period to 15 minutes and the minimum traffic that must be generated in the idle timeout period to 1024 bytes.

```
[AC-isp-dm1] authorization-attribute idle-cut 15 1024
```

```
[AC-isp-dm1] quit
```

7. Configure portal authentication:

Create a portal authentication server.

```
[AC] portal server newpt
```

```
[AC-portal-server-newpt] ip 192.168.0.111 key simple 123456
```

```
[AC-portal-server-newpt] port 50100
```

Specify CMCC as the type of portal authentication server **newpt**.

```
[AC-portal-server-newpt] server-type cmcc
```

```
[AC-portal-server-newpt] quit
```

Specify **http://192.168.0.111:8080/portal** as the URL of portal Web server **newpt**.

```
[AC] portal web-server newpt
```

```
[AC-portal-websvr-newpt] url http://192.168.0.111:8080/portal
```

Configure the portal redirection URL to carry the **ssid**, **wlanuserip**, and **wlanacname** parameters, and their values are the wireless SSID, the user's IP address, and the AC's name (required by a CMCC portal Web server).

```
[AC-portal-websvr-newpt] url-parameter ssid ssid
```

```
[AC-portal-websvr-newpt] url-parameter wlanuserip source-address
```

```
[AC-portal-websvr-newpt] url-parameter wlanacname value AC
```

Specify CMCC as the type of portal Web server **newpt**.

```
[AC-portal-websvr-newpt] server-type cmcc
```

```
[AC-portal-websvr-newpt] quit
```

Configure a portal-free rule numbered **0** to allow portal users to access the portal Web server (whose IP address is 192.168.0.111) without authentication.

```

[AC] portal free-rule 0 destination ip 192.168.0.111 24
# Configure a portal-free rule to permit traffic from aggregate interface 1.
[AC] portal free-rule 1 source interface Bridge-Aggregation 1
# Configure destination-based portal-free rules to permit traffic destined for the DNS server.
[AC] portal free-rule 2 destination ip any udp 53
[AC] portal free-rule 3 destination ip any tcp 53
# Enable portal roaming.
[AC] portal roaming enable
# Disable the Rule ARP entry feature for portal clients.
[AC] undo portal refresh arp enable
# Enable validity check on wireless portal clients.
[AC] portal host-check enable
# Enable direct portal authentication on service template st1.
[AC] wlan service-template st1
[AC-wlan-st-st1] portal enable method direct
# Specify ISP domain dm1 as the portal authentication domain.
[AC-wlan-st-st1] portal domain dml
# Specify portal Web server newpt on service template st1 for portal authentication.
[AC-wlan-st-st1] portal apply web-server newpt
[AC-wlan-st-st1] quit

```

8. Configure MAC-trigger authentication (portal MAC-based quick authentication):

```

# Create a MAC binding server named mts and enter its view.
[AC] portal mac-trigger-server mts
# Specify 192.168.0.111 as the IP address of MAC binding server mts.
[AC-portal-mac-trigger-server-mts] ip 192.168.0.111
# Specify CMCC as the type of MAC binding server mts.
[AC-portal-mac-trigger-server-mts] server-type cmcc
[AC-portal-mac-trigger-server-mts] quit
# Specify MAC binding server mts on service template st1.
[AC] wlan service-template st1
[AC-wlan-st-st1] portal apply mac-trigger-server mts
# Configure the source IP address for outgoing portal packets as 2.2.2.1.
[AC-wlan-st-st1] portal bas-ip 2.2.2.1
# Enable service template st1.
[AC-wlan-st-st1] service-template enable
[AC-wlan-st-st1] quit

```

Configuring the switch

Create VLAN 100. The switch will use this VLAN to forward traffic on the CAPWAP tunnel between the AC and the AP.

```

<Switch> system-view
[Switch] vlan 100
[Switch-vlan100] quit

```

Create VLAN 200. The switch will use this VLAN to forward client traffic.

```

[Switch] vlan 200
[Switch-vlan200] quit

```

Create VLAN 2. The switch will use this VLAN to connect to the INC server.

```
[Switch] vlan 2
[Switch-vlan2] quit
```

Configure GigabitEthernet 1/0/1(the port connected to the AC) as a trunk port and assign the port to VLAN 100 and VLAN 200.

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[Switch-GigabitEthernet1/0/1] quit
```

Configure GigabitEthernet 1/0/2 (the port connected to the AP) as a trunk port and assign the port to VLAN 100 and VLAN 200. Set the PVID of the port to VLAN 100.

```
[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] port link-type trunk
[Switch-GigabitEthernet1/0/2] port trunk permit vlan 100 200
[Switch-GigabitEthernet1/0/2] port trunk pvid vlan 100
```

Enable PoE on GigabitEthernet 1/0/2.

```
[Switch-GigabitEthernet1/0/2] poe enable
[Switch-GigabitEthernet1/0/2] quit
```

Configure GigabitEthernet 1/0/3 (the port connected to the INC server) as an access port and assign the access port to VLAN 2.

```
[Switch] interface gigabitethernet 1/0/3
[Switch-GigabitEthernet1/0/3] port link-type access
[Switch-GigabitEthernet1/0/3] port access vlan 2
[Switch-GigabitEthernet1/0/3] quit
```

Assign an IP address to VLAN-interface 200.

```
[Switch] interface vlan-interface 200
[Switch-Vlan-interface200] ip address 2.2.2.100 255.255.255.0
[Switch-Vlan-interface200] quit
```

Assign an IP address to VLAN-interface 2.

```
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] ip address 192.168.0.100 255.255.255.0
[Switch-Vlan-interface2] quit
```

Verifying the configuration

Display information about MAC binding server mts.

```
[AC] display portal mac-trigger-server name mts
Portal mac trigger server name: mts

  Version           : 1.0
  Server type       : CMCC
  IP                 : 192.168.0.111
  Port              : 50100
  VPN instance      : Not configured
  Aging time        : 300 seconds
  Free-traffic threshold : 0 bytes
  NAS-Port-Type     : Not configured
  Binding retry times : 3
```

```

Binding retry interval   : 1 seconds
Authentication timeout   : 3 minutes
Excluded attribute list  : 1
Local-binding            : Disabled
Local-binding aging-time : 12 hours
AAA-fail nobinding       : Disabled

```

A user can perform portal authentication through a Web browser. Before passing portal authentication, the user can access only the authentication page **http://192.168.0.111:8080/portal**. All Web requests from the user will be redirected to the authentication page. After passing portal authentication, the user can access other network resources.

For the first portal authentication, the user is required to enter the username and password. When the user goes offline and then accesses the network again, the user does not need to enter the authentication username and password.

Display information about all portal users.

```

[AC] display portal user all
Total portal users: 1
Username: Client
  AP name: office
  Radio ID: 2
  SSID: service
  Portal server: newpt
  State: Online
  VPN instance: N/A
  MAC          IP          VLAN   Interface
  0021-6330-0933 2.2.2.2    200    WLAN-BSS1/0/1
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

- AC:


```

#
vlan 100
#
vlan 200
#
wlan service-template st1
  ssid service
  vlan 200
  client association-location ap
  client forwarding-location ap vlan 200
  client-security authentication-location ap
  akm mode psk

```

```

preshared-key pass-phrase cipher $c$3$0Lf6pOZ6bxrf25nodjOJKYEfnZ6g6ErccHyQ
cipher-suite ccmp
security-ie rsn
portal enable method direct
portal domain dm1
portal bas-ip 2.2.2.1
portal apply web-server newpt
portal apply mac-trigger-server mts
service-template enable
#
interface Vlan-interface100
ip address 2.2.1.1 255.255.255.0
#
interface Vlan-interface200
ip address 2.2.2.1 255.255.255.0
#
interface GigabitEthernet1/0/1
port link-type trunk
port trunk permit vlan 1 100 200
#
ip route-static 192.168.0.0 16 2.2.2.100
#
radius session-control enable
#
radius scheme rs1
primary authentication 192.168.0.111
primary accounting 192.168.0.111
key authentication cipher $c$3$Sqqqz7lDs4XPnethmAgyAKVlke7qwEkYbQ==
key accounting cipher $c$3$4J/JBRGwgqB4F213furJmKB6JWYXBFjWE6g==
user-name-format without-domain
nas-ip 2.2.2.1
#
radius dynamic-author server
client ip 192.168.0.111 key cipher $c$3$AkTEB7OgMYnCqsfDeplhoAgXUek/rVrLZw==
#
domain dm1
authorization-attribute idle-cut 15 1024
authentication portal radius-scheme rs1
authorization portal radius-scheme rs1
accounting portal none
#
portal host-check enable
portal free-rule 0 destination ip 192.168.0.0 255.255.255.0
portal free-rule 1 source interface Bridge-Aggregation 1
portal free-rule 2 destination ip any udp 53
portal free-rule 3 destination ip any tcp 53
#
portal roaming enable

```

```

undo portal refresh arp enable
#
portal web-server newpt
url http://192.168.0.111:8080/portal
server-type cmcc
url-parameter ssid ssid
url-parameter wlanacname value AC
url-parameter wlanuserip source-address
#
portal server newpt
ip 192.168.0.111
server-type cmcc
#
portal mac-trigger-server mts
ip 192.168.0.111 key cipher $c$3$AkTEB7OgMYnCqsfDeplhoAgXUek/rVrLZw==
server-type cmcc
#
wlan ap-group group1
ap office
hybrid-remote-ap enable
ap-model AP 3620
map-configuration flash:/map.txt
radio 1
radio 2
radio enable
service-template st1
#
wlan ap office model AP 3620
serial-id 219801A28N819CE0002T
#

```

- **Switch:**

```

#
vlan 2
#
vlan 100
#
vlan 200
#
interface Vlan-interface2
ip address 192.168.0.100 255.255.255.0
#
interface Vlan-interface200
ip address 2.2.2.100 255.255.255.0
#
interface GigabitEthernet1/0/1
port link-type trunk
port trunk permit vlan 1 100 200
#

```



```
interface GigabitEthernet1/0/2
port link-type trunk
  port trunk permit vlan 1 100 200
port trunk pvid vlan 100
poe enable
#
interface GigabitEthernet1/0/3
  port link-type access
  port access vlan 2
#
```

Related documentation

- *AP and WT Management Command Reference in INTELBRAS Access Controllers Command References*
- *AP and WT Management Configuration Guide in INTELBRAS Access Controllers Configuration Guides*
- *User Access and Authentication Command Reference in INTELBRAS Access Controllers Command References*
- *User Access and Authentication Configuration Guide in INTELBRAS Access Controllers Configuration Guides*
- *WLAN Access Command Reference in INTELBRAS Access Controllers Command References*
- *WLAN Access Configuration Guide in INTELBRAS Access Controllers Configuration Guides*

INTELBRAS Access Controllers

MAC Authentication with Guest VLAN

Assignment

Configuration Examples

Copyright © 2024 Intelbras S.A All rights reserved.

No part of this manual may be reproduced or transmitted in any form or by any means without prior written consent of Intelbras S.A

Except for the trademarks of Intelbras S.A, any trademarks that may be mentioned in this document are the property of their respective owners.

The information in this document is subject to change without notice.

Contents

Introduction	1
Prerequisites	1
Example: Configuring MAC authentication with guest VLAN assignment	1
Network configuration	1
Restrictions and guidelines	1
Procedures	2
Configuring the AC	2
Configuring the switch	5
Configuring the RADIUS server	5
Verifying the configuration	8
Configuration files	9
Related documentation	11

Introduction

The following information provides an example for configuring a guest VLAN for wireless clients that fail MAC authentication.

Prerequisites

The following information applies to Comware-based access controllers and access points. Procedures and information in the examples might be slightly different depending on the software or hardware version of the access controllers and access points.

The configuration examples 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.

The following information is provided based on the assumption that you have basic knowledge of AAA, MAC authentication, WLAN authentication, and WLAN access.

Example: Configuring MAC authentication with guest VLAN assignment

Network configuration

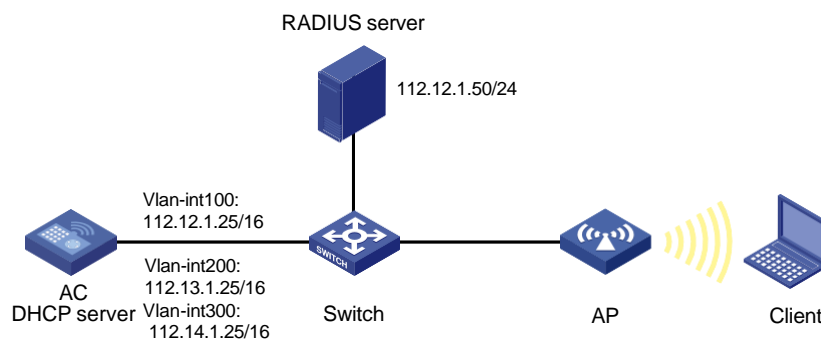
As shown in [Figure 1](#), the AC acts as a DHCP server to provide IP addresses for the AP and the client. The AC centrally forwards the client traffic.

To control the client's access to network resources, complete the following tasks:

- Configure VLAN 200 as the access VLAN of the client.
- Configure the AC to use the RADIUS server to perform MAC authentication for the client.
- Configure VLAN 300 as the guest VLAN on the service template that the client uses to access the network.

The device reauthenticates a client every 30 seconds in the guest VLAN.

Figure 1 Network diagram



Restrictions and guidelines

When you configure MAC authentication for wireless clients, follow these restrictions and guidelines:

- Use the actual serial ID of an AP to uniquely identify that AP.
- Remove the ports that connect the AC to the AP from VLAN 1 in case there are too many packets in VLAN 1.
- Some endpoints by default use random MAC addresses. To ensure successful MAC authentication for such an endpoint, disable the endpoint from using a random MAC address.

Procedures

Configuring the AC

1. Configure interfaces on the AC:

Create VLAN 100 and VLAN-interface 100, and assign an IP address to the VLAN interface. The AC will use this IP address to establish CAPWAP tunnels with the AP.

```
<AC> system-view
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 112.12.1.25 16
[AC-Vlan-interface100] quit
```

Create VLAN 200 and VLAN-interface 200, and assign an IP address to the VLAN interface. VLAN 200 will be used for client access.

```
[AC] vlan 200
[AC-vlan200] quit
[AC] interface vlan-interface 200
[AC-Vlan-interface200] ip address 112.13.1.25 16
[AC-Vlan-interface200] quit
```

Create VLAN 300 and VLAN-interface 300, and assign an IP address to the VLAN interface. The AC will use VLAN 300 as a guest VLAN to accommodate clients that fail MAC authentication.

```
[AC] vlan 300
[AC-vlan300] quit
[AC] interface vlan-interface 300
[AC-Vlan-interface300] ip address 112.14.1.25 16
[AC-Vlan-interface300] quit
```

Configure GigabitEthernet 1/0/1 (the port connected to the switch) as a trunk port, remove the port from VLAN 1, assign the port to VLANs 100, 200, and 300.

```
[AC] interface gigabitethernet 1/0/1
[AC-GigabitEthernet1/0/1] port link-type trunk
[AC-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[AC-GigabitEthernet1/0/1] port trunk permit vlan 100 200 300
[AC-GigabitEthernet1/0/1] quit
```

2. Configure DHCP:

Enable DHCP.

```
[AC] dhcp enable
```

Create a DHCP address pool named **vlan100**, and specify subnet 112.12.0.0/16 and gateway IP address 112.12.1.25 in the DHCP address pool.

```
[AC] dhcp server ip-pool vlan100
[AC-dhcp-pool-vlan100] network 112.12.0.0 mask 255.255.0.0
```

```
[AC-dhcp-pool-vlan100] gateway-list 112.12.1.25
[AC-dhcp-pool-vlan100] quit
```

Create a DHCP address pool named **vlan200**, and specify subnet 112.13.0.0/16 and gateway IP address 112.13.1.25 in the DHCP address pool. In this example, the address of the DNS server is 112.13.1.25 (the gateway address). You must replace it with the actual address of the DNS server on your network.

```
[AC] dhcp server ip-pool vlan200
[AC-dhcp-pool-vlan200] network 112.13.0.0 mask 255.255.0.0
[AC-dhcp-pool-vlan200] gateway-list 112.13.1.25
[AC-dhcp-pool-vlan200] dns-list 112.13.1.25
[AC-dhcp-pool-vlan200] quit
```

Create a DHCP address pool named **vlan300**, and specify subnet 112.14.0.0/16 and gateway IP address 112.14.1.25 in the DHCP address pool. In this example, the address of the DNS server is 112.14.1.25 (the gateway address). You must replace it with the actual address of the DNS server on your network.

```
[AC] dhcp server ip-pool vlan300
[AC-dhcp-pool-vlan300] network 112.14.0.0 mask 255.255.0.0
[AC-dhcp-pool-vlan300] gateway-list 112.14.1.25
[AC-dhcp-pool-vlan300] dns-list 112.14.1.25
[AC-dhcp-pool-vlan300] quit
```

3. Configure RADIUS-based MAC authentication:

Create a RADIUS scheme named **office** and enter its view.

```
[AC] radius scheme office
```

Specify the IP addresses of the primary authentication and accounting RADIUS servers.

```
[AC-radius-office] primary authentication 112.12.1.50
[AC-radius-office] primary accounting 112.12.1.50
```

Specify the shared keys for RADIUS authentication and accounting.

```
[AC-radius-office] key authentication simple 123456789
[AC-radius-office] key accounting simple 123456789
```

Exclude the ISP domain names from the usernames sent to the RADIUS servers.

```
[AC-radius-office] user-name-format without-domain
```

Specify IP address 112.12.1.25 as the source IP address for outgoing RADIUS packets.

```
[AC-radius-office] nas-ip 112.12.1.25
[AC-radius-office] quit
```

Create an ISP domain named **office1** and enter its view.

```
[AC] domain office1
```

Apply RADIUS scheme **office** to ISP domain **office1** for LAN user authentication, authorization, and accounting.

```
[AC-isp-office1] authentication lan-access radius-scheme office
[AC-isp-office1] authorization lan-access radius-scheme office
[AC-isp-office1] accounting lan-access radius-scheme office
```

Configure the idle cut feature for clients in ISP domain **office1**.

```
[AC-isp-office1] authorization-attribute idle-cut 15 1024
[AC-isp-office1] quit
```

Configure the AC to use the MAC address of each user as both the username and password for MAC authentication. The MAC addresses are in hexadecimal notation without hyphens and with letters in lower case. (The configuration in this step is the default configuration. This step is optional.)

```
[AC] mac-authentication user-name-format mac-address without-hyphen lowercase
```

4. Configure a wireless service:

Create a service template named **1** and enter its view.

```
[AC] wlan service-template 1
```

Configure the SSID of service template **1** as **service**.

```
[AC-wlan-st-1] ssid service
```

Assign clients coming online through the service template to VLAN 200.

```
[AC-wlan-st-1] vlan 200
```

Set the PSK AKM mode and configure simple character string of **12345678** as the PSK.

```
[AC-wlan-st-1] akm mode psk
```

```
[AC-wlan-st-1] preshared-key pass-phrase simple 12345678
```

Set the CCMP cipher suite for frame encryption and enable the RSN IE in beacon and probe responses.

```
[AC-wlan-st-1] cipher-suite ccmp
```

```
[AC-wlan-st-1] security-ie rsn
```

Enable the AC to forward client data traffic. If the AC forwards client data traffic by default, skip this step.

```
[AC-wlan-st-1] client forwarding-location ac
```

Set the authentication mode to MAC authentication.

```
[AC-wlan-st-1] client-security authentication-mode mac
```

Specify the MAC authentication domain as ISP domain **office1**.

```
[AC-wlan-st-1] mac-authentication domain office1
```

5. Configure a guest VLAN:

Specify VLAN 300 as the guest VLAN for clients that fail MAC authentication on service template **1**.

```
[AC-wlan-st-1] client-security authentication fail-vlan 300
```

Enable the service template.

```
[AC-wlan-st-1] service-template enable
```

```
[AC-wlan-st-1] quit
```

6. Configure AP settings:

❗ **IMPORTANT:**

In a large-scale network, configure AP groups as a best practice.

Create a manual AP named **officeap**, and specify the AP model and serial ID.

```
[AC] wlan ap officeap model AP 3620
```

```
[AC-wlan-ap-officeap] serial-id 219801A28N819CE0002T
```

```
[AC-wlan-ap-officeap] quit
```

Create AP group **group1** and create an AP grouping rule by AP names to add AP **officeap** to AP group **group1**.

```
[AC] wlan ap-group group1
```

```
[AC-wlan-ap-group-group1] ap officeap
```

Bind service template **1** to radio 2 in AP group **group1**.

```
[AC-wlan-ap-group-group1] ap-model AP 3620
```

```
[AC-wlan-ap-group-group1-ap-model-AP 3620] radio 2
```

```
[AC-wlan-ap-group-group1-ap-model-AP 3620-radio-2] service-template 1
```

Enable radio 2.

```
[AC-wlan-ap-group-group1-ap-model-AP 3620-radio-2] radio
```

```
enable [AC-wlan-ap-group-group1-ap-model-AP 3620-radio-2] quit
```

```
[AC-wlan-ap-group-group1-ap-model-AP 3620]
quit [AC-wlan-ap-group-group1] quit
```

Configuring the switch

Create VLAN 100. The switch will use this VLAN to forward the traffic on the CAPWAP tunnels between the AC and AP.

```
<Switch> system-view
[Switch] vlan 100
[Switch-vlan100] quit
```

Create VLAN 200. The switch will use this VLAN to forward packets for wireless clients.

```
[Switch] vlan 200
[Switch-vlan200] quit
```

Create VLAN 300. The switch will use this VLAN to forward packets in the guest VLAN.

```
[Switch] vlan 300
[Switch-vlan300] quit
```

Configure GigabitEthernet 1/0/1 (the port connected to the AC) as a trunk port, remove the port from VLAN 1, assign the trunk port to VLAN 100.

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100
[Switch-GigabitEthernet1/0/1] quit
```

Configure GigabitEthernet 1/0/2 (the port connected to the AP) as an access port. Assign the access port to VLAN 100.

```
[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] port link-type access
[Switch-GigabitEthernet1/0/2] port access vlan 100
```

Enable PoE on GigabitEthernet 1/0/2.

```
[Switch-GigabitEthernet1/0/2] poe enable
[Switch-GigabitEthernet1/0/2] quit
```

Configuring the RADIUS server

In this example, the RADIUS server runs INC PLAT 7.1(E0303P10) and INC UAM 7.1(E0303P10).

1. Add an access device:

- a. Log in to INC and click the **User** tab.
- b. From the navigation tree, select **User Access Policy > Access Device Management > Access Device**.
- c. Click **Add**.
The **Add Access Device** page opens.
- d. In the **Device List** area, click **Add Manually** to add the device at **112.12.1.25** as an access device.
This IP address is the source IP address specified on the AC for outgoing RADIUS packets.
- e. In the **Access Configuration** area, configure the following parameters, as shown in [Figure 2](#):
 - Enter **123456789** in the **Shared Key** and **Confirm Shared Key** fields.

The key is consistent with the shared key configured on the AC.

- Use the default values for other parameters.

f. Click **OK**.

Figure 2 Adding an access device

User > User Access Policy > Access Device Management > Access Device > Add Access Device

Access Configuration

Authentication Port * 1812 Accounting Port * 1813

RADIUS Accounting Partially/Not Supported Service Type LAN Access Service

Access Device Type H3C(General) Service Group Ungrouped

Shared Key * ***** Confirm Shared Key * *****

Access Device Group --

Device List

Select Add Manually Clear All

Device Name	Device IP	Device Model	Comments	Delete
	112.12.1.25			

Total Items: 1.

OK Cancel

2. Add an access policy:

a. Click the **User** tab.

b. From the navigation tree, select **User Access Policy > Access Policy**.

c. Click **Add**.

d. On the **Add Access Policy** page, configure the following parameters, as shown in [Figure 3](#):

- Enter **office** in the **Access Policy Name** field.
- Use the default values for other parameters.

e. Click **OK**.

Figure 3 Adding an access policy

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

Basic Information

Access Policy Name * office

Service Group * Ungrouped

Description

Authorization Information

Access Period None Allocate IP * No

Downstream Rate(Kbps) Upstream Rate(Kbps)

Priority

Certificate Authentication ☒ None ☐ EAP

Certificate Type EAP-TLS Authn

Deploy VLAN

☐ Deploy User Profile

☐ Deploy ACL

☐ RSA Authentication

Deploy User Group

3. Add an access service:

a. Click the **User** tab.

- b. From the navigation tree, select **User Access Policy > Access Service**.
- c. Click **Add**.
- d. On the **Add Access Service** page, configure the following parameters, as shown in [Figure 4](#):
 - Enter **office_mac** in the **Service Name** field.
 - Select **office** from the **Default Access Policy** list.
 - Use the default values for other parameters.
- e. 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 Max. Number of Bound Endpoints * Default Max. Number of Online Endpoints *

Description

☒ Available ☐ Transparent Authentication on Portal Endpoints

Access Scenario List

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

4. Add an access user:
 - a. Click the **User** tab.
 - b. From the navigation tree, select **Access User > Access User**.
The access user list opens.
 - c. Click **Add**.
The **Add Access User** page opens.
 - d. In the **Access Information** area, add a user, as shown in [Figure 5](#):
 - Click **Add User**.
 - On the dialog box that opens, enter **adm_office_mac** in the **User Name** and **Identity Number** fields.
 - Click **Check Availability** to verify the validity of the username and identity number.
 - Click **OK**.
 - e. In the **Access Information** area, configure the following parameters, as shown in [Figure 6](#):
 - Enter **admin** in the **Account Name** field.
 - Enter **123456** in the **Password** and **Confirm Password** fields.
-
- NOTE:**
- For the client to fail MAC authentication, configure a different username and password on the RADIUS server than on the AC.
-
- f. In the **Access Service** area, select **office_mac** from the list.
 - g. Click **OK**.

Figure 5 Adding a user

Figure 6 Adding an access user account

Service Name	Service Suffix	Status	Allocate IP
<input type="checkbox"/> dot1x		Available	
<input checked="" type="checkbox"/> office_mac		Available	
<input type="checkbox"/> wjh1x		Available	

Verifying the configuration

The client requests to access the network.

On the AC, verify that the wireless client fails MAC authentication and is assigned to VLAN 300.

```
[AC] display wlan client
Total number of clients: 1
```

MAC address	User name	AP name	R IP address	VLAN
3ca9-f414-4c20	3ca9f4144c20	officeap	2 112.14.0.2	300

Verify that the wireless client in the guest VLAN can access network resources only in VLAN 300 before passing MAC authentication. (Details not shown.)

Modify the username and password on the RADIUS server to the MAC address of the client. The MAC address is in hexadecimal notation without hyphens, and letters are in lower case. (Details not shown.)

Display MAC authentication information after the wireless client in the guest VLAN passes MAC authentication.

```
[AC] display mac-authentication
Global MAC authentication parameters:
    MAC authentication          : Enabled
    Authentication method      : PAP
    DR member configuration conflict : Unknown
User name format              : MAC address in lowercase (xxxxxxxxxxxx)
    Username                   : 3ca9f4144c20
    Password                   : $c$3$KWMkvq/FnQ2opPqBnpSTs3NPhVKrSOvqFPLAECSiDQ==
    Offline detect period      : 180 s
Quiet period                  : 180 s
Server timeout                : 100 s
    Reauth period              : 3600 s
    User aging period for critical VLAN : 1000 s
    User aging period for guest VLAN   : 1000 s
    Authentication domain       : Not configured, use default domain
Online MAC-auth wired users   : 0
Online MAC-auth wireless users : 1

Silent MAC users:
    MAC address      VLAN ID  From port      Port index

AP name: officeap Radio ID: 2 SSID: service
BSSID              : 741f-4ad4-8d50
MAC authentication  : Enabled
Authentication domain : officel
Max online users    : 4096
Authentication attempts : successful 0, failed 42
```

Configuration files

- AC:

```
#
dhcp enable
#
vlan 1
#
vlan 100
#
vlan 200
#
vlan 300
#
dhcp server ip-pool vlan100
```

```

gateway-list 112.12.1.25
network 112.12.0.0 mask 255.255.0.0
#
dhcp server ip-pool vlan200
gateway-list 112.13.1.25
network 112.13.0.0 mask 255.255.0.0
dns-list 112.13.1.25
#
dhcp server ip-pool vlan300
gateway-list 112.14.1.25
network 112.14.0.0 mask 255.255.0.0
dns-list 112.14.1.25
#
wlan service-template 1
ssid service
vlan 200
client forwarding-location ac
akm mode psk
preshared-key pass-phrase cipher $c$3$9tIUHskAUVqCH9/EPrL26ldkcEQnngexUEFj
cipher-suite ccmp
security-ie rsn
client-security authentication-mode mac
client-security authentication fail-vlan 300
mac-authentication domain office1
service-template enable
#
interface Vlan-interface100
ip address 112.12.1.25 255.255.0.0
#
interface Vlan-interface200
ip address 112.13.1.25 255.255.0.0
#
interface Vlan-interface300
ip address 112.14.1.25 255.255.0.0
#
interface GigabitEthernet1/0/1
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 100 200 300
#
radius scheme office
primary authentication 112.12.1.50
primary accounting 112.12.1.50
key authentication cipher $c$3$IrnigzRDMkG7Jk1FNf2+tm04+zvnCwiaJzI9TA==
key accounting cipher $c$3$ehledYNyJ+vTlcYcyUEisTa+ZXvWqU1O2QlSYg==
user-name-format without-domain
nas-ip 112.12.1.25
#

```

```

domain office1
  authorization-attribute idle-cut 15 1024
  authentication lan-access radius-scheme office
  authorization lan-access radius-scheme office
  accounting lan-access radius-scheme office
#
wlan ap-group group1
  ap officeap
  ap-model AP 3620
  radio 1
  radio 2
  radio enable
  service-template 1
#
wlan ap officeap model AP 3620
  serial-id 219801A28N819CE0002T
#

```

- **Switch:**

```

#
vlan 1
#
vlan 100
#
vlan 200
#
vlan 300
#
interface GigabitEthernet1/0/1
  port link-type trunk
  undo port trunk permit vlan 1
  port trunk permit vlan 100
#
interface GigabitEthernet1/0/2
  port access vlan 100
  poe enable
#

```

Related documentation

- *AP and WT Management Configuration Guide in INTELBRAS Access Controllers Configuration Guides*
- *AP and WT Management Command Reference in INTELBRAS Access Controllers Command References*
- *Network Connectivity Configuration Guide in INTELBRAS Access Controllers Configuration Guides*
- *Network Connectivity Command Reference in INTELBRAS Access Controllers Command References*
- *User Access and Authentication Configuration Guide in INTELBRAS Access Controllers Configuration Guides*

- *User Access and Authentication Command Reference in INTELBRAS Access Controllers Command References*

- *WLAN Access Configuration Guide in INTELBRAS Access Controllers Configuration Guides*
- *WLAN Access Command Reference in INTELBRAS Access Controllers Command References*

INTELBRAS Access Controllers

MAC Authentication with Guest VLAN Assignment (IPv6)

Configuration Examples

Copyright © 2024 Intelbras S.A All rights reserved.

No part of this manual may be reproduced or transmitted in any form or by any means without prior written consent of Intelbras S.A

Except for the trademarks of Intelbras S.A, any trademarks that may be mentioned in this document are the property of their respective owners.

The information in this document is subject to change without notice.

Contents

Introduction	1
Prerequisites	1
Example: Configuring MAC authentication with guest VLAN assignment (IPv6)	1
Network configuration	1
Restrictions and guidelines	1
Procedures	2
Configuring the AC	2
Configuring the switch	5
Configuring the RADIUS server	6
Verifying the configuration	9
Configuration files	10
Related documentation	12

Introduction

The following information provides an example for configuring a guest VLAN to accommodate clients that fail MAC authentication on an IPv6 network.

Prerequisites

The following information applies to Comware-based access controllers and access points. Procedures and information in the examples might be slightly different depending on the software or hardware version of the access controllers and access points.

The configuration examples 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.

The following information is provided based on the assumption that you have basic knowledge of AAA, MAC authentication, WLAN authentication, and WLAN access.

Example: Configuring MAC authentication with guest VLAN assignment (IPv6)

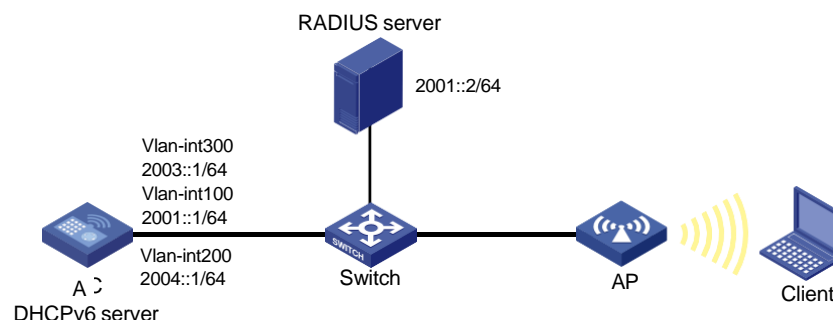
Network configuration

As shown in [Figure 1](#), the AC acts as a DHCPv6 server to provide IPv6 addresses for the AP and its attached clients. The AC centrally forwards client traffic.

To control the access of clients to network resources:

- Configure VLAN 200 as the access VLAN of the clients.
- Use the AC with a RADIUS server to perform MAC authentication for the clients.
- Configure VLAN 300 as the guest VLAN in the service template for the clients. A client is moved to the guest VLAN if it fails authentication and will stay in the guest VLAN until it passes re-authentication, which is performed every 30 seconds.

Figure 1 Network diagram



Restrictions and guidelines

When you configure MAC authentication for wireless clients, follow these restrictions and guidelines:

- Use the actual serial ID of an AP to uniquely identify that AP.
- To prevent too many packets from entering VLAN 1, configure the switch's interface that connects the switch to the AP to deny packets from VLAN 1.
- Some endpoints by default use random MAC addresses. To ensure successful MAC authentication for such an endpoint, disable the endpoint from using a random MAC address.

Procedures

Configuring the AC

1. Configure interfaces on the AC:

Create VLAN 100 and VLAN-interface 100, and assign an IPv6 address to the VLAN interface. The AC will use this IP address to establish CAPWAP tunnels with the AP.

```
<AC> system-view
```

```
[AC] vlan 100
```

```
[AC-vlan100] quit
```

```
[AC] interface vlan-interface 100
```

```
[AC-Vlan-interface100] ipv6 address 2001::1 64
```

Disable RA message suppression on VLAN-interface 100.

```
[AC-Vlan-interface100] undo ipv6 nd ra halt
```

Set the managed address configuration flag (M) to 1 in RA advertisements to be sent.

```
[AC-Vlan-interface100] ipv6 nd autoconfig managed-address-flag
```

Set the other stateful configuration flag (O) to 1 in RA advertisements to be sent.

```
[AC-Vlan-interface100] ipv6 nd autoconfig other-flag
```

```
[AC-Vlan-interface100] quit
```

Create VLAN 200 and VLAN-interface 200, and assign an IPv6 address to the VLAN interface. The client will use VLAN 200 to access the WLAN.

```
[AC] vlan 200
```

```
[AC-vlan200] quit
```

```
[AC] interface vlan-interface 200
```

```
[AC-Vlan-interface200] ipv6 address 2004::1 64
```

Disable RA message suppression on VLAN-interface 200.

```
[AC-Vlan-interface200] undo ipv6 nd ra halt
```

Set the managed address configuration flag (M) to 1 in RA advertisements to be sent.

```
[AC-Vlan-interface200] ipv6 nd autoconfig managed-address-flag
```

Set the other stateful configuration flag (O) to 1 in RA advertisements to be sent.

```
[AC-Vlan-interface200] ipv6 nd autoconfig other-flag
```

```
[AC-Vlan-interface200] quit
```

Create VLAN 300 and VLAN-interface 300, and assign an IPv6 address to the VLAN interface. The AC will use VLAN 300 as a guest VLAN to accommodate clients that fail MAC authentication.

```
[AC] vlan 300
```

```
[AC-vlan300] quit
```

```
[AC] interface vlan-interface 300
```

```
[AC-Vlan-interface300] ipv6 address 2003::1 64
```

Disable RA message suppression on VLAN-interface 300.

```
[AC-Vlan-interface300] undo ipv6 nd ra halt
```

Set the managed address configuration flag (M) to 1 in RA advertisements to be sent.

```
[AC-Vlan-interface300] ipv6 nd autoconfig managed-address-flag
```

Set the other stateful configuration flag (O) to 1 in RA advertisements to be sent.

```
[AC-Vlan-interface300] ipv6 nd autoconfig other-flag
```

```
[AC-Vlan-interface300] quit
```

Configure GigabitEthernet 1/0/1 (the port connected to the switch) as a trunk port, remove the port from VLAN 1, and assign the port to VLANs 100, 200, and 300.

```
[AC] interface gigabitEthernet1/0/1
```

```
[AC-GigabitEthernet1/0/1] port link-type trunk
```

```
[AC-GigabitEthernet1/0/1] undo port trunk permit vlan 1
```

```
[AC-GigabitEthernet1/0/1] port trunk permit vlan 100 200 300
```

```
[AC-GigabitEthernet1/0/1] quit
```

2. Configure the DHCPv6 service:

Enable the DHCPv6 server on VLAN-interface 100 and VLAN-interface 200, apply address pool **vlan100** to VLAN-interface 100, and apply address pool **vlan200** to VLAN-interface 200.

```
[AC] interface vlan-interface 100
```

```
[AC-Vlan-interface100] ipv6 dhcp select server
```

```
[AC-Vlan-interface100] ipv6 dhcp server apply pool vlan100
```

```
[AC-Vlan-interface100] quit
```

```
[AC] interface vlan-interface 200
```

```
[AC-Vlan-interface200] ipv6 dhcp select server
```

```
[AC-Vlan-interface200] ipv6 dhcp server apply pool vlan200
```

```
[AC-Vlan-interface200] quit
```

Create a DHCPv6 address pool named **vlan100**, and specify subnet 2001::/64 in the DHCPv6 address pool.

```
[AC] ipv6 dhcp pool vlan100
```

```
[AC-dhcpv6-pool-vlan100] network 2001::/64
```

```
[AC-dhcpv6-pool-vlan100] quit
```

Create a DHCPv6 address pool named **vlan200**, and specify subnet 2004::/64 in the DHCPv6 address pool.

```
[AC] ipv6 dhcp pool vlan200
```

```
[AC-dhcpv6-pool-vlan200] network 2004::/64
```

```
[AC-dhcpv6-pool-vlan200] quit
```

Create a DHCPv6 address pool named **vlan300**, and specify subnet 2003::/64 in the DHCPv6 address pool.

```
[AC] ipv6 dhcp pool vlan300
```

```
[AC-dhcpv6-pool-vlan300] network 2003::/64
```

```
[AC-dhcpv6-pool-vlan300] quit
```

3. Configure RADIUS-based MAC authentication:

Create a RADIUS scheme named **office** and enter its view.

```
[AC] radius scheme office
```

Specify the IP addresses of the primary authentication and accounting RADIUS servers.

```
[AC-radius-office] primary authentication ipv6 2001::2 64
```

```
[AC-radius-office] primary accounting ipv6 2001::2 64
```

Specify the shared keys for RADIUS authentication and accounting.

```
[AC-radius-office] key authentication simple 123456789
```

```
[AC-radius-office] key accounting simple 123456789
```

Exclude ISP domain names from usernames sent to the RADIUS servers.

```
[AC-radius-office] user-name-format without-domain
# Specify IPv6 address 2001::1 as the source IPv6 address of outgoing RADIUS packets.
[AC-radius-office] nas-ip ipv6 2001::1
[AC-radius-office] quit

# Create an ISP domain named office1 and enter its view.
[AC] domain office1

# Apply RADIUS scheme office to ISP domain office1 for LAN user authentication,
authorization, and accounting.
[AC-isp-office1] authentication lan-access radius-scheme office
[AC-isp-office1] authorization lan-access radius-scheme office
[AC-isp-office1] accounting lan-access radius-scheme office

# Configure the idle cut feature for clients in ISP domain office1.
[AC-isp-office1] authorization-attribute idle-cut 15 1024
[AC-isp-office1] quit

# Configure the AC to use the MAC address of each user as both the username and password
for MAC authentication. The MAC addresses are in hexadecimal notation without hyphens, and
letters are in lower case. (The configuration in this step is the default configuration. This step is
optional.)
[AC] mac-authentication user-name-format mac-address without-hyphen lowercase
```

4. Configure a wireless service:

```
# Create a service template named 1 and enter its view.
[AC] wlan service-template 1

# Set the SSID of service template 1 to service.
[AC-wlan-st-1] ssid service

# Assign clients coming online through the service template to VLAN 200.
[AC-wlan-st-1] vlan 200

# Set the PSK AKM mode and configure simple character string of 12345678 as the PSK.
[AC-wlan-st-1] akm mode psk
[AC-wlan-st-1] preshared-key pass-phrase simple 12345678

# Set the CCMP cipher suite for frame encryption and enable the RSN IE in beacon and probe
responses.
[AC-wlan-st-1] cipher-suite ccmp
[AC-wlan-st-1] security-ie rsn

# Enable the AC to forward client data traffic. If the AC forwards client data traffic by default,
skip this step.
[AC-wlan-st-1] client forwarding-location ac

# Enable snooping ND packets.
[AC-wlan-st-1] client ipv6-snooping nd-learning enable

# Enable snooping DHCPv6 packets.
[AC-wlan-st-1] client ipv6-snooping dhcpv6-learning enable

# Set the authentication mode to MAC authentication.
[AC-wlan-st-1] client-security authentication-mode mac

# Specify the MAC authentication domain as ISP domain office1.
[AC-wlan-st-1] mac-authentication domain office1
```

5. Configure a guest VLAN:

```
# Specify VLAN 300 as the guest VLAN for clients that fail MAC authentication on service
template 1.
[AC-wlan-st-1] client-security authentication fail-vlan 300
```

Enable the service template.

```
[AC-wlan-st-1] service-template enable
[AC-wlan-st-1] quit
```

6. Configure AP settings:

! IMPORTANT:

In a large-scale network, configure AP groups as a best practice.

Create a manual AP named **officeap**, and specify the AP model and serial ID.

```
[AC] wlan ap officeap model AP 3620
[AC-wlan-ap-officeap] serial-id 219801A28N819CE0002T
[AC-wlan-ap-officeap] quit
```

Create AP group **group1** and create an AP grouping rule by AP names to add AP **officeap** to AP group **group1**.

```
[AC] wlan ap-group group1
[AC-wlan-ap-group-group1] ap officeap
```

Bind service template 1 to radio 2 in AP group **group1**.

```
[AC-wlan-ap-group-group1] ap-model AP 3620
[AC-wlan-ap-group-group1-ap-model-AP 3620] radio 2
[AC-wlan-ap-group-group1-ap-model-AP 3620-radio-2] service-template 1
```

Enable radio 2.

```
[AC-wlan-ap-group-group1-ap-model-AP 3620-radio-2] radio
enable [AC-wlan-ap-group-group1-ap-model-AP 3620-radio-2] quit
[AC-wlan-ap-group-group1-ap-model-AP 3620]
quit [AC-wlan-ap-group-group1] quit
```

Configuring the switch

Create VLAN 100. The switch will use this VLAN to forward the traffic on the CAPWAP tunnels between the AC and AP.

```
<Switch> system-view
[Switch] vlan 100
[Switch-vlan100] quit
```

Create VLAN 200. The switch will use this VLAN to forward packets for wireless clients.

```
[Switch] vlan 200
[Switch-vlan200] quit
```

Create VLAN 300. The switch will use this VLAN to forward packets in the guest VLAN.

```
[Switch] vlan 300
[Switch-vlan300] quit
```

Configure GigabitEthernet 1/0/1 (the port connected to the AC) as a trunk port, remove the port from VLAN 1, and assign the trunk port to VLAN 100.

```
[Switch] interface gigabitEthernet1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100
[Switch-GigabitEthernet1/0/1] quit
```

Configure GigabitEthernet 1/0/2 (the port connected to the AP) as an access port. Assign the access port to VLAN 100.

```
[Switch] interface gigabitEthernet1/0/2
[Switch-GigabitEthernet1/0/2] port link-type access
[Switch-GigabitEthernet1/0/2] port access vlan 100
# Enable PoE on GigabitEthernet 1/0/2.
[Switch-GigabitEthernet1/0/2] poe enable
[Switch-GigabitEthernet1/0/2] quit
```

Configuring the RADIUS server

This example uses INC PLAT 7.1 (E0303P10) and INC UAM 7.1 (E0303P10) to show the procedure.

1. Add an access device:
 - a. Log in to INC.
 - b. Click the **User** tab.
 - c. From the navigation tree, select **User Access Policy > Access Device Management > Access Device**.
 - d. Click **Add**.
The **Add Access Device** page opens.
 - e. In the **Device List** area, click **Add IPv6 Dev**.
 - f. Enter 2001::1 as the start IPv6 address, and then click **OK**.
This IPv6 address is the source IPv6 address specified on the AC for outgoing RADIUS packets.
 - g. In the **Access Configuration** area, configure the following parameters, as shown in [Figure 2](#):
 - Enter **123456789** in the **Shared Key** and **Confirm Shared Key** fields.
The key is consistent with the shared key configured on the AC.
 - Use the default values for other parameters.
 - h. Click **OK**.

Figure 2 Adding an access device

User > User Access Policy > Access Device Management > Access Device > Add Access Device

Access Configuration

Authentication Port *	1812	Accounting Port *	1813
Service Type	LAN Access Service		
Access Device Type	H3C(General)	Service Group	Ungrouped
Shared Key *	*****	Confirm Shared Key *	*****
Access Device Group	--		
Certificate Authentication	<input checked="" type="radio"/> None <input type="radio"/> EAP		
Certificate Type	EAP-TLS Authn		

Device List

Select	Add Manually	Add IPv6 Dev	Clear All	
Device Name	Device IP	Device Model	Comments	Delete
	2001:0000:0000:0000:0000:0000:0000:0001			

Total Items: 1.

OK Cancel

2. Add an access policy:
 - a. Click the **User** tab.
 - b. From the navigation tree, select **User Access Policy > Access Policy**.
 - c. Click **Add**.
 - d. On the **Add Access Policy** page, configure the following parameters, as shown in [Figure 3](#):
 - Enter **office** in the **Access Policy Name** field.
 - Use the default values for other parameters.
 - e. Click **OK**.

Figure 3 Adding an access policy

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

Basic Information

Access Policy Name * office

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 Auth

Deploy VLAN

☐ Deploy User Profile

☐ Deploy ACL

Deploy User Group

3. Add an access service:
 - a. Click the **User** tab.
 - b. From the navigation tree, select **User Access Policy > Access Service**.
 - c. Click **Add**.
 - d. On the **Add Access Service** page, configure the following parameters, as shown in [Figure 4](#):
 - Enter **office_mac** in the **Service Name** field.
 - Select **office** from the **Default Access Policy** list.
 - Use the default values for other parameters.
 - e. Click **OK**.

Figure 4 Adding an access service

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

Basic Information

Service Name * office_mac Service Suffix

Service Group * Ungrouped Default Access Policy * office

Default Proprietary Attribute Assignment Policy * Do not use

Default Max. Number of Bound Endpoints * 0 Default Max. Number of Online Endpoints * 0

Description

☒ Available ☐ Transparent Authentication on Portal Endpoints

Access Scenario List

Add

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

OK Cancel

4. Add an access user:
 - a. Click the **User** tab.
 - b. From the navigation tree, select **Access User > Access User**.
The access user list opens.
 - c. Click **Add**.
The **Add Access User** page opens.
 - d. In the **Access Information** area, add a user, as shown in [Figure 5](#):
 - Click **Add User**.
 - On the dialog box that opens, enter **adm_office_mac** in the **User Name** and **Identity Number** fields.
 - Click **Check Availability** to verify the validity of the username and identity number.
 - Click **OK**.
 - e. In the **Access Information** area, configure the MAC authentication user account, as shown in [Figure 6](#):
 - Enter **admin** in the **Account Name** field.
 - Enter **123456** in the **Password** and **Confirm Password** fields.
-
- NOTE:**
- To test the guest VLAN functionality, the user account settings in this example are inconsistent with the MAC authentication username and password format configured on the AC. On a live network, you must make sure the usernames and passwords for the clients are their MAC addresses in the format specified on the AC.
-
- f. In the **Access Service** area, select **office_mac** from the list.
 - g. Click **OK**.

Figure 5 Adding a user

Figure 6 Adding an access user account

Service Name	Service Suffix	Status	Allocate IP
<input type="checkbox"/> dot1x		Available	
<input checked="" type="checkbox"/> office_mac		Available	
<input type="checkbox"/> wjh1x		Available	

Verifying the configuration

Attempt to access the network from a client.

On the AC, verify that the wireless client fails MAC authentication and is assigned to VLAN 300.

```
[AC] display wlan client ipv6
```

```
Total number of clients: 1
```

MAC address	AP name	IPv6 address	VLAN
3ca9-f414-4c20	officeap	2003::2	300

Verify that the wireless client in the guest VLAN can access network resources only in VLAN 300 before passing MAC authentication. (Details not shown.)

Modify the username and password on the RADIUS server to the MAC address of the client. The MAC address is in hexadecimal notation without hyphens, and letters are in lower case. (Details not shown.)

Display MAC authentication information after the wireless client in the guest VLAN passes MAC authentication.

```
[AC] display mac-authentication
Global MAC authentication parameters:
  MAC authentication      : Enabled
  Authentication method   : PAP
  DR member configuration conflict : Unknown
  User name format       : MAC address in lowercase (xxxxxxxxxxxx)
  Username               : mac
  Password               : Not configured
  Offline detect period  : 300 s
  Quiet period           : 60 s
  Server timeout         : 100 s
  Reauth period          : 3600 s
  User aging period for critical VLAN : 1000 s
  User aging period for guest VLAN   : 1000 s
  Authentication domain  : Not configured, use default domain
  Online MAC-auth wired users : 0
  Online MAC-auth wireless users : 1
```

Silent MAC users:

MAC address	VLAN ID	From port	Port index
AP name: officeap Radio ID: 2 SSID: service			
BSSID	: 741f-4ad4-8d50		
MAC authentication	: Enabled		
Authentication domain	: officel		
Max online users	: 4096		
Authentication attempts	: successful 0, failed 42		

Configuration files

- AC:

```
#
vlan 100
#
vlan 200
#
vlan 300
#
ipv6 dhcp pool vlan100
 network 2001::/64
#
```

```

ipv6 dhcp pool vlan200
    network 2004::/64
#
ipv6 dhcp pool vlan300
    network 2003::/64
#
wlan service-template 1
    ssid service
    vlan 200
    client forwarding-location ac
    akm mode psk
    preshared-key pass-phrase cipher $c$3$9tIUH$KAUVqCH9/EPRL26ldkcEQnngeXUEFj
    cipher-suite ccmp
    security-ie rsn
    client-security authentication-mode mac
    client-security authentication fail-vlan 300
    mac-authentication domain office1
    client ipv6-snooping nd-learning enable
    client ipv6-snooping dhcpv6-learning enable
    service-template enable
#
interface Vlan-interface100
    ipv6 dhcp select server
    ipv6 dhcp server apply pool vlan100
    ipv6 address 2001::1/64
    ipv6 nd autoconfig managed-address-flag
    ipv6 nd autoconfig other-flag
    undo ipv6 nd ra halt
#
interface Vlan-interface200
    ipv6 dhcp select server
    ipv6 dhcp server apply pool vlan100
    ipv6 address 2004::1/64
    ipv6 nd autoconfig managed-address-flag
    ipv6 nd autoconfig other-flag
    undo ipv6 nd ra halt
#
interface Vlan-interface300
    ipv6 address 2003::1/64
    ipv6 nd autoconfig managed-address-flag
    ipv6 nd autoconfig other-flag
    undo ipv6 nd ra halt
#
interface GigabitEthernet1/0/1
    port link-type trunk
    undo port trunk permit vlan 1
    port trunk permit vlan 100 200 300
#

```

```

radius scheme office
  primary authentication ipv6 2001::2 64
  primary accounting ipv6 2001::2 64
  key authentication cipher $c$3$IrnigzRDMkG7Jk1FNf2+tm04+zvnCwiaJzI9TA==
  key accounting cipher $c$3$ehledYNyJ+vTlcYcyUEisTa+ZXvWqU1O2Q1SYg==
  user-name-format without-domain
  nas-ip ipv6 2001::1
#
domain officel
  authorization-attribute idle-cut 15 1024
  authentication lan-access radius-scheme office
  authorization lan-access radius-scheme office
  accounting lan-access radius-scheme office
#
wlan ap-group group1
  ap officeap
  ap-model AP 3620
    radio 1
    radio 2
    radio enable
    service-template 1
#
wlan ap officeap model AP 3620
  serial-id 219801A28N819CE0002T
#

```

- **Switch:**

```

#
vlan 100
#
vlan 200
#
vlan 300
#
interface GigabitEthernet1/0/1
  port link-type trunk
  undo port trunk permit vlan 1
  port trunk permit vlan 100
#
interface GigabitEthernet1/0/2
  port access vlan 100
  poe enable
#

```

Related documentation

- *AP and WT Management Configuration Guide in INTELBRAS Access Controllers Configuration Guides*
- *AP and WT Management Command Reference in INTELBRAS Access Controllers Command References*

- *Network Connectivity Configuration Guide in INTELBRAS Access Controllers Configuration Guides*
- *Network Connectivity Command Reference in INTELBRAS Access Controllers Command References*
- *User Access and Authentication Configuration Guide in INTELBRAS Access Controllers Configuration Guides*
- *User Access and Authentication Command Reference in INTELBRAS Access Controllers Command References*
- *WLAN Access Configuration Guide in INTELBRAS Access Controllers Configuration Guides*
- *WLAN Access Command Reference in INTELBRAS Access Controllers Command References*

INTELBRAS Access Controllers

Local MAC-And-802.1X Authentication

Configuration Examples

Copyright © 2024 Intelbras S.A All rights reserved.

No part of this manual may be reproduced or transmitted in any form or by any means without prior written consent of Intelbras S.A

Except for the trademarks of Intelbras S.A, any trademarks that may be mentioned in this document are the property of their respective owners.

The information in this document is subject to change without notice.

Contents

Introduction	1
Prerequisites	1
Example: Configuring local MAC-and-802.1X authentication for wireless clients	1
Network configuration	1
Restrictions and guidelines	2
Procedures	2
Configuring the AC	2
Configuring the switch	4
Configuring the iNode client	5
Verifying the configuration	9
Configuration files	10
Related documentation	11

Introduction

The following information provides an example for configuring local MAC-and-802.1X authentication in a wireless network.

Prerequisites

The following information applies to Comware-based access controllers and access points. Procedures and information in the examples might be slightly different depending on the software or hardware version of the access controllers and access points.

The configuration examples 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.

The following information is provided based on the assumption that you have basic knowledge of MAC authentication, WLAN access, WLAN user access authentication, and 802.1X authentication.

Example: Configuring local MAC-and-802.1X authentication for wireless clients

Network configuration

As shown in [Figure 1](#), an AP is attached to a PoE port on a switch, which acts as a DHCP server to assign IP addresses to the AP and the client.

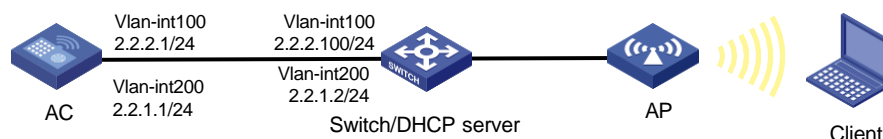
Configure the AC to meet the following requirements:

- The AC first performs local MAC authentication for the client.
 - If the client fails the MAC authentication, the AC stops authenticating the client.
 - If the client passes the MAC authentication, the AC performs local 802.1X authentication for the client.

The client can access the network only after it passes both MAC authentication and 802.1X authentication.

- The AC uses open system authentication to authenticate the client at the data link layer. This is the default authentication method.

Figure 1 Network diagram



Restrictions and guidelines

When you configure local MAC-and-802.1X authentication for wireless clients, follow these restrictions and guidelines:

- Use the actual serial ID of an AP to uniquely identify that AP.
- Make sure the username and password configured on the AC are the same as the MAC address of the client. The username and password formats comply with the MAC authentication user account format.
- The AC can perform local 802.1X authentication only for the iNode client.
- Some endpoints by default use random MAC addresses. To ensure successful MAC authentication for such an endpoint, disable the endpoint from using a random MAC address.

Procedures

Configuring the AC

1. Configure interfaces on the AC:

Create VLAN 100 and VLAN-interface 100, and assign an IP address to the VLAN interface. The AC will use this IP address to establish CAPWAP control and data tunnels with the AP.

```
<AC> system-view
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 2.2.2.1 24
[AC-Vlan-interface100] quit
```

Create VLAN 200 and VLAN-interface 200, and assign an IP address to the VLAN interface. VLAN 200 will be used for client access.

```
[AC] vlan 200
[AC-vlan200] quit
[AC] interface vlan-interface 200
[AC-Vlan-interface200] ip address 2.2.1.1 24
[AC-Vlan-interface200] quit
```

Configure GigabitEthernet 1/0/1 (the port connected to the switch) as a trunk port, and assign the port to VLAN 100 and VLAN 200.

```
[AC] interface gigabitEthernet 1/0/1
[AC-GigabitEthernet1/0/1] port link-type trunk
[AC-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[AC-GigabitEthernet1/0/1] quit
```

2. Configure a local user for 802.1X authentication:

Create a network access user named **localuser** and set the password to **localpass** in plaintext form.

```
[AC] local-user localuser class network
[AC-luser-network-localuser] password simple localpass
```

Set the service type to **lan-access**.

```
[AC-luser-network-localuser] service-type lan-access
[AC-luser-network-localuser] quit
```

3. Configure a local user for MAC authentication:

Create a network access user. Set both the username and password to the client's MAC address **3ca9f4144c20**.

```
[AC] local-user 3ca9f4144c20 class network
[AC-luser-network-3ca9f4144c20] password simple 3ca9f4144c20
```

Set the service type to **lan-access**.

```
[AC-luser-network-3ca9f4144c20] service-type lan-access
[AC-luser-network-3ca9f4144c20] quit
```

4. Configure the AC to use the MAC address of each user as both the username and password for MAC authentication. The MAC addresses are in hexadecimal notation without hyphens and with letters in lower case. (The configuration in this step is the default configuration. This step is optional.)

```
[AC] mac-authentication user-name-format mac-address without-hyphen lowercase
```

5. Configure a local authentication domain:

Create ISP domain **bbb** and enter its view.

```
[AC] domain bbb
```

Configure the ISP domain to use local authentication, authorization, and accounting for LAN access wireless clients.

```
[AC-isp-bbb] authentication lan-access local
[AC-isp-bbb] authorization lan-access local
[AC-isp-bbb] accounting lan-access local
[AC-isp-bbb] quit
```

6. Set the 802.1X authentication method to CHAP.

```
[AC] dot1x authentication-method chap
```

7. Configure a service template:

Create service template **service** and enter its view.

```
[AC] wlan service-template service
```

Set the SSID of the service template to **service**.

```
[AC-wlan-st-service] ssid service
```

Assign VLAN 200 to the matching clients.

```
[AC-wlan-st-service] vlan 200
```

Set the user access authentication mode to MAC-and-802.1X authentication.

```
[AC-wlan-st-service] client-security authentication-mode mac-and-dot1x
```

Specify ISP domain **bbb** for 802.1X authentication clients in the service template.

```
[AC-wlan-st-service] dot1x domain bbb
```

Specify ISP domain **bbb** for MAC authentication clients in the service template.

```
[AC-wlan-st-service] mac-authentication domain bbb
```

Enable the AC to forward client data traffic. If the AC forwards client data traffic by default, skip this step.

```
[AC-wlan-st-service] client forwarding-location ac
```

Enable the service template.

```
[AC-wlan-st-service] service-template enable
[AC-wlan-st-service] quit
```

8. Configure AP settings:

❗ IMPORTANT:

In a large-scale network, configure AP groups as a best practice.

Create manual AP **office**, and specify the AP model and serial ID.

```
[AC] wlan ap office model AP 3620
[AC-wlan-ap-office] serial-id 219801A28N819CE0002T
[AC-wlan-ap-office] quit

# Create AP group group1 and create an AP grouping rule by AP names to add AP office to AP group group1.
[AC] wlan ap-group group1
[AC-wlan-ap-group-group1] ap office

# Bind service template service to radio 1 in AP group group1.
[AC-wlan-ap-group-group1] ap-model AP 3620
[AC-wlan-ap-group-group1-ap-model-AP 3620] radio 1
[AC-wlan-ap-group-group1-ap-model-AP 3620-radio-1] service-template service

# Enable radio 1.
[AC-wlan-ap-group-group1-ap-model-AP 3620-radio-1] radio
enable [AC-wlan-ap-group-group1-ap-model-AP 3620-radio-1] quit
[AC-wlan-ap-group-group1-ap-model-AP 3620]
quit [AC-wlan-ap-group-group1] quit
```

Configuring the switch

Enable the DHCP server.

```
<Switch> system-view
[Switch] dhcp enable
```

Create VLAN 100. The switch will use this VLAN to forward the traffic on the CAPWAP tunnels between the AC and AP.

```
[Switch] vlan 100
[Switch-vlan100] quit
```

Create VLAN 200. The switch will use this VLAN to forward packets for wireless clients.

```
[Switch] vlan 200
[Switch-vlan200] quit
```

Configure GigabitEthernet 1/0/1 (the port connected to the AC) as a trunk port, and assign the trunk port to VLAN 100 and VLAN 200.

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[Switch-GigabitEthernet1/0/1] quit
```

Configure GigabitEthernet 1/0/2 (the port connected to the AP) as an access port. Assign the access port to VLAN 100.

```
[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] port link-type access
[Switch-GigabitEthernet1/0/2] port access vlan 100
```

Enable PoE on GigabitEthernet 1/0/2.

```
[Switch-GigabitEthernet1/0/2] poe enable
[Switch-GigabitEthernet1/0/2] quit
```

Assign IP address 2.2.2.100/24 to VLAN-interface 100.

```
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ip address 2.2.2.100 255.255.255.0
[Switch-Vlan-interface100] quit
```

Assign IP address 2.2.1.2/24 to VLAN-interface 200.

```
[Switch] interface vlan-interface 200
[Switch-Vlan-interface200] ip address 2.2.1.2 255.255.255.0
[Switch-Vlan-interface200] quit
```

Create a DHCP address pool named **100**, and specify subnet 2.2.2.0/24 and gateway IP address 2.2.2.1 in the DHCP address pool.

```
[Switch] dhcp server ip-pool 100
[Switch-dhcp-pool-100] network 2.2.2.0 mask 255.255.255.0
[Switch-dhcp-pool-100] gateway-list 2.2.2.1
[Switch-dhcp-pool-100] quit
```

Create a DHCP address pool named **200**, and specify subnet 2.2.1.0/24 and gateway IP address 2.2.1.1 in the DHCP address pool. In this example, the address of the DNS server is 2.2.1.1 (the gateway address). You must replace it with the actual address of the DNS server on your network.

```
[Switch] dhcp server ip-pool 200
[Switch-dhcp-pool-200] network 2.2.1.0 mask 255.255.255.0
[Switch-dhcp-pool-200] gateway-list 2.2.1.1
[Switch-dhcp-pool-200] dns-list 2.2.1.1
[Switch-dhcp-pool-200] quit
```

Configuring the iNode client

1. Run the iNode client and click **Wireless Connection**, as shown in [Figure 2](#). In this example, the client version is iNode PC 7.1.

Figure 2 iNode Client



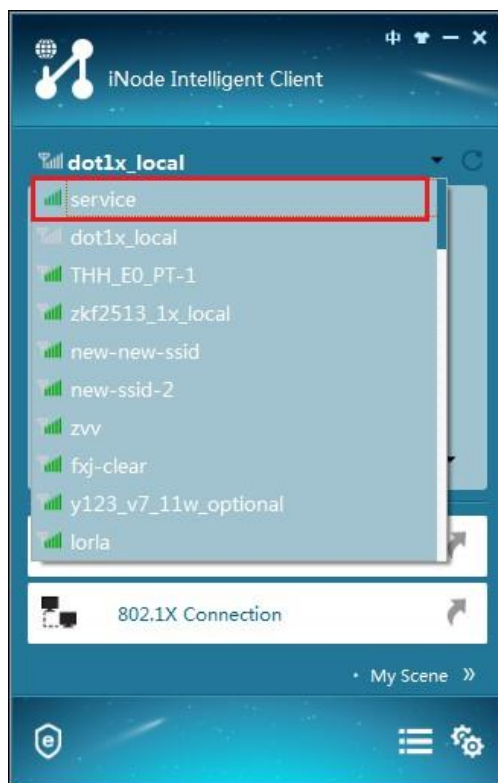
2. Click the inverted triangle icon at the upper right corner of the page, as shown in [Figure 3](#).

Figure 3 Wireless connection



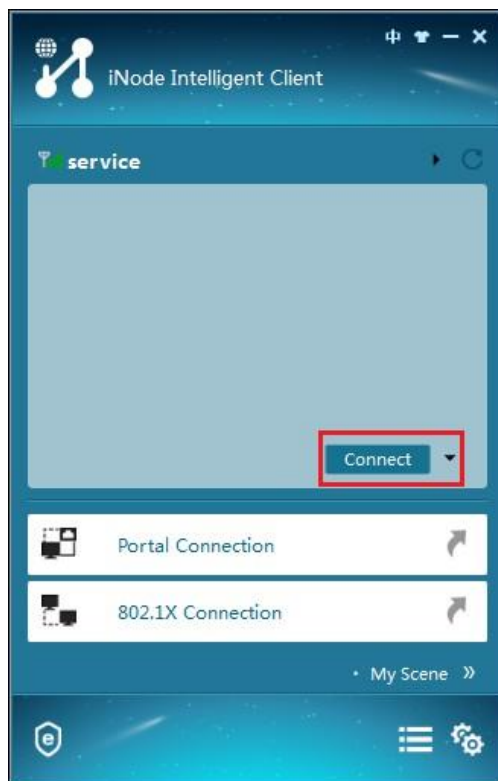
3. Double-click the wireless service with the SSID of **service**, as shown in [Figure 4](#).

Figure 4 Selecting an wireless service



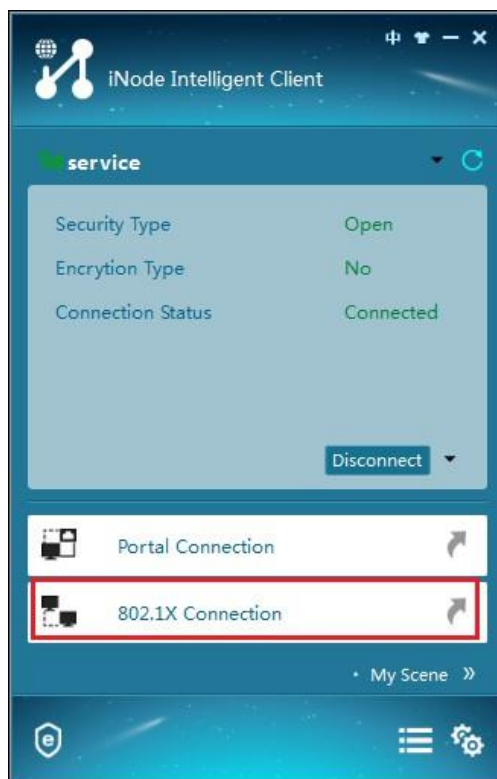
4. Click **Connect** as shown in [Figure 5](#).

Figure 5 Connecting to the wireless network



5. Click **802.1X Connection** as shown in [Figure 6](#).

Figure 6 802.1X connection



6. Enter a username and password as shown in [Figure 7](#). In this example, the username is **localuser** and the password is **localpass**.

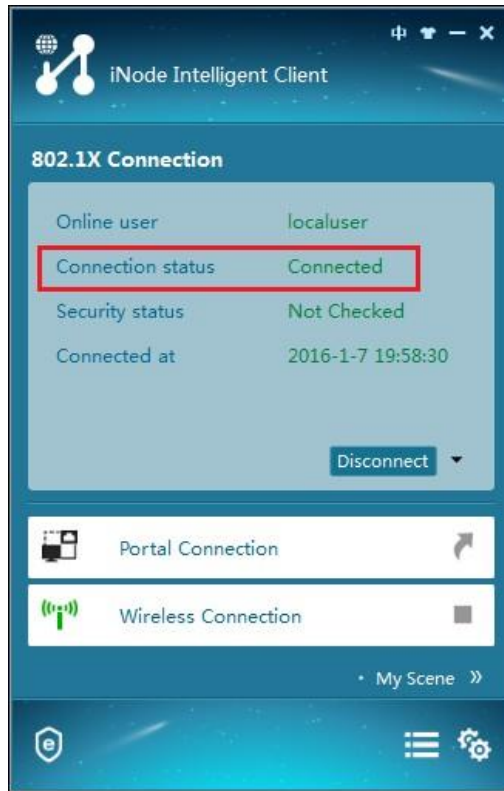
Figure 7 Entering the username and password



7. Click the inverted triangle icon next to **Connect** and select **Properties**.
8. In the dialog box that opens, select a wireless NIC to use and clear the option for uploading the client version information.
9. Return to the iNode 802.1X connection page.
10. Click **Connect**.

The iNode client displays the connection state as shown in [Figure 8](#).

Figure 8 Successful 802.1X authentication



Verifying the configuration

Use a client with a MAC address other than 3ca9f4144c20 to visit the Internet. Verify the following items:

- The client cannot pass MAC authentication.
- The AC does not perform 802.1X authentication for the client after the client fails MAC authentication.
- The client cannot visit the Internet.

Use the client with MAC address 3ca9f4144c20 to visit the Internet. Verify that the client can access the Internet after it passes both MAC authentication and 802.1X authentication. (Details not shown.)

On the AC, display online 802.1X user information to verify that the 802.1X user has come online.

```
[AC] display dot1x connection
User MAC address      : 0015-00bf-e84d
AP name               : office
Radio ID              : 1
SSID                  : service
BSSID                 : 741f-4ad4-1fe0
Username              : localuser
Authentication domain : bbb
IPv4 address          : 2.2.1.3
Authentication method : CHAP
Initial VLAN          : 200
Authorization VLAN    : 200
```

Authorization ACL number : N/A
Authorization user profile : N/A
Termination action : N/A
Session timeout period : N/A
Online from : 2019/12/04 17:37:55
Online duration : 0h 4m 20s

Configuration files

- AC:

```
#
vlan 100
#
vlan 200
#
wlan service-template service
  ssid service
  vlan 200
  client forwarding-location ac
  client-security authentication-mode mac-and-dot1x
  dot1x domain bbb
  mac-authentication domain bbb
  service-template enable
#
interface Vlan-interface100
  ip address 2.2.2.1 255.255.255.0
#
interface Vlan-interface200
  ip address 2.2.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
  port link-mode bridge
  port link-type trunk
  port trunk permit vlan 1 100 200
#
domain bbb
  authentication lan-access local
  authorization lan-access local
  accounting lan-access local
#
local-user localuser class network
  password cipher $c$3$+5Yra0KsaLci/RxEa4lyYKxxiw6jwMCCOg==
  service-type lan-access
#
local-user 3ca9f4144c20 class network
  password cipher $c$3$KWMkvq/FnQ2opPqBnpSTs3NPhVKrSOvqFPLAECSiDQ==
  service-type lan-access
#
```

```

wlan ap-group group1
  ap office
  ap-model AP 3620
  radio 1
    radio enable
    service-template service
  radio 2
#
wlan ap office model AP 3620
  serial-id 219801A28N819CE0002T
#
• Switch:
#
dhcp enable
#
vlan 100
#
vlan 200
#
dhcp server ip-pool 100
  gateway-list 2.2.2.1
  network 2.2.2.0 mask 255.255.255.0
#
dhcp server ip-pool 200
  gateway-list 2.2.1.1
  network 2.2.1.0 mask 255.255.255.0
  dns-list 2.2.1.1
#
interface Vlan-interface100
  ip address 2.2.2.100 255.255.255.0
#
interface Vlan-interface200
  ip address 2.2.1.2 255.255.255.0
#
interface GigabitEthernet1/0/1
  port link-type trunk
  port trunk permit vlan 1 100 200
#
interface GigabitEthernet1/0/2
  port link-type access
  port access permit vlan 100
  poe enable
#

```

Related documentation

- *AP and WT Management Configuration Guide in INTELBRAS Access Controllers Configuration Guides*

- *AP and WT Management Command Reference in INTELBRAS Access Controllers Command References*
- *Network Connectivity Configuration Guide in INTELBRAS Access Controllers Configuration Guides*
- *Network Connectivity Command Reference in INTELBRAS Access Controllers Command References*
- *User Access and Authentication Configuration Guide in INTELBRAS Access Controllers Configuration Guides*
- *User Access and Authentication Command Reference in INTELBRAS Access Controllers Command References*
- *WLAN Access Configuration Guide in INTELBRAS Access Controllers Configuration Guides*
- *WLAN Access Command Reference in INTELBRAS Access Controllers Command References*

INTELBRAS Access Controllers Local 802.1X Authentication Configuration Examples

Copyright © 2024 Intelbras S.A All rights reserved.

No part of this manual may be reproduced or transmitted in any form or by any means without prior written consent of Intelbras S.A

Except for the trademarks of Intelbras S.A, any trademarks that may be mentioned in this document are the property of their respective owners.

The information in this document is subject to change without notice.

Contents

Introduction	1
Prerequisites	1
Example: Configuring local 802.1X authentication for wireless clients	1
Network configuration	1
Restrictions and guidelines	1
Procedures	2
Configuring the AC	2
Configuring the switch	3
Configuring the iNode client	4
Verifying the configuration	9
Configuration files	11
Related documentation	12

Introduction

The following information provides an example for configuring local 802.1X authentication on a wireless network.

Prerequisites

The following information applies to Comware-based access controllers and access points. Procedures and information in the examples might be slightly different depending on the software or hardware version of the access controllers and access points.

The configuration examples 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.

The following information is provided based on the assumption that you have basic knowledge of WLAN access, WLAN user access authentication, and 802.1X authentication.

Example: Configuring local 802.1X authentication for wireless clients

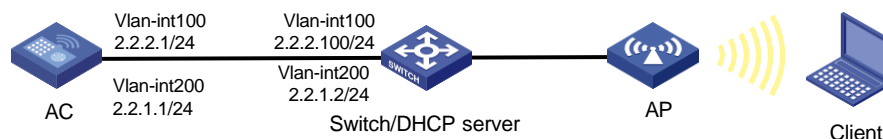
Network configuration

As shown in [Figure 1](#), the switch acts as a DHCP server to assign IP addresses to the AP and the client.

Configure the AC to meet the following requirements:

- Perform local 802.1X authentication to control the network access of the client.
- Use open system authentication to authenticate the client at the data link layer. This is the default authentication method.

Figure 1 Network diagram



Restrictions and guidelines

When you configure local 802.1X authentication for wireless clients, follow these restrictions and guidelines:

- Use the serial ID labeled on the AP's rear panel to specify an AP.
- Local 802.1X authentication does not support EAP relay.

Procedures

Configuring the AC

1. Configure interfaces on the AC:

Create VLAN 100 and VLAN-interface 100, and assign an IP address to the VLAN interface. The AC will use this IP address to establish CAPWAP control and data tunnels with the AP.

```
<AC> system-view
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 2.2.2.1 24
[AC-Vlan-interface100] quit
```

Create VLAN 200 and VLAN-interface 200, and assign an IP address to the VLAN interface. VLAN 200 will be used for client access.

```
[AC] vlan 200
[AC-vlan200] quit
[AC] interface vlan-interface 200
[AC-Vlan-interface200] ip address 2.2.1.1 24
[AC-Vlan-interface200] quit
```

Configure GigabitEthernet 1/0/1 (the port connected to the switch) as a trunk port, and assign the port to VLAN 100 and VLAN 200.

```
[AC] interface gigabitethernet 1/0/1
[AC-GigabitEthernet1/0/1] port link-type trunk
[AC-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[AC-GigabitEthernet1/0/1] quit
```

2. Configure a local user:

Create a network access user named **localuser** and set the password to **localpass** in plaintext form.

```
[AC] local-user localuser class network
[AC-luser-network-localuser] password simple localpass
# Set the service type to lan-access.
[AC-luser-network-localuser] service-type lan-access
[AC-luser-network-localuser] quit
```

3. Configure a local authentication domain:

Create ISP domain **bbb** and enter its view.

```
[AC] domain bbb
```

Configure the ISP domain to use local authentication, authorization, and accounting for LAN access wireless clients.

```
[AC-isp-bbb] authentication lan-access local
[AC-isp-bbb] authorization lan-access local
[AC-isp-bbb] accounting lan-access local
[AC-isp-bbb] quit
```

4. Set the 802.1X authentication method to CHAP.

```
[AC] dot1x authentication-method chap
```

5. Configure a service template:

Create service template **service** and enter its view.

```
[AC] wlan service-template service
# Set the SSID of the service template to service.
[AC-wlan-st-service] ssid service
# Assign VLAN 200 to the matching clients.
[AC-wlan-st-service] vlan 200
# Set the user access authentication mode to 802.1X authentication.
[AC-wlan-st-service] client-security authentication-mode dot1x
# Specify ISP domain bbb for 802.1X authentication clients in the service template.
[AC-wlan-st-service] dot1x domain bbb
# Enable the AC to forward client data traffic. If the AC forwards client data traffic by default,
skip this step.
[AC-wlan-st-service] client forwarding-location ac
# Enable the service template.
[AC-wlan-st-service] service-template enable
[AC-wlan-st-service] quit
```

6. Configure AP settings:

! IMPORTANT:

In a large-scale network, configure AP groups as a best practice.

Create manual AP **office**, and specify the AP model and serial ID.

```
[AC] wlan ap office model AP 3620
[AC-wlan-ap-office] serial-id 219801A28N819CE0003T
[AC-wlan-ap-office] quit
```

Create AP group **group1** and create an AP grouping rule by AP names to add AP **office** to AP group **group1**.

```
[AC] wlan ap-group group1
[AC-wlan-ap-group-group1] ap office
```

Bind service template **service** to radio 1 in AP group **group1**.

```
[AC-wlan-ap-group-group1] ap-model AP 3620
[AC-wlan-ap-group-group1-ap-model-AP 3620] radio 1
[AC-wlan-ap-group-group1-ap-model-AP 3620-radio-1] service-template service
```

Enable radio 1.

```
[AC-wlan-ap-group-group1-ap-model-AP 3620-radio-1] radio
enable [AC-wlan-ap-group-group1-ap-model-AP 3620-radio-1] quit
[AC-wlan-ap-group-group1-ap-model-AP 3620]
quit [AC-wlan-ap-group-group1] quit
```

Configuring the switch

Enable the DHCP server.

```
<Switch> system-view
[Switch] dhcp enable
```

Create VLAN 100. The switch will use this VLAN to forward the traffic on the CAPWAP tunnels between the AC and AP.

```
[Switch] vlan 100
[Switch-vlan100] quit
```

Create VLAN 200. The switch will use this VLAN to forward packets for wireless clients.

```
[Switch] vlan 200
[Switch-vlan200] quit
```

Configure GigabitEthernet 1/0/1 (the port connected to the AC) as a trunk port, and assign the trunk port to VLAN 100 and VLAN 200.

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[Switch-GigabitEthernet1/0/1] quit
```

Configure GigabitEthernet 1/0/2 (the port connected to the AP) as a trunk port, assign the port to VLAN 100 and VLAN 200, and set the PVID of the port to 100.

```
[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] port link-type trunk
[Switch-GigabitEthernet1/0/2] port trunk permit vlan 100 200
[Switch-GigabitEthernet1/0/2] port trunk pvid vlan 100
```

Enable PoE on GigabitEthernet 1/0/2.

```
[Switch-GigabitEthernet1/0/2] poe enable
[Switch-GigabitEthernet1/0/2] quit
```

Assign IP address 2.2.2.100/24 to VLAN-interface 100.

```
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ip address 2.2.2.100 255.255.255.0
[Switch-Vlan-interface100] quit
```

Assign IP address 2.2.1.2/24 to VLAN-interface 200.

```
[Switch] interface vlan-interface 200
[Switch-Vlan-interface200] ip address 2.2.1.2 255.255.255.0
[Switch-Vlan-interface200] quit
```

Create a DHCP address pool named **100, and specify subnet 2.2.2.0/24 and gateway IP address 2.2.2.1 in the DHCP address pool.**

```
[Switch] dhcp server ip-pool 100
[Switch-dhcp-pool-100] network 2.2.2.0 mask 255.255.255.0
[Switch-dhcp-pool-100] gateway-list 2.2.2.1
[Switch-dhcp-pool-100] option 138 ip-address 2.2.2.1
[Switch-dhcp-pool-100] quit
```

Create a DHCP address pool named **200, and specify subnet 2.2.1.0/24 and gateway IP address 2.2.1.1 in the DHCP address pool.**

```
[Switch] dhcp server ip-pool 200
[Switch-dhcp-pool-200] network 2.2.1.0 mask 255.255.255.0
[Switch-dhcp-pool-200] gateway-list 2.2.1.1
[Switch-dhcp-pool-200] quit
```

Configuring the iNode client

Prerequisites

In this example, the client version is iNode PC 7.1.

Connecting to the wireless network

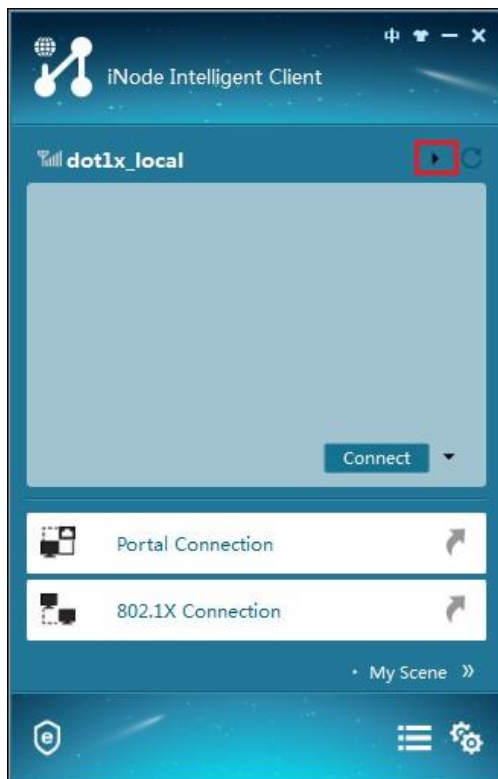
1. Run the iNode client, and then click **Wireless Connection**, as shown in [Figure 2](#).

Figure 2 iNode Client



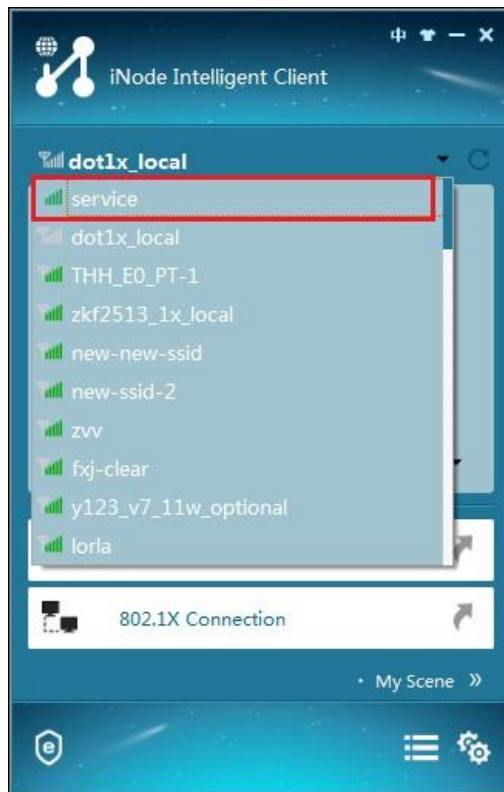
2. Click triangle icon in the wireless connection title bar, as shown in [Figure 3](#).

Figure 3 Wireless connection



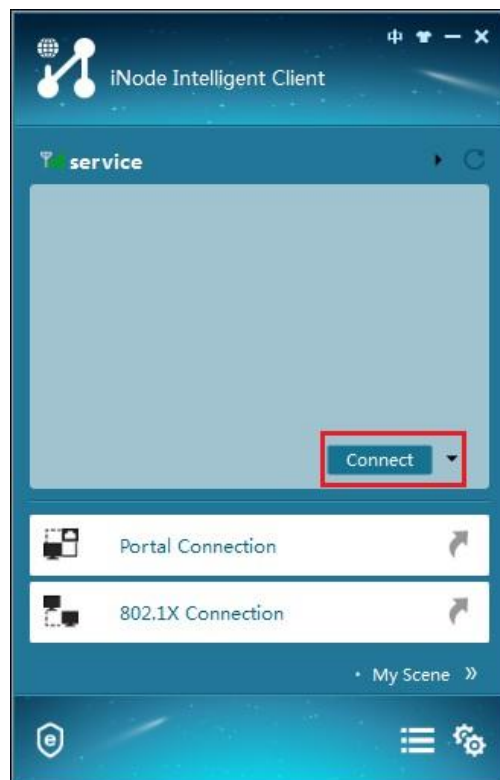
3. Double-click the wireless service with SSID **service**, as shown in [Figure 4](#).

Figure 4 Selecting a wireless service



4. Click **Connect**, as shown in [Figure 5](#).

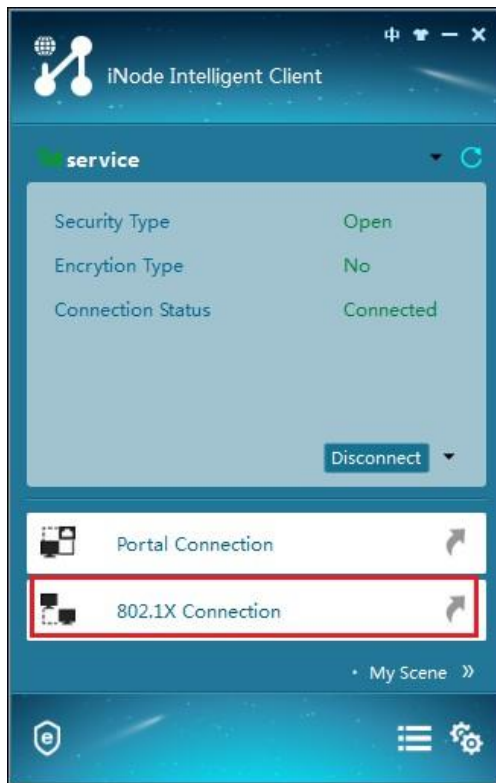
Figure 5 Connecting to the wireless network



Configuring 802.1X authentication

1. Click **802.1X Connection**, as shown in [Figure 6](#).

Figure 6 802.1X connection



2. Enter username **localuser** and password **localpass**, as shown in [Figure 7](#).

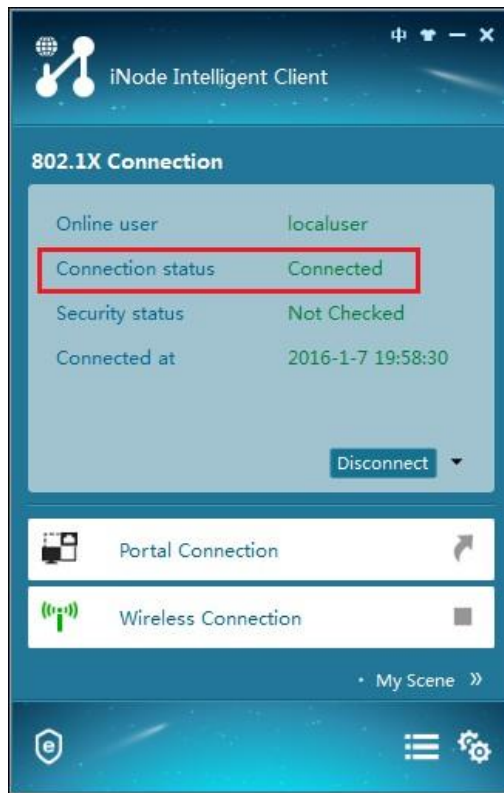
Figure 7 Entering the username and password



3. Click the inverted triangle icon next to **Connect** and select **Properties**.
4. In the dialog box that opens, select a wireless NIC and clear the option for uploading the client version.
5. Return to the iNode 802.1X connection screen.
6. Click **Connect**.

The iNode client displays the connection state as shown in [Figure 8](#).

Figure 8 Successful 802.1X authentication



Verifying the configuration

Display online 802.1X user information.

```
[AC] display dot1x connection
```

```
User MAC address      : 0015-00bf-e84d
AP name                : office
Radio ID               : 1
SSID                   : service
BSSID                  : 741f-4ad4-1fe0
Username               : localuser
Authentication domain  : bbb
IPv4 address           : 2.2.1.3
Authentication method  : CHAP
Initial VLAN           : 200
Authorization VLAN     : 200
Authorization ACL number : N/A
Authorization user profile : N/A
Termination action     : N/A
Session timeout period : N/A
Online from            : 2019/12/04 17:37:55
Online duration        : 0h 4m 20s
```

Display service template information.


```

[AC] display wlan service-template service
Service template name      : service
SSID                      : service
SSID-hide                 : Disabled
User-isolation            : Disabled
Service template status   : Enabled
Maximum clients per BSS   : Not configured
Frame format              : Dot3
Seamless roam status      : Disabled
Seamless roam RSSI threshold : 50
Seamless roam RSSI gap    : 20
VLAN ID                   : 200
AKM mode                  : Not configured
Security IE               : Not configured
Cipher suite              : Not configured
TKIP countermeasure time  : 0 sec
PTK lifetime              : 43200 sec
GTK rekey                 : Enabled
GTK rekey method          : Time-based
GTK rekey time            : 86400 sec
GTK rekey client-offline  : Disabled
User authentication mode   : 802.1X
Intrusion protection      : Disabled
Intrusion protection mode  : Temporary-block
Temporary block time      : 180 sec
Temporary service stop time : 20 sec
Fail VLAN ID              : Not configured
802.1X handshake          : Disabled
802.1X handshake secure   : Disabled
802.1X domain             : bbb
MAC-auth domain           : Not configured
Max 802.1X users          : 4096
Max MAC-auth users        : 4096
802.1X re-authenticate    : Disabled
Authorization fail mode    : Online
Accounting fail mode      : Online
Authorization              : Permitted
Key derivation             : SHA1
PMF status                : Disabled
Hotspot policy number     : Not configured
Forwarding policy status  : Disabled
Forwarding policy name    : Not configured
FT status                 : Disabled
QoS trust                 : Port
QoS priority              : 0

```

Configuration files

- AC:

```
#
vlan 100
#
vlan 200
#
wlan service-template service
    ssid service
    vlan 200
    client forwarding-location ac
    client-security authentication-mode dot1x
    dot1x domain bbb
    service-template enable
#
interface Vlan-interface100
    ip address 2.2.2.1 255.255.255.0
#
interface Vlan-interface200
    ip address 2.2.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
    port link-mode bridge
    port link-type trunk
    port trunk permit vlan 1 100 200
#
domain bbb
    authentication lan-access local
    authorization lan-access local
    accounting lan-access local
#
local-user localuser class network
    password cipher $c$3$+5Yra0KsaLci/RxEa4lyYKxxiw6jwMCCog==
    service-type lan-access
#
wlan ap-group group1
    ap office
    ap-model AP 3620
        radio 1
            radio enable
            service-template service
        radio 2
#
wlan ap office model AP 3620
    serial-id 219801A28N819CE0003T
#
```

- Switch:

```

#
dhcp enable
#
vlan 100
#
vlan 200
#
dhcp server ip-pool 100
network 2.2.2.0 mask 255.255.255.0
gateway-list 2.2.2.1
option 138 ip-address 2.2.2.1
#
dhcp server ip-pool 200
network 2.2.1.0 mask 255.255.255.0
gateway-list 2.2.1.1
#
interface Vlan-interface100
ip address 2.2.2.100 255.255.255.0
#
interface Vlan-interface200
ip address 2.2.1.2 255.255.255.0
#
interface GigabitEthernet1/0/1
port link-type trunk
port trunk permit vlan 1 100 200
#
interface GigabitEthernet1/0/2
port link-type trunk
port access permit vlan 100 200
port trunk pvid vlan 100
poe enable
#

```

Related documentation

- *AP and WT Management Configuration Guide in INTELBRAS Access Controllers Configuration Guides*
- *AP and WT Management Command Reference in INTELBRAS Access Controllers Command References*
- *Network Connectivity Configuration Guide in INTELBRAS Access Controllers Configuration Guides*
- *Network Connectivity Command Reference in INTELBRAS Access Controllers Command References*
- *User Access and Authentication Configuration Guide in INTELBRAS Access Controllers Configuration Guides*
- *User Access and Authentication Command Reference in INTELBRAS Access Controllers Command References*
- *WLAN Access Configuration Guide in INTELBRAS Access Controllers Configuration Guides*
- *WLAN Access Command Reference in INTELBRAS Access Controllers Command References*

INTELBRAS Access Controllers

Local RADIUS-Based 802.1X Authentication in EAP Relay Mode

Configuration Examples

Copyright © 2024 Intelbras S.A All rights reserved.

No part of this manual may be reproduced or transmitted in any form or by any means without prior written consent of Intelbras S.A

Except for the trademarks of Intelbras S.A, any trademarks that may be mentioned in this document are the property of their respective owners.

The information in this document is subject to change without notice.

Contents

Introduction	1
Prerequisites	1
Example: Configuring local RADIUS-based 802.1X authentication in EAP relay mode	1
Network configuration	1
Restrictions and guidelines	2
Procedures	2
Configuring the AC	2
Configuring the switch	5
Verifying the configuration	6
Configuration files	8
Related documentation	10

Introduction

The following information provides an example of configuring 802.1X authentication in EAP relay mode when the AC acts as both the access device and RADIUS server.

Prerequisites

The following information applies to Comware-based access controllers and access points. Procedures and information in the examples might be slightly different depending on the software or hardware version of the access controllers and access points.

The configuration examples 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.

The following information is provided based on the assumption that you have basic knowledge of WLAN access, WLAN security, WLAN access authentication, and 802.1X features.

Example: Configuring local RADIUS-based 802.1X authentication in EAP relay mode

Network configuration

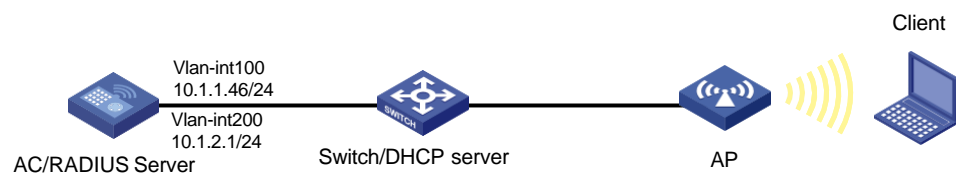
As shown in [Figure 1](#):

- The switch acts as a DHCP server to assign IP addresses to the AP and the client.
- The AC acts as both the access device and RADIUS server for the client.
- When the client accesses a wireless service, it must pass 802.1X EAP-PEAP authentication and obtain the required authorization information.

Configure the AC to meet the following requirements:

- Use the local RADIUS server to perform authentication and authorization for wireless 802.1X users.
- Use open system authentication to authenticate the client at the data link layer. This is the default authentication method.
- Use the 802.1X AKM mode to secure data transmission between the client and the AP.
- Use CCMP as the cipher suite.

Figure 1 Network diagram



Restrictions and guidelines

Use the actual serial ID of an AP to uniquely identify that AP.

Procedures

Configuring the AC

1. Install the freeradius image file.

```
<AC> install activate feature cfa0:/freeradius.bin slot 1
Verifying the file cfa0:/freeradius.bin on slot 1...Done.
Identifying the upgrade methods    Done.
Upgrade summary according to following table:

cfa0:/freeradius.bin
  Running Version      New Version
  None                Feature 5531

  Slot                Upgrade Way
  1                   Service Upgrade
Upgrading software images to compatible versions. Continue? [Y/N]:
Y
This operation might take several minutes, please wait.....Done.
<AC> install activate feature cfa0:/freeradius.bin slot 2
Copying file cfa0:/freeradius.bin to slot2#cfa0:/freeradius.bin ...Done.
Verifying the file cfa0:/freeradius.bin on slot 2.  Done.
Identifying the upgrade methods....Done.
Upgrade summary according to following table:

cfa0:/freeradius.bin
  Running Version      New Version
  None                Feature 5531

  Slot                Upgrade Way
  2                   Service Upgrade
Upgrading software images to compatible versions. Continue? [Y/N]:y
This operation might take several minutes, please wait. ....Done.
<AC> install commit
```

2. Use FTP or TFTP to transfer the required certificate files to the storage media of the AC and verify that the file transfer has succeeded.

```
<AC> dir *.pem
Directory of cfa0:
 0 -rw-          3428 Feb 06 2018 13:46:34   ca.pem
 1 -rw-          3345 Feb 06 2018 16:42:10   client.pem
 2 -rw-          3345 Feb 06 2018 13:46:50   server.pem
```

3. Configure interfaces on the AC:

Create VLAN 100 and VLAN-interface 100, and assign an IP address to the VLAN interface. The AC will use this IP address to establish CAPWAP tunnels with the AP.

```
<AC> system-view
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 10.1.1.46 24
[AC-Vlan-interface100] quit
```

Create VLAN 200 and VLAN-interface 200, and assign an IP address to the VLAN interface. VLAN 200 will be used for client access.

```
[AC] vlan 200
[AC-vlan200] quit
[AC] interface vlan-interface 200
[AC-Vlan-interface200] ip address 10.1.2.1 24
[AC-Vlan-interface200] quit
```

Configure GigabitEthernet 1/0/1 (the port connected to the switch) as a trunk port, and assign the port to VLAN 100 and VLAN 200.

```
[AC] interface gigabitethernet 1/0/1
[AC-GigabitEthernet1/0/1] port link-type trunk
[AC-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[AC-GigabitEthernet1/0/1] quit
```

4. Configure EAP relay as the method for the 802.1X module to exchange packets with the local RADIUS server.

```
[AC] dot1x authentication-method eap
```

5. Configure a RADIUS scheme:

Create a RADIUS scheme named **1x-local** and enter its view.

```
[AC] radius scheme 1x-local
```

Specify the server at 10.1.2.1 as the primary authentication server and set the shared key of authentication packets to **12345678** in plaintext form.

```
[AC-radius-1x-local] primary authentication 10.1.2.1
[AC-radius-1x-local] key authentication simple 12345678
```

Exclude the domain name from the usernames sent to the RADIUS server.

```
[AC-radius-1x-local] user-name-format without-domain
[AC-radius-1x-local] quit
```

6. Configure an authentication domain:

Create an ISP domain named **1x-local** and enter its view.

```
[AC] domain 1x-local
```

Configure the ISP domain to use RADIUS scheme **1x-local** for LAN user authentication and authorization and to not perform accounting for LAN users.

```
[AC-isp-1x-local] authentication lan-access radius-scheme 1x-local
[AC-isp-1x-local] authorization lan-access radius-scheme 1x-local
[AC-isp-1x-local] accounting lan-access none
[AC-isp-1x-local] quit
```

7. Configure a RADIUS user:

Create a network access user named **dot1x** and enter its view.

```
[AC] local-user dot1x class network
```

Set the user password to **123456** in plaintext form.

```
[AC-luser-network-dot1x] password simple 123456
```


- ```
Allow the user to use the LAN access service.
[AC-luser-network-dot1x] service-type lan-access

Assign the network-operator user role to the user.
[AC-luser-network-dot1x] authorization-attribute user-role network-operator
[AC-luser-network-dot1x] quit
```
8. Configure EAP authentication on the RADIUS server:
 

```
Set the EAP authentication method to peap-mschapv2.
[AC] eap-profile dot1x
[AC-eap-profile-dot1x] method peap-mschapv2

Specify a CA certificate for EAP authentication.
[AC-eap-profile-dot1x] ca-file ca.pem

Specify a local certificate for EAP authentication.
[AC-eap-profile-dot1x] certificate-file server.pem

Specify the private key file of the local certificate for EAP authentication.
[AC-eap-profile-dot1x] private-key-file server.pem

Configure the private key password of the local certificate.
[AC-eap-profile-dot1x] private-key-password simple whatever
[AC-eap-profile-dot1x] quit

Specify an EAP profile for the local RADIUS server.
[AC] radius-server eap-profile dot1x
```
  9. Specify the RADIUS client at 10.1.2.1 and set the shared key to **12345678** in plaintext form for secure communication with the client.
 

```
[AC] radius-server client ip 10.1.2.1 key simple 12345678
```
  10. Restart the RADIUS server and activate the RADIUS server settings.
 

```
[AC] radius-server activate
```
  11. Configure a service template:
 

```
Create a service template named 1x-local and enter its view.
[AC] wlan service-template 1x-local

Set the SSID of the service template to dot1x-local.
[AC-wlan-st-1x-local] ssid dot1x-local

Assign clients coming online through the service template to VLAN 200.
[AC-wlan-st-1x-local] vlan 200

Set the AKM mode to 802.1X.
[AC-wlan-st-1x-local] akm mode dot1x

Set the cipher suite to CCMP.
[AC-wlan-st-1x-local] cipher-suite ccmp

Enable the RSN IE in beacon and probe responses.
[AC-wlan-st-1x-local] security-ie rsn

Set the authentication mode to 802.1X.
[AC-wlan-st-1x-local] client-security authentication-mode dot1x

Specify ISP domain 1x-local for authenticating 802.1X clients.
[AC-wlan-st-1x-local] dot1x domain 1x-local

Enable the AC to forward client data traffic. If the AC forwards client data traffic by default, skip this step.
[AC-wlan-st-1x-local] client forwarding-location ac

Enable the service template.
[AC-wlan-st-1x-local] service-template enable
```

```
[AC-wlan-st-1x-local] quit
```

## 12. Configure AP settings:

### ❗ IMPORTANT:

In a large-scale network, configure AP groups as a best practice.

# Create a manual AP named **aptest** and enter its view.

```
[AC] wlan ap aptest model AP 3620
```

# Specify the serial ID of the AP.

```
[AC-wlan-ap-apest] serial-id 219801A28N819CE0002T
```

```
[AC-wlan-ap-apest] quit
```

# Create AP group **group1** and create an AP grouping rule by AP names to add AP **apest** to AP group **group1**.

```
[AC] wlan ap-group group1
```

```
[AC-wlan-ap-group-group1] ap aptest
```

# Bind service template **1x-local** to radio 1 in AP group **group1**, and enable radio 1.

```
[AC-wlan-ap-group-group1] ap-model AP 3620
```

```
[AC-wlan-ap-group-group1-ap-model-AP 3620] radio 1
```

```
[AC-wlan-ap-group-group1-ap-model-AP 3620-radio-1] service-template 1x-local [AC-wlan-ap-group-group1-ap-model-AP 3620-radio-1] radio enable
```

```
[AC-wlan-ap-group-group1-ap-model-AP 3620-radio-1] quit
```

# Bind service template **1x-local** to radio 2 in AP group **group1**, and enable radio 2.

```
[AC-wlan-ap-group-group1-ap-model-AP 3620] radio 2
```

```
[AC-wlan-ap-group-group1-ap-model-AP 3620-radio-2] service-template 1x-local [AC-wlan-ap-group-group1-ap-model-AP 3620-radio-2] radio enable
```

```
[AC-wlan-ap-group-group1-ap-model-AP 3620]
```

```
quit [AC-wlan-ap-group-group1] quit
```

## Configuring the switch

# Create VLAN 100. The switch will use this VLAN to forward the traffic on the CAPWAP tunnels between the AC and AP.

```
<Switch> system-view
```

```
[Switch] vlan 100
```

```
[Switch-vlan100] quit
```

# Create VLAN 200. The switch will use this VLAN to forward packets for wireless clients.

```
[Switch] vlan 200
```

```
[Switch-vlan200] quit
```

# Set the link type of GigabitEthernet 1/0/1 (the port connected to the AC) to trunk, and assign the trunk port to VLAN 100 and VLAN 200.

```
[Switch] interface gigabitethernet 1/0/1
```

```
[Switch-GigabitEthernet1/0/1] port link-type trunk
```

```
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100 200
```

```
[Switch-GigabitEthernet1/0/1] quit
```

# Set the link type of GigabitEthernet 1/0/2 (the port connected to the AP) to access, and assign the access port to VLAN 100.

```
[Switch] interface gigabitethernet 1/0/2
```

```
[Switch-GigabitEthernet1/0/2] port link-type access
```

```
[Switch-GigabitEthernet1/0/2] port access vlan 100
```

**# Enable PoE on GigabitEthernet 1/0/2.**

```
[Switch-GigabitEthernet1/0/2] poe enable
```

```
[Switch-GigabitEthernet1/0/2] quit
```

**# Create VLAN-interface 100 and assign an IP address to the VLAN interface.**

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

```
[Switch-Vlan-interface100] ip address 10.1.1.2 24
```

```
[Switch-Vlan-interface100] quit
```

**# Create VLAN-interface 200 and assign an IP address to the VLAN interface.**

```
[Switch] interface vlan-interface 200
```

```
[Switch-Vlan-interface200] ip address 10.1.2.2 24
```

```
[Switch-Vlan-interface200] quit
```

**# Create a DHCP address pool named **100**, and specify a subnet and a gateway IP address in the DHCP address pool. The IP address of the AP is assigned from this pool.**

```
[Switch] dhcp server ip-pool 100
```

```
[Switch-dhcp-pool-100] network 10.1.1.0 mask 255.255.255.0
```

```
[Switch-dhcp-pool-100] gateway-list 10.1.1.2
```

```
[Switch-dhcp-pool-100] quit
```

**# Create a DHCP address pool named **200**, and specify a subnet, a gateway IP address, and a DNS server in the DHCP address pool. In this example, the address of the DNS server is 10.1.2.2. You must replace it with the actual address of the DNS server on your network. The IP address of the client is assigned from this pool.**

```
[Switch] dhcp server ip-pool 200
```

```
[Switch-dhcp-pool-200] network 10.1.2.0 mask 255.255.255.0
```

```
[Switch-dhcp-pool-200] gateway-list 10.1.2.1
```

```
[Switch-dhcp-pool-200] dns-list 10.1.2.2
```

```
[Switch-dhcp-pool-200] quit
```

**# Enable DHCP.**

```
[Switch] dhcp enable
```

## Verifying the configuration

1. On the client, verify that the client can pass 802.1X authentication, associate with the AP, and access the wireless network after you enter the correct username and password. (Details not shown.)
2. On the AC, perform the following tasks to verify that the client has passed authentication and come online:

**# Display detailed WLAN client information.**

```
[AC] display wlan client verbose
```

```
Total number of clients: 1
```

|              |                  |
|--------------|------------------|
| MAC address  | : 1044-0037-2e9f |
| IPv4 address | : 10.1.2.3       |
| IPv6 address | : N/A            |
| Username     | : dot1x          |
| AID          | : 1              |
| AP ID        | : 20             |
| AP name      | : aptest         |

```

Radio ID : 1
SSID : 15209_local_1x_eap_peap_5560h
BSSID : d461-fe62-1537
VLAN ID : 200
Sleep count : 0
Wireless mode : 802.11ac
Channel bandwidth : 80MHz
SM power save : Disabled
Short GI for 20MHz : Supported
Short GI for 40MHz : Supported
Short GI for 80MHz : Supported
Short GI for 160/80+80MHz : Not supported
STBC RX capability : Supported
STBC TX capability : Not supported
LDPC RX capability : Supported
Beamformee STS capability : 1
Number of Sounding Dimensions : 0
SU beamformee capability : Supported
MU beamformee capability : Supported
Block Ack : N/A
Supported VHT-MCS set : NSS1 0, 1, 2, 3, 4, 5, 6, 7, 8, 9
Supported HT MCS set : 0, 1, 2, 3, 4, 5, 6, 7
Supported rates : 6, 9, 12, 18, 24, 36,
 48, 54 Mbps
QoS mode : WMM
Listen interval : 3
RSSI : 0
Rx/Tx rate : 0/0 Mbps
Speed : N/A
Authentication method : Open system
Security mode : RSN
AKM mode : 802.1X
Cipher suite : CCMP
User authentication mode : 802.1X
WPA3 status : Disabled
Authorization CAR : N/A
Authorization ACL ID : N/A
Authorization user profile : N/A
Roam status : N/A
Key derivation : SHA1
PMF status : N/A
Forwarding policy name : Not configured
Online time : 0days 0hours 0minutes 6seconds
FT status : Inactive

```

#### # Display online 802.1X client information.

```
[AC] display dot1x connection
```

```
Total connections: 1
```

```
User MAC address : 1044-0037-2e9f
```

```

AP name : aptest
Radio ID : 1
SSID : dot1x-local
BSSID : d461-fe62-1537
Username : dot1x
Authentication domain : hk-local
IPv4 address : 10.1.2.3
Authentication method : EAP
Initial VLAN : 200
Authorization VLAN : 200
Authorization ACL number : N/A
Authorization user profile : N/A
Authorization CAR : N/A
Termination action : N/A
Session timeout last from : N/A
Session timeout period : N/A
Online from : 2020/05/22 11:54:58
Online duration : 0h 0m 20s

```

## Configuration files

- AC:
 

```

#
dot1x authentication-method eap
#
vlan 100
#
vlan 200
#
wlan service-template 1x-local
ssid dot1x-local
vlan 200
client forwarding-location ac
akm mode dot1x
cipher-suite ccmp
security-ie rsn
client-security authentication-mode dot1x
dot1x domain 1x-local
service-template enable
#
interface Vlan-interface100
ip address 10.1.1.46 255.255.255.0
#
interface Vlan-interface200
ip address 10.1.2.1 255.255.255.0
#
interface GigabitEthernet1/0/1
port link-mode bridge

```

```

port link-type trunk
port trunk permit vlan 1 100 200
#
eap-profile dot1x
method peap-mschapv2
ca-file ca.pem
certificate-file server.pem
private-key-file server.pem
private-key-password simple whatever
#
radius-server eap-profile 1x
#
radius-server client ip 10.1.2.1 key simple 12345678
#
local-user dot1x class network
password simple 12345678
service-type lan-access
authorization-attribute user-role network-operator
#
radius scheme 1x-local
primary authentication 10.1.2.1
key authentication simple 12345678
user-name-format without-domain
#
domain 1x-local
authentication lan-access radius-scheme 1x-local
authorization lan-access radius-scheme 1x-local
accounting lan-access none
#
wlan ap-group group1
ap aptest
ap-model AP 3620
radio 1
radio enable
service-template 1x-local
radio 2
radio enable
service-template 1x-local
gigabitethernet 1
#
wlan ap aptest model AP 3620
serial-id 219801A28N819CE0002T
#

```

- **Switch:**

```

#
dhcp enable
#
vlan 100

```

```

#
vlan 200
#
dhcp server ip-pool 100
 gateway-list 10.1.1.2
 network 10.1.1.0 mask 255.255.255.0
#
dhcp server ip-pool 200
 gateway-list 10.1.2.1
 network 10.1.2.0 mask 255.255.255.0
 dns-list 10.1.2.2
#
interface Vlan-interface100
 ip address 10.1.1.2 255.255.255.0
#
interface Vlan-interface200
 ip address 10.1.2.2 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 1 100 200
#
interface GigabitEthernet1/0/2
 port link-type access
 port access vlan 100
 poe enable
#

```

## Related documentation

- *User Access and Authentication Configuration Guide in INTELBRAS Access Controllers Configuration Guides*
- *User Access and Authentication Command Reference in INTELBRAS Access Controllers Command References*
- *WLAN Access Configuration Guide in INTELBRAS Access Controllers Configuration Guides*
- *WLAN Access Command Reference in INTELBRAS Access Controllers Command References*

# INTELBRAS Access Controllers Remote 802.1X Authentication Configuration Examples

---

Copyright © 2024 Intelbras S.A All rights reserved.

No part of this manual may be reproduced or transmitted in any form or by any means without prior written consent of Intelbras S.A

Except for the trademarks of Intelbras S.A, any trademarks that may be mentioned in this document are the property of their respective owners.

The information in this document is subject to change without notice.



# Contents

|                                                        |    |
|--------------------------------------------------------|----|
| Introduction .....                                     | 1  |
| Prerequisites .....                                    | 1  |
| Example: Configuring remote 802.1X authentication..... | 1  |
| Network configuration.....                             | 1  |
| Restrictions and guidelines .....                      | 2  |
| Procedures .....                                       | 2  |
| Configuring the AC.....                                | 2  |
| Configuring the switch .....                           | 4  |
| Configuring the RADIUS server .....                    | 5  |
| Verifying the configuration .....                      | 8  |
| Configuration files.....                               | 10 |
| Related documentation .....                            | 12 |

# Introduction

The following information provides an example for configuring remote 802.1X authentication for wireless clients.

## Prerequisites

The following information applies to Comware-based access controllers and access points. Procedures and information in the examples might be slightly different depending on the software or hardware version of the access controllers and access points.

The configuration examples 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.

The following information is provided based on the assumption that you have basic knowledge of WLAN access, WLAN security, WLAN authentication, and 802.1X.

## Example: Configuring remote 802.1X authentication

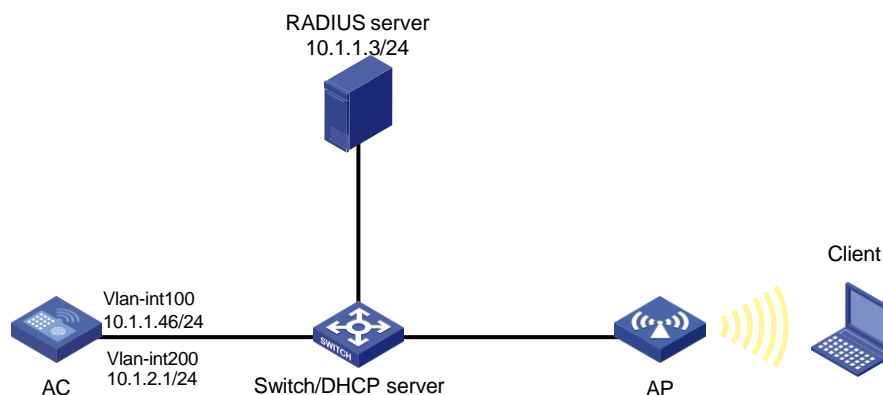
### Network configuration

As shown in [Figure 1](#), the switch acts as a DHCP server to assign IP addresses to the AP and the client. The RADIUS server runs on INC.

Configure the AC, the client, the switch, and the RADIUS server to meet the following requirements:

- The AC uses the RADIUS server to perform 802.1X authentication for the wireless client.
- The AC uses the open system authentication for the client at the data link layer. This is the default authentication method.
- The AC uses the 802.1X AKM mode to secure data transmission between the client and the AP.
- The cipher suite is CCMP.

**Figure 1 Network diagram**



# Restrictions and guidelines

When you configure remote 802.1X authentication for wireless clients, follow these restrictions and guidelines:

- Use the serial ID labeled on the AP's rear panel to specify an AP.
- For the INC server to dynamically change the client authorization information or forcibly disconnect clients, enable the RADIUS session-control feature on the AC.
- To avoid dynamic authorization failures when the client is coming online, configure the RADIUS DAE server (DAS) feature.

## Procedures

### Configuring the AC

#### 1. Configure interfaces on the AC:

# Create VLAN 100 and VLAN-interface 100, and assign an IP address to the VLAN interface. The AC will use this IP address to establish CAPWAP tunnels with the AP.

```
<AC> system-view
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 10.1.1.46 24
[AC-Vlan-interface100] quit
```

# Create VLAN 200 and VLAN-interface 200, and assign an IP address to the VLAN interface. VLAN 200 will be used for client access.

```
[AC] vlan 200
[AC-vlan200] quit
[AC] interface vlan-interface 200
[AC-Vlan-interface200] ip address 10.1.2.1 24
[AC-Vlan-interface200] quit
```

# Configure GigabitEthernet 1/0/1 (the port connected to the switch) as a trunk port, and assign the port to VLAN 100 and VLAN 200.

```
[AC] interface gigabitEthernet 1/0/1
[AC-GigabitEthernet1/0/1] port link-type trunk
[AC-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[AC-GigabitEthernet1/0/1] quit
```

#### 2. Configure a RADIUS scheme:

# Create a RADIUS scheme named **radius1** and enter its view.

```
[AC] radius scheme radius1
```

# Specify the IP addresses of the primary authentication and accounting RADIUS servers.

```
[AC-radius-radius1] primary authentication 10.1.1.3
[AC-radius-radius1] primary accounting 10.1.1.3
```

# Set the shared key to **12345** in plain text for secure communication with the servers.

```
[AC-radius-radius1] key authentication simple 12345
[AC-radius-radius1] key accounting simple 12345
```

# Specify IP address 10.1.2.1 as the source IP address for outgoing RADIUS packets.

```
[AC-radius-radius1] nas-ip 10.1.2.1
```

```
[AC-radius-radius1] quit
```

# Create an ISP domain named **dom1** and enter its view.

```
[AC] domain dom1
```

# Apply RADIUS scheme **radius1** to ISP domain **dom1** for LAN user authentication, authorization, and accounting.

```
[AC-isp-dom1] authentication lan-access radius-scheme radius1
```

```
[AC-isp-dom1] authorization lan-access radius-scheme radius1
```

```
[AC-isp-dom1] accounting lan-access radius-scheme radius1
```

```
[AC-isp-dom1] quit
```

# Enable the RADIUS session-control feature.

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

# Enable the RADIUS DAS feature and enter RADIUS DAS view.

```
[AC] radius dynamic-author server
```

# Specify the RADIUS server at 10.1.1.3 as a DAC and set the shared key to **12345** in plain text for validating DAE packets from the RADIUS server.

```
[AC-radius-da-server] client ip 10.1.1.3 key simple 12345
```

```
[AC-radius-da-server] quit
```

3. Configure the AC to use EAP relay to authenticate 802.1X clients.

```
[AC] dot1x authentication-method eap
```

4. Configure a wireless service:

# Create a service template named **service** and enter its view.

```
[AC] wlan service-template service
```

# Configure the SSID of the service template as **service**.

```
[AC-wlan-st-service] ssid service
```

# Assign clients coming online through the service template to VLAN 200.

```
[AC-wlan-st-service] vlan 200
```

# Set the AKM mode to 802.1X.

```
[AC-wlan-st-service] akm mode dot1x
```

# Set the cipher suite to CCMP.

```
[AC-wlan-st-service] cipher-suite ccmp
```

# Enable the RSN IE in beacon and probe responses.

```
[AC-wlan-st-service] security-ie rsn
```

# Set the authentication mode to 802.1X.

```
[AC-wlan-st-service] client-security authentication-mode dot1x
```

# Specify ISP domain **dom1** for authenticating 802.1X clients.

```
[AC-wlan-st-service] dot1x domain dom1
```

# Enable the AC to forward client data traffic. If the AC forwards client data traffic by default, skip this step.

```
[AC-wlan-st-service] client forwarding-location ac
```

# Enable the service template.

```
[AC-wlan-st-service] service-template enable
```

```
[AC-wlan-st-service] quit
```

5. Configure AP settings:

---

**! IMPORTANT:**

In a large-scale network, configure AP groups as a best practice.

---

# Create a manual AP named **office**, and specify the AP model and serial ID

```
[AC] wlan ap office model AP 3620
[AC-wlan-ap-office] serial-id 219801A28N819CE0002T
[AC-wlan-ap-office] quit
```

# Create AP group **group1** and create an AP grouping rule by AP names to add AP **office** to AP group **group1**.

```
[AC] wlan ap-group group1
[AC-wlan-ap-group-group1] ap office
```

# Bind service template **service** to radio 1 in AP group **group1**.

```
[AC-wlan-ap-group-group1] ap-model AP 3620
[AC-wlan-ap-group-group1-ap-model-AP 3620] radio 1
[AC-wlan-ap-group-group1-ap-model-AP 3620-radio-1] service-template service
```

# Enable radio 1.

```
[AC-wlan-ap-group-group1-ap-model-AP 3620-radio-1] radio
enable [AC-wlan-ap-group-group1-ap-model-AP 3620-radio-1] quit
[AC-wlan-ap-group-group1-ap-model-AP 3620]
quit [AC-wlan-ap-group-group1] quit
```

## Configuring the switch

# Create VLAN 100. The switch will use this VLAN to forward the traffic on the CAPWAP tunnels between the AC and AP.

```
<Switch> system-view
[Switch] vlan 100
[Switch-vlan100] quit
```

# Create VLAN 200. The switch will use this VLAN to forward packets for wireless clients.

```
[Switch] vlan 200
[Switch-vlan200] quit
```

# Configure GigabitEthernet 1/0/1 (the port connected to the AC) as a trunk port, and assign the trunk port to VLANs 100 and 200.

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[Switch-GigabitEthernet1/0/1] quit
```

# Configure GigabitEthernet 1/0/2 (the port connected to the AP) as an access port, and assign the port to VLAN 100.

```
[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] port link-type access
[Switch-GigabitEthernet1/0/2] port access vlan 100
```

# Enable PoE on GigabitEthernet 1/0/2.

```
[Switch-GigabitEthernet1/0/2] poe enable
[Switch-GigabitEthernet1/0/2] quit
```

# Create VLAN-interface 100, and assign an IP address to the VLAN interface.

```
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ip address 10.1.1.47 24
[Switch-Vlan-interface100] quit
```

# Create VLAN-interface 200, and assign an IP address to the VLAN interface.

```
[Switch] interface vlan-interface 200
[Switch-Vlan-interface200] ip address 10.1.2.2 24
[Switch-Vlan-interface200] quit
```

# Configure DHCP pool **100** to assign an IP address to the AP.

```
[Switch] dhcp server ip-pool 100
[Switch-dhcp-pool-100] network 10.1.1.0 mask 255.255.255.0
[Switch-dhcp-pool-100] gateway-list 10.1.1.46
[Switch-dhcp-pool-100] quit
```

# Configure DHCP pool **200** to assign an IP address to the client. In this example, the address of the DNS server is 10.1.2.1 (the gateway address). You must replace it with the actual address of the DNS server on your network.

```
[Switch] dhcp server ip-pool 200
[Switch-dhcp-pool-200] network 10.1.2.0 mask 255.255.255.0
[Switch-dhcp-pool-200] gateway-list 10.1.2.1
[Switch-dhcp-pool-200] dns-list 10.1.2.1
[Switch-dhcp-pool-200] quit
```

# Enable DHCP.

```
[Switch] dhcp enable
```

## Configuring the RADIUS server

In this example, the RADIUS server runs INC PLAT 7.1(E0302) and INC UAM 7.1(E0302).

1. Add the AC to INC as an access device:
  - a. Log in to INC and click the **User** tab.
  - b. From the navigation tree, select **User Access Policy > Access Device Management > Access Device**.
  - c. Click **Add**.  
The **Add Access Device** page opens.
  - d. In the **Access Configuration** area, configure the following parameters, as shown in [Figure 2](#):
    - Enter **12345** in the **Shared Key** and **Confirm Shared Key** fields.
    - Use the default values for other parameters.
  - e. In the **Device List** area, click **Select** or **Add Manually** to add the device at **10.1.2.1** as an access device.
  - f. Click **OK**.

**Figure 2 Adding an access device**

User > User Access Policy > Access Device Management > Access Device > Add Access Device

### Access Configuration

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

### Device List

Select Add Manually Clear All

| Device Name | Device IP | Device Model | Comments | Delete |
|-------------|-----------|--------------|----------|--------|
|             | 10.1.2.1  |              |          |        |

Total Items: 1.

OK Cancel

2. Add an access policy:
  - a. Click the **User** tab.
  - b. From the navigation tree, select **User Access Policy > Access Policy**.
  - c. Click **Add**.
  - d. On the **Add Access Policy** page, configure the following parameters, as shown in [Figure 3](#):
    - Enter **dot1x** in the **Access Policy Name** field.
    - Select **EAP** for the **Certificate Authentication** field.
    - Select **EAP-PEAP Auth** from the **Certificate Type** list, and select **MS-CHAPV2 Auth** from the **Certificate Sub-Type** list.

The certificate sub-type on the INC server must be the same as the identity authentication method configured on the client.
  - e. Click **OK**.

**Figure 3 Adding an access policy**

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

---

Basic Information

Access Policy Name \*

Service Group \*

Description

---

Authorization Information

Access Period

Allocate IP \*

Downstream Rate(Kbps)

Upstream Rate(Kbps)

Priority

☐ RSA Authentication

Certificate Authentication ☐ None ☒ EAP

Certificate Type

Certificate Sub-Type

Deploy VLAN

☐ Deploy User Profile

☐ Deploy ACL

Deploy User Group

3. Add an access service:
  - a. Click the **User** tab.
  - b. From the navigation tree, select **User Access Policy > Access Service**.
  - c. Click **Add**.
  - d. On the **Add Access Service** page, configure the following parameters, as shown in [Figure 4](#):
    - Enter **dot1x** in the **Service Name** field.
    - Select **dot1x** from the **Default Access Policy** list.
  - e. 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 Max. Number of Bound Endpoints \*

Default Max. Number of Online Endpoints \*

Description

☒ Available ☐ Transparent Authentication on Portal Endpoints

---

Access Scenario List

| Access Scenario | Access Policy | Proprietary Attribute Assignment Policy | Priority | Modify | Delete |
|-----------------|---------------|-----------------------------------------|----------|--------|--------|
| No match found. |               |                                         |          |        |        |

4. Add an access user:
  - a. Click the **User** tab.
  - b. From the navigation tree, select **Access User > All Access Users**.



The access user list opens.

**c. Click Add.**

The **Add Access User** page opens.

**d. In the Access Information area, configure the following parameters, as shown in Figure 5:**

- Click **Select** or **Add User** to associate the user with INC Platform user **user**.
- Enter **dot1x** in the **Account Name** field.
- Enter **dot1x123** in the **Password** and **Confirm Password** fields.

**e. In the Access Service area, select dot1x from the list.**

**f. Click OK.**

**Figure 5 Adding an access user account**

User Name \*

Account Name \*

☐ Trial Account ☐ Default BYOD User ☐ MAC Authentication 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

Max. Transparent Portal Bindings

Login Message

**Access Service**

|                                     | Service Name | Service Suffix | Status    | Allocate IP |
|-------------------------------------|--------------|----------------|-----------|-------------|
| <input checked="" type="checkbox"/> | dot1x        |                | Available |             |

## Verifying the configuration

1. On the client, verify that the client can pass authentication, associate with the AP, and access the wireless network. (Details not shown.)
2. On the AC, perform the following tasks to verify that the user has passed authentication and come online:

# Display detailed WLAN client information.

```
[AC] display wlan client verbose
```

```
Total number of clients: 1
```

```
MAC address : cc3a-61a8-fb8c
IPv4 address : 10.1.2.3
IPv6 address : N/A
Username : dot1x
AID : 1
AP ID : 3
AP name : office
Radio ID : 1
```

|                            |                                     |
|----------------------------|-------------------------------------|
| SSID                       | : service                           |
| BSSID                      | : 741f-4ad4-1fe0                    |
| VLAN ID                    | : 200                               |
| Sleep count                | : 0                                 |
| Wireless mode              | : 802.11ac                          |
| Channel bandwidth          | : 80MHz                             |
| SM power save              | : Disabled                          |
| Short GI for 20MHz         | : Supported                         |
| Short GI for 40MHz         | : Supported                         |
| Short GI for 80MHz         | : Supported                         |
| Short GI for 160/80+80MHz  | : Not supported                     |
| STBC RX capability         | : Not supported                     |
| STBC TX capability         | : Not supported                     |
| LDPC RX capability         | : Not supported                     |
| SU beamformee capability   | : Not supported                     |
| MU beamformee capability   | : Not supported                     |
| Beamformee STS capability  | : N/A                               |
| Block Ack                  | : N/A                               |
| Supported VHT-MCS set      | : NSS1 0, 1, 2, 3, 4, 5, 6, 7, 8, 9 |
| Supported HT MCS set       | : 0, 1, 2, 3, 4, 5, 6, 7            |
| Supported rates            | : 6, 9, 12, 18, 24, 36, 48, 54 Mbps |
| QoS mode                   | : WMM                               |
| Listen interval            | : 10                                |
| RSSI                       | : 0                                 |
| Rx/Tx rate                 | : 0/0                               |
| Authentication method      | : Open system                       |
| Security mode              | : RSN                               |
| AKM mode                   | : 802.1X                            |
| Cipher suite               | : CCMP                              |
| User authentication mode   | : 802.1X                            |
| Authorization ACL ID       | : N/A                               |
| Authorization user profile | : N/A                               |
| Roam status                | : N/A                               |
| Key derivation             | : SHA1                              |
| PMF status                 | : N/A                               |
| Forwarding policy name     | : N/A                               |
| Online time                | : 0days 0hours 0minutes 15seconds   |
| FT status                  | : Inactive                          |

#### # Display online 802.1X client information.

[AC] display dot1x connection

Total connections: 1

|                  |                  |
|------------------|------------------|
| User MAC address | : cc3a-61a8-fb8c |
| AP name          | : office         |
| Radio ID         | : 1              |
| SSID             | : service        |
| BSSID            | : 741f-4ad4-1fe0 |
| Username         | : dot1x          |

```

Authentication domain : dom1
IPv4 address : 10.1.2.3
Authentication method : EAP
Initial VLAN : 200
Authorization VLAN : 200
Authorization ACL number : N/A
Authorization user profile : N/A
Termination action : Default
Session timeout period : 36000001 s
Online from : 2015/12/21 11:27:11
Online duration : 0h 1m 1s

```

## Configuration files

- AC:

```

#
 dot1x authentication-method eap
#
vlan 100
#
vlan 200
#
wlan service-template service
 ssid service
 vlan 200
 client forwarding-location ac
 akm mode dot1x
 cipher-suite ccmp
 security-ie rsn
 client-security authentication-mode dot1x
 dot1x domain dom1
 service-template enable
#
interface Vlan-interface100
 ip address 10.1.1.46 255.255.255.0
#
interface Vlan-interface200
 ip address 10.1.2.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 1 100 200
#
radius scheme radius1
 primary authentication 10.1.1.3
 primary accounting 10.1.1.3
 key authentication cipher c3$Bb61SHV2ZsVYPJU2+RFB/8ntk0uCQkmdA==
 key accounting cipher c3$w03NfxnBmfDuedv9/xo7ESnoxKjowmmX9A==

```

```

nas-ip 10.1.2.1
#
radius dynamic-author server
 client ip 10.1.1.3 key cipher c3$AkTEB7OgMYnCqsfDeplhoAgXUek/rVrLZw==
#
radius session-control enable
#
domain dom1
 authentication lan-access radius-scheme radius1
 authorization lan-access radius-scheme radius1
 accounting lan-access radius-scheme radius1
#
wlan ap-group group1
 ap office
 ap-model AP 3620
 radio 1
 radio enable
 service-template service
 radio 2
#
wlan ap office model AP 3620
 serial-id 219801A28N819CE0002T
#

```

- **Switch:**

```

#
 dhcp enable
#
vlan 100
#
vlan 200
#
dhcp server ip-pool 100
 gateway-list 10.1.1.46
 network 10.1.1.0 mask 255.255.255.0
#
dhcp server ip-pool 200
 gateway-list 10.1.2.1
 network 10.1.2.0 mask 255.255.255.0
 dns-list 10.1.2.1
#
interface Vlan-interface100
 ip address 10.1.1.47 255.255.255.0
#
interface Vlan-interface200
 ip address 10.1.2.2 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-type trunk

```

```
port trunk permit vlan 1 100 200
#
interface GigabitEthernet1/0/2
port access vlan 100
poe enable
#
```

## Related documentation

- *AP and WT Management Configuration Guide in INTELBRAS Access Controllers Configuration Guides*
- *AP and WT Management Command Reference in INTELBRAS Access Controllers Command References*
- *Network Connectivity Configuration Guide in INTELBRAS Access Controllers Configuration Guides*
- *Network Connectivity Command Reference in INTELBRAS Access Controllers Command References*
- *User Access and Authentication Configuration Guide in INTELBRAS Access Controllers Configuration Guides*
- *User Access and Authentication Command Reference in INTELBRAS Access Controllers Command References*
- *WLAN Access Configuration Guide in INTELBRAS Access Controllers Configuration Guides*
- *WLAN Access Command Reference in INTELBRAS Access Controllers Command References*

# INTELBRAS Access Controllers

## Remote 802.1X Authentication (IPv6) Configuration Examples

---

Copyright © 2024 Intelbras S.A All rights reserved.

No part of this manual may be reproduced or transmitted in any form or by any means without prior written consent of Intelbras S.A

Except for the trademarks of Intelbras S.A, any trademarks that may be mentioned in this document are the property of their respective owners.

The information in this document is subject to change without notice.

# Contents

|                                                                            |    |
|----------------------------------------------------------------------------|----|
| Introduction .....                                                         | 1  |
| Prerequisites .....                                                        | 1  |
| Example: Configuring remote authentication for 802.1X clients (IPv6) ..... | 1  |
| Network configuration .....                                                | 1  |
| Restrictions and guidelines .....                                          | 2  |
| Procedures .....                                                           | 2  |
| Configuring the AC .....                                                   | 2  |
| Configuring the switch .....                                               | 4  |
| Configuring the RADIUS server .....                                        | 6  |
| Configuring the client .....                                               | 9  |
| Verifying the configuration .....                                          | 9  |
| Configuration files .....                                                  | 10 |
| Related documentation .....                                                | 13 |

# Introduction

The following information provides an example for configuring remote 802.1X authentication for wireless clients on an IPv6 network.

## Prerequisites

The following information applies to Comware-based access controllers and access points. Procedures and information in the examples might be slightly different depending on the software or hardware version of the access controllers and access points.

The configuration examples 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.

The following information is provided based on the assumption that you have basic knowledge of IPv6 basics, WLAN access, WLAN security, WLAN authentication, and 802.1X.

## Example: Configuring remote authentication for 802.1X clients (IPv6)

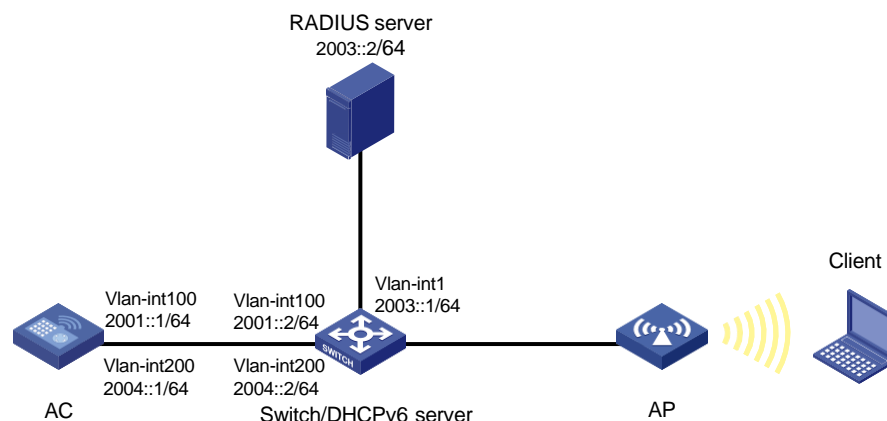
### Network configuration

As shown in [Figure 1](#), the switch acts as a DHCPv6 server to assign IPv6 addresses to the AP and the client. INC acts as the RADIUS server.

Configure the AC, the client, the switch, and the RADIUS server to meet the following requirements:

- The AC uses the RADIUS server to perform 802.1X authentication for the wireless client.
- The AC uses the open system authentication for the client at the data link layer. This is the default authentication method.
- The AC uses the 802.1X AKM mode to secure data transmission between the client and the AP.
- The cipher suite is CCMP.

**Figure 1 Network diagram**





# Restrictions and guidelines

When you configure remote 802.1X authentication for wireless clients, follow these restrictions and guidelines:

- Use the actual serial ID of an AP to uniquely identify that AP.
- For the INC server to dynamically change the client authorization information or forcibly disconnect clients, enable the RADIUS session-control feature on the AC.

## Procedures

### Configuring the AC

#### 1. Configure interfaces on the AC:

# Create VLAN 100 and VLAN-interface 100, and assign an IPv6 address to the VLAN interface. The AC will use this IP address to establish CAPWAP tunnels with the AP.

```
<AC> system-view
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ipv6 address 2001::1 64
[AC-Vlan-interface100] quit
```

# Create VLAN 200 and VLAN-interface 200, and assign an IPv6 address to the VLAN interface. VLAN 200 will be used for client access.

```
[AC] vlan 200
[AC-vlan200] quit
[AC] interface vlan-interface 200
[AC-Vlan-interface200] ipv6 address 2004::1 64
[AC-Vlan-interface200] quit
```

# Configure GigabitEthernet 1/0/1 (the port connected to the switch) as a trunk port, and assign the port to VLAN 1, VLAN 100, and VLAN 200.

```
[AC] interface gigabitethernet 1/0/1
[AC-GigabitEthernet1/0/1] port link-type trunk
[AC-GigabitEthernet1/0/1] port trunk permit vlan 1 100 200
[AC-GigabitEthernet1/0/1] quit
```

#### 2. Configure a RADIUS scheme:

# Create a RADIUS scheme named **radius1** and enter its view.

```
[AC] radius scheme radius1
```

# Specify the IPv6 addresses of the primary authentication and accounting RADIUS servers.

```
[AC-radius-radius1] primary authentication ipv6 2003::2
[AC-radius-radius1] primary accounting ipv6 2003::2
```

# Set the shared key to **12345** in plain text for secure communication with the servers.

```
[AC-radius-radius1] key authentication simple 12345
[AC-radius-radius1] key accounting simple 12345
```

# Specify IPv6 address 2001::1 as the source IPv6 address of outgoing RADIUS packets.

```
[AC-radius-radius1] nas-ip ipv6 2001::1
[AC-radius-radius1] quit
```

# Create an ISP domain named **dom1** and enter its view.

```
[AC] domain dom1
```

# Apply RADIUS scheme **radius1** to ISP domain **dom1** for LAN user authentication, authorization, and accounting.

```
[AC-isp-dom1] authentication lan-access radius-scheme radius1
```

```
[AC-isp-dom1] authorization lan-access radius-scheme radius1
```

```
[AC-isp-dom1] accounting lan-access radius-scheme radius1
```

```
[AC-isp-dom1] quit
```

# Enable the RADIUS session-control feature.

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

# Enable the RADIUS DAS feature and enter RADIUS DAS view.

```
[AC] radius dynamic-author server
```

# Specify the RADIUS server at 2003::2 as a DAC and set the shared key to **12345** in plain text for validating DAE packets from the RADIUS server.

```
[AC-radius-da-server] client ipv6 2003::2 key simple 12345
```

```
[AC-radius-da-server] quit
```

3. Configure the AC to use EAP relay to authenticate 802.1X clients.

```
[AC] dot1x authentication-method eap
```

4. Configure a wireless service:

# Create a service template named **service** and enter its view.

```
[AC] wlan service-template service
```

# Set the SSID of the service template to **service**.

```
[AC-wlan-st-service] ssid service
```

# Assign clients coming online through the service template to VLAN 200.

```
[AC-wlan-st-service] vlan 200
```

# Set the AKM mode to 802.1X authentication.

```
[AC-wlan-st-service] akm mode dot1x
```

# Set the cipher suite to CCMP and enable the RSN-IE in beacon and probe responses.

```
[AC-wlan-st-service] cipher-suite ccmp
```

```
[AC-wlan-st-service] security-ie rsn
```

# Set the authentication mode to 802.1X authentication.

```
[AC-wlan-st-service] client-security authentication-mode dot1x
```

# Specify ISP domain **dom1** for authenticating 802.1X clients.

```
[AC-wlan-st-service] dot1x domain dom1
```

# Enable snooping DHCPv6 packets and enable snooping ND packets.

```
[AC-wlan-st-service] client ipv6-snooping dhcpv6-learning enable
```

```
[AC-wlan-st-service] client ipv6-snooping nd-learning enable
```

# Enable the AC to forward client data traffic. If the AC forwards client data traffic by default, skip this step.

```
[AC-wlan-st-service] client forwarding-location ac
```

# Enable the service template.

```
[AC-wlan-st-service] service-template enable
```

```
[AC-wlan-st-service] quit
```

5. Configure AP settings:

---

**! IMPORTANT:**

In a large-scale network, configure AP groups as a best practice.

---

# Create a manual AP named **ap1**, and specify the AP model and serial ID.

```
[AC] wlan ap ap1 model AP 3620
[AC-wlan-ap-ap1] serial-id 219801A28N819CE0002T
[AC-wlan-ap-ap1] quit

Create AP group group1 and create an AP grouping rule by AP names to add AP ap1 to AP group group1.
[AC] wlan ap-group group1
[AC-wlan-ap-group-group1] ap ap1

Bind service template service to radio 1 in AP group group1.
[AC-wlan-ap-group-group1] ap-model AP 3620
[AC-wlan-ap-group-group1-ap-model-AP 3620] radio 1
[AC-wlan-ap-group-group1-ap-model-AP 3620-radio-1] service-template service

Enable radio 1.
[AC-wlan-ap-group-group1-ap-model-AP 3620-radio-1] radio
enable [AC-wlan-ap-group-group1-ap-model-AP 3620-radio-1] quit
[AC-wlan-ap-group-group1-ap-model-AP 3620]
quit [AC-wlan-ap-group-group1] quit
```

6. Configure a static route destined for the RADIUS server.

```
[AC] ipv6 route-static 2003:: 64 2004::2
```

## Configuring the switch

- Configure VLAN settings:
 

# Create VLAN 100. The switch will use this VLAN to forward the traffic on the CAPWAP tunnels between the AC and AP.

```
<Switch> system-view
[Switch] vlan 100
[Switch-vlan100] quit
```

# Create VLAN 200. The switch will use this VLAN to forward packets for wireless clients.

```
[Switch] vlan 200
[Switch-vlan200] quit
```

# Configure GigabitEthernet 1/0/1 (the port connected to the AC) as a trunk port, and assign the port to VLAN 1, VLAN 100, and VLAN 200.

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 1 100 200
[Switch-GigabitEthernet1/0/1] quit
```

# Configure GigabitEthernet 1/0/2 (the port connected to the AP) as an access port, and assign the port to VLAN 100.

```
[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] port link-type access
[Switch-GigabitEthernet1/0/2] port access vlan 100
```

# Enable PoE on GigabitEthernet 1/0/2.

```
[Switch-GigabitEthernet1/0/2] poe enable
[Switch-GigabitEthernet1/0/2] quit
```

# Create VLAN-interface 1 and assign an IPv6 address to the VLAN interface.

```
[Switch] interface vlan-interface 1
[Switch-Vlan-interface1] ipv6 address 2003::1 64
[Switch-Vlan-interface1] quit
```

**# Create VLAN-interface 100 and assign an IPv6 address to the VLAN interface.**

```
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ipv6 address 2001::2 64
[Switch-Vlan-interface100] quit
```

**# Create VLAN-interface 200 and assign an IPv6 address to the VLAN interface.**

```
[Switch] interface vlan-interface 200
[Switch-Vlan-interface200] ipv6 address 2004::2 64
[Switch-Vlan-interface200] quit
```

## **2. Configure the DHCPv6 service:**

**# Create DHCPv6 address pool 1, specify the subnet 2001::/64 in the DHCPv6 address pool, and specify 2001::1 as the gateway address. The switch assigns an IPv6 address to the AP from this pool.**

```
[Switch] ipv6 dhcp pool 1
[Switch-dhcp6-pool-1] network 2001::/64
[Switch-dhcp6-pool-1] gateway-list 2001::1
```

**# Configure Option 52 that specifies the AC's IPv6 address 2001::1 and exclude the IPv6 address from dynamic assignment.**

```
[Switch-dhcp6-pool-1] option 52 hex 20010000000000000000000000000001
[Switch-dhcp6-pool-1] quit
[Switch] ipv6 dhcp server forbidden-address 2001::1
```

**# Apply address pool 1 to VLAN-interface 100 and enable the DHCPv6 server on the VLAN interface.**

```
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ipv6 dhcp server apply pool 1
[Switch-Vlan-interface100] ipv6 dhcp select server
```

**# Set the managed address configuration flag (M) and the other stateful configuration flag (O) to 1 in RA advertisements to be sent, and disable RA message suppression on VLAN-interface 100.**

```
[Switch-Vlan-interface100] ipv6 nd autoconfig managed-address-flag
[Switch-Vlan-interface100] ipv6 nd autoconfig other-flag
[Switch-Vlan-interface100] undo ipv6 nd ra halt
[Switch-Vlan-interface100] quit
```

**# Create DHCPv6 address pool 2, specify the subnet 2004::/64 in the DHCPv6 address pool, and specify 2004::2 as the gateway address. The switch assigns an IPv6 address to the client from this pool.**

```
[Switch] ipv6 dhcp pool 2
[Switch-dhcp6-pool-2] network 2004::/64
[Switch-dhcp6-pool-2] gateway-list 2004::2
[Switch-dhcp6-pool-2] quit
```

**# Exclude IPv6 address 2004::1 from dynamic assignment.**

```
[Switch] ipv6 dhcp server forbidden-address 2004::1
```

**# Apply address pool 2 to VLAN-interface 200 and enable the DHCPv6 server on the VLAN interface.**

```
[Switch] interface Vlan-interface 200
[Switch-Vlan-interface200] ipv6 dhcp server apply pool 2
[Switch-Vlan-interface200] ipv6 dhcp select server
```

**# Set the managed address configuration flag (M) and the other stateful configuration flag (O) to 1 in RA advertisements to be sent, and disable RA message suppression on VLAN-interface 200.**

```
[Switch-Vlan-interface200] ipv6 nd autoconfig managed-address-flag
[Switch-Vlan-interface200] ipv6 nd autoconfig other-flag
[Switch-Vlan-interface200] undo ipv6 nd ra halt
[Switch-Vlan-interface200] quit
```

## Configuring the RADIUS server

This example uses INC PLAT 7.1 and INC UAM 7.1 to show the procedure.

Make sure the EAP-PEAP certificate has been installed on the server.

1. Add the AC to INC as an access device:
  - a. Log in to INC.
  - b. Click the **User** tab.
  - c. From the navigation tree, select **User Access Policy > Access Device Management > Access Device**.
  - d. Click **Add**.  
The **Add Access Device** page opens.
  - e. Configure access device parameters, as shown in [Figure 2](#):
    - In the **Access Configuration** area, set the authentication and accounting shared keys to **12345** and use the default settings of other parameters.
    - In the **Device List** area, click **Select** or **Add IPv6 Dev** to add the device at 2001::1 to INC as an access device. If you click **Add IPv6 Dev**, enter 2001::1 as the start IPv6 address and click **OK** in the dialog box that opens.
  - f. Click **OK**.

**Figure 2 Adding an access device**

Access Configuration

|                            |                                                                 |                      |           |
|----------------------------|-----------------------------------------------------------------|----------------------|-----------|
| Authentication Port *      | 1812                                                            | Accounting Port *    | 1813      |
| Service Type               | LAN Access Service                                              |                      |           |
| Access Device Type         | H3C(General)                                                    | Service Group        | Ungrouped |
| Shared Key *               | *****                                                           | Confirm Shared Key * | *****     |
| Access Device Group        | --                                                              |                      |           |
| Certificate Authentication | <input checked="" type="radio"/> None <input type="radio"/> EAP |                      |           |
| Certificate Type           | EAP-TLS Authn                                                   |                      |           |

Device List

Select Add Manually Add IPv6 Dev Clear All

| Device Name     | Device IP | Device Model | Comments | Delete |
|-----------------|-----------|--------------|----------|--------|
| No match found. |           |              |          |        |
| Total Items: 0. |           |              |          |        |

2. Add an access policy:
  - a. Click the **User** tab.
  - b. From the navigation tree, select **User Access Policy > Access Policy**.
  - c. Click **Add**.
  - d. On the **Add Access Policy** page, configure the following parameters, as shown in [Figure 3](#):
    - Enter **dot1x** in the **Access Policy Name** field.
    - Select **EAP** for the **Certificate Authentication** field.

- Select **EAP-PEAP Auth** from the **Certificate Type** list, and select **MS-CHAPV2 Auth** from the **Certificate Sub-Type** list.

The certificate sub-type on the INC server must be the same as the identity authentication method configured on the client.

e. Click **OK**.

**Figure 3 Adding an access policy**

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

**Basic Information**

Access Policy Name \*

Service Group \*

Description

**Authorization Information**

Access Period

Allocate IP \*

Downstream Rate(Kbps)

Upstream Rate(Kbps)

Priority

☐ RSA Authentication

Certificate Authentication ☐ None ☒ EAP

Certificate Type

Certificate Sub-Type

Deploy VLAN

☐ Deploy User Profile

☐ Deploy ACL

Deploy User Group

3. Add an access service:

a. Click the **User** tab.

b. From the navigation tree, select **User Access Policy > Access Service**.

c. Click **Add**.

d. On the **Add Access Service** page, configure the following parameters, as shown in [Figure 4](#):

- Enter **dot1x** in the **Service Name** field.
- Select **dot1x** from the **Default Access Policy** list.

e. 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 Max. Number of Bound Endpoints \*  Default Max. Number of Online Endpoints \*

Description

☒ Available ? ☐ Transparent Authentication on Portal Endpoints ?

**Access Scenario List**

| Access Scenario | Access Policy | Proprietary Attribute Assignment Policy | Priority | Modify | Delete |
|-----------------|---------------|-----------------------------------------|----------|--------|--------|
| No match found. |               |                                         |          |        |        |

4. Add an access user:
  - a. Click the **User** tab.
  - b. From the navigation tree, select **Access User > Access User**.  
The access user list opens.
  - c. Click **Add**.  
The **Add Access User** page opens.
  - d. In the **Access Information** area, configure the following parameters, as shown in Figure 5:
    - Click **Select** or **Add User** to associate the user with INC Platform user **user**.
    - Enter **dot1x** in the **Account Name** field.
    - Enter **dot1x123** in the **Password** and **Confirm Password** fields.
  - e. In the **Access Service** area, select **dot1x** from the list.
  - f. Click **OK**.

**Figure 5 Adding an access user account**

User > All Access Users > Add Access User

**Access account**

**Access Information**

User Name \*

Account Name \*

☐ Trial Account ☐ Default BYOD User ☐ MAC Authentication 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

Max. Transparent Portal Bindings

Login Message

**Access Service**

|                                     | Service Name | Service Suffix | Status    | Allocate IP |
|-------------------------------------|--------------|----------------|-----------|-------------|
| <input checked="" type="checkbox"/> | dot1x        |                | Available |             |

# Configuring the client

Use a mobile phone to connect to the wireless network with SSID **service**:

1. Select PEAP as the EAP authentication method.
2. Enter **dot1x** as the identity and enter password **dot1x123**.  
Use the default settings of other parameters.
3. Connect to the wireless network.

## Verifying the configuration

1. On the client, verify that the client can pass authentication, associate with the AP, and access the wireless network. (Details not shown.)
2. On the AC, perform the following tasks to verify that the user has passed authentication and come online:

# Display detailed WLAN client information.

```
[AC] display wlan client verbose
```

Total number of clients: 1

|                                  |                                        |
|----------------------------------|----------------------------------------|
| MAC address                      | : 3829-5a40-9589                       |
| IPv4 address                     | : N/A                                  |
| IPv6 address                     | : 2004::4                              |
| Username                         | : dot1x                                |
| AID                              | : 1                                    |
| AP ID                            | : 2                                    |
| AP name                          | : ap1                                  |
| Radio ID                         | : 1                                    |
| SSID                             | : service                              |
| BSSID                            | : ac74-090a-6421                       |
| VLAN ID                          | : 200                                  |
| Sleep count                      | : 0                                    |
| Wireless mode                    | : 802.11an                             |
| Channel bandwidth                | : 40MHz                                |
| 20/40 BSS Coexistence Management | : Supported                            |
| SM power save                    | : Enabled                              |
| SM power save mode               | : Static                               |
| Short GI for 20MHz               | : Supported                            |
| Short GI for 40MHz               | : Supported                            |
| STBC RX capability               | : Supported                            |
| STBC TX capability               | : Not supported                        |
| LDPC RX capability               | : Not supported                        |
| Block Ack                        | : N/A                                  |
| Supported HT MCS set             | : 0, 1, 2, 3, 4, 5, 6, 7               |
| Supported rates                  | : 6, 9, 12, 18, 24, 36,<br>48, 54 Mbps |
| QoS mode                         | : WMM                                  |
| Listen interval                  | : 2                                    |
| RSSI                             | : 0                                    |
| Rx/Tx rate                       | : 0/0 Mbps                             |



```

Authentication method : Open system
Security mode : RSN
AKM mode : 802.1X
Cipher suite : CCMP
User authentication mode : 802.1X
Authorization ACL ID : N/A
Authorization user profile : N/A
Roam status : N/A
Key derivation : SHA1
PMF status : N/A
Forwarding policy name : Not configured
Online time : 0days 0hours 0minutes 1seconds
FT status : Inactive

```

#### # Display online 802.1X client information.

```

[AC] display dot1x connection
Total connections: 1
User MAC address : 3829-5a40-9589
AP name : ap1
Radio ID : 1
SSID : service
BSSID : ac74-090a-6421
Username : dot1x
Authentication domain : dom1
IPv6 address : 2004::4
Authentication method : EAP
Initial VLAN : 200
Authorization VLAN : 200
Authorization ACL number : N/A
Authorization user profile : N/A
Termination action : Radius-Request
Session timeout period : 86401 s
Online from : 2018/07/18 10:36:00
Online duration : 0h 0m 19s

```

## Configuration files

- AC:
 

```

#
dot1x authentication-method eap
#
vlan 1
#
vlan 100
#
vlan 200
#
wlan service-template service
ssid service

```

```

vlan 200
client forwarding-location ac
akm mode dot1x
cipher-suite ccmp
security-ie rsn
client-security authentication-mode dot1x
dot1x domain dom1
client ipv6-snooping nd-learning enable
client ipv6-snooping dhcpv6-learning enable
service-template enable
#
interface Vlan-interface100
 ipv6 address 2001::1/64
#
interface Vlan-interface200
 ipv6 address 2004::1/64
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 100 200
#
ipv6 route-static 2003:: 64 2004::2
#
radius session-control enable
#
radius scheme radius1
 primary authentication ipv6 2003::2
 primary accounting ipv6 2003::2
 key authentication cipher c3$Nc0p9aAdEZsigfKkc+BN0VwrlStmtFHa
 key accounting cipher c3$1Ui0GNVopIKWmUamDZB0pK2pSJ9+C7U5
 nas-ip ipv6 2001::1
#
radius dynamic-author server
 client ipv6 2003::2 key cipher c3$m0GMY0tNJT94RiwVyD80JG2zYwSUfpNV
#
domain dom1
 authentication lan-access radius-scheme radius1
 authorization lan-access radius-scheme radius1
 accounting lan-access radius-scheme radius1
#
wlan ap-group group1
 ap ap1
 ap-model AP 3620
 radio 1
 radio enable
 service-template service
 radio 2

```

```
#
wlan ap ap1 model AP 3620
serial-id 219801A28N819CE0002T
#
```

- Switch:

```
#
ipv6 dhcp server forbidden-address 2001::1
ipv6 dhcp server forbidden-address 2004::1
#
vlan 1
#
vlan 100
#
vlan 200
#
ipv6 dhcp pool 1
network 2001::/64
option 52 hex 20010000000000000000000000000001
gateway-list 2001::1
#
ipv6 dhcp pool 2
network 2004::/64
gateway-list 2004::2
#
interface Vlan-interface1
ipv6 address 2003::1/64
#
interface Vlan-interface100
ipv6 dhcp select server
ipv6 dhcp server apply pool 1
ipv6 address 2001::2/64
ipv6 nd autoconfig managed-address-flag
ipv6 nd autoconfig other-flag
undo ipv6 nd ra halt
#
interface Vlan-interface200
ipv6 dhcp select server
ipv6 dhcp server apply pool 2
ipv6 address 2004::2/64
ipv6 nd autoconfig managed-address-flag
ipv6 nd autoconfig other-flag
undo ipv6 nd ra halt
#
interface GigabitEthernet1/0/1
port link-type trunk
port trunk permit vlan 1 100 200
#
interface GigabitEthernet1/0/2
```

```
port access vlan 100
poe enable
#
```

## Related documentation

- *AP and WT Management Configuration Guide in INTELBRAS Access Controllers Configuration Guides*
- *AP and WT Management Command Reference in INTELBRAS Access Controllers Command References*
- *Network Connectivity Configuration Guide in INTELBRAS Access Controllers Configuration Guides*
- *Network Connectivity Command Reference in INTELBRAS Access Controllers Command References*
- *User Access and Authentication Configuration Guide in INTELBRAS Access Controllers Configuration Guides*
- *User Access and Authentication Command Reference in INTELBRAS Access Controllers Command References*
- *WLAN Access Configuration Guide in INTELBRAS Access Controllers Configuration Guides*
- *WLAN Access Command Reference in INTELBRAS Access Controllers Command References*

# INTELBRAS Access Controllers

## Remote 802.1X Authentication in WPA3-Enterprise Mode

### Configuration Examples

---

Copyright © 2024 Intelbras S.A All rights reserved.

No part of this manual may be reproduced or transmitted in any form or by any means without prior written consent of Intelbras S.A

Except for the trademarks of Intelbras S.A, any trademarks that may be mentioned in this document are the property of their respective owners.

The information in this document is subject to change without notice.

# Contents

|                                                                                    |    |
|------------------------------------------------------------------------------------|----|
| Introduction .....                                                                 | 1  |
| Prerequisites .....                                                                | 1  |
| Example: Configuring remote 802.1X authentication in WPA3-Enterprise mode<br>..... | 1  |
| Network configuration .....                                                        | 1  |
| Restrictions and guidelines .....                                                  | 2  |
| Procedures .....                                                                   | 2  |
| Configuring the AC .....                                                           | 2  |
| Configuring the switch .....                                                       | 4  |
| Configuring the RADIUS server .....                                                | 5  |
| Configuring the wireless client .....                                              | 7  |
| Verifying the configuration .....                                                  | 7  |
| Configuration files .....                                                          | 9  |
| Related documentation .....                                                        | 11 |

# Introduction

The following information provides an example of configuring remote 802.1X authentication in WPA3-Enterprise mode.

## Prerequisites

The following information applies to Comware-based access controllers and access points. Procedures and information in the examples might be slightly different depending on the software or hardware version of the access controllers and access points.

The configuration examples 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.

The following information is provided based on the assumption that you have basic knowledge of WLAN access, WLAN security, WLAN access authentication, and 802.1X features.

## Example: Configuring remote 802.1X authentication in WPA3-Enterprise mode

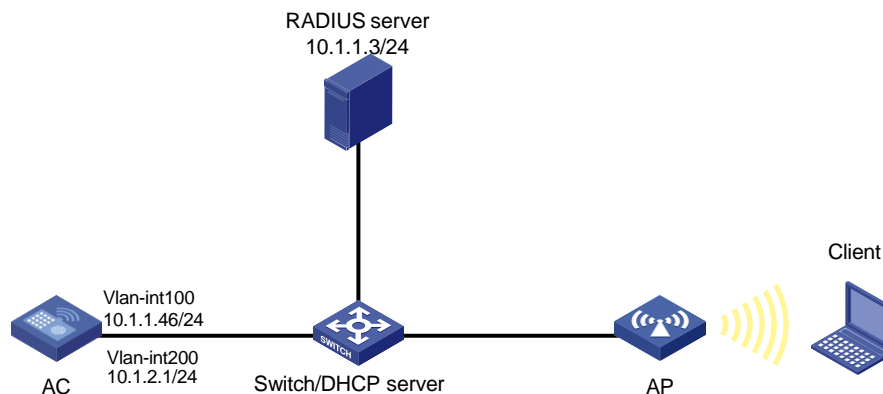
### Network configuration

As shown in [Figure 1](#), the switch acts as a DHCP server to assign IP addresses to the AP and the client. The RADIUS server is an INC server.

Configure the AC, the client, the switch, and the RADIUS server to meet the following requirements:

- The AC uses the RADIUS server to perform authentication, authorization, and accounting for the wireless client. The 802.1X EAP-PEAP authentication method is used.
- The AC uses the open system authentication for the client at the data link layer. This is the default authentication method at the data link layer.
- The AC uses the 802.1X AKM mode to secure data transmission between the client and the AP.
- The cipher suite is GCMP and the security mode is WPA3-Enterprise.

**Figure 1 Network diagram**



# Restrictions and guidelines

Use the actual serial ID of an AP to uniquely identify that AP.

## Procedures

### Configuring the AC

#### 1. Configure interfaces:

# Create VLAN 100, create VLAN-interface 100, and assign an IP address to the VLAN interface. The AC will use this IP address to establish CAPWAP tunnels with the AP.

```
<AC> system-view
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 10.1.1.46 24
[AC-Vlan-interface100] quit
```

# Create VLAN 200, create VLAN-interface 100, and assign an IP address to the VLAN interface. The AC assigns VLAN 200 to a client when the client comes online.

```
[AC] vlan 200
[AC-vlan200] quit
[AC] interface vlan-interface 200
[AC-Vlan-interface200] ip address 10.1.2.1 24
[AC-Vlan-interface200] quit
```

# Set the link type of GigabitEthernet 1/0/1 (the interface connected to the switch) to trunk, and permit traffic from VLAN 100 and VLAN 200 to pass through the interface.

```
[AC] interface gigabitethernet 1/0/1
[AC-GigabitEthernet1/0/1] port link-type trunk
[AC-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[AC-GigabitEthernet1/0/1] quit
```

#### 2. Configure a RADIUS scheme:

# Create RADIUS scheme **radius1** and enter its view.

```
[AC] radius scheme radius1
```

# Specify the RADIUS server at 10.1.1.3 as the primary authentication and accounting servers.

```
[AC-radius-radius1] primary authentication 10.1.1.3
[AC-radius-radius1] primary accounting 10.1.1.3
```

# Set the shared key to **12345** in plaintext form for secure communication with the RADIUS authentication server.

```
[AC-radius-radius1] key authentication simple 12345
```

# Set the shared key to **12345** in plaintext form for secure communication with the RADIUS accounting server.

```
[AC-radius-radius1] key accounting simple 12345
```

# Specify IP address 10.1.2.1 as the source IP address for outgoing RADIUS packets.

```
[AC-radius-radius1] nas-ip 10.1.2.1
[AC-radius-radius1] quit
```

# Create ISP domain **dom1** and enter its view.

```
[AC] domain dom1
```



# Configure the ISP domain to use RADIUS scheme **radius1** for 802.1X user authentication, authorization, and accounting.

```
[AC-isp-dom1] authentication lan-access radius-scheme radius1
[AC-isp-dom1] authorization lan-access radius-scheme radius1
[AC-isp-dom1] accounting lan-access radius-scheme radius1
[AC-isp-dom1] quit
```

3. Specify EAP relay as the method to exchange packets with the RADIUS server.

```
[AC] dot1x authentication-method eap
```

4. Configure a service template:

# Create service template **wpa3\_enterprise** and enter its view.

```
[AC] wlan service-template wpa3_enterprise
```

# Set the SSID to **wpa3**.

```
[AC-wlan-st-wpa3_enterprise] ssid wpa3
```

# Specify VLAN 200 for the service template.

```
[AC-wlan-st-wpa3_enterprise] vlan 200
```

# Set the AKM mode to 802.1X.

```
[AC-wlan-st-wpa3_enterprise] akm mode dot1x
```

# Specify the GCMP cipher suite and enable the RSN IE in beacon and probe responses. Support for the GCMP cipher suite depends on the AP model.

```
[AC-wlan-st-wpa3_enterprise] cipher-suite gcmp
```

```
[AC-wlan-st-wpa3_enterprise] security-ie rsn
```

# Set the access authentication mode to 802.1X authentication.

```
[AC-wlan-st-wpa3_enterprise] client-security authentication-mode dot1x
```

# Specify ISP domain **dom1** for authenticating the 802.1X client.

```
[AC-wlan-st-wpa3_enterprise] dot1x domain dom1
```

# Set the WPA3 security mode to WPA3-Enterprise.

```
[AC-wlan-st-wpa3_enterprise] wpa3 enterprise
```

# Enable management frame protection in mandatory mode.

```
[AC-wlan-st-wpa3_enterprise] pmf mandatory
```

# Enable the AC to forward client data traffic. If the AC forwards client data traffic by default, skip this step.

```
[AC-wlan-st-wpa3_enterprise] client forwarding-location ac
```

# Enable the service template.

```
[AC-wlan-st-wpa3_enterprise] service-template enable
```

```
[AC-wlan-st-wpa3_enterprise] quit
```

5. Configure AP settings:

---

❗ **IMPORTANT:**

In a large-scale network, configure AP groups as a best practice.

---

# Create manual AP **office** and specify the AP model and serial ID.

```
[AC] wlan ap office model AP 3620
[AC-wlan-ap-office] serial-id 219801A28N819CE0002T
[AC-wlan-ap-office] quit
```

# Create AP group **group1** and create an AP grouping rule by AP names to add AP **office** to AP group **group1**.

```
[AC] wlan ap-group group1
[AC-wlan-ap-group-group1] ap office
```

**# Bind service template `wpa3_enterprise` to radio 1 in AP group `group1`.**

```
[AC-wlan-ap-group-group1] ap-model AP 3620
[AC-wlan-ap-group-group1-ap-model-AP 3620] radio 1
[AC-wlan-ap-group-group1-ap-model-AP 3620-radio-1] service-template wpa3_enterprise
```

**# Enable radio 1.**

```
[AC-wlan-ap-group-group1-ap-model-AP 3620-radio-1] radio
enable [AC-wlan-ap-group-group1-ap-model-AP 3620-radio-1] quit
[AC-wlan-ap-group-group1-ap-model-AP 3620]
quit [AC-wlan-ap-group-group1] quit
```

## Configuring the switch

### 1. Configure interfaces:

**# Create VLAN 100 and VLAN 200, create VLAN-interface 100 and VLAN-interface 200, and assign IP addresses to the VLAN interfaces. VLAN 100 is used to forward CAPWAP tunnel traffic between the AC and AP. VLAN 200 is used to forward wireless client packet.**

```
<Switch> system-view
[Switch] vlan 100
[Switch-vlan100] quit
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ip address 10.1.1.47 24
[Switch-Vlan-interface100] quit
[Switch] vlan 200
[Switch-vlan200] quit
[Switch] interface vlan-interface 200
[Switch-Vlan-interface200] ip address 10.1.2.2 24
[Switch-Vlan-interface200] quit
```

**# Set the link type of GigabitEthernet 1/0/1 (the interface connected to the AC), and permit traffic from VLAN 100 and VLAN 200 to pass through the interface.**

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[Switch-GigabitEthernet1/0/1] quit
```

**# Set the link type of GigabitEthernet 1/0/2 (the interface connected to the AP) to access, and permit traffic from VLAN 100 to pass through the interface.**

```
[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] port link-type access
[Switch-GigabitEthernet1/0/2] port access vlan 100
```

**# Enable PoE on GigabitEthernet 1/0/2.**

```
[Switch-GigabitEthernet1/0/2] poe enable
[Switch-GigabitEthernet1/0/2] quit
```

### 2. Configure DHCP:

**# Enable DHCP.**

```
[Switch] dhcp enable
```

**# Create a DHCP address pool named `100`, and specify subnet 10.1.1.0/24 and gateway IP address 10.1.1.47 in the DHCP address pool.**

```
[Switch] dhcp server ip-pool 100
[Switch-dhcp-pool-100] network 10.1.1.0 mask 255.255.255.0
[Switch-dhcp-pool-100] gateway-list 10.1.1.47
```

```
[Switch-dhcp-pool-100] quit
```

# Create a DHCP address pool named **200**, and specify subnet 10.1.2.0/24 and gateway IP address 10.1.2.2 in the DHCP address pool. In this example, the address of the DNS server is 10.1.2.2 (the gateway address). You must replace it with the actual address of the DNS server on your network.

```
[Switch] dhcp server ip-pool 200
```

```
[Switch-dhcp-pool-200] network 10.1.2.0 mask 255.255.255.0
```

```
[Switch-dhcp-pool-200] gateway-list 10.1.2.2
```

```
[Switch-dhcp-pool-200] dns-list 10.1.2.2
```

```
[Switch-dhcp-pool-200] quit
```

## Configuring the RADIUS server

### Prerequisites

The RADIUS server runs INC PLAT 7.3 and INC UAM 7.3.

Make sure the RADIUS server has been installed with the EAP-PEAP certificate.

### Adding the AC as an access device to INC

1. Log in to INC and click the **User** tab.
2. From the navigation tree, select **User Access Policy > Access Device Management > Access Device**.
3. Click **Add**.  
The **Add Access Device** page opens.
4. In the **Access Configuration** area, configure the following parameters, as shown in [Figure 2](#):
  - Enter **12345** in the **Shared Key** and **Confirm Shared Key** fields. The shared key must be the same as the authentication and accounting shared keys configured on the AC.
  - Use the default values for other parameters.
5. In the **Device List** area, click **Select** or **Add Manually** to add the AC at 10.1.2.1 as an access device.  
The IP address must be the source IP address specified for outgoing RADIUS packets in the RADIUS scheme on the AC.
6. Click **OK**.

Figure 2 Adding an access device

### Adding an access policy

1. From the navigation tree, select **User Access Policy > Access Policy**.
2. Click **Add**.

3. On the **Add Access Policy** page, configure the following parameters, as shown in [Figure 3](#):
  - Enter **dot1x** in the **Access Policy Name** field.
  - Select **EAP-PEAP** from the **Preferred EAP Type** list, and select **EAP-MSCHAPv2** from the **Subtype** list.

The certificate subtype on the INC server must be the same as the identity authentication method configured on the client.
4. Click **OK**.

**Figure 3 Adding an access policy**

## Adding an access service

1. From the navigation tree, select **User Access Policy > Access Service**.
2. Click **Add**.
3. On the **Add Access Service** page, configure the following parameters, as shown in [Figure 4](#):
  - Enter **dot1x** in the **Service Name** field.
  - Select **dot1x** from the **Default Access Policy** list.
4. Click **OK**.

**Figure 4 Adding an access service**

## Adding an access user

1. From the navigation tree, select **Access User > Access User**.  
The access user list opens.
2. Click **Add**.  
The **Add Access User** page opens.

3. In the **Access Information** area, configure the following parameters, as shown in [Figure 5](#):
  - a. Click **Select** or **Add User** to associate the user with INC Platform user **user**.
  - b. Enter **dot1x** in the **Account Name** field.
  - c. Enter **dot1x123** in the **Password** and **Confirm Password** fields.
4. In the **Access Service** area, select **dot1x** from the list.
5. Click **OK**.

**Figure 5 Adding an access user account**

The screenshot shows the 'Add Access User' configuration page. The 'Access Information' section includes fields for User Name (set to 'user'), Account Name (set to 'dot1x'), Password (set to 'dot1x123'), and Confirm Password (set to 'dot1x123'). There are also checkboxes for 'Trial Account', 'Default BYOD User', 'MAC Authentication User', 'Computer User', and 'Fast Access User'. The 'Access Service' section shows a table with four services: 'dot1x', 'dot1x Service', 'MACauth Services', and 'service1', all with status 'Available'.

| Service Name     | Service Suffix | Status    | Allocate IP |
|------------------|----------------|-----------|-------------|
| dot1x            |                | Available |             |
| dot1x Service    | bbb            | Available |             |
| MACauth Services | 2000           | Available |             |
| service1         | test           | Available |             |

## Configuring the wireless client

### Restrictions and guidelines

Support for WPA3 depends on the wireless client model.

The configuration procedure is slightly different depending on the wireless client model. The following information only briefly describes the configuration procedure on a mobile phone.

### Procedure

1. Open the WLAN list page of the mobile phone, and click the wireless network named **wpa3**. On the page that opens, configure the following parameters:
  - Set the phase 2 authentication method to MSCHAPv2.
  - Configure to not validate the CA certificate.
  - Set the identity to **dot1x**.
  - Enter password **dot1x123**.
2. Click **Connect**.

## Verifying the configuration

1. On the client, verify that the client has passed authentication and associated with the AP, and it can access the wireless network. (Details not shown.)
2. On the AC, perform the following tasks to verify that the user has passed authentication and come online:

# Display detailed WLAN client information.

```
[AC] display wlan client verbose
Total number of clients: 1
```

|                                 |                                                                                          |
|---------------------------------|------------------------------------------------------------------------------------------|
| MAC address                     | : ccc9-5de2-512d                                                                         |
| IPv4 address                    | : 10.1.2.3                                                                               |
| IPv6 address                    | : N/A                                                                                    |
| Username                        | : dot1x                                                                                  |
| AID                             | : 1                                                                                      |
| AP ID                           | : 1                                                                                      |
| AP name                         | : office                                                                                 |
| Radio ID                        | : 1                                                                                      |
| Channel                         | : 52                                                                                     |
| SSID                            | : wpa3                                                                                   |
| BSSID                           | : f474-8879-ea60                                                                         |
| VLAN ID                         | : 200                                                                                    |
| Sleep count                     | : 0                                                                                      |
| Wireless mode                   | : 802.11ax                                                                               |
| Channel bandwidth               | : 80MHz                                                                                  |
| SM power save                   | : Disabled                                                                               |
| Short GI for 20MHz              | : Supported                                                                              |
| Short GI for 40MHz              | : Supported                                                                              |
| Short GI for 80MHz              | : Supported                                                                              |
| Short GI for 160/80+80MHz       | : Not supported                                                                          |
| STBC RX capability              | : Not supported                                                                          |
| STBC TX capability              | : Not supported                                                                          |
| LDPC RX capability              | : Supported                                                                              |
| Beamformee STS capability       | : N/A                                                                                    |
| Number of Sounding Dimensions   | : N/A                                                                                    |
| SU beamformee capability        | : Not supported                                                                          |
| MU beamformee capability        | : Not supported                                                                          |
| Block Ack                       | : N/A                                                                                    |
| Supported VHT-MCS set           | : NSS1 0, 1, 2, 3, 4, 5, 6, 7, 8, 9<br>NSS2 0, 1, 2, 3, 4, 5, 6, 7, 8, 9                 |
| Supported HT MCS set            | : 0, 1, 2, 3, 4, 5, 6, 7,<br>8, 9, 10, 11, 12, 13, 14,<br>15                             |
| Supported rates                 | : 6, 9, 12, 18, 24, 36,<br>48, 54 Mbps                                                   |
| 5G 40And80MHz Channel bandwidth | : Supported                                                                              |
| 5G 160MHz Channel bandwidth     | : Not Supported                                                                          |
| 5G 8080MHz Channel bandwidth    | : Not Supported                                                                          |
| OFDMA random access RUs         | : Not supported                                                                          |
| Supported HE-MCS set            | : NSS1 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11<br>NSS2 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11 |
| TWT scheduled                   | : no                                                                                     |
| QoS mode                        | : WMM                                                                                    |
| Listen interval                 | : 20                                                                                     |
| RSSI                            | : 0                                                                                      |
| Rx/Tx rate                      | : 0/0 Mbps                                                                               |
| Speed                           | : N/A                                                                                    |
| Authentication method           | : Open system                                                                            |

```

Security mode : RSN
AKM mode : 802.1X
Cipher suite : GCMP
User authentication mode : 802.1X
WPA3 status : Enabled
Authorization CAR : N/A
Authorization ACL ID : N/A
Authorization user profile : N/A
Roam status : N/A
Key derivation : SHA384
PMF status : Enabled
Forwarding policy name : Not configured
Online time : 0days 0hours 0minutes 8seconds
FT status : Inactive
BTM mode : Inactive

```

### # Display online 802.1X client information.

```

[AC] display dot1x connection
Total connections: 1
User MAC address : ccc9-5de2-512d
AP name : office
Radio ID : 1
SSID : wpa3
BSSID : f474-8879-ea60
Username : dot1x
Authentication domain : dom1
IPv4 address : 192.168.100.17
Authentication method : EAP
Initial VLAN : 200
Authorization VLAN : 200
Authorization ACL number : N/A
Authorization user profile : N/A
Authorization CAR : N/A
Authorization URL : N/A
Authorization IPv6 URL : N/A
Termination action : Default
Session timeout last from : 2021/03/18 14:42:20
Session timeout period : 86400 s
Online from : 2021/03/18 14:42:20
Online duration : 0h 2m 44s

```

## Configuration files

- AC:
 

```

#
dot1x authentication-method eap
#
vlan 100
#

```

```

vlan 200
#
wlan service-template wpa3_enterprise
 ssid wpa3
 vlan 200
 client forwarding-location ac
 akm mode dot1x
 cipher-suite gcmp
 security-ie rsn
 wpa3 enterprise
 client-security authentication-mode dot1x
 dot1x domain dom1
 pmf mandatory
 service-template enable
#
interface Vlan-interface100
 ip address 10.1.1.46 255.255.255.0
#
interface Vlan-interface200
 ip address 10.1.2.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 100 200
#
radius scheme radius1
 primary authentication 10.1.1.3
 primary accounting 10.1.1.3
 key authentication cipher c3$Bb61SHV2ZsVYPJU2+RFB/8ntk0uCQkmdA==
 key accounting cipher c3$w03NfxnBmfDuedv9/xo7ESnoxKjowmmX9A==
 nas-ip 10.1.2.1
#
domain dom1
 authentication lan-access radius-scheme radius1
 authorization lan-access radius-scheme radius1
 accounting lan-access radius-scheme radius1
#
wlan ap-group group1
 ap office
 ap-model AP 3620
 radio 1
 radio enable
 service-template wpa3_enterprise
 radio 2
#
wlan ap office model AP 3620
 serial-id 219801A28N819CE0002T
#

```



- **Switch:**

```
#
 dhcp enable
#
vlan 100
#
vlan 200
#
dhcp server ip-pool 100
 gateway-list 10.1.1.47
 network 10.1.1.0 mask 255.255.255.0
#
dhcp server ip-pool 200
 gateway-list 10.1.2.2
 network 10.1.2.0 mask 255.255.255.0
 dns-list 10.1.2.2
#
interface Vlan-interface100
 ip address 10.1.1.47 255.255.255.0
#
interface Vlan-interface200
 ip address 10.1.2.2 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 1 100 200
#
interface GigabitEthernet1/0/2
 port link-type access
 port access vlan 100
 poe enable
#
```

## Related documentation

- *User Access and Authentication Configuration Guide in INTELBRAS Access Controllers Configuration Guides*
- *User Access and Authentication Command Reference in INTELBRAS Access Controllers Command References*
- *WLAN Access Configuration Guide in INTELBRAS Access Controllers Configuration Guides*
- *WLAN Access Command Reference in INTELBRAS Access Controllers Command References*

# INTELBRAS Access Controllers

## 802.1X Authentication with ACL Assignment Through INC Server

### Configuration Examples

---

Copyright © 2024 Intelbras S.A All rights reserved.

No part of this manual may be reproduced or transmitted in any form or by any means without prior written consent of Intelbras S.A

Except for the trademarks of Intelbras S.A, any trademarks that may be mentioned in this document are the property of their respective owners.

The information in this document is subject to change without notice.

# Contents

|                                                                                               |    |
|-----------------------------------------------------------------------------------------------|----|
| Introduction .....                                                                            | 1  |
| Prerequisites .....                                                                           | 1  |
| Example: Configuring 802.1X authentication with ACL assignment through an<br>INC server ..... | 1  |
| Network configuration .....                                                                   | 1  |
| Restrictions and guidelines .....                                                             | 2  |
| Procedures .....                                                                              | 2  |
| Configuring the AC .....                                                                      | 2  |
| Configuring the switch .....                                                                  | 4  |
| Configuring the RADIUS server .....                                                           | 5  |
| Verifying the configuration .....                                                             | 8  |
| Configuration files .....                                                                     | 9  |
| Related documentation .....                                                                   | 11 |

# Introduction

The following information provides an example for configuring 802.1X authentication with ACL assignment through an INC server.

## Prerequisites

The following information applies to Comware-based access controllers and access points. Procedures and information in the examples might be slightly different depending on the software or hardware version of the access controllers and access points.

The configuration examples 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.

The following information is provided based on the assumption that you have basic knowledge of 802.1X, AAA, WLAN authentication, and WLAN access.

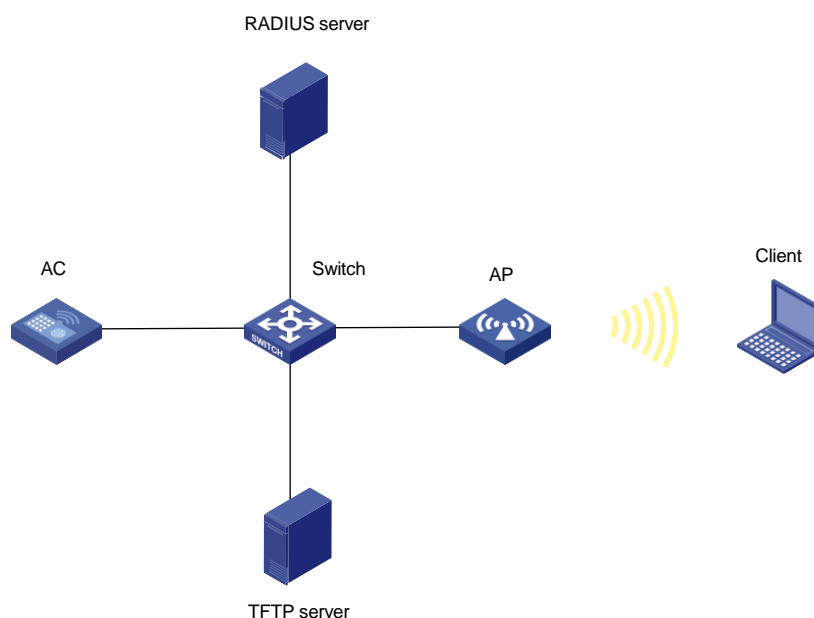
## Example: Configuring 802.1X authentication with ACL assignment through an INC server

### Network configuration

As shown in [Figure 1](#), the client must pass 802.1X authentication to access the wireless network. The RADIUS server runs on INC and provides AAA services for the client.

Configure RADIUS-based ACL assignment to deny the access of the client to the TFTP server.

**Figure 1 Network diagram**



**Table 1 Interface and IP address assignment**

| Device        | Interface          | IP address       |
|---------------|--------------------|------------------|
| AC            | VLAN-interface 100 | 138.100.1.101/16 |
|               | VLAN-interface 200 | 138.200.1.101/16 |
| RADIUS server |                    | 8.1.1.50/16      |
| TFTP server   |                    | 8.1.1.5/16       |
| Switch        | VLAN-interface 100 | 138.100.1.100/16 |
|               | VLAN-interface 200 | 138.200.1.100/16 |
|               | VLAN-interface 8   | 8.1.1.100/16     |

## Restrictions and guidelines

Use the actual serial ID of an AP to uniquely identify that AP.

## Procedures

### Configuring the AC

**1. Configure interfaces on the AC:**

# Create VLAN 100 and VLAN-interface 100, and assign an IP address to the VLAN interface. The AC will use this IP address to establish CAPWAP tunnels with the AP.

```
<AC> system-view
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 138.100.1.101 16
[AC-Vlan-interface100] quit
```

# Create VLAN 200 and VLAN-interface 200, and assign an IP address to the VLAN interface. VLAN 200 will be used for client access.

```
[AC] vlan 200
[AC-vlan200] quit
[AC] interface vlan-interface 200
[AC-Vlan-interface200] ip address 138.200.1.101 16
[AC-Vlan-interface200] quit
```

# Configure GigabitEthernet 1/0/1 (the port connected to the switch) as a trunk port, remove the port from VLAN 1, and assign the port to VLANs 100 and 200.

```
[AC] interface gigabitethernet 1/0/1
[AC-GigabitEthernet1/0/1] port link-type trunk
[AC-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[AC-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[AC-GigabitEthernet1/0/1] quit
```

**2. Configure 802.1X authentication:**

# Enable port security globally.

```
[AC] port-security enable
```

# Configure the AC to use EAP relay to authenticate 802.1X clients.

```
[AC] dot1x authentication-method eap
Create a RADIUS scheme named office and enter its view.
[AC] radius scheme office
Specify the IP addresses of the primary authentication and accounting RADIUS servers.
[AC-radius-office] primary authentication 8.1.1.50
[AC-radius-office] primary accounting 8.1.1.50
Set the shared key to 12345678 in plain text for secure communication with the servers.
[AC-radius-office] key authentication simple 12345678
[AC-radius-office] key accounting simple 12345678
Specify IP address 138.100.1.101 as the source IP address for outgoing RADIUS packets.
[AC-radius-office] nas-ip 138.100.1.101
[AC-radius-office] quit
Create an ISP domain named office and enter its view.
[AC] domain office
Apply RADIUS scheme office to ISP domain office for LAN user authentication and
authorization, and do not perform accounting for LAN users in the domain.
[AC-isp-office] authentication lan-access radius-scheme office
[AC-isp-office] authorization lan-access radius-scheme office
[AC-isp-office] accounting lan-access none
[AC-isp-office] quit
```

### 3. Configure a wireless service:

```
Create a service template named 1 and enter its view.
[AC] wlan service-template 1
Configure the SSID of the service template as service.
[AC-wlan-st-1] ssid service
Assign clients coming online through the service template to VLAN 200.
[AC-wlan-st-1] vlan 200
Set the AKM mode to 802.1X.
[AC-wlan-st-1] akm mode dot1x
Set the authentication mode to 802.1X.
[AC-wlan-st-1] client-security authentication-mode dot1x
Specify ISP domain office for authenticating 802.1X clients.
[AC-wlan-st-1] dot1x domain office
Set the cipher suite to CCMP.
[AC-wlan-st-1] cipher-suite ccmp
Enable the RSN IE in beacon and probe responses.
[AC-wlan-st-1] security-ie rsn
Enable the AC to forward client data traffic. If the AC forwards client data traffic by default,
skip this step.
[AC-wlan-st-1] client forwarding-location ac
Enable the service template.
[AC-wlan-st-1] service-template enable
[AC-wlan-st-1] quit
```

### 4. Configure AP settings:

#### ❗ IMPORTANT:

In a large-scale network, configure AP groups as a best practice.

# Create a manual AP named **ap1**, and specify the AP model and serial ID

```
[AC] wlan ap ap1 model AP 3620
[AC-wlan-ap-ap1] serial-id 219801A28N819CE0002T
[AC-wlan-ap-ap1] quit
```

# Create AP group **group1** and create an AP grouping rule by AP names to add AP **ap1** to AP group **group1**.

```
[AC] wlan ap-group group1
[AC-wlan-ap-group-group1] ap ap1
```

# Bind service template **1** to radio **1** in AP group **group1**.

```
[AC-wlan-ap-group-group1] ap-model AP 3620
[AC-wlan-ap-group-group1-ap-model-AP 3620] radio 1
[AC-wlan-ap-group-group1-ap-model-AP 3620-radio-1] service-template 1
```

# Enable radio **1**.

```
[AC-wlan-ap-group-group1-ap-model-AP 3620-radio-1] radio
enable [AC-wlan-ap-group-group1-ap-model-AP 3620-radio-1] quit
[AC-wlan-ap-group-group1-ap-model-AP 3620]
quit [AC-wlan-ap-group-group1] quit
```

5. Configure ACL 3001 to deny packets destined for IP address 8.1.1.5.

```
[AC] acl advanced 3001
[AC-acl-ipv4-adv-3001] rule 1 deny ip destination 8.1.1.5 0
[AC-acl-ipv4-adv-3001] quit
```

6. Configure a static route whose next hop address is 138.100.1.100.

```
[AC] ip route-static 0.0.0.0 0.0.0.0 138.100.1.100
```

## Configuring the switch

1. Configure interfaces on the switch:

# Create VLAN 100 and VLAN-interface 100, and assign an IP address to the VLAN interface. The switch will use this VLAN to communicate with the AC.

```
<Switch> system-view
[Switch] vlan 100
[Switch-vlan100] quit
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ip address 138.100.1.100 16
[Switch-Vlan-interface100] quit
```

# Create VLAN 200 and VLAN-interface 200, and assign an IP address to the VLAN interface. The switch will use this VLAN to communicate with the client.

```
[Switch] vlan 200
[Switch-vlan200] quit
[Switch] interface vlan-interface 200
[Switch-Vlan-interface200] ip address 138.200.1.100 16
[Switch-Vlan-interface200] quit
```

# Create VLAN 8 and VLAN-interface 8, and assign an IP address to the VLAN interface. The switch will use this VLAN to communicate with the RADIUS servers.

```
[Switch] vlan 8
[Switch-vlan8] quit
[Switch] interface vlan-interface 8
[Switch-Vlan-interface8] ip address 8.1.1.100 16
```

```
[Switch-Vlan-interface8] quit
```

# Configure GigabitEthernet 1/0/1 (the port connected to the AC) as a trunk port, and assign the trunk port to all VLANs.

```
[Switch] interface gigabitethernet 1/0/1
```

```
[Switch-GigabitEthernet1/0/1] port link-type trunk
```

```
[Switch-GigabitEthernet1/0/1] port trunk permit vlan all
```

```
[Switch-GigabitEthernet1/0/1] quit
```

## 2. Configure DHCP:

# Enable DHCP.

```
[Switch] dhcp enable
```

# Configure DHCP pool **vlan100** to assign an IP address to the AP. Specify subnet 138.100.0.0/16 and gateway address 138.100.1.100 in the pool.

```
[Switch] dhcp server ip-pool vlan100
```

```
[Switch-dhcp-pool-vlan100] network 138.100.0.0 mask 255.255.0.0
```

```
[Switch-dhcp-pool-vlan100] gateway-list 138.100.1.100
```

```
[Switch-dhcp-pool-vlan100] quit
```

# Configure DHCP pool **vlan200** to assign an IP address to the client. Specify subnet 138.200.0.0/16 and gateway address 138.200.1.100 in the pool. In this example, the address of the DNS server is 138.200.1.100 (the gateway address). You must replace it with the actual address of the DNS server on your network.

```
[Switch] dhcp server ip-pool vlan200
```

```
[Switch-dhcp-pool-vlan200] network 138.200.0.0 mask 255.255.0.0
```

```
[Switch-dhcp-pool-vlan200] gateway-list 138.200.1.100
```

```
[Switch-dhcp-pool-vlan200] dns-list 138.200.1.100
```

```
[Switch-dhcp-pool-vlan200] quit
```

# Configuring the RADIUS server

In this example, the RADIUS server runs INC PLAT 7.1(E0302) and INC INC - WSM 7.1(E0303).

## 1. Add an access device:

a. Log in to INC and click the **User** tab.

b. From the navigation tree, select **User Access Policy > Access Device Management > Access Device**.

c. Click **Add**.

The **Add Access Device** page opens.

d. In the **Access Configuration** area, configure the following parameters, as shown in [Figure 2](#):

- Enter **12345678** in the **Shared Key** and **Confirm Shared Key** fields.
- Use the default values for other parameters.

e. In the **Device List** area, click **Add Manually** to add the device at **138.100.1.101** as an access device.

f. Click **OK**.



**Figure 2 Adding an access device**

2. Add an access policy:
  - a. Click the **User** tab.
  - b. From the navigation tree, select **User Access Policy > Access Policy**.
  - c. Click **Add**.
  - d. On the **Add Access Policy** page, configure the following parameters, as shown in Figure 3:
    - Enter **wjh1x** in the **Access Policy Name** field.
    - Select **EAP** for the **Certificate Authentication** field.
    - Select **EAP-PEAP Auth** from the **Certificate Type** list, and select **MS-CHAPV2 Auth** from the **Certificate Sub-Type** list.
    - Select **Deploy ACL** and **Add Manually**, and enter an ACL number that is the same as the ACL configured on the AC.
    - Use the default values for other parameters.
  - e. Click **OK**.

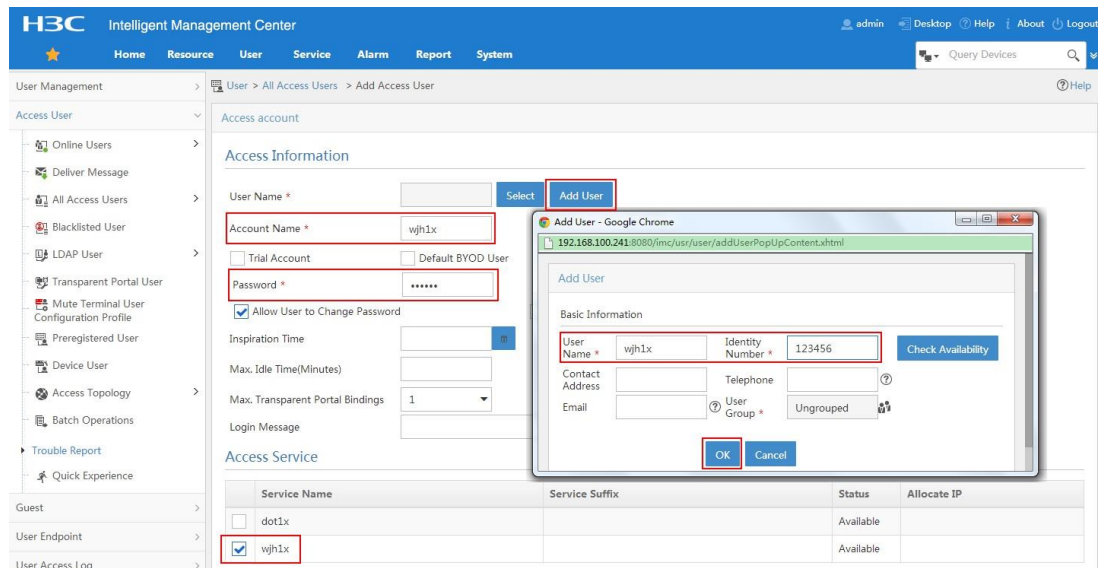
**Figure 3 Adding an access policy**

3. Add an access service:
  - a. Click the **User** tab.
  - b. From the navigation tree, select **User Access Policy > Access Service**.
  - c. Click **Add**.
  - d. On the **Add Access Service** page, configure the following parameters, as shown in [Figure 4](#):
    - Enter **wjh1x** in the **Service Name** field.
    - Select **wjh1x** from the **Default Access Policy** list.
    - Use the default values for other parameters.
  - e. Click **OK**.

**Figure 4 Adding an access service**

4. Add an access user:
  - a. Click the **User** tab.
  - b. From the navigation tree, select **Access User > All Access Users**.  
The access user list opens.
  - c. Click **Add**.  
The **Add Access User** page opens.
  - d. In the **Access Information** area, configure the following parameters, as shown in [Figure 5](#):
    - Click **Add User**. On the dialog box that opens, enter **wjh1x** and **123456** in the **User Name** and **Identity Number** fields, respectively. Click **Check Availability** to verify the validity of the username and identity number, and then click **OK**.
    - Enter **wjh1x** in the **Account Name** field.
    - Enter **12345678** in the **Password** and **Confirm Password** fields.
  - e. In the **Access Service** area, select **wjh1x** from the list.
  - f. Click **OK**.

**Figure 5 Adding an access user account**



## Verifying the configuration

# On the client, use the username and password configured on the RADIUS server for wireless access. (Details not shown.)

# Verify that the client has passed authentication and come online.

```
<AC> display wlan client verbose
```

```
Total number of clients: 1
MAC address : 0015-00ba-0428
IPv4 address : 138.200.0.1
IPv6 address : N/A
Username : wjl1x
AID : 1
AP ID : 1
AP name : ap1
Radio ID : 1
SSID : service
BSSID : 5866-ba71-3960
VLAN ID : 200
Sleep count : 0
Wireless mode : 802.11ac
Channel bandwidth : 40MHz
SM power save : Disabled
Short GI for 20MHz : Supported
Short GI for 40MHz : Supported
STBC RX capability : Supported
STBC TX capability : Not supported
LDPC RX capability : Not supported
Block Ack : N/A
Supported HT MCS set : 0, 1, 2, 3, 4, 5, 6, 7,
```

```

8, 9, 10, 11, 12, 13, 14,
15
Supported rates : 6, 9, 12, 18, 24, 36,
 48, 54 Mbps
QoS mode : WMM
Listen interval : 250
RSSI : 0
Rx/Tx rate : 0/0
Authentication method : Open system
Security mode : RSN
AKM mode : 802.1X
Cipher suite : CCMP
User authentication mode : 802.1X
Authorization ACL ID : 3001
Authorization user profile : N/A
Roam status : N/A
Key derivation : SHA1
PMF status : N/A
Forwarding policy name : N/A
Online time : 0days 0hours 0minutes 17seconds
FT status : Inactive

```

# Verify that the client can ping 8.1.1.50 successfully and cannot ping 8.1.1.5. (Details not shown.)

## Configuration files

- AC:
 

```

#
port-security enable
#
dot1x authentication-method eap
#
vlan 100
#
vlan 200
#
wlan service-template 1
 ssid service
 client forwarding-location ac
 vlan 200
 akm mode dot1x
 cipher-suite ccmp
 security-ie rsn
 client-security authentication-mode dot1x
 dot1x domain office
 service-template enable
#
interface Vlan-interface100
 ip address 138.100.1.101 255.255.0.0

```

```

#
interface Vlan-interface200
 ip address 138.200.1.101 255.255.0.0
#
interface GigabitEthernet1/0/1
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100 200
#
ip route-static 0.0.0.0 0.0.0.0 138.100.1.100
#
acl advanced 3001
 rule 1 deny ip destination 8.1.1.5 0
#
radius scheme office
 primary authentication 8.1.1.50
 primary accounting 8.1.1.50
 key authentication cipher c3$h7ouSYGGL5EgJZ6HpwIIgRdgiLKJCd6zZxE4
 key accounting cipher c3$qf3E+i6hAgx/rpYxDAPL0E0NSDWHZCZ3OI1g
 nas-ip 138.100.1.101
#
domain office
 authentication lan-access radius-scheme office
 authorization lan-access radius-scheme office
 accounting lan-access none
#
wlan ap-group group1
 ap ap1
 ap-model AP 3620
 radio 1
 radio enable
 service-template 1
#
wlan ap ap1 model AP 3620
 serial-id 219801A28N819CE0002T
#

```

- **Switch:**

```

#
vlan 8
#
vlan 100
#
vlan 200
#
dhcp server ip-pool vlan100
 network 138.100.0.0 mask 255.255.0.0
 gateway-list 138.100.1.100
#

```

```

dhcp server ip-pool vlan200
network 138.200.0.0 mask 255.255.0.0
gateway-list 138.200.1.100
dns-list 138.200.1.100
#
interface Vlan-interface8
ip address 8.1.1.100 255.255.0.0
#
interface Vlan-interface100
ip address 138.100.1.100 255.255.0.0
#
interface Vlan-interface200
ip address 138.200.1.100 255.255.0.0
#
interface GigabitEthernet1/0/1
port link-type trunk
port trunk permit vlan all
#
dhcp enable

```

## Related documentation

- *AP and WT Management Configuration Guide in INTELBRAS Access Controllers Configuration Guides*
- *AP and WT Management Command Reference in INTELBRAS Access Controllers Command References*
- *Network Connectivity Configuration Guide in INTELBRAS Access Controllers Configuration Guides*
- *Network Connectivity Command Reference in INTELBRAS Access Controllers Command References*
- *User Access and Authentication Configuration Guide in INTELBRAS Access Controllers Configuration Guides*
- *User Access and Authentication Command Reference in INTELBRAS Access Controllers Command References*
- *WLAN Access Configuration Guide in INTELBRAS Access Controllers Configuration Guides*
- *WLAN Access Command Reference in INTELBRAS Access Controllers Command References*

# INTELBRAS Access Controllers

## 802.1X Authentication with User Profile Assignment Through INC server

### Configuration Examples

---

Copyright © 2024 Intelbras S.A All rights reserved.

No part of this manual may be reproduced or transmitted in any form or by any means without prior written consent of Intelbras S.A

Except for the trademarks of Intelbras S.A, any trademarks that may be mentioned in this document are the property of their respective owners.

The information in this document is subject to change without notice.

# Contents

|                                                                                                        |    |
|--------------------------------------------------------------------------------------------------------|----|
| Introduction .....                                                                                     | 1  |
| Prerequisites .....                                                                                    | 1  |
| Example: Configuring 802.1X authentication with user profile assignment<br>through an INC server ..... | 1  |
| Network configuration .....                                                                            | 1  |
| Restrictions and guidelines .....                                                                      | 2  |
| Procedures .....                                                                                       | 2  |
| Configuring the AC .....                                                                               | 2  |
| Configuring the switch .....                                                                           | 4  |
| Configuring the RADIUS server .....                                                                    | 5  |
| Verifying the configuration .....                                                                      | 8  |
| Configuration files .....                                                                              | 10 |
| Related documentation .....                                                                            | 12 |



# Introduction

The following information provides an example for configuring 802.1X authentication with user profile assignment through an INC server.

## Prerequisites

The following information applies to Comware-based access controllers and access points. Procedures and information in the examples might be slightly different depending on the software or hardware version of the access controllers and access points.

The configuration examples 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.

The following information is provided based on the assumption that you have basic knowledge of 802.1X, AAA, WLAN authentication, and WLAN access.

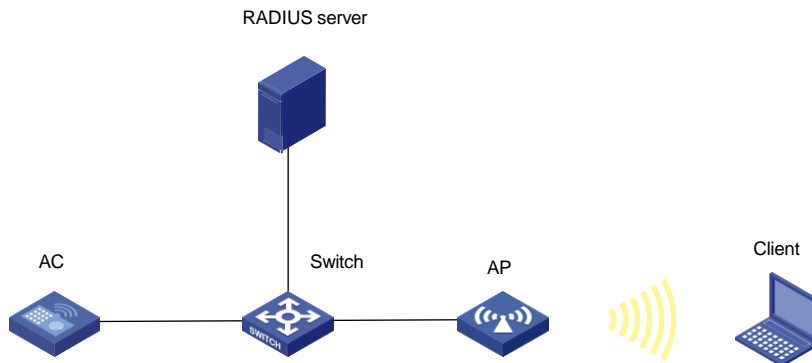
## Example: Configuring 802.1X authentication with user profile assignment through an INC server

### Network configuration

As shown in [Figure 1](#), the client must pass 802.1X authentication to access the wireless network. The RADIUS server runs on INC and provides AAA services for the client.

Configure RADIUS-based user profile assignment to limit both the outgoing and incoming traffic rates to 2 Mbps for the client.

**Figure 1 Network diagram**



**Table 1 Interface and IP address assignment**

| Device | Interface          | IP address       |
|--------|--------------------|------------------|
| AC     | VLAN-interface 100 | 138.100.1.101/16 |
|        | VLAN-interface 200 | 138.200.1.101/16 |

| Device        | Interface          | IP address       |
|---------------|--------------------|------------------|
| RADIUS server |                    | 8.1.1.50/16      |
| Switch        | VLAN-interface 100 | 138.100.1.100/16 |
|               | VLAN-interface 200 | 138.200.1.100/16 |
|               | VLAN-interface 8   | 8.1.1.100/16     |

## Restrictions and guidelines

Use the actual serial ID of an AP to uniquely identify that AP.

## Procedures

### Configuring the AC

#### 1. Configure interfaces on the AC:

# Create VLAN 100 and VLAN-interface 100, and assign an IP address to the VLAN interface. The AC will use this IP address to establish CAPWAP tunnels with the AP.

```
<AC> system-view
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 138.100.1.101 16
[AC-Vlan-interface100] quit
```

# Create VLAN 200 and VLAN-interface 200, and assign an IP address to the VLAN interface. VLAN 200 will be used for client access.

```
[AC] vlan 200
[AC-vlan200] quit
[AC] interface vlan-interface 200
[AC-Vlan-interface200] ip address 138.200.1.101 16
[AC-Vlan-interface200] quit
```

# Configure GigabitEthernet 1/0/1 (the port connected to the switch) as a trunk port, remove the port from VLAN 1, and assign the port to VLANs 100 and 200.

```
[AC] interface gigabitethernet 1/0/1
[AC-GigabitEthernet1/0/1] port link-type trunk
[AC-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[AC-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[AC-GigabitEthernet1/0/1] quit
```

#### 2. Configure 802.1X authentication:

# Enable port security globally.

```
[AC] port-security enable
```

# Configure the AC to use EAP relay to authenticate 802.1X clients.

```
[AC] dot1x authentication-method eap
```

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

```
[AC] radius scheme office
```

# Specify the IP addresses of the primary authentication and accounting RADIUS servers.

```
[AC-radius-office] primary authentication 8.1.1.50
```

```
[AC-radius-office] primary accounting 8.1.1.50
Set the shared key to 12345678 in plain text for secure communication with the servers.
[AC-radius-office] key authentication simple 12345678
[AC-radius-office] key accounting simple 12345678
Specify IP address 138.100.1.101 as the source IP address for outgoing RADIUS packets.
[AC-radius-office] nas-ip 138.100.1.101
[AC-radius-office] quit
Create an ISP domain named office and enter its view.
[AC] domain office
Apply RADIUS scheme office to ISP domain office for LAN user authentication and
authorization, and do not perform accounting for LAN users in the domain.
[AC-isp-office] authentication lan-access radius-scheme office
[AC-isp-office] authorization lan-access radius-scheme office
[AC-isp-office] accounting lan-access none
[AC-isp-office] quit
```

### 3. Configure a wireless service:

```
Create a service template named 1 and enter its view.
[AC] wlan service-template 1
Configure the SSID of the service template as service.
[AC-wlan-st-1] ssid service
Assign clients coming online through the service template to VLAN 200.
[AC-wlan-st-1] vlan 200
Set the AKM mode to 802.1X.
[AC-wlan-st-1] akm mode dot1x
Set the authentication mode to 802.1X.
[AC-wlan-st-1] client-security authentication-mode dot1x
Specify ISP domain office for authenticating 802.1X clients.
[AC-wlan-st-1] dot1x domain office
Set the cipher suite to CCMP.
[AC-wlan-st-1] cipher-suite ccmp
Enable the RSN IE in beacon and probe responses.
[AC-wlan-st-1] security-ie rsn
Enable the AC to forward client data traffic. If the AC forwards client data traffic by default,
skip this step.
[AC-wlan-st-1] client forwarding-location ac
Enable the service template.
[AC-wlan-st-1] service-template enable
[AC-wlan-st-1] quit
```

### 4. Configure AP settings:

#### ⚠ IMPORTANT:

In a large-scale network, configure AP groups as a best practice.

```
Create a manual AP named ap1, and specify the AP model and serial ID
[AC] wlan ap ap1 model AP 3620
[AC-wlan-ap-ap1] serial-id 219801A28N819CE0002T
[AC-wlan-ap-ap1] quit
```

# Create AP group **group1** and create an AP grouping rule by AP names to add AP **ap1** to AP group **group1**.

```
[AC] wlan ap-group group1
[AC-wlan-ap-group-group1] ap ap1
```

# Bind service template 1 to radio 1 in AP group **group1**.

```
[AC-wlan-ap-group-group1] ap-model AP 3620
[AC-wlan-ap-group-group1-ap-model-AP 3620] radio 1
[AC-wlan-ap-group-group1-ap-model-AP 3620-radio-1] service-template 1
```

# Enable radio 1.

```
[AC-wlan-ap-group-group1-ap-model-AP 3620-radio-1] radio
enable [AC-wlan-ap-group-group1-ap-model-AP 3620-radio-1] quit
[AC-wlan-ap-group-group1-ap-model-AP 3620]
quit [AC-wlan-ap-group-group1] quit
```

5. Configure a user profile named **aaa**, and configure a CAR policy to limit both the incoming and outgoing traffic rates to 2Mbps.

```
[AC] user-profile aaa
[AC-user-profile-aaa] qos car inbound any cir 2048
[AC-user-profile-aaa] qos car outbound any cir 2048
```

6. Configure a static route whose next hop address is 138.100.1.100.

```
[AC] ip route-static 0.0.0.0 0.0.0.0 138.100.1.100
```

## Configuring the switch

1. Configure interfaces on the switch:

# Create VLAN 100 and VLAN-interface 100, and assign an IP address to the VLAN interface. The switch will use this VLAN to communicate with the AC.

```
<Switch> system-view
[Switch] vlan 100
[Switch-vlan100] quit
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ip address 138.100.1.100 16
[Switch-Vlan-interface100] quit
```

# Create VLAN 200 and VLAN-interface 200, and assign an IP address to the VLAN interface. The switch will use this VLAN to communicate with the client.

```
[Switch] vlan 200
[Switch-vlan200] quit
[Switch] interface vlan-interface 200
[Switch-Vlan-interface200] ip address 138.200.1.100 16
[Switch-Vlan-interface200] quit
```

# Create VLAN 8 and VLAN-interface 8, and assign an IP address to the VLAN interface. The switch will use this VLAN to communicate with the RADIUS servers.

```
[Switch] vlan 8
[Switch-vlan8] quit
[Switch] interface vlan-interface 8
[Switch-Vlan-interface8] ip address 8.1.1.100 16
[Switch-Vlan-interface8] quit
```

# Configure GigabitEthernet 1/0/1 (the port connected to the AC) as a trunk port, and assign the trunk port to all VLANs.

```
[Switch] interface gigabitethernet 1/0/1
```

```
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] port trunk permit vlan all
[Switch-GigabitEthernet1/0/1] quit
```

**# Configure GigabitEthernet 1/0/2 (the port connected to the AP) as a trunk port, assign the port to VLAN 100, and remove the port from VLAN 1. Set the PVID of the port to VLAN 100.**

```
[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] port link-type trunk
[Switch-GigabitEthernet1/0/2] undo port trunk permit vlan 1
[Switch-GigabitEthernet1/0/2] port trunk permit vlan 100
[Switch-GigabitEthernet1/0/2] port trunk pvid vlan 100
```

**# Enable PoE on GigabitEthernet 1/0/2.**

```
[Switch-GigabitEthernet1/0/2] poe enable
[Switch-GigabitEthernet1/0/2] quit
```

**# Configure GigabitEthernet 1/0/3 (the port connected to the RADIUS server) as an access port, and assign the port to VLAN 8.**

```
[Switch] interface gigabitethernet 1/0/3
[Switch-GigabitEthernet1/0/3] port link-type access
[Switch-GigabitEthernet1/0/3] port access vlan 8
```

## 2. Configure the DHCP server:

**# Enable DHCP.**

```
[Switch] dhcp enable
```

**# Configure DHCP pool **vlan100** to assign an IP address to the AP. Specify subnet 138.100.0.0/16 and gateway address 138.100.1.100 in the pool.**

```
[Switch] dhcp server ip-pool vlan100
[Switch-dhcp-pool-vlan100] network 138.100.0.0 mask 255.255.0.0
[Switch-dhcp-pool-vlan100] gateway-list 138.100.1.100
[Switch-dhcp-pool-vlan100] quit
```

**# Configure DHCP pool **vlan200** to assign an IP address to the client. Specify subnet 138.200.0.0/16 and gateway address 138.200.1.100 in the pool. In this example, the address of the DNS server is 138.200.1.100 (the gateway address). You must replace it with the actual address of the DNS server on your network.**

```
[Switch] dhcp server ip-pool vlan200
[Switch-dhcp-pool-vlan200] network 138.200.0.0 mask 255.255.0.0
[Switch-dhcp-pool-vlan200] gateway-list 138.200.1.100
[Switch-dhcp-pool-vlan200] dns-list 138.200.1.100
[Switch-dhcp-pool-vlan200] quit
```

## Configuring the RADIUS server

In this example, the RADIUS server runs INC PLAT 7.1(E0302) and INC INC - WSM 7.1(E0303).

### 1. Add an access device:

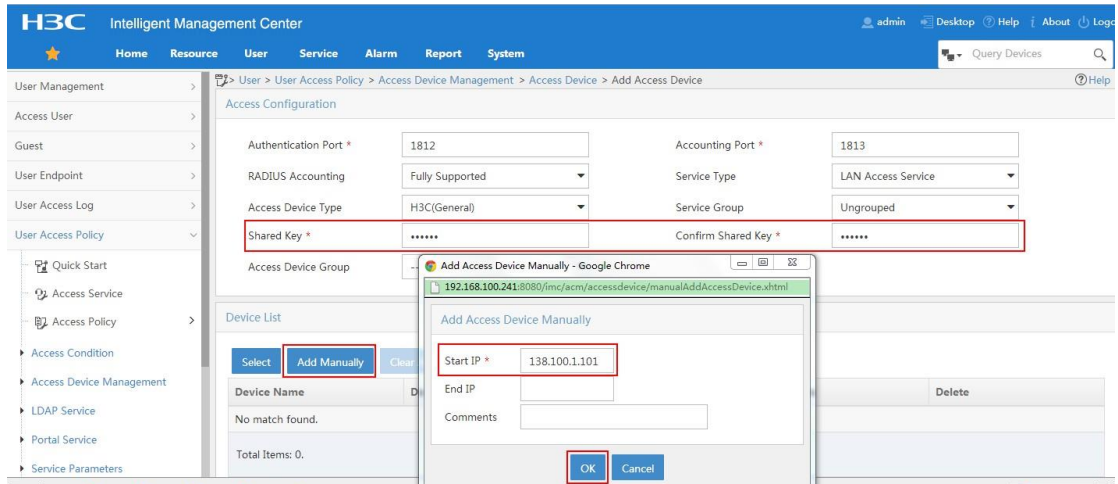
- a. Log in to INC and click the **User** tab.
- b. From the navigation tree, select **User Access Policy > Access Device Management > Access Device**.
- c. Click **Add**.

The **Add Access Device** page opens.

- d. In the **Access Configuration** area, configure the following parameters, as shown in [Figure 2](#):

- Enter **12345678** in the **Shared Key** and **Confirm Shared Key** fields.
  - Use the default values for other parameters.
- e. In the **Device List** area, click **Add Manually** to add the device at **138.100.1.101** as an access device.
- f. Click **OK**.

**Figure 2 Adding an access device**



2. Add an access policy:
  - a. Click the **User** tab.
  - b. From the navigation tree, select **User Access Policy > Access Policy**.
  - c. Click **Add**.
  - d. On the **Add Access Policy** page, configure the following parameters, as shown in [Figure 3](#):
    - Enter **wjh1x** in the **Access Policy Name** field.
    - Select **EAP** for the **Certificate Authentication** field.
    - Select **EAP-PEAP Auth** from the **Certificate Type** list, and select **MS-CHAPV2 Auth** from the **Certificate Sub-Type** list.
    - Select **Deploy User Profile**, and enter a user profile name that is the same as the user profile configured on the AC.
    - Use the default values for other parameters.
  - e. Click **OK**.

**Figure 3 Adding an access policy**

H3C Intelligent Management Center

admin Desktop Help About Logout

Home Resource User Service Alarm Report System

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

Access User > Basic Information

Guest >

User Endpoint >

User Access Log >

User Access Policy >

Quick Start

Access Service

Access Policy >

Access Condition

Access Device Management

LDAP Service

Portal Service

Service Parameters

Third-Party Authentication

Access Policy Name \* wjh1x

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-PEAP Auth Certificate Sub-Type MS-CHAPV2

Deploy VLAN

☒ Deploy User Profile aaa Deploy User Group

☐ Deploy ACL

**3. Add an access service:**

a. Click the **User** tab.

b. From the navigation tree, select **User Access Policy > Access Service**.

c. Click **Add**.

d. On the **Add Access Service** page, configure the following parameters, as shown in Figure 4:

- Enter **wjh1x** in the **Service Name** field.
- Select **wjh1x** from the **Default Access Policy** list.
- Use the default values for other parameters.

e. Click **OK**.

**Figure 4 Adding an access service**

H3C Intelligent Management Center

admin Desktop Help About Logout

Home Resource User Service Alarm Report System

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

Access User > Basic Information

Guest >

User Endpoint >

User Access Log >

User Access Policy >

Quick Start

Access Service

Access Policy >

Access Condition

Access Device Management

LDAP Service

Portal Service

Service Parameters

Third-Party Authentication

Service Name \* wjh1x Service Suffix

Service Group \* Ungrouped Default Access Policy \* wjh1x

Default Proprietary Attribute Assignment Policy \* Do not use

Default Max. Number of Bound Endpoints \* 0 Default Max. Number of Online Endpoints \* 0

Description

☒ Available ☐ Transparent Authentication on Portal Endpoints

Access Scenario List

Add

| Access Scenario | Access Policy | Proprietary Attribute Assignment Policy | Priority | Modify | Delete |
|-----------------|---------------|-----------------------------------------|----------|--------|--------|
| No match found. |               |                                         |          |        |        |

OK Cancel

**4. Add an access user:**

a. Click the **User** tab.

b. From the navigation tree, select **Access User > All Access Users**.

The access user list opens.

c. Click **Add**.

The **Add Access User** page opens.

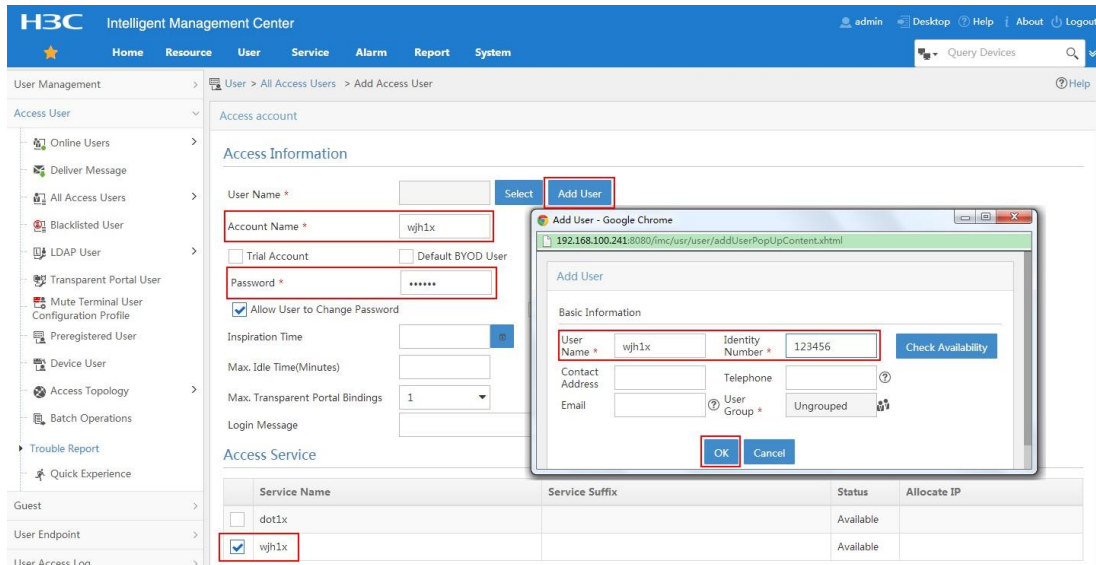
d. In the **Access Information** area, configure the following parameters, as shown in [Figure 5](#):

- Click **Add User**. On the dialog box that opens, enter **wjh1x** and **123456** in the **User Name** and **Identity Number** fields, respectively. Click **Check Availability** to verify the validity of the username and identity number, and then click **OK**.
- Enter **wjh1x** in the **Account Name** field.
- Enter **12345678** in the **Password** and **Confirm Password** fields.

e. In the **Access Service** area, select **wjh1x** from the list.

f. Click **OK**.

**Figure 5** Adding an access user account



## Verifying the configuration

# On the client, use the username and password configured on the RADIUS server for wireless access. (Details not shown.)

# Verify that the client has passed authentication and come online.

```
<AC> display wlan client verbose
```

```
Total number of clients: 1
```

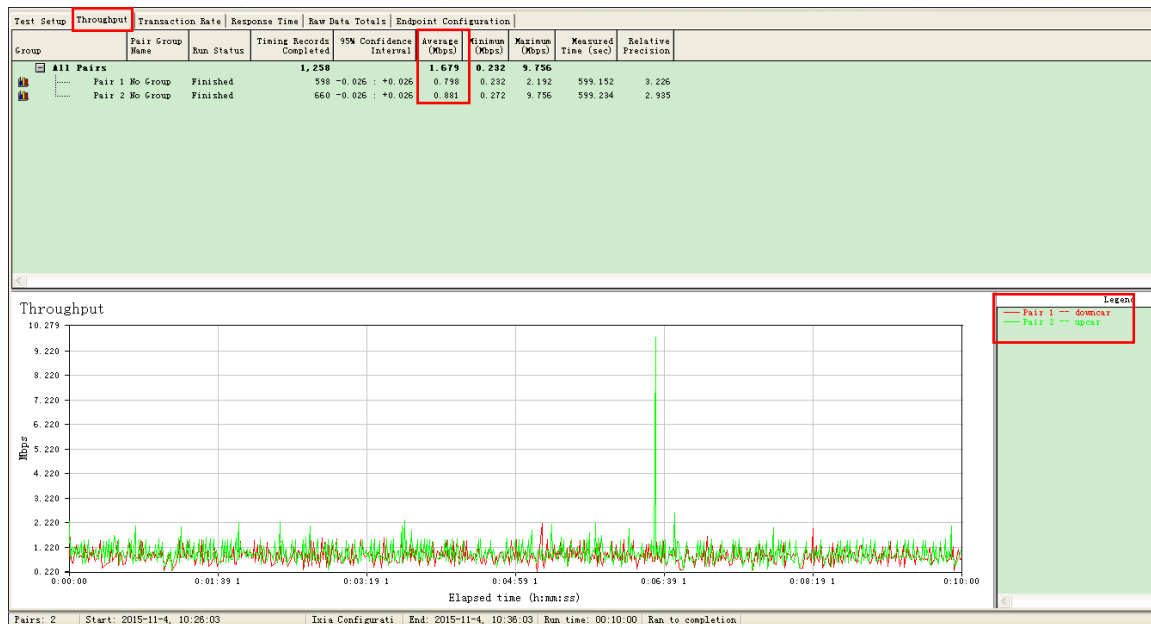
```
MAC address : 0015-00ba-0428
IPv4 address : 138.200.0.1
IPv6 address : N/A
Username : wjh1x
AID : 1
AP ID : 1
AP name : ap1
Radio ID : 1
SSID : service
BSSID : 5866-ba71-3960
VLAN ID : 200
Sleep count : 0
Wireless mode : 802.11ac
```



|                            |                                                              |
|----------------------------|--------------------------------------------------------------|
| Channel bandwidth          | : 40MHz                                                      |
| SM power save              | : Disabled                                                   |
| Short GI for 20MHz         | : Supported                                                  |
| Short GI for 40MHz         | : Supported                                                  |
| STBC RX capability         | : Supported                                                  |
| STBC TX capability         | : Not supported                                              |
| LDPC RX capability         | : Not supported                                              |
| Block Ack                  | : N/A                                                        |
| Supported HT MCS set       | : 0, 1, 2, 3, 4, 5, 6, 7,<br>8, 9, 10, 11, 12, 13, 14,<br>15 |
| Supported rates            | : 6, 9, 12, 18, 24, 36,<br>48, 54 Mbps                       |
| QoS mode                   | : WMM                                                        |
| Listen interval            | : 250                                                        |
| RSSI                       | : 0                                                          |
| Rx/Tx rate                 | : 0/0                                                        |
| Authentication method      | : Open system                                                |
| Security mode              | : RSN                                                        |
| AKM mode                   | : 802.1X                                                     |
| Cipher suite               | : CCMP                                                       |
| User authentication mode   | : 802.1X                                                     |
| Authorization ACL ID       | : N/A                                                        |
| Authorization user profile | : aaa                                                        |
| Roam status                | : N/A                                                        |
| Key derivation             | : SHA1                                                       |
| PMF status                 | : N/A                                                        |
| Forwarding policy name     | : N/A                                                        |
| Online time                | : 0days 0hours 0minutes 17seconds                            |
| FT status                  | : Inactive                                                   |

**# Use the IxChariot tool to test the incoming and outgoing traffic rates and verify that the rates are within the limit.**

Figure 6 Test result



## Configuration files

- AC:
 

```
#
port-security enable
#
dot1x authentication-method eap
#
vlan 100
#
vlan 200
#
wlan service-template 1
 ssid service
 client forwarding-location ac
 vlan 200
 akm mode dot1x
 cipher-suite ccmp
 security-ie rsn
 client-security authentication-mode dot1x
 dot1x domain office
 service-template enable
#
interface Vlan-interface100
 ip address 138.100.1.101 255.255.0.0
#
interface Vlan-interface200
 ip address 138.200.1.101 255.255.0.0
```

```

#
interface GigabitEthernet1/0/1
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100 200
#
ip route-static 0.0.0.0 0.0.0.0 138.100.1.100
#
user-profile aaa
 qos car inbound any cir 2048 cbs 128000 ebs 0
 qos car outbound any cir 2048 cbs 128000 ebs 0
#
radius scheme office
 primary authentication 8.1.1.50
 primary accounting 8.1.1.50
 key authentication cipher c3$h7ouSYGGL5EgJZ6HpwIIgRdgiLKJCd6zZxE4
 key accounting cipher c3$qf3E+i6hAgx/rpYxDAPL0E0NSDWHZCZ3OIlg
 nas-ip 138.100.1.101
#
domain office
 authentication lan-access radius-scheme office
 authorization lan-access radius-scheme office
 accounting lan-access none
#
wlan ap-group group1
 ap ap1
 ap-model AP 3620
 radio 1
 radio enable
 service-template 1
#
wlan ap ap1 model AP 3620
 serial-id 219801A28N819CE0002T
#

```

- **Switch:**

```

#
vlan 8
#
vlan 100
#
vlan 200
#
dhcp server ip-pool vlan100
 network 138.100.0.0 mask 255.255.0.0
 gateway-list 138.100.1.100
#
dhcp server ip-pool vlan200
 network 138.200.0.0 mask 255.255.0.0

```

```

gateway-list 138.200.1.100
dns-list 138.200.1.100
#
interface Vlan-interface8
ip address 8.1.1.100 255.255.0.0
#
interface Vlan-interface100
ip address 138.100.1.100 255.255.0.0
#
interface Vlan-interface200
ip address 138.200.1.100 255.255.0.0
#
interface GigabitEthernet1/0/1
port link-type trunk
port trunk permit vlan all
#
interface GigabitEthernet1/0/2
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 100
port trunk pvid vlan 100
poe enable
#
interface GigabitEthernet1/0/3
port link-type access
port access vlan 8
#
dhcp enable

```

## Related documentation

- *AP and WT Management Configuration Guide in INTELBRAS Access Controllers Configuration Guides*
- *AP and WT Management Command Reference in INTELBRAS Access Controllers Command References*
- *Network Connectivity Configuration Guide in INTELBRAS Access Controllers Configuration Guides*
- *Network Connectivity Command Reference in INTELBRAS Access Controllers Command References*
- *User Access and Authentication Configuration Guide in INTELBRAS Access Controllers Configuration Guides*
- *User Access and Authentication Command Reference in INTELBRAS Access Controllers Command References*
- *WLAN Access Configuration Guide in INTELBRAS Access Controllers Configuration Guides*
- *WLAN Access Command Reference in INTELBRAS Access Controllers Command References*

# INTELBRAS Access Controllers EAD Authentication Configuration Examples

---

Copyright © 2024 Intelbras S.A All rights reserved.

No part of this manual may be reproduced or transmitted in any form or by any means without prior written consent of Intelbras S.A

Except for the trademarks of Intelbras S.A, any trademarks that may be mentioned in this document are the property of their respective owners.

The information in this document is subject to change without notice.

# Contents

|                                               |    |
|-----------------------------------------------|----|
| Introduction .....                            | 1  |
| Prerequisites .....                           | 1  |
| Example: Configuring EAD authentication ..... | 1  |
| Network configuration .....                   | 1  |
| Restrictions and guidelines .....             | 1  |
| Procedures .....                              | 1  |
| Configuring the AC .....                      | 1  |
| Configuring the switch .....                  | 4  |
| Configuring the RADIUS server .....           | 5  |
| Configuring the iNode client .....            | 10 |
| Verifying the configuration .....             | 13 |
| Configuration files .....                     | 15 |
| Related documentation .....                   | 17 |

# Introduction

The following information provides an example for configuring EAD authentication for wireless clients.

## Prerequisites

The following information applies to Comware-based access controllers and access points. Procedures and information in the examples might be slightly different depending on the software or hardware version of the access controllers and access points.

The configuration examples 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.

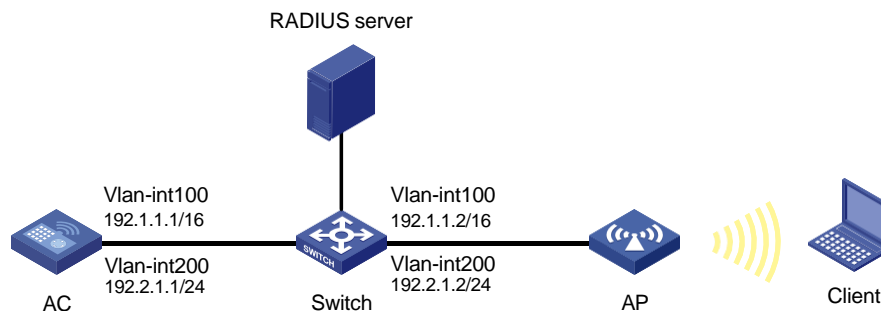
The following information is provided based on the assumption that you have basic knowledge of WLAN access and EAD authentication.

## Example: Configuring EAD authentication

### Network configuration

As shown in [Figure 1](#), the switch acts as the DHCP server to assign IP addresses to the AP and the client. Configure EAD authentication on the AC to authenticate the client.

**Figure 1 Network diagram**



## Restrictions and guidelines

Use the actual serial ID of an AP to uniquely identify that AP.

## Procedures

### Configuring the AC

1. Configure interfaces on the AC:  
# Create VLAN 100 and VLAN-interface 100, and assign an IP address to the VLAN interface.  
The AC will use this IP address to establish CAPWAP tunnels with the AP.



```
<AC> system-view
```

```
[AC] vlan 100
```

```
[AC-vlan100] quit
```

```
[AC] interface vlan-interface 100
```

```
[AC-Vlan-interface100] ip address 192.1.1.1 16
```

```
[AC-Vlan-interface100] quit
```

**# Create VLAN 200 and VLAN-interface 200, and assign an IP address to the VLAN interface. The client will use VLAN 200 to access the WLAN.**

```
[AC] vlan 200
```

```
[AC-vlan200] quit
```

```
[AC] interface vlan-interface 200
```

```
[AC-Vlan-interface200] ip address 192.2.1.1 24
```

```
[AC-Vlan-interface200] quit
```

**# Configure GigabitEthernet 1/0/1 (the port connected to the switch) as a trunk port, assign the port to VLAN 100 and VLAN 200, and remove the port from VLAN1.**

```
[AC] interface gigabitethernet 1/0/1
```

```
[AC-GigabitEthernet1/0/1] port link-type trunk
```

```
[AC-GigabitEthernet1/0/1] undo port trunk permit vlan 1
```

```
[AC-GigabitEthernet1/0/1] port trunk permit vlan 100 200
```

```
[AC-GigabitEthernet1/0/1] quit
```

**2. Enable port security and specify the EAP relay mode for 802.1X authentication.**

```
[AC] port-security enable
```

```
[AC] dot1x authentication-method eap
```

**3. Configure a RADIUS scheme:**

**# Create a RADIUS scheme named **radius1** and enter its view.**

```
[AC] radius scheme radius1
```

**# Specify the IP addresses of the primary authentication and accounting RADIUS servers.**

```
[AC-radius-radius1] primary authentication 8.1.1.16
```

```
[AC-radius-radius1] primary accounting 8.1.1.16
```

**# Set the shared key to **example** in plaintext form for secure communication with the servers.**

```
[AC-radius-radius1] key authentication simple example
```

```
[AC-radius-radius1] key accounting simple example
```

**# Set the real-time accounting interval to 3 minutes.**

```
[AC-radius-radius1] timer realtime-accounting 3
```

**# Specify IP address 192.1.1.1 as the source IP address for outgoing RADIUS packets.**

```
[AC-radius-radius1] nas-ip 192.1.1.1
```

**4. Configure an authentication domain:**

**# Create an ISP domain named **radius1** and enter its view.**

```
[AC] domain radius1
```

**# Apply RADIUS scheme **radius1** to ISP domain **radius1** for LAN user authentication, authorization, and accounting.**

```
[AC-isp-radius1] authentication lan-access radius-scheme radius1
```

```
[AC-isp-radius1] authorization lan-access radius-scheme radius1
```

```
[AC-isp-radius1] accounting lan-access radius-scheme radius1
```

**5. Configure ACLs:**

**# Create IPv4 advanced ACL 3000 and enter its view.**

```
[AC] acl advanced 3000
```

# Create an ACL rule to permit all IP packets.

```
[AC-acl-ipv4-adv-3000] rule permit ip
[AC-acl-ipv4-adv-3000] quit
```

# Create IPv4 advanced ACL 3001 and enter its view.

```
[AC] acl advanced 3001
```

# Create an ACL rule to permit all UDP packets.

```
[AC-acl-ipv4-adv-3001] rule permit udp
```

# Create an ACL rule to deny all TCP packets.

```
[AC-acl-ipv4-adv-3001] rule deny tcp
[AC-acl-ipv4-adv-3001] quit
```

## 6. Configure a wireless service:

# Create a service template named **1** and enter its view.

```
[AC] wlan service-template 1
```

# Configure the SSID of the service template as **service**.

```
[AC-wlan-st-service] ssid service
```

# Assign clients coming online through the service template to VLAN 200.

```
[AC-wlan-st-1] vlan 200
```

# Set the AKM mode to 802.1X.

```
[AC-wlan-st-1] akm mode dot1x
```

# Set the CCMP cipher suite for frame encryption and enable the RSN-IE in the beacon and probe responses.

```
[AC-wlan-st-1] cipher-suite ccmp
[AC-wlan-st-1] security-ie rsn
```

# Set the authentication mode to 802.1X.

```
[AC-wlan-st-1] client-security authentication-mode dot1x
```

# Specify ISP domain **radius1** for authenticating 802.1X clients.

```
[AC-wlan-st-1] dot1x domain radius1
```

# Enable the AC to forward client data traffic. If the AC forwards client data traffic by default, skip this step.

```
[AC-wlan-st-1] client forwarding-location ac
```

# Enable the service template.

```
[AC-wlan-st-1] service-template enable
[AC-wlan-st-1] quit
```

## 7. Configure AP settings:

### ⚠ IMPORTANT:

In a large-scale network, configure AP groups as a best practice.

# Create an AP named **officeap** with model AP 3620.

```
[AC] wlan ap officeap model AP 3620
```

# Set the serial ID of the AP to 219801A28N819CE0002T.

```
[AC-wlan-ap-officeap] serial-id 219801A28N819CE0002T
[AC-wlan-ap-officeap] quit
```

# Create AP group **group1** and create an AP grouping rule by AP names to add AP **officeap** to AP group **group1**.

```
[AC] wlan ap-group group1
[AC-wlan-ap-group-group1] ap officeap
```

# Bind service template **1** to radio 2 in AP group **group1**.

```
[AC-wlan-ap-group-group1] ap-model AP 3620
[AC-wlan-ap-group-group1-ap-model-AP 3620] radio 2
[AC-wlan-ap-group-group1-ap-model-AP 3620-radio-2] service-template 1
Enable radio 2.
[AC-wlan-ap-group-group1-ap-model-AP 3620-radio-2] radio
enable [AC-wlan-ap-group-group1-ap-model-AP 3620-radio-2] quit
[AC-wlan-ap-group-group1-ap-model-AP 3620]
quit [AC-wlan-ap-group-group1] quit
```

8. Configure a static route destined for the RADIUS server:

```
[AC] ip route-static 8.0.0.0 8 192.2.1.2
```

## Configuring the switch

### 1. Configure interfaces on the switch:

# Create VLAN 100 and VLAN-interface 100, and assign an IP address to the VLAN interface. The switch will use this VLAN to forward CAPWAP packets between the AC and the AP.

```
<Switch> system-view
[Switch] vlan 100
[Switch-vlan100] quit
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ip address 192.1.1.2 16
[Switch-Vlan-interface100] quit
```

# Create VLAN 200 and VLAN-interface 200, and assign an IP address to the VLAN interface. The switch will use this VLAN to forward client traffic.

```
[Switch] vlan 200
[Switch-vlan200] quit
[Switch] interface vlan-interface 200
[Switch-Vlan-interface200] ip address 192.2.1.2 24
[Switch-Vlan-interface200] quit
```

# Create VLAN 8 and VLAN-interface 8, and assign an IP address to the VLAN interface. The switch will use this VLAN to communicate with the RADIUS server.

```
[Switch] vlan 8
[Switch-vlan8] quit
[Switch] interface vlan-interface 8
[Switch-Vlan-interface8] ip address 8.1.1.2 8
[Switch-Vlan-interface8] quit
```

# Configure GigabitEthernet 1/0/1 (the port connected to the AC) as a trunk port, assign the port to VLAN 100 and VLAN 200, and remove the port from VLAN 1.

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[Switch-GigabitEthernet1/0/1] quit
```

# Configure GigabitEthernet 1/0/2 (the port connected to the AP) as a trunk port, assign the port to VLAN 100, and remove the port from VLAN 1. Set the PVID of the port to VLAN 100.

```
[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] port link-type trunk
[Switch-GigabitEthernet1/0/2] undo port trunk permit vlan 1
[Switch-GigabitEthernet1/0/2] port trunk permit vlan 100
```

```
[Switch-GigabitEthernet1/0/2] port trunk pvid vlan 100
```

# Enable PoE on GigabitEthernet 1/0/2.

```
[Switch-GigabitEthernet1/0/2] poe enable
```

```
[Switch-GigabitEthernet1/0/2] quit
```

# Configure GigabitEthernet 1/0/3 (the port connected to the RADIUS server) as an access port, and assign the port to VLAN 8.

```
[Switch] interface gigabitethernet 1/0/3
```

```
[Switch-GigabitEthernet1/0/3] port link-type access
```

```
[Switch-GigabitEthernet1/0/3] port access vlan 8
```

## 2. Configure the DHCP service:

# Enable DHCP.

```
[Switch] dhcp enable
```

# Create a DHCP address pool named **vlan100**, and specify subnet 192.1.0.0/16 for dynamic allocation.

```
[Switch] dhcp server ip-pool vlan100
```

```
[Switch-dhcp-pool-vlan100] network 192.1.0.0 mask 255.255.255.0
```

# Exclude 192.1.1.1 from dynamic allocation and specify gateway IP address 192.1.1.2 for DHCP address pool **vlan100**.

```
[Switch-dhcp-pool-vlan100] forbidden-ip 192.1.1.1
```

```
[Switch-dhcp-pool-vlan100] gateway-list 192.1.1.2
```

```
[Switch-dhcp-pool-vlan100] quit
```

# Create a DHCP address pool named **vlan200**, and specify subnet 192.2.1.0/24 for dynamic allocation.

```
[Switch] dhcpserverip-pool vlan200
```

```
[Switch-dhcp-pool-vlan200] network 192.2.1.0 mask 255.255.255.0
```

# Exclude 192.2.1.1 from dynamic allocation and specify gateway IP address 192.2.1.2 for DHCP address pool **vlan200**. In this example, the address of the DNS server is 192.2.1.2 (the gateway address). You must replace it with the actual address of the DNS server on your network.

```
[Switch-dhcp-pool-vlan200] forbidden-ip 192.2.1.1
```

```
[Switch-dhcp-pool-vlan200] gateway-list 192.2.1.2
```

```
[Switch-dhcp-pool-vlan200] dns-list 192.2.1.2
```

```
[Switch-dhcp-pool-vlan200] quit
```

## Configuring the RADIUS server

In this example, the RADIUS server runs INC PLAT 7.2 and INC EAD 7.2.

Make sure the client has been installed with the EAP-PEAP certificate.

### Adding an access device

1. Log in to INC.
2. Click the **User** tab.
3. From the navigation tree, select **User Access Policy > Access Device Management > Access Device**.

The **Access Device** page opens, as shown in [Figure 2](#).

**Figure 2 Access Device page**

User > User Access Policy > Access Device Management > Access Device

★ Add to My Favorites ⓘ Help

Query Access Devices Advanced Query

Device IP Address Range From  To

Device Name  Access Device Type

Query Reset

Add Delete Modify Deploy More Refresh

Not Limited to Platform Devices AAA Deploy Result Command Deploy Result

4. Click **Add**.  
The **Add Access Device** page opens.
5. Configure access device parameters, as shown in [Figure 3](#):
  - a. In the **Shared Key** field, enter **example**.
  - b. Use the default settings of other parameters in the **Access Configuration** area.
  - c. In the **Device List** area, manually add an access device with the IP address of 192.1.1.1.  
(Details not shown.)
  - d. Click **OK**.

**Figure 3 Adding an access device**

User > User Access Policy > Access Device Management > Access Device > Add Access Device

Access Configuration

Authentication Port \* 1812 Accounting Port \* 1813

RADIUS Accounting Fully Supported Service Type LAN Access Service

Access Device Type H3C(General) Service Group Ungrouped

Shared Key \* \*\*\*\*\* Confirm Shared Key \* \*\*\*\*\*

Access Device Group ..

Device List

Select Add Manually Clear All

| Device Name | Device IP | Device Model | Comments | Delete |
|-------------|-----------|--------------|----------|--------|
|             | 192.1.1.1 |              |          |        |


Total Items: 1.

OK Cancel

## Configuring a security policy

1. Click the **User** tab.
2. From the navigation tree, select **User Security Policy > Security Policy**.  
The security policy page opens, as shown in [Figure 4](#).

**Figure 4 Security Policy page**



User > User Security Policy > Security Policy Add to My Favorites Help

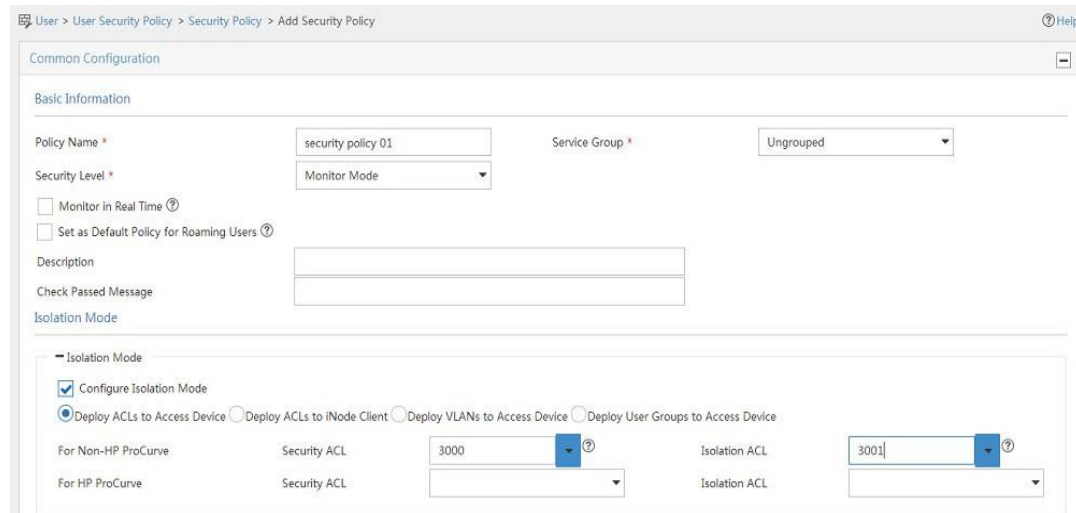
**Add** **Refresh**

| Policy Name ▲      | Security Level ▾ | Isolation Mode ▾ | Security ACL or VLAN ▾ | Isolation ACL or VLAN ▾ | Service Group ▾ | Modify | Delete |
|--------------------|------------------|------------------|------------------------|-------------------------|-----------------|--------|--------|
| 1                  | Kick Out Mode    | Not Deploy       |                        |                         | Ungrouped       |        |        |
| dafaf              | Monitor Mode     | Not Deploy       |                        |                         | Ungrouped       |        |        |
| security policy 01 | Monitor Mode     | Deploy ACLs to   | 3000                   | 3001                    | Ungrouped       |        |        |

Total Items: 3.

3. Click **Add**.  
The **Add Security Policy** page opens.
4. Configure security policy parameters, as shown in [Figure 5](#):
  - a. In the **Policy Name** field, enter **security policy 01**.
  - b. Select **Monitor Mode** from the **Security Level** list.
  - c. Select **Configure Isolation Mode**.
  - d. Select **Deploy ACLs to Access Device**.
  - e. Configure **3000** and **3001** for the **Security ACL** and **Isolation ACL** fields, respectively.
  - f. Use the default settings of other parameters.
  - g. Click **OK**.

**Figure 5 Adding an security policy**



User > User Security Policy > Security Policy > Add Security Policy Help

Common Configuration [-]

Basic Information

Policy Name \*  Service Group \*

Security Level \*

☐ Monitor in Real Time ?

☐ Set as Default Policy for Roaming Users ?

Description

Check Passed Message

Isolation Mode

☒ Configure Isolation Mode

☒ Deploy ACLs to Access Device ☐ Deploy ACLs to iNode Client ☐ Deploy VLANs to Access Device ☐ Deploy User Groups to Access Device

For Non-HP ProCurve Security ACL  ? Isolation ACL  ?

For HP ProCurve Security ACL  Isolation ACL

## Configuring an access policy

1. Click the **User** tab.
2. From the navigation tree, select **User Access Policy > Access Policy**.  
The **Access Policy** page opens, as shown in [Figure 6](#).

**Figure 6 Access Policy page**

User > User Access Policy > Access Policy

Query Access Policies

Access Policy Name:  Service Group:  Query Reset

Add SSID Access Control Hard Disk Serial Number Access MAC Address Endpoint Motherboard Serial Number Pool Access ACL

| Access Policy Name | Description | Service Group | Modify | Delete |
|--------------------|-------------|---------------|--------|--------|
| EAD                |             | Ungrouped     |        |        |
| eap-md5            |             | Ungrouped     |        |        |

3. Click **Add**.  
The **Add Access Policy** page opens.
4. Configure access policy parameters, as shown in [Figure 7](#):
  - a. In the **Access Policy Name** field, enter **EAD**.
  - b. Select **EAP-PEAP** from the **Preferred EAP Type** list, and select **EAP-MSCHAPv2** from the **Subtype** list.
  - c. Use the default settings of other parameters.
  - d. Click **OK**.

**Figure 7 Adding an access policy**

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

Basic Information

Access Policy Name \*:

Service Group \*:

Description:

Authorization Information

|                                                                    |                                                                        |
|--------------------------------------------------------------------|------------------------------------------------------------------------|
| Access Period: <input type="text" value="None"/>                   | Allocate IP *: <input type="text" value="No"/>                         |
| Downstream Rate (Kbps): <input type="text"/>                       | Upstream Rate (Kbps): <input type="text"/>                             |
| Priority: <input type="text"/>                                     | Deploy User Group: <input type="text"/>                                |
| Preferred EAP Type: <input type="text" value="EAP-PEAP"/>          | Subtype: <input type="text" value="EAP-MSCHAPv2"/>                     |
| EAP Auto Negotiate: <input type="text" value="Disable"/>           | Maximum Online Duration for a Logon (Minutes): <input type="text"/>    |
| Deploy Address Pool: <input type="text"/>                          | Deploy VLAN: <input type="text"/>                                      |
| <input type="checkbox"/> Deploy User Profile: <input type="text"/> | Deploy VSI name: <input type="text"/>                                  |
| <input type="checkbox"/> Deploy ACL: <input type="text"/>          | Authentication Password: <input type="text" value="Account Password"/> |
| Offline Check Period (Hours): <input type="text"/>                 |                                                                        |

## Adding an access service

1. Click the **User** tab.
2. From the navigation tree, select **User Access Policy > Access Service**.
3. Click **Add**.  
The **Add Access Service** page opens.
4. Configure access service parameters, as shown in [Figure 8](#):
  - a. Enter **EAD** in the **Service Name** field.
  - b. Select **security policy 01** from the **Default Security Policy** list.
  - c. Select **EAD** from the **Default Access Policy** list.
  - d. Use the default settings of other parameters.
  - e. Click **OK**.

**Figure 8 Adding an access service**

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

Basic Information

Service Name \*: EAD

Service Group \*: Ungrouped

Default Security Policy \*: security policy 01

Default Proprietary Attribute Assignment Policy \*: Do not use

Default Max. Devices for Single Account \*: 0

Daily Max. Online Duration \*: 0

Description

☒ Available

Service Suffix

Default Access Policy \*: EAD

Default Internet Access Policy \*: Do not use

Default Max. Number of Online Endpoints \*: 0

☒ Transparent Authentication

## Adding an access user account

1. Click the **User** tab.
2. From the navigation tree, select **Access User > All Access Users**.

The **Access User** page opens, as shown in Figure 9.

**Figure 9 Access User page**

User > All Access Users

Query Access Users

Account Name: [text box] User Name: [text box]

User Group: [text box] Service Name: [text box]

Query Reset

Add Batch Import Modify Account Add to Blacklist Cancel Account Apply for Service Cancel Service More

|                          | Account Name | User Name | User Group | Creation Date | Start Time | End Time | Account Status | Modify |
|--------------------------|--------------|-----------|------------|---------------|------------|----------|----------------|--------|
| <input type="checkbox"/> | g1           | g1        | Ungrouped  | 2018-06-25    |            |          | Normal         |        |
| <input type="checkbox"/> | new          | new       | Ungrouped  | 2018-06-25    |            |          | Normal         |        |

3. Click **Add**.
- The **Add Access User** page opens.
4. Configure access user parameters, as shown in Figure 10:
  - a. Click **Add User** next to the **User Name** field. On the **Add User** page that opens, enter **EAD\_guest** in the **User Name** field, enter an ID number in the **Identity Number** field, and then click **OK**, as shown in Figure 11.
  - b. Enter **EAD\_guest** in the **Account Name** field.
  - c. Enter **12345678** in the **Password** and **Confirm Password** fields.
  - d. In the access service list, select **EAD**.
  - e. Use the default settings of other parameters.
  - f. Click **OK**.



**Figure 10 Adding a user**

**Add User**

**Basic Information**

User Name \*  Identity Number \*

Contact Address  Telephone

Email  User Group \*

**Figure 11 Adding an access user account**

User > All Access Users > Add Access User

**Access Information**

User Name \*

Account Name \*

☐ Trial Account ☐ Default BYOD User ☐ MAC Authentication User ☐ Computer User ☐ Fast Access User

Password \*  Confirm Password \*

☒ Allow User to Change Password ☐ Enable Password Strategy ☐ Modify Password at Next Login

Start Time  End Time

Max. Idle Time (Minutes)  Max. Concurrent Logins

Login Message

**Access Service**

|                                     | Service Name | Service Suffix | Default Security Policy | Status    | Allocate IP |
|-------------------------------------|--------------|----------------|-------------------------|-----------|-------------|
| <input checked="" type="checkbox"/> | EAD          |                | security policy 01      | Available |             |
| <input type="checkbox"/>            | test         | test           | 1                       | Available |             |

## Configuring the iNode client

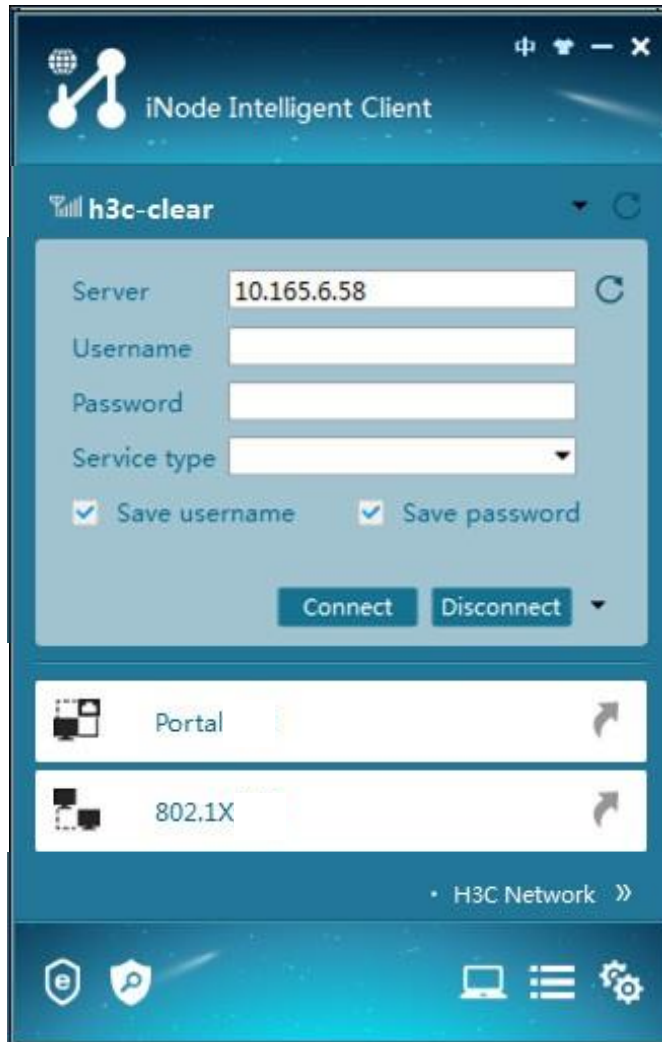
1. Run the iNode client, as shown in [Figure 12](#).

**Figure 12 iNode Client**



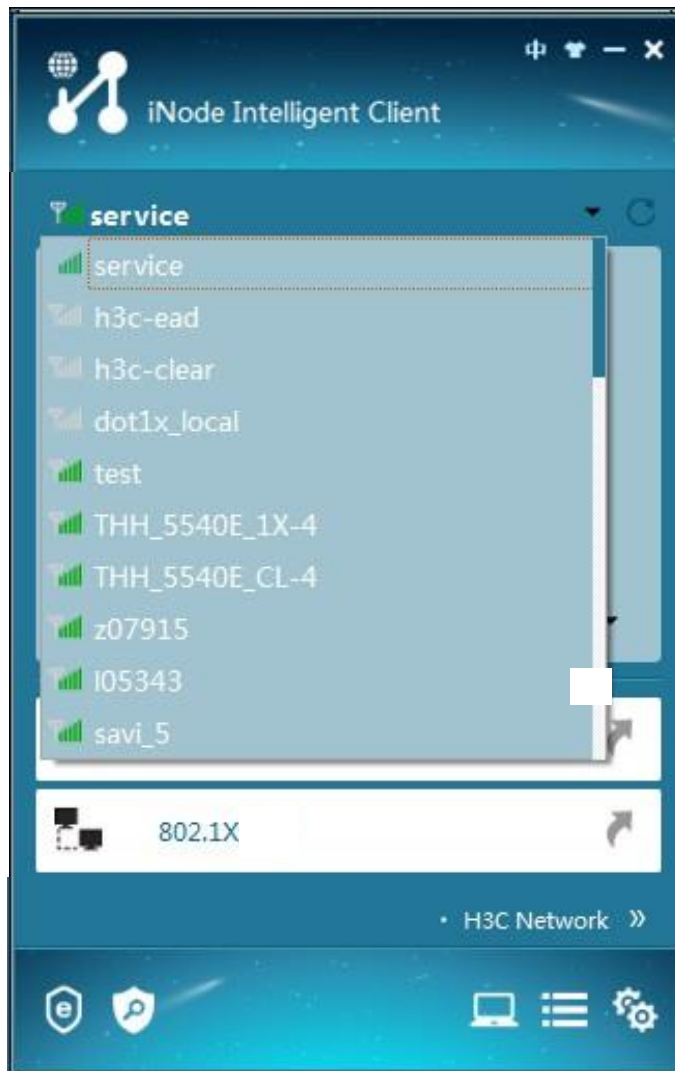
2. Change the connection from portal connection to wireless connection.  
The wireless connection page opens, as shown in [Figure 13](#).

Figure 13 Wireless connection



3. Click the inverted triangle icon at the upper right corner of the page, and select the wireless service with the SSID of **service**, as shown in [Figure 14](#).

Figure 14 Selecting an wireless service



4. Click the inverted triangle icon next to **Disconnect** and select **Properties**.
5. In the dialog box that opens, configure WAP2 and AES as the security type and encryption type, respectively, and then configure 802.1X properties. In this example, set the packet type to multicast for 802.1X packets and specify PEAP as the authentication method.
6. Return to the iNode wireless connection page, enter **EAD\_guest** in the **Username** field and **12345678** in the **Password** field.
7. Click **Connect**.

After the connection is established, the iNode client displays the security type and encryption type.

## Verifying the configuration

# Display 802.1X session information.

```
<AC> display dot1x sessions
AP name: officeap Radio ID: 2 SSID: service
Online 802.1X users: 1
 MAC address Auth state
```

0015-00bf-e84d      Authenticated

The output shows that the 802.1X user has come online.

# Display detailed WLAN client information.

<AC> display wlan client verbose

Total number of clients: 1

|                           |                                                                          |
|---------------------------|--------------------------------------------------------------------------|
| MAC address               | : 0015-00bf-e84d                                                         |
| IPv4 address              | : 192.2.1.3                                                              |
| IPv6 address              | : N/A                                                                    |
| Username                  | : ead guest                                                              |
| AID                       | : 1                                                                      |
| AP ID                     | : 2                                                                      |
| AP name                   | : officeap                                                               |
| Radio ID                  | : 2                                                                      |
| SSID                      | : service                                                                |
| BSSID                     | : 3891-d58a-8930                                                         |
| VLAN ID                   | : 200                                                                    |
| Sleep count               | : 18                                                                     |
| Wireless mode             | : 802.11ac                                                               |
| Channel bandwidth         | : 80MHz                                                                  |
| SM power save             | : Disabled                                                               |
| Short GI for 20MHz        | : Supported                                                              |
| Short GI for 40MHz        | : Supported                                                              |
| Short GI for 80MHz        | : Supported                                                              |
| Short GI for 160/80+80MHz | : Not supported                                                          |
| STBC RX capability        | : Supported                                                              |
| STBC TX capability        | : Not supported                                                          |
| LDPC RX capability        | : Not supported                                                          |
| SU beamformee capability  | : Not supported                                                          |
| MU beamformee capability  | : Not supported                                                          |
| Beamformee STS capability | : N/A                                                                    |
| Block Ack                 | : TID 0    Out                                                           |
| Supported VHT-MCS set     | : NSS1 0, 1, 2, 3, 4, 5, 6, 7, 8, 9<br>NSS2 0, 1, 2, 3, 4, 5, 6, 7, 8, 9 |
| Supported HT MCS set      | : 0, 1, 2, 3, 4, 5, 6, 7,<br>8, 9, 10, 11, 12, 13, 14,<br>15             |
| Supported rates           | : 6, 9, 12, 18, 24, 36,<br>48, 54 Mbps                                   |
| QoS mode                  | : WMM                                                                    |
| Listen interval           | : 250                                                                    |
| RSSI                      | : 34                                                                     |
| Rx/Tx rate                | : 58.5/324                                                               |
| Authentication method     | : Open system                                                            |
| Security mode             | : RSN                                                                    |
| AKM mode                  | : 802.1X                                                                 |
| Cipher suite              | : CCMP                                                                   |
| User authentication mode  | : 802.1X                                                                 |

|                            |                                   |
|----------------------------|-----------------------------------|
| Authorization ACL ID       | : 3000                            |
| Authorization user profile | : N/A                             |
| Roam status                | : N/A                             |
| Key derivation             | : SHA1                            |
| PMF status                 | : N/A                             |
| Forwarding policy name     | : N/A                             |
| Online time                | : 0days 0hours 2minutes 49seconds |
| FT status                  | : Inactive                        |

The output shows that ACL 3000 has been deployed, which means the EAD security policy has been deployed.

## Configuration files

- AC:
 

```
#
dot1x authentication-method eap
#
port-security enable
#
vlan 100
#
vlan 200
#
wlan service-template 1
ssid service
client forwarding-location ac
vlan 200
akm mode dot1x
cipher-suite ccmp
security-ie rsn
client-security authentication-mode dot1x
dot1x domain radius1
service-template enable
#
interface Vlan-interface100
ip address 192.1.1.1 255.255.0.0
#
interface Vlan-interface200
ip address 192.2.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 100 200
#
ip route-static 8.0.0.0 8 192.2.1.2
#
acl advanced 3000
```

```

rule 0 permit ip
#
acl advanced 3001
rule 0 permit udp
rule 5 deny tcp
#
radius scheme radius1
primary authentication 8.1.1.16
primary accounting 8.1.1.16
key authentication cipher c3$YCjREST8/BuXrsEKyY9nY8QQfmrN3w==
key accounting cipher c3$yPGJYnF7FE+/36JrXfn+DYGq/8ngZA==
timer realtime-accounting 3
nas-ip 192.1.1.1
#
domain radius1
authentication lan-access radius-scheme radius1
authorization lan-access radius-scheme radius1
accounting lan-access radius-scheme radius1
#
wlan ap-group group1
 ap officeap
 ap-model AP 3620
 radio 2
 radio enable
 service-template 1
#
wlan ap officeap model AP 3620
serial-id 219801A28N819CE0002T
#

```

- **Switch:**

```

#
dhcp enable
#
vlan8
#
vlan 100
#
vlan 200
#
dhcp server ip-pool vlan100
gateway-list 192.1.1.2
network 192.1.0.0 mask 255.255.0.0
forbidden-ip 192.1.1.1
#
dhcp server ip-pool vlan200
gateway-list 192.2.1.2
network 192.2.1.0 mask 255.255.255.0
dns-list 192.2.1.2

```

```

forbidden-ip 192.2.1.1
#
interface Vlan-interface8
ip address 8.1.1.2 255.0.0.0
#
interface Vlan-interface100
ip address 192.1.1.2 255.255.255.0
#
interface Vlan-interface200
ip address 192.2.1.2 255.255.255.0
#
interface GigabitEthernet1/0/1
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 100 200
#
interface GigabitEthernet1/0/2
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 100
port trunk pvid vlan 100
poe enable
#
interface GigabitEthernet1/0/3
port link-type access
port access vlan 8
#

```

## Related documentation

- *AP and WT Management Configuration Guide in INTELBRAS Access Controllers Configuration Guides*
- *AP and WT Management Command Reference in INTELBRAS Access Controllers Command References*
- *Network Connectivity Configuration Guide in INTELBRAS Access Controllers Configuration Guides*
- *Network Connectivity Command Reference in INTELBRAS Access Controllers Command References*
- *User Access and Authentication Configuration Guide in INTELBRAS Access Controllers Configuration Guides*
- *User Access and Authentication Command Reference in INTELBRAS Access Controllers Command References*
- *WLAN Access Configuration Guide in INTELBRAS Access Controllers Configuration Guides*
- *WLAN Access Command Reference in INTELBRAS Access Controllers Command References*



# INTELBRAS Access Controllers

## EAD Authentication (IPv6)

### Configuration Examples

---

Copyright © 2024 Intelbras S.A All rights reserved.

No part of this manual may be reproduced or transmitted in any form or by any means without prior written consent of Intelbras S.A

Except for the trademarks of Intelbras S.A, any trademarks that may be mentioned in this document are the property of their respective owners.

The information in this document is subject to change without notice.

# Contents

|                                                      |    |
|------------------------------------------------------|----|
| Introduction .....                                   | 1  |
| Prerequisites .....                                  | 1  |
| Example: Configuring EAD authentication (IPv6) ..... | 1  |
| Network configuration .....                          | 1  |
| Restrictions and guidelines .....                    | 1  |
| Procedures .....                                     | 2  |
| Configuring the AC .....                             | 2  |
| Configuring the switch .....                         | 4  |
| Configuring the RADIUS server .....                  | 6  |
| Configuring the client .....                         | 11 |
| Verifying the configuration .....                    | 11 |
| Configuration files .....                            | 13 |
| Related documentation .....                          | 15 |

# Introduction

The following information provides an example for configuring EAD authentication for wireless clients on an IPv6 network.

## Prerequisites

The following information applies to Comware-based access controllers and access points. Procedures and information in the examples might be slightly different depending on the software or hardware version of the access controllers and access points.

The configuration examples 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.

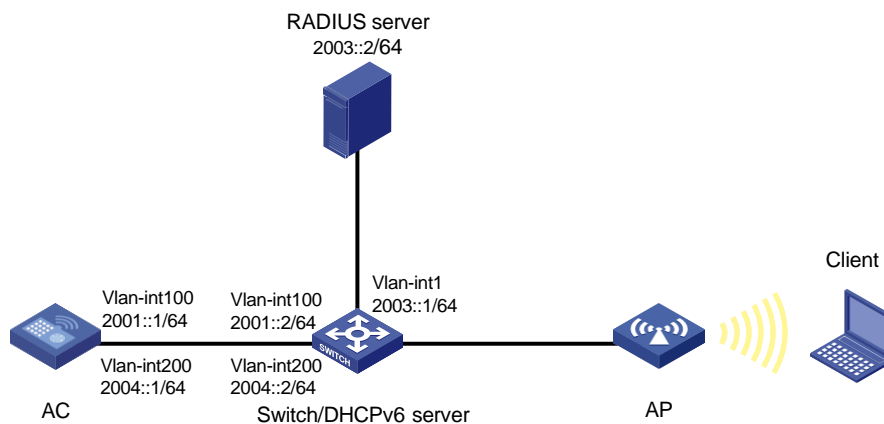
The following information is provided based on the assumption that you have basic knowledge of WLAN access and EAD authentication.

## Example: Configuring EAD authentication (IPv6)

### Network configuration

As shown in [Figure 1](#), the switch acts as a DHCPv6 server to assign IPv6 addresses to the AP and the client. Configure EAD authentication on the AC to authenticate the client.

**Figure 1 Network diagram**



### Restrictions and guidelines

Use the actual serial ID of an AP to uniquely identify that AP.

# Procedures

## Configuring the AC

### 1. Configure interfaces on the AC:

# Create VLAN 100 and VLAN-interface 100, and assign an IPv6 address to the VLAN interface. The AC will use this IP address to establish CAPWAP tunnels with the AP.

```
<AC> system-view
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ipv6 address 2001::1 64
[AC-Vlan-interface100] quit
```

# Create VLAN 200 and VLAN-interface 200, and assign an IPv6 address to the VLAN interface. The client will use VLAN 200 to access the WLAN.

```
[AC] vlan 200
[AC-vlan200] quit
[AC] interface vlan-interface 200
[AC-Vlan-interface200] ipv6 address 2004::1 64
[AC-Vlan-interface200] quit
```

# Configure GigabitEthernet 1/0/1 (the port connected to the switch) as a trunk port, and assign the port to VLAN 1, VLAN 100, and VLAN 200.

```
[AC] interface gigabitEthernet 1/0/1
[AC-GigabitEthernet1/0/1] port link-type trunk
[AC-GigabitEthernet1/0/1] port trunk permit vlan 1 100 200
[AC-GigabitEthernet1/0/1] quit
```

### 2. Enable port security and enable EAP relay for 802.1X authentication.

```
[AC] port-security enable
[AC] dot1x authentication-method eap
```

### 3. Configure a RADIUS scheme:

# Create a RADIUS scheme named **radius1** and enter its view.

```
[AC] radius scheme radius1
```

# Specify the server at 2003::2 as the primary authentication RADIUS server.

```
[AC-radius-radius1] primary authentication ipv6 2003::2
```

# Specify the server at 2003::2 as the primary accounting RADIUS server.

```
[AC-radius-radius1] primary accounting ipv6 2003::2
```

# Set the shared key to **12345** in plaintext form for secure communication with the RADIUS authentication server.

```
[AC-radius-radius1] key authentication simple 12345
```

# Set the shared key to **12345** in plaintext form for secure communication with the RADIUS accounting server.

```
[AC-radius-radius1] key accounting simple 12345
```

# Set the real-time accounting interval to 3 minutes.

```
[AC-radius-radius1] timer realtime-accounting 3
```

# Specify IPv6 address 2001::1 as the source IPv6 address of outgoing RADIUS packets.

```
[AC-radius-radius1] nas-ip ipv6 2001::1
[AC-radius-radius1] quit
```

4. Configure an authentication domain:

# Create an ISP domain named **dom1** and enter its view.

```
[AC] domain dom1
```

# Apply RADIUS scheme **radius1** to ISP domain **dom1** for LAN user authentication, authorization, and accounting.

```
[AC-isp-dom1] authentication lan-access radius-scheme radius1
```

```
[AC-isp-dom1] authorization lan-access radius-scheme radius1
```

```
[AC-isp-dom1] accounting lan-access radius-scheme radius1
```

```
[AC-isp-dom1] quit
```

5. Configure ACLs:

# Create IPv6 advanced ACL 3000 and enter its view.

```
[AC] acl ipv6 advanced 3000
```

# Create an ACL rule to permit all IPv6 packets.

```
[AC-acl-ipv6-adv-3000] rule permit ipv6
```

```
[AC-acl-ipv6-adv-3000] quit
```

# Create IPv6 advanced ACL 3001 and enter its view.

```
[AC] acl ipv6 advanced 3001
```

# Create an ACL rule to permit all UDP packets.

```
[AC-acl-ipv6-adv-3001] rule permit udp
```

# Create an ACL rule to deny all TCP packets.

```
[AC-acl-ipv6-adv-3001] rule deny tcp
```

```
[AC-acl-ipv6-adv-3001] quit
```

6. Configure a wireless service:

# Create a service template named **service** and enter its view.

```
[AC] wlan service-template service
```

# Set the SSID of the service template to **service**.

```
[AC-wlan-st-service] ssid service
```

# Assign clients coming online through the service template to VLAN 200.

```
[AC-wlan-st-service] vlan 200
```

# Set the AKM mode to 802.1X authentication.

```
[AC-wlan-st-service] akm mode dot1x
```

# Set the CCMP cipher suite for frame encryption and enable the RSN-IE in the beacon and probe responses.

```
[AC-wlan-st-service] cipher-suite ccmp
```

```
[AC-wlan-st-service] security-ie rsn
```

# Set the authentication mode to 802.1X authentication.

```
[AC-wlan-st-service] client-security authentication-mode dot1x
```

# Specify ISP domain **dom1** as the 802.1X authentication domain.

```
[AC-wlan-st-service] dot1x domain dom1
```

# Enable snooping DHCPv6 packets and enable snooping ND packets.

```
[AC-wlan-st-service] client ipv6-snooping dhcpv6-learning enable
```

```
[AC-wlan-st-service] client ipv6-snooping nd-learning enable
```

# Enable the AC to forward client data traffic. If the AC forwards client data traffic by default, skip this step.

```
[AC-wlan-st-service] client forwarding-location ac
```

# Enable the service template.

```
[AC-wlan-st-service] service-template enable
```

```
[AC-wlan-st-service] quit
```

## 7. Configure AP settings:

### ! IMPORTANT:

In a large-scale network, configure AP groups as a best practice.

# Create a manual AP named **ap1** and specify its model and serial ID.

```
[AC] wlan ap ap1 model AP 3620
[AC-wlan-ap-ap1] serial-id 219801A28N819CE0002T
[AC-wlan-ap-ap1] quit
```

# Create AP group **group1** and create an AP grouping rule by AP names to add AP **ap1** to AP group **group1**.

```
[AC] wlan ap-group group1
[AC-wlan-ap-group-group1] ap ap1
```

# Bind service template **service** to radio 1 in AP group **group1**.

```
[AC-wlan-ap-group-group1] ap-model AP 3620
[AC-wlan-ap-group-group1-ap-model-AP 3620] radio 1
[AC-wlan-ap-group-group1-ap-model-AP 3620-radio-1] service-template service
```

# Enable radio 1.

```
[AC-wlan-ap-group-group1-ap-model-AP 3620-radio-1] radio
enable [AC-wlan-ap-group-group1-ap-model-AP 3620-radio-1] quit
[AC-wlan-ap-group-group1-ap-model-AP 3620]
quit [AC-wlan-ap-group-group1] quit
```

## 8. Configure a static route destined for the RADIUS server.

```
[AC] ipv6 route-static 2003:: 64 2004::2
```

# Configuring the switch

## 1. Configure interfaces on the switch:

# Create VLAN 100. The switch will use this VLAN to forward CAPWAP packets between the AC and the AP.

```
<Switch> system-view
[Switch] vlan 100
[Switch-vlan100] quit
```

# Create VLAN-interface 100 and assign an IPv6 address to the VLAN interface.

```
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ipv6 address 2001::2 64
[Switch-Vlan-interface100] quit
```

# Create VLAN 200. The switch will use this VLAN to forward client traffic.

```
[Switch] vlan 200
[Switch-vlan200] quit
```

# Create VLAN-interface 200 and assign an IPv6 address to the VLAN interface.

```
[Switch] interface vlan-interface 200
[Switch-Vlan-interface200] ipv6 address 2004::2 64
[Switch-Vlan-interface200] quit
```

# Create VLAN-interface 1, and assign an IPv6 address to the VLAN interface. The switch will use this VLAN to communicate with the RADIUS server.

```
[Switch] vlan 1
```

```
[Switch-vlan1] quit
[Switch] interface vlan-interface 1
[Switch-Vlan-interface1] ipv6 address 2003::1 64
[Switch-Vlan-interface1] quit
```

**# Configure GigabitEthernet 1/0/1 (the port connected to the AC) as a trunk port, and assign the port to VLAN 1, VLAN 100, and VLAN 200.**

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 1 100 200
[Switch-GigabitEthernet1/0/1] quit
```

**# Configure GigabitEthernet 1/0/2 (the port connected to the AP) as an access port, and assign the port to VLAN 100.**

```
[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] port link-type access
[Switch-GigabitEthernet1/0/2] port access vlan 100
```

**# Enable PoE on GigabitEthernet 1/0/2.**

```
[Switch-GigabitEthernet1/0/2] poe enable
[Switch-GigabitEthernet1/0/2] quit
```

## 2. Configure the DHCPv6 service:

**# Create DHCPv6 address pool 1, specify the subnet 2001::/64 in the DHCPv6 address pool, and specify 2001::1 as the gateway address. The switch assigns an IPv6 address to the AP from this pool.**

```
[Switch] ipv6 dhcp pool 1
[Switch-dhcp6-pool-1] network 2001::/64
[Switch-dhcp6-pool-1] gateway-list 2001::1
```

**# Configure Option 52 that specifies the AC's IPv6 address 2001::1 and exclude the IPv6 address from dynamic assignment.**

```
[Switch-dhcp6-pool-1] option 52 hex 20010000000000000000000000000001
[Switch-dhcp6-pool-1] quit
[Switch] ipv6 dhcp server forbidden-address 2001::1
```

**# Apply address pool 1 to VLAN-interface 100 and enable the DHCPv6 server on the VLAN interface.**

```
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ipv6 dhcp server apply pool 1
[Switch-Vlan-interface100] ipv6 dhcp select server
```

**# Set the managed address configuration flag (M) and the other stateful configuration flag (O) to 1 in RA advertisements to be sent, and disable RA message suppression on VLAN-interface 100.**

```
[Switch-Vlan-interface100] ipv6 nd autoconfig managed-address-flag
[Switch-Vlan-interface100] ipv6 nd autoconfig other-flag
[Switch-Vlan-interface100] undo ipv6 nd ra halt
[Switch-Vlan-interface100] quit
```

**# Create DHCPv6 address pool 2, specify the subnet 2004::/64 in the DHCPv6 address pool, and specify 2004::2 as the gateway address. The switch assigns an IPv6 address to the client from this pool.**

```
[Switch] ipv6 dhcp pool 2
[Switch-dhcp6-pool-2] network 2004::/64
[Switch-dhcp6-pool-2] gateway-list 2004::2
[Switch-dhcp6-pool-2] quit
```

```
Exclude IPv6 address 2004::1 from dynamic assignment.
[Switch] ipv6 dhcp server forbidden-address 2004::1

Apply address pool 2 to VLAN-interface 200 and enable the DHCPv6 server on the VLAN
interface.
[Switch] interface Vlan-interface 200
[Switch-Vlan-interface200] ipv6 dhcp server apply pool 2
[Switch-Vlan-interface200] ipv6 dhcp select server

Set the managed address configuration flag (M) and the other stateful configuration flag (O) to
1 in RA advertisements to be sent, and disable RA message suppression on VLAN-interface
200.
[Switch-Vlan-interface200] ipv6 nd autoconfig managed-address-flag
[Switch-Vlan-interface200] ipv6 nd autoconfig other-flag
[Switch-Vlan-interface200] undo ipv6 nd ra halt
[Switch-Vlan-interface200] quit
```

## Configuring the RADIUS server

This example uses INC PLAT 7.1 and INC EAD 7.1 to show the procedure.

Make sure the EAP-PEAP certificate has been installed on the server.

### Adding the AC to INC as an access device

1. Log in to INC.
2. Click the **User** tab.
3. From the navigation tree, select **User Access Policy > Access Device Management > Access Device**.  
The **Access Device** page opens.
4. Click **Add**.  
The **Add Access Device** page opens.
5. Configure access device parameters, as shown in [Figure 2](#):
  - a. In the **Access Configuration** area, set the authentication and accounting shared keys to **12345** and use the default settings of other parameters.
  - b. In the **Device List** area, click **Select** or **Add IPv6 Dev** to add the device at 2001::1 to INC as an access device. If you click **Add IPv6 Dev**, enter 2001::1 as the start IPv6 address and click **OK** in the dialog box that opens.
  - c. Click **OK**.



**Figure 2 Adding an access device**

## Configuring a security policy

1. Click the **User** tab.
2. From the navigation tree, select **User Security Policy > Security Policy**.

The security policy page opens, as shown in [Figure 3](#).

**Figure 3 Security Policy page**

3. Click **Add**.  
The **Add Security Policy** page opens.
4. Configure security policy parameters, as shown in [Figure 4](#):
  - a. In the **Policy Name** field, enter **security policy01**.
  - b. Select **Monitor Mode** from the **Security Level** list.
  - c. Select **Configure Isolation Mode**.
  - d. Select **Deploy ACLs to Access Device**.
  - e. Configure **3000** and **3001** for the **Security ACL** and **Isolation ACL** fields, respectively.
  - f. Use the default settings of other parameters.
  - g. Click **OK**.

**Figure 4 Adding an security policy**

User > User Security Policy > Security Policy > Add Security Policy

Common Configuration

Basic Information

Policy Name \* security policy01 Service Group \* Ungrouped

Security Level \* Monitor Mode

☐ Monitor in Real Time ?

☐ Set as Default Policy for Roaming Users ?

Description

Check Passed Message

Isolation Mode

☒ Configure Isolation Mode

☒ Deploy ACLs to Access Device ☐ Deploy ACLs to iNode Client ☐ Deploy VLANs to Access Device

For Non-HP ProCurve Security ACL 3000 Isolation ACL 3001

For HP ProCurve Security ACL Isolation ACL

## Configuring an access policy

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

The **Access Policy** page opens, as shown in Figure 5.

**Figure 5 Access Policy page**

User > User Access Policy > Access Policy

★ Add to My Favorites ? Help

Query Access Policy

Access Policy Name Service Group Query Reset

Add

SSID Access Control Hard Disk Serial Number Access MAC Address Access ACL

| Access Policy Name | Description | Service Group | Modify | Delete |
|--------------------|-------------|---------------|--------|--------|
| No match found.    |             |               |        |        |

0-0 of 0. Page 1 of 1.

3. Click **Add**.
- The **Add Access Policy** page opens.
4. Configure access policy parameters, as shown in Figure 6:
  - a. In the **Access Policy Name** field, enter **EAD**.
  - b. Select **EAP** for the **Certificate Authentication** field.
  - c. Select **EAP-PEAP Auth** from the **Certificate Type** list, and select **MS-CHAPV2 Auth** from the **Certificate Sub-Type** list.
  - d. Use the default settings of other parameters.
  - e. Click **OK**.

**Figure 6 Adding an access policy**

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

### Basic Information

Access Policy Name \*

Service Group \*

Description

### Authorization Information

Access Period

Allocate IP \*

Downstream Rate(Kbps)

Upstream Rate(Kbps)

Priority

☐ RSA Authentication

Certificate Authentication ☐ None ☒ EAP

Certificate Type

Certificate Sub-Type

Deploy VLAN

☐ Deploy User Profile

☐ Deploy ACL

Deploy User Group

## Adding an access service

1. Click the **User** tab.
2. From the navigation tree, select **User Access Policy > Access Service**.  
The **Access Service** page opens, as shown in [Figure 7](#).

**Figure 7 Access Service page**

User > User Access Policy > Access Service

Add Refresh

| Service Name    | Description | Service Suffix | Service Group | Modify | Delete |
|-----------------|-------------|----------------|---------------|--------|--------|
| No match found. |             |                |               |        |        |

3. Click **Add**.  
The **Add Access Service** page opens.
4. Configure access service parameters, as shown in [Figure 8](#):
  - a. Enter **EAD** in the **Service Name** field.
  - b. Select **security policy01** from the **Default Security Policy** list.
  - c. Select **EAD** from the **Default Access Policy** list.
  - d. Use the default settings of other parameters.
  - e. Click **OK**.

**Figure 8 Adding an access service**

The screenshot shows the 'Add Access Service' page. The breadcrumb navigation is 'User > User Access Policy > Access Service > Add Access Service'. The page is divided into two main sections: 'Basic Information' and 'Access Scenario List'. In the 'Basic Information' section, the 'Service Name' is 'EAD', 'Service Group' is 'Ungrouped', 'Default Security Policy' is 'security policy01', 'Default Proprietary Attribute Assignment Policy' is 'Do not use', 'Default Max. Number of Bound Endpoints' is '0', 'Default Max. Number of Online Endpoints' is '0', 'Description' is empty, 'Available' is checked, and 'Transparent Authentication' is checked. The 'Access Scenario List' section shows a table with columns: Access Scenario, Access Policy, Security Policy, Proprietary Attribute Assignment Policy, Internet Access Configuration, Priority, Modify, and Delete. The table is empty with the message 'No match found.' Below the table are 'OK' and 'Cancel' buttons.

## Adding an access user account

1. Click the **User** tab.
2. From the navigation tree, select **Access User > Access User**.  
The **All Access Users** page opens, as shown in [Figure 9](#).

**Figure 9 All Access Users page**

The screenshot shows the 'All Access Users' page. The breadcrumb navigation is 'User > All Access Users'. The page has a 'Query Access Users' section with fields for 'Account Name', 'User Name', 'User Group', and 'Service Name', and buttons for 'Query' and 'Reset'. Below this is a row of action buttons: 'Add', 'Batch Import', 'Modify Account', 'Add to Blacklist', 'Cancel Account', 'Apply for Service', 'Cancel Service', and 'More'. The main table has columns: Account Name, User Name, User Group, Creation Date, Start Time, End Time, Account Status, and Modify. The table is empty with the message 'No match found.' Below the table is a pagination bar showing '0-0 of 0, Page 1 of 1.' and navigation buttons.

3. Click **Add**.  
The **Add Access User** page opens, as shown in [Figure 10](#).

**Figure 10 Add Access User page**

The screenshot shows the 'Add Access User' page. The breadcrumb navigation is 'User > All Access Users > Add Access User'. The page is titled 'Access Information'. It has fields for 'User Name', 'Account Name', 'Password', 'Confirm Password', 'Start Time', 'End Time', 'Max. Idle Time(Minutes)', 'Max. Concurrent Logins', and 'Login Message'. There are checkboxes for 'Trial Account', 'Default BYOD User', 'MAC Authentication User', 'Computer User', 'Fast Access User', 'Allow User to Change Password', 'Enable Password Strategy', and 'Modify Password at Next Login'. There are 'Select' and 'Add User' buttons next to the 'User Name' field.

4. Configure access user parameters, as shown in [Figure 11](#):
  - a. Click **Add User** next to the **User Name** field. On the **Add User** page that opens, enter **EAD\_guest** in the **User Name** field, enter an ID number in the **Identity Number** field, and then click **OK**, as shown in [Figure 12](#).

- b. Enter **EAD\_guest** in the **Account Name** field.
- c. Enter **12345678** in the **Password** and **Confirm Password** fields.
- d. In the access service list, select **EAD**.
- e. Use the default settings of other parameters.
- f. Click **OK**.

**Figure 11 Adding an access user account**

User > All Access Users > Add Access User

**Access Information**

User Name \*  Select Add User

Account Name \*

☐ Trial Account ☐ Default BYOD User ☐ MAC Authentication User ☐ Computer User ☐ Fast Access User

Password \*  Confirm Password \*

☒ Allow User to Change Password ☐ Enable Password Strategy ☐ Modify Password at Next Login

Start Time  ... End Time  ...

Max. Idle Time(Minutes)  Max. Concurrent Logins

Login Message

**Access Service**

|                                     | Service Name | Service Suffix | Default Security Policy | Status    | Allocate IP |
|-------------------------------------|--------------|----------------|-------------------------|-----------|-------------|
| <input checked="" type="checkbox"/> | EAD          |                | security policy01       | Available |             |

**Figure 12 Adding a user**

**Add User**

**Basic Information**

User Name \*  Identity Number \*  Check Availability

Contact Address  Telephone  ?

Email  ? User Group \*  ...

OK Cancel

## Configuring the client

Use a mobile phone to connect to the wireless network with SSID **service**:

1. Select PEAP as the EAP authentication method.
2. Enter **EAD\_guest** as the identity and enter password **12345678**.  
Use the default settings of other parameters.
3. Connect to the wireless network.

## Verifying the configuration

# Display 802.1X session information.

```
<AC> display dot1x sessions
```

```

AP name: ap1 Radio ID: 1 SSID: service
 Online 802.1X users: 1
 MAC address Auth state
 3829-5a40-9589 Authenticated

```

#### # Display detailed WLAN client information.

```
<AC> display wlan client verbose
```

```
Total number of clients: 1
```

```

MAC address : 3829-5a40-9589
IPv4 address : N/A
IPv6 address : 2004::3
Username : EAD guest
AID : 1
AP ID : 2
AP name : ap1
Radio ID : 1
SSID : service
BSSID : ac74-090a-6421
VLAN ID : 200
Sleep count : 18
Wireless mode : 802.11an
Channel bandwidth : 40MHz
20/40 BSS Coexistence Management : Supported
SM power save : Enabled
SM power save mode : Static
Short GI for 20MHz : Supported
Short GI for 40MHz : Supported
STBC RX capability : Supported
STBC TX capability : Not supported
LDPC RX capability : Not supported
Block Ack : TID 0 Both
Supported HT MCS set : 0, 1, 2, 3, 4, 5, 6, 7
Supported rates : 6, 9, 12, 18, 24, 36,
 48, 54 Mbps
QoS mode : WMM
Listen interval : 2
RSSI : 30
Rx/Tx rate : 0/0 Mbps
Authentication method : Open system
Security mode : RSN
AKM mode : 802.1X
Cipher suite : CCMP
User authentication mode : 802.1X
Authorization ACL ID : 3001
Authorization user profile : N/A
Roam status : N/A
Key derivation : SHA1
PMF status : N/A

```

```
Forwarding policy name : Not configured
Online time : 0days 0hours 0minutes 2seconds
FT status : Inactive
```

The output shows that ACL 3001 has been deployed, which indicates that the EAD security policy has been deployed.

## Configuration files

- AC:

```
#
dot1x authentication-method eap
#
port-security enable
#
vlan 1
#
vlan 100
#
vlan 200
#
wlan service-template service
 ssid service
 vlan 200
 client forwarding-location ac
 akm mode dot1x
 cipher-suite ccmp
 security-ie rsn
 client-security authentication-mode dot1x
 dot1x domain dom1
 client ipv6-snooping nd-learning enable
 client ipv6-snooping dhcpv6-learning enable
 service-template enable
#
interface Vlan-interface100
 ipv6 address 2001::1/64
#
interface Vlan-interface200
 ipv6 address 2004::1/64
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 100 200
#
 ipv6 route-static 2003:: 64 2004::2
#
acl ipv6 advanced 3000
 rule 0 permit ipv6
```

```

#
acl ipv6 advanced 3001
 rule 0 permit udp
 rule 5 deny tcp
#
radius scheme radius1
 primary authentication ipv6 2003::2
 primary accounting ipv6 2003::2
 key authentication cipher c3$CAoJIYj1WmUo808RrsxOvXcfUpkZLcPY
 key accounting cipher c3$9YjVI/VV3rlbbKw7TZOnaGZGY/gD0pKU
 timer realtime-accounting 3
 nas-ip ipv6 2001::1
#
domain dom1
 authentication lan-access radius-scheme radius1
 authorization lan-access radius-scheme radius1
 accounting lan-access radius-scheme radius1
#
wlan ap-group group1
 ap ap1
 ap-model AP 3620
 radio 1
 radio enable
 service-template service
 radio 2
#
wlan ap ap1 model AP 3620
 serial-id 219801A28N819CE0002T
#

```

- **Switch:**

```

#
 ipv6 dhcp server forbidden-address 2001::1
 ipv6 dhcp server forbidden-address 2004::1
#
vlan 1
#
vlan 100
#
vlan 200
#
ipv6 dhcp pool 1
 network 2001::/64
 option 52 hex 20010000000000000000000000000001
 gateway-list 2001::1
#
ipv6 dhcp pool 2
 network 2004::/64
 gateway-list 2004::2

```



```

#
interface Vlan-interface1
 ipv6 address 2003::1/64
#
interface Vlan-interface100
 ipv6 dhcp select server
 ipv6 dhcp server apply pool 1
 ipv6 address 2001::2/64
 ipv6 nd autoconfig managed-address-flag
 ipv6 nd autoconfig other-flag
 undo ipv6 nd ra halt
#
interface Vlan-interface200
 ipv6 dhcp select server
 ipv6 dhcp server apply pool 2
 ipv6 address 2004::2/64
 ipv6 nd autoconfig managed-address-flag
 ipv6 nd autoconfig other-flag
 undo ipv6 nd ra halt
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 1 100 200
#
interface GigabitEthernet1/0/2
 port access vlan 100
 poe enable
#

```

## Related documentation

- *AP and WT Management Configuration Guide in INTELBRAS Access Controllers Configuration Guides*
- *AP and WT Management Command Reference in INTELBRAS Access Controllers Command References*
- *Network Connectivity Configuration Guide in INTELBRAS Access Controllers Configuration Guides*
- *Network Connectivity Command Reference in INTELBRAS Access Controllers Command References*
- *User Access and Authentication Configuration Guide in INTELBRAS Access Controllers Configuration Guides*
- *User Access and Authentication Command Reference in INTELBRAS Access Controllers Command References*
- *WLAN Access Configuration Guide in INTELBRAS Access Controllers Configuration Guides*
- *WLAN Access Command Reference in INTELBRAS Access Controllers Command References*