

# INTELBRAS Access Controllers

## Local Forwarding Mode and 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 forwarding mode and local portal 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
Configuring the DHCP server .....	5
Verifying the configuration .....	5
Configuration files .....	8
Related documentation .....	9

# Introduction

The following information provides an example of configuring local portal authentication 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 authentication, WLAN access, and WLAN high availability.

## Example: Configuring local forwarding mode and local portal authentication

### Network configuration

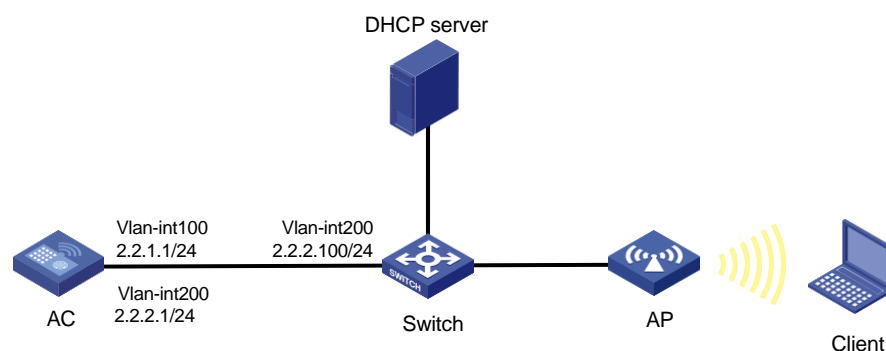
As shown in [Figure 1](#):

- The AP and the client obtain IP addresses from the DHCP server.
- The AP and the AC use VLAN 100 to establish CAPWAP tunnels, and the client uses VLAN 200 to access the wireless network.
- The AC acts as the portal authentication server and portal Web server.

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.

**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.

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 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 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 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**.

```
[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 APs to forward client data traffic from all VLANs.

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

# 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
[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 **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 AP group **group1**.

```
[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
```

## 4. Configure an ISP domain:

# Create an ISP domain named **dm1**.

```
<AC> system-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
```

# 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
```

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

## 5. 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
```

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

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

```
[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 for the local portal Web service.

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

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

# Create two destination-based portal-free rules to permit traffic to the DNS server.

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

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

# Add a network access user named **123**, set the password of the user, and assign the portal service to the user.

```
[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 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
```

```
# 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 tunnels between the AC and the AP.

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

# Create VLAN 200, create VLAN-interface 200, and assign an IP address to the VLAN interface. The switch will use this VLAN to forward packets for wireless clients.

```
[Switch] vlan 200
[Switch-vlan200] quit
[Switch] interface vlan-interface 200
[Switch-Vlan-interface200] ip address 2.2.2.100 255.255.255.0
[Switch-Vlan-interface200] 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.

```
[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
```

## Configuring the DHCP server

Configure required settings on the DHCP server. (Details not shown.)

## Verifying the configuration

### Verifying local portal authentication

# 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. (Details not shown.)

# Display online portal user information on the AC.

```
[AC] display portal user all
Total portal users: 1
```

```

Username: Client
  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.

## Verifying local forwarding mode

# Display portal filtering rules on the AC.

```

[AC] display portal rule all ap ap1
Slot 1:

```

The output shows that the AC does not have portal filtering rules, indicating that the AC does not forward client data traffic.

# Display portal filtering rules on the AP.

```

[AP] display portal rule all

```

IPv4 portal rules on WLAN-BSS1/0/16:

Rule 1:

```

Type           : Static
Action          : Permit
Protocol        : Any
Status          : Active
Source:
  IP            : 0.0.0.0
  Mask          : 0.0.0.0
  Port          : Any
  MAC           : 0000-0000-0000
  Interface     : WLAN-BSS1/0/16
  VLAN          : Any
Destination:
  IP            : 2.2.2.1
  Mask          : 255.255.255.255
  Port          : Any

```

Rule 2:

```

Type           : Dynamic
Action          : Permit
Status          : Active
Source:
  IP            : 2.2.2.2

```



MAC : 0021-6330-0933  
Interface : WLAN-BSS1/0/16  
VLAN : Any

Rule 3:

Type : Static  
Action : Redirect  
Status : Active  
Source:  
IP : 0.0.0.0  
Mask : 0.0.0.0  
Interface : WLAN-BSS1/0/16  
VLAN : Any  
Protocol : TCP  
Destination:  
IP : 0.0.0.0  
Mask : 0.0.0.0  
Port : 443

Rule 4:

Type : Static  
Action : Redirect  
Status : Active  
Source:  
IP : 0.0.0.0  
Mask : 0.0.0.0  
Interface : WLAN-BSS1/0/16  
VLAN : Any  
Protocol : TCP  
Destination:  
IP : 0.0.0.0  
Mask : 0.0.0.0  
Port : 80

Rule 5:

Type : Static  
Action : Deny  
Status : Active  
Source:  
IP : 0.0.0.0  
Mask : 0.0.0.0  
Interface : WLAN-BSS1/0/16  
VLAN : Any  
Destination:  
IP : 0.0.0.0  
Mask : 0.0.0.0

The output shows that the AP has portal filtering rules, indicating that the AP forwards client data traffic.

# 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 simple 12345678
    cipher-suite ccmp
    security-ie rsn
    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-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/portal
url-parameter wlanuserip source-address
#
```

- ```
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 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 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*

# INTELBRAS Access Controllers

## Local Forwarding Mode Direct 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 forwarding mode direct portal authentication..... | 1  |
| Network configuration.....                                                   | 1  |
| Analysis .....                                                               | 2  |
| Restrictions and guidelines .....                                            | 2  |
| Procedures .....                                                             | 2  |
| Configuring INC.....                                                         | 2  |
| Editing the AP configuration file.....                                       | 8  |
| Configuring the AC.....                                                      | 8  |
| Configuring the switch .....                                                 | 11 |
| Configuring the DHCP server .....                                            | 12 |
| Verifying the configuration .....                                            | 12 |
| Configuration files.....                                                     | 14 |
| Related documentation .....                                                  | 16 |

# Introduction

The following information provides an example of configuring direct portal authentication in a wireless network where APs directly forward client traffic.

## 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.

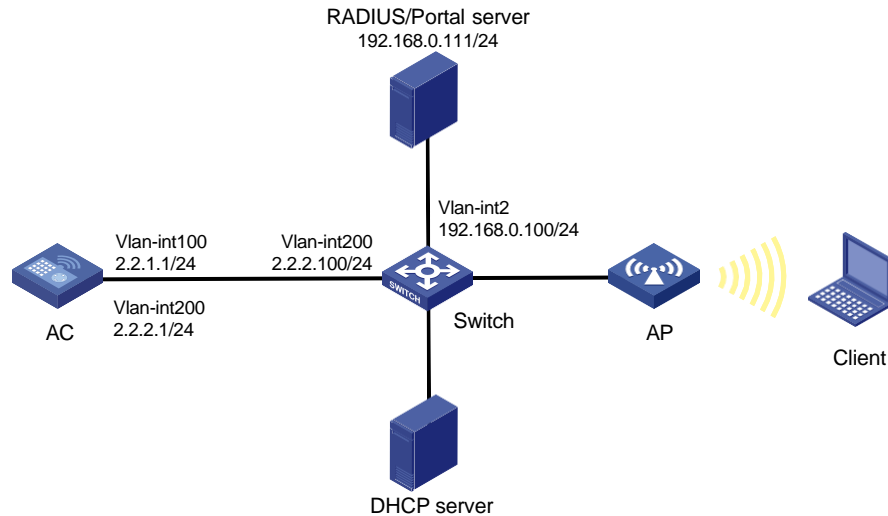
## Example: Configuring local forwarding mode direct portal authentication

### Network configuration

As shown in [Figure 1](#):

- The AP and the client obtain IP addresses from the DHCP server.
- The AP and the AC use VLAN 100 to establish CAPWAP tunnels, and the client uses VLAN 200 to access the wireless network.
- The AP directly forwards traffic of the client.
- The INC server acts as the portal authentication server, portal Web server, and RADIUS server.
- The AC performs direct portal authentication on clients. Before passing portal authentication, the client can access only the portal Web server. After passing portal authentication, the client can access other network resources.
- The client user can access network resources on any Layer 2 ports in its access VLAN without re-authentication.
- The INC server can dynamically change authorization information for the user and can log out the user.

**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 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.

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

To add GigabitEthernet 1/0/1 of the AP to the local forwarding VLAN (VLAN 200), edit the AP's configuration file and upload it to the AC's storage medium.

## 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 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 **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.
  - 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 *          | radius          | Confirm Shared Key * | radius             |
| 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 **Add Access Policy** page.
  - c. Enter the policy name.
  - d. Select the service group.

This example uses the default service 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 \*

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. Set the user. If the user exists, click **Select** to select the existing user. If the user does not exist, 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**

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

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. Log in to INC and click the **User** tab.
  - b. From the navigation tree, select **User Access Policy > Portal Service > Server**.
  - c. Configure the portal server parameters.  
This example uses the default settings.
  - d. 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 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.
  - 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**.
  - b. Click **Add** to open the **Add Device** page.
  - c. Enter the device name **NAS**.
  - d. Select **CMCC 1.0** from the **Version** list.
  - e. Enter the IP address of the AC's interface connected to the client.
  - f. Select whether to support 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 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. In the device list on the portal device configuration page, click the **Port Group Information Management** icon in the **Operation** row 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.

The port group configuration page opens, as shown in Figure 10.

**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

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

## 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. 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 CAPWAP tunnels with APs.

```
<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, 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:

```
[AC] ip route-static 192.168.0.0 255.255.255.0 2.2.2.100
```

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
```

# 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
```

# 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
```

```
[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 the RADIUS scheme:

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

```
<AC> system-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 192.168.0.111
```

```
[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 of 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
```

# Enable the RADIUS DAE server feature and enter RADIUS DAE server view.

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

# Configure the IP address of the RADIUS DAE client as 192.168.0.111, and the shared key for secure communication with the client as **radius**.

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

## 6. 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
```

## 7. Configure portal authentication:

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

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

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

```
[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 the server's URL as **http://192.168.0.111:8080/portal**.

```
[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. (These 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
```

# 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 portal-free rules to allow users to access the DNS server without
authentication.
[AC] portal free-rule 1 destination ip any udp 53
[AC] portal free-rule 2 destination ip any tcp 53
# 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
# 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 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 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. This VLAN is 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 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 a trunk port. Assign the trunk port to VLAN 100 and VLAN 200. Set the PVID of the trunk 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 the port.**

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

**# Create VLAN-interface 200 and assign it an IP address.**

```
[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 it an IP address.**

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

## Configuring the DHCP server

Configure required settings on the DHCP server. (Details not shown.)

## 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 the online portal user information on the AC.**

```
[AC] display portal user all
Total portal users: 1
Username: Client
  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 client successfully passes portal authentication and comes online.

**# Display portal filtering rules on the AC and the AP.**

[AC] display portal rule all ap ap1  
Slot 1:  
[AP] display portal rule all

IPv4 portal rules on WLAN-BSS1/0/16:

Rule 1:

|              |                   |
|--------------|-------------------|
| Type         | : Static          |
| Action       | : Permit          |
| Protocol     | : Any             |
| Status       | : Active          |
| Source:      |                   |
| IP           | : 0.0.0.0         |
| Mask         | : 0.0.0.0         |
| Port         | : Any             |
| MAC          | : 0000-0000-0000  |
| Interface    | : WLAN-BSS1/0/16  |
| VLAN         | : Any             |
| Destination: |                   |
| IP           | : 192.168.0.111   |
| Mask         | : 255.255.255.255 |
| Port         | : Any             |

Rule 2:

|           |                  |
|-----------|------------------|
| Type      | : Dynamic        |
| Action    | : Permit         |
| Status    | : Active         |
| Source:   |                  |
| IP        | : 2.2.2.2        |
| MAC       | : 0021-6330-0933 |
| Interface | : WLAN-BSS1/0/16 |
| VLAN      | : Any            |

Rule 3:

|              |                  |
|--------------|------------------|
| Type         | : Static         |
| Action       | : Redirect       |
| Status       | : Active         |
| Source:      |                  |
| IP           | : 0.0.0.0        |
| Mask         | : 0.0.0.0        |
| Interface    | : WLAN-BSS1/0/16 |
| VLAN         | : Any            |
| Protocol     | : TCP            |
| Destination: |                  |
| IP           | : 0.0.0.0        |
| Mask         | : 0.0.0.0        |
| Port         | : 443            |

Rule 4:

```

Type           : Static
Action          : Redirect
Status          : Active
Source:
  IP            : 0.0.0.0
  Mask          : 0.0.0.0
  Interface     : WLAN-BSS1/0/16
  VLAN          : Any
  Protocol      : TCP
Destination:
  IP            : 0.0.0.0
  Mask          : 0.0.0.0
  Port          : 80

Rule 5:
Type           : Static
Action          : Deny
Status          : Active
Source:
  IP            : 0.0.0.0
  Mask          : 0.0.0.0
  Interface     : WLAN-BSS1/0/16
  VLAN          : Any
Destination:
  IP            : 0.0.0.0
  Mask          : 0.0.0.0

```

The output shows that the AC does not have portal filtering rules for the AP and the AP has the portal filtering rules. This is because the local forwarding mode is used.

## 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 simple 12345678
  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$3$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 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-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$3$AkTEB7OgMYnCqsfDeplhoAgXUek/rVrLZw==
  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 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*

# INTELBRAS Access Controllers

## Local Forwarding Mode Direct 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 forwarding mode direct IPv6 portal authentication<br>..... | 1  |
| Network configuration.....                                                            | 1  |
| Analysis .....                                                                        | 2  |
| Restrictions and guidelines .....                                                     | 2  |
| Procedures .....                                                                      | 2  |
| Configuring INC.....                                                                  | 2  |
| Editing the AP configuration file.....                                                | 8  |
| Configuring the AC.....                                                               | 8  |
| Configuring the switch .....                                                          | 11 |
| Configuring the DHCPv6 server .....                                                   | 12 |
| Verifying the configuration .....                                                     | 12 |
| Configuration files.....                                                              | 14 |
| Related documentation .....                                                           | 16 |



# Introduction

The following information provides examples for configuring direct IPv6 portal authentication in a wireless network where APs directly forward client traffic.

## 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.

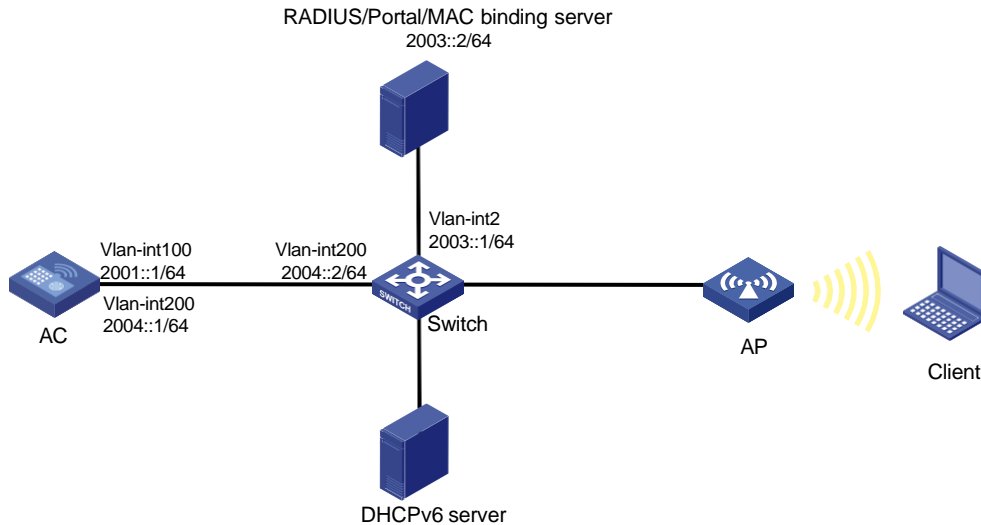
## Example: Configuring local forwarding mode direct IPv6 portal authentication

### Network configuration

As shown in [Figure 1](#):

- The AP and the client obtain IPv6 addresses from the DHCPv6 server.
- The AP and the AC use VLAN 100 to establish CAPWAP tunnels, and the client uses VLAN 200 to access the wireless network.
- The AP directly forwards traffic of the client.
- The INC server acts as the portal authentication server, portal Web server, and RADIUS server.
- The AC performs direct IPv6 portal authentication on clients. Before passing IPv6 portal authentication, the client can access only the portal Web server. After passing IPv6 portal authentication, the client can access other network resources.
- The client user can access network resources on any Layer 2 ports in its access VLAN without re-authentication.
- The INC server can dynamically change authorization information for the user and can log out the user.

**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 the portal roaming feature.

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

To add GigabitEthernet 1/0/1 of the AP to the local forwarding VLAN (VLAN 200), edit the AP's configuration file and upload it to the AC's storage medium.

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.

Configure DNS if necessary. In this example, DNS is not required.

## Restrictions and guidelines

When you configure direct portal authentication, follow these 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.
- 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(E0303), INC INC - EIA 7.1(E0304), and INC EIP 7.1(E0304).

#### 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. 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 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**

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 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. 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, select the access policy configured in the previous step as the default access policy, and use the default settings for other parameters.
  - d. 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 from the **User Name** list or click **Add User** to add a new user.

- d. Enter the account name.
- e. Enter and confirm the password.
- f. Use the default settings for other parameters.
- g. Click **OK**.

**Figure 5 Adding an access user**

The screenshot shows the 'Add Access User' configuration page. The breadcrumb trail is 'User > All Access Users > Add Access User'. The page title is 'Access account'. Under the 'Access Information' section, there are several fields and checkboxes:

- User Name \***: A text box containing 'Client1' with a 'Select' button and an 'Add User' button.
- Account Name \***: A text box containing 'Client'.
- Trial Account**: ☐
- Default BYOD User**: ☐
- MAC Authentication User**: ☐
- Computer User**: ☐
- Fast Access User**: ☐
- Password \***: A text box with masked characters '\*\*\*\*\*'.
- Confirm Password \***: A text box with masked characters '\*\*\*\*\*'.
- Allow User to Change Password**: ☒
- Enable Password Strategy**: ☐
- Modify Password at Next Login**: ☐
- Inspiration Time**: A text box with a calendar icon.
- Expiration Time**: A text box with a calendar icon.
- Max. Idle Time(Minutes)**: A text box.
- Max. Concurrent Logins**: A text box containing '1'.
- Max. Transparent Portal Bindings**: A dropdown menu showing '1'.
- Login Message**: A text box.

## Configuring the portal server

1. Configure the portal authentication service:
  - a. Log in to INC and click the **User** tab.
  - b. From the navigation tree, select **User Access Policy > Portal Service > Server**.
  - c. Configure the portal server parameters.  
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 trail is 'User > User Access Policy > Portal Service > Server'. The page title is 'Portal Server'. Under the 'Basic Information' section, there is a 'Log Level' dropdown menu set to 'Info'. Under the 'Portal Server' section, there are several fields:

- Request Timeout(Seconds) \***: A text box containing '4' with a help icon.
- Server Heartbeat Interval(Seconds) \***: A text box containing '20' with a help icon.
- User Heartbeat Interval(Minutes) \***: A text box containing '5' with a help icon.
- LB Device Address**: A text box.
- LB Device IPv6 Address**: A text box.

Under the 'Portal Web' section, there are several fields:

- Request Timeout(Seconds) \***: A text box containing '15' with a help icon.
- Packet Code**: A text box with a help icon.
- Verify Endpoint Requests**: A dropdown menu set to 'Yes'.
- Use Cache**: A dropdown menu set to 'Yes'.
- HTTP Heartbeat Display**: A dropdown menu set to 'New Page'.
- HTTPS Heartbeat Display**: A dropdown menu set to 'Original Page'.
- Portal Page**: A text box containing a list of 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 an IP group:

- a. From the navigation tree, select **User Access Policy > Portal Service > IP Group** to open the portal IP group configuration page.
- b. Click **Add** to open the **Add IP Group** page.
- c. Enter the IP group name.
- d. Select **Yes** from the **IPv6** field.
- 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. Click **OK**.

**Figure 7 Adding an IP group**

3. Add a portal device:
  - a. Select **User Access Policy > Portal Service > Device** from the navigation tree to open the portal device configuration page.
  - b. Click **Add** to open the **Add Device** page.
  - c. Enter the device name.
  - d. Select **Portal 3.0** from the **Version** list.
  - e. Enter the IP address of the AC's interface connected to the client.
  - f. Select whether to support 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 8 Adding a 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 the portal device with the IP group:
  - a. In the device list on the portal device configuration page, 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 | IPv6 Address | Last Deployed at | Deploy Result | Operation |
|-------------|------------|---------------|------------|--------------|------------------|---------------|-----------|
| NAS         | Portal 3.0 | Ungrouped     |            | 2004:1       |                  | Not Deployed  |           |

1-1 of 1, Page 1 of 1

The port group configuration page opens.

**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 *             | 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

- b. Click **Add** to open the **Add Port Group** page as shown in [Figure 11](#).
  - c. Enter the port group name.
  - d. Select the configured IP group.

The IP address used by the user to access the network must be within this IP group.
  - e. Use the default settings for other parameters.
  - f. Click **OK**.

**Figure 11 Adding a port group**

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

Add Port Group

|                               |               |                                    |             |
|-------------------------------|---------------|------------------------------------|-------------|
| Port Group Name *             | 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 > Validate** to commit the configuration changes.

## 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

- Configuring VLANs and interfaces:

# Create VLAN 100 and VLAN-interface 100. Assign the VLAN interface an IPv6 address. The AC will establish CAPWAP tunnels with APs in this VLAN.

```
<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 M flag to 1 and the O flag to 1 in RA advertisements to be sent on VLAN-interface 100.

```
[AC-Vlan-interface100] ipv6 nd autoconfig managed-address-flag
[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 M flag to 1 and the O flag to 1 in RA advertisements to be sent on VLAN-interface 200.**

```
[AC-Vlan-interface200] ipv6 nd autoconfig managed-address-flag
[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, 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:

```
[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
```

**# Enable snooping DHCPv6 and ND packets.**

```
[AC-wlan-st-st1] client ipv6-snooping dhcpv6-learning enable
[AC-wlan-st-st1] client ipv6-snooping nd-learning enable
```

**# 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
```

**# 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
[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 the RADIUS scheme:

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

```
<AC> system-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 ipv6 2003::2
```

```
[AC-radius-rs1] primary accounting ipv6 2003::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 2001::1 as the source IPv6 address of outgoing RADIUS packets.**

```
[AC-radius-rs1] nas-ip ipv6 2001::1
```

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

**# Enable the RADIUS session-control feature.**

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

**# Enable the RADIUS DAE server feature and enter RADIUS DAE server view.**

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

**# Specify a RADIUS DAE client at IPv6 address 2003::2 and configure the shared key for secure communication with the client as **radius**.**

```
[AC-radius-da-server] client ipv6 2003::2 key simple radius
```

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

## 6. Configure the 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. 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** and specify the server's IPv6 address as **2003::2**.

```
[AC] portal server newpt
[AC-portal-server-newpt] ipv6 2003::2 key simple 123456
[AC-portal-server-newpt] quit
```

# Create a portal Web server named **newpt** and specify the server's URL as **http://[2003::2]:8080/portal**.

```
[AC] portal web-server newpt
[AC-portal-websvr-newpt] 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 IPv6 address, and the AC's name.

```
[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 the portal roaming feature.

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

# Configure two portal-free rules to allow users to access the DNS server without authentication.

```
[AC] portal free-rule 1 destination ip any udp 53
[AC] portal free-rule 2 destination ip any tcp 53
```

# Configure a portal-free rule. Set the rule number to 3 and the source interface to aggregate interface 1. This rule allows users on the aggregate interface to access the network resources without authentication.

```
[AC] portal free-rule 3 source interface Bridge-Aggregation1
```

# Enable direct IPv6 portal authentication on service template **st1**.

```
[AC] wlan service-template st1
[AC-wlan-st-st1] portal ipv6 enable method direct
```

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

```
[AC-wlan-st-st1] portal ipv6 domain dm1
```

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

```
[AC-wlan-st-st1] portal ipv6 apply web-server newpt
```

# Enable portal to support IPv4/IPv6 dual stack on service template **st1**.

```
[AC-wlan-st-st1] portal dual-stack enable
```

# Configure the BAS-IPv6 attribute as 2001::1.

```
[AC-wlan-st-st1] portal bas-ipv6 2001::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 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. This VLAN is 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 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 a trunk port. Assign the trunk
port to VLAN 100 and VLAN 200. Set the PVID of the trunk port to 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 port.
[Switch-GigabitEthernet1/0/2] poe enable
[Switch-GigabitEthernet1/0/2] quit
# Create VLAN-interface 200 and assign it an IPv6 address.
[Switch] interface vlan-interface 200
[Switch-Vlan-interface200] ipv6 address 2004::2 64
[Switch-Vlan-interface200] quit
# Create VLAN-interface 2 and assign it an IPv6 address.
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] ipv6 address 2003::1 64
[Switch-Vlan-interface2] quit
```

## Configuring the DHCPv6 server

Configure required settings on the DHCPv6 server. (Details not shown.)

## 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://\[2003::2\]:8080/portal](http://[2003::2]:8080/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: ap1
  Radio ID: 2
  SSID: service
  Portal server: newpt
  State: Online
```

```

VPN instance: N/A
MAC           IP           VLAN   Interface
0021-6330-0933 2004::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 client successfully passes portal authentication and comes online.

#### # Display portal filtering rules on the AC and the AP.

```

[AC] display portal rule all ap ap1
Slot 1:
[AP] display portal rule all

```

IPv6 portal rules on WLAN-BSS1/0/16:

```

Rule 1:
  Type           : Static
  Action          : Permit
  Protocol        : Any
  Status          : Active
  Source:
    IP            : ::
    Prefix length : 0
    Port          : Any
    MAC           : 0000-0000-0000
    Interface     : WLAN-BSS1/0/16
    VLAN          : Any
  Destination:
    IP            : 2003::2
    Prefix length : 128
    Port          : Any

```

```

Rule 2:
  Type           : Dynamic
  Action          : Permit
  Status          : Active
  Source:
    IP            : 2004::2
    MAC           : 0021-6330-0933
    Interface     : WLAN-BSS1/0/16
    VLAN          : Any

```

The output shows that the AC does not have portal filtering rules for the AP and the AP has the portal filtering rules. This is because the local forwarding mode is used.

# 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 simple 12345678
  cipher-suite ccmp
  security-ie rsn
  client ipv6-snooping nd-learning enable
  client ipv6-snooping dhcpv6-learning enable
  portal ipv6 enable method direct
  portal ipv6 domain dml
  portal bas-ipv6 2001::1
  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 1 100 200
#
  ipv6 route-static 2003:: 64 2004::2
#
  radius session-control enable
#
radius scheme rs1
  primary authentication ipv6 2003::2
  primary accounting ipv6 2003::2
```

```

key authentication cipher $c$3$Sggqz7lDs4XPnethmAgyAKVlke7qwEkYbQ==
key accounting cipher $c$3$4J/JBRGwqB4F2l3furJmKB6JWYXBFjWE6g==
user-name-format without-domain
nas-ip ipv6 2001::1
#
radius dynamic-author server
  client ip ipv6 2003::2 key cipher $c$3$AkTEB7OgMYnCqsfDeplhoAgXUek/rVrLZw==
#
domain dml
  authorization-attribute idle-cut 15 1024
  authentication portal radius-scheme rs1
  authorization portal radius-scheme rs1
  accounting portal none
#
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 newpt
  url http://[2003::2]:8080/portal
  url-parameter ssid ssid
  url-parameter wlanacname value AC
  url-parameter wlanuserip source-address
#
portal server newpt
  ipv6 2003::2 key cipher $c$3$wulCg6I4PTcPTgPeKRF/7w9jIqIEq2xlTw==
#
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

```



```
    ipv6 address 2003::1 64
#
interface Vlan-interface200
    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 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*

# INTELBRAS Access Controllers

## Local Forwarding 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 ..... | 1 |
| Network configuration .....                 | 1 |
| Restrictions and guidelines .....           | 1 |
| Procedures .....                            | 2 |
| Configuring the configuration file .....    | 2 |
| Configuring the AC .....                    | 2 |
| Configuring the switch .....                | 3 |
| Verifying the configuration .....           | 4 |
| Configuration files .....                   | 4 |
| Related documentation .....                 | 6 |

# Introduction

The following information provides an example for configuring WLAN local forwarding.

## 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.

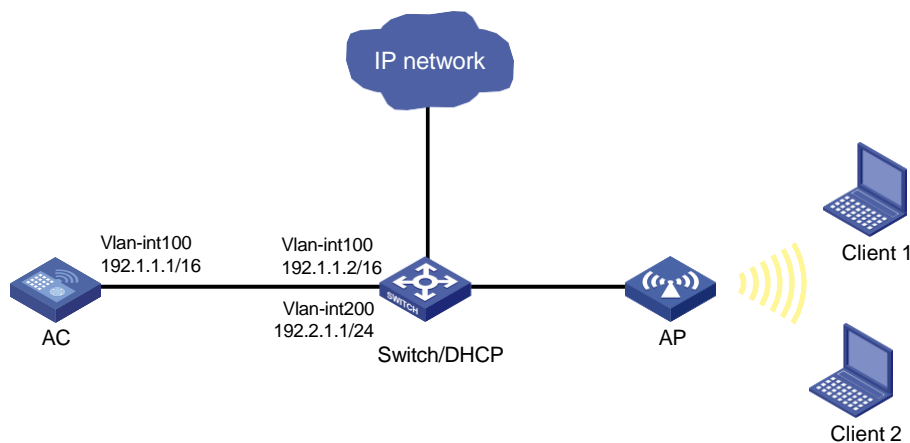
This document assumes that you have basic knowledge of WLAN local forwarding.

## Example: Configuring local forwarding

### Network configuration

As shown in [Figure 1](#), the switch acts as a DHCP server to assign IP addresses to the AP and the clients. The AP establishes CAPWAP tunnels with the AC in VLAN 100 and clients use VLAN 200 to access the WLAN. Configure local forwarding on the AC to enable the AP to forward client traffic.

**Figure 1 Network diagram**



## Restrictions and guidelines

When you configure WLAN local forwarding, follow these restrictions and guidelines:

- Make sure there is no Tab or space at the end of the **map-configuration** command.
- Use the serial ID labeled on the AP's rear panel to specify an AP.
- If a backup AC is available, make sure the map-configuration file has been upgraded to the backup AC.

# Procedures

## Configuring the configuration file

# Create a .txt file named **apcfg.txt** and enter the following content:

```
system-view
vlan 200
quit
interface GigabitEthernet 1/0/1
port link-type trunk
port trunk permit vlan 200
```

# Upload the file to the AC.

## Configuring the AC

### 1. Configure AC interfaces:

# 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 192.1.1.1 16
[AC-Vlan-interface100] quit
```

# Configure GigabitEthernet1/0/1 that connects the AC to the switch as a trunk port, and assign the port to VLAN 100.

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

### 2. Configure wireless services:

# Create service template 1 and enter its view.

```
[AC] wlan service-template 1
```

# Configure the SSID as **service**.

```
[AC-wlan-st-1] ssid service
```

# Set the PSK AKM mode and specify plaintext string **12345678** as the preshared key.

```
[AC-wlan-st-1] akm mode psk
[AC-wlan-st-1] preshared-key pass-phrase simple 12345678
```

# Set the CCMP cipher suite and enable RSN security IE.

```
[AC-wlan-st-1] cipher-suite ccmp
[AC-wlan-st-1] security-ie rsn
```

# Enable local forwarding.

```
[AC-wlan-st-1] client forwarding-location ap
```

# Enable the service template.

```
[AC-wlan-st-1] service-template enable
[AC-wlan-st-1] quit
```

### 3. Configure the AP:

---

**NOTE:**

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

---

# Create manual AP **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 add the AP to the AP group.

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

# Bind service template 1 and VLAN 200 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 1 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
```

4. Deploy configuration file **apcfg.txt** to AP **officeap**.

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

## Configuring the switch

1. Configure switch interfaces:

# Create VLAN 100 and VLAN-interface 100, and assign an IP address to the VLAN interface. The switch will use VLAN 100 to forward 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 VLAN 200 to forward client traffic.

```
[Switch] vlan 200
[Switch-vlan200] quit
[Switch] interface vlan-interface 200
[Switch-Vlan-interface200] ip address 192.2.1.1 24
[Switch-Vlan-interface200] quit
```

# Configure GigabitEthernet 1/0/1 that connects the switch to the AC as a trunk port, and assign the port to VLAN 100.

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

# Configure GigabitEthernet 1/0/2 that connects the switch to the AP as a trunk port, remove the port from VLAN 1, set the PVID to VLAN 100, and assign the port to VLANs 100 and 200.

```
[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 100 200
[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
```

## 2. Configure DHCP:

# Enable DHCP.

```
[Switch] dhcp enable
```

# Create DHCP address pool **vlan100** to assign an IP address to the AP, and specify subnet 192.1.0.0/16 in the DHCP address pool.

```
[Switch] dhcp server ip-pool vlan100
[Switch-dhcp-pool-vlan100] network 192.1.0.0 mask 255.255.0.0
```

# Exclude IP address 192.1.1.1 from dynamic allocation in the address pool.

```
[Switch-dhcp-pool-vlan100] forbidden-ip 192.1.1.1
```

# Specify the gateway address as 192.1.1.2 in the DHCP address pool.

```
[Switch-dhcp-pool-vlan100] gateway-list 192.1.1.2
```

```
[Switch-dhcp-pool-vlan100] quit
```

# Create DHCP address pool **vlan200** to assign IP addresses to clients, and specify subnet 192.2.1.0/24 in the DHCP address pool.

```
[Switch] dhcp server ip-pool vlan200
[Switch-dhcp-pool-vlan200] network 192.2.1.0 mask 255.255.255.0
```

# Specify the gateway address as 192.2.1.1 and specify the DNS server address in the DHCP address pool. In this example, the gateway also acts as a DNS server.

```
[Switch-dhcp-pool-vlan200] gateway-list 192.2.1.1
```

```
[Switch-dhcp-pool-vlan200] dns-list 192.2.1.1
```

```
[Switch-dhcp-pool-vlan200] quit
```

# Verifying the configuration

# Ping Client 1 on Client 2 and ping Client 2 on Client 1.

# Capture packets and verify that client traffic is forwarded by the AP.

**Figure 2 ICMP packets from clients**

| No. | Time      | Source      | Destination   | Protocol | Length | Info                                                                        |
|-----|-----------|-------------|---------------|----------|--------|-----------------------------------------------------------------------------|
| 20  | 1.2460000 | 100.1.1.2   | 100.1.1.4     | OpenFlc  | 78     | Type: OFPT_ECHO_REPLY                                                       |
| 21  | 1.2461840 | 100.1.1.4   | 100.1.1.2     | TCP      | 66     | 34823->6633 [ACK] Seq=9 Ack=9 Win=8325 Len=0 TSval=70705140 TSecr=89318666  |
| 22  | 1.3657260 | 160.1.1.100 | 160.1.255.255 | NBNS     | 92     | Name query NB ISATAP<00>                                                    |
| 23  | 1.3657800 | 160.1.1.100 | 160.1.255.255 | NBNS     | 96     | Name query NB ISATAP<00>                                                    |
| 24  | 1.3667740 | 100.1.3.3   | 100.1.3.255   | NBNS     | 96     | Name query NB ISATAP<00>                                                    |
| 25  | 1.5311010 | 100.1.1.4   | 100.1.1.2     | CAPWAP   | 72     | CAPWAP-Data Keep-Alive                                                      |
| 26  | 1.5319030 | 100.1.1.2   | 100.1.1.4     | CAPWAP   | 76     | CAPWAP-Data Keep-Alive                                                      |
| 27  | 2.0907940 | 192.2.1.3   | 192.2.1.4     | ICMP     | 78     | Echo (ping) request id=0x0001, seq=4245/38160, ttl=128 (no response found!) |
| 28  | 2.0908940 | 192.2.1.4   | 192.2.1.3     | ICMP     | 78     | Echo (ping) reply id=0x0001, seq=4245/38160, ttl=128 (request in 27)        |
| 29  | 2.1156650 | 160.1.1.100 | 160.1.255.255 | NBNS     | 92     | Name query NB ISATAP<00>                                                    |
| 30  | 2.1157930 | 160.1.1.100 | 160.1.255.255 | NBNS     | 96     | Name query NB ISATAP<00>                                                    |
| 31  | 2.1819120 | 100.1.3.3   | 100.1.3.255   | NBNS     | 96     | Name query NB ISATAP<00>                                                    |

Frame 27: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface 0  
 Ethernet II, Src: Azurewaw\_4c:b5:59 (6c:71:d9:4c:b5:59), Dst: D-LinkCo\_b1:69:ae (5c:d9:98:b1:69:ae)  
 802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 300  
 Internet Protocol Version 4, Src: 100.1.3.3 (100.1.3.3), Dst: 100.1.3.5 (100.1.3.5)  
 Internet Control Message Protocol

# Configuration files

- AC:

```

#
Vlan 100
#
wlan service-template 1
    ssid service
    client forwarding-location ap
    akm mode psk
    preshared-key pass-phrase cipher $c$3$N//5BVbsOqdBTxi+7MJZKT6Zqh5MAMys2ZzM
    cipher-suite ccmp
    security-ie rsn
    service-template enable
#
interface Vlan-interface100
    ip address 192.1.1.1 255.255.0.0
#
interface GigabitEthernet1/0/1
    port link-type trunk
    port trunk permit vlan 1 100
#
wlan ap-group group1
    ap officeap
    ap-model AP 3620
    radio 2
        radio enable
        service-template 1 vlan 200
        map-configuration flash:/apcfg.txt
#
wlan ap officeap model AP 3620
    serial-id 219801A28N819CE0002T
#

```

- **Switch:**

```

#
    dhcp enable
#
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 192.2.1.1
    network 192.2.1.0 mask 255.255.255.0
    dns-list 192.2.1.1
#

```



```
interface Vlan-interface100
 ip address 192.1.1.2 255.255.0.0
#
interface Vlan-interface200
 ip address 192.2.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 100
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100 200
 port trunk pvid vlan 100
#
```

## Related documentation

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

# INTELBRAS Access Controllers

## Wired Port Local Forwarding through Wireless Terminator

### 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 wired port local forwarding through WT ..... | 1 |
| Network requirements .....                                        | 1 |
| Configuration procedures .....                                    | 1 |
| Configuring the AC .....                                          | 1 |
| Verifying the configuration .....                                 | 3 |

# Introduction

The following information provides a wired port local forwarding through wireless terminator (WT) configuration example.

## 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.

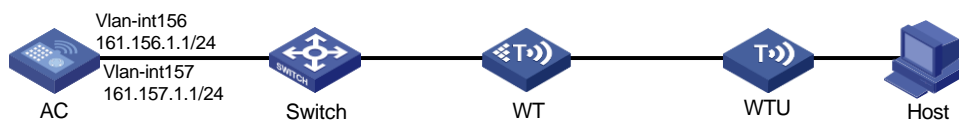
The following information is provided based on the assumption that you have basic knowledge of WLAN access, AP management, and DHCP.

## Example: Configuring wired port local forwarding through WT

### Network requirements

As shown in [Figure 1](#), the AC connects to the WT through the switch and the WT connects to the host through the wireless terminator unit (WTU). The AC acts as a DHCP server to assign IP addresses to the WT and host. The WTU runs in version 2 and supports wireless and wired connection.

**Figure 1 Network diagram**



## Configuration procedures

### Configuring the AC

#### 1. Configure AC interfaces:

# Create VLAN 156, and assign an IP address to VLAN-interface 156. The WT will use this address to establish CAPWAP tunnels with the AC.

```
<AC> system-view
[AC] vlan 156
[AC-vlan156] quit
[AC] interface vlan-interface 156
[AC-Vlan-interface156] ip address 161.156.1.1 24
[AC-Vlan-interface156] quit
```

# Create VLAN 157, and assign an IP address to VLAN-interface 157. The client will use this VLAN to access the WLAN.

```
[AC] vlan 157
[AC-vlan157] quit
[AC] interface vlan-interface 157
[AC-Vlan-interface157] ip address 161.157.1.1 24
[AC-Vlan-interface157] quit
```

# Configure GigabitEthernet 1/0/1 that connect the AC to the switch as a trunk port, and assign the port to VLANs 156 and 157.

```
[AC] interface gigabitethernet 1/0/1
[AC-GigabitEthernet1/0/1] port link-type trunk
[AC-GigabitEthernet1/0/1] port trunk permit vlan 156 157
[AC-GigabitEthernet1/0/1] quit
```

## 2. Configure DHCP:

# Enable DHCP.

```
<AC> system-view
[AC] dhcp enable
```

# Configure DHCP address pool **wt** and specify subnet 161.156.1.0/24 and gateway address 161.156.1.2 in the address pool.

```
[AC] dhcp server ip-pool wt
[AC-dhcp-pool-wt] network 161.156.1.0 mask 255.255.255.0
[AC-dhcp-pool-wt] gateway-list 161.156.1.2
[AC-dhcp-pool-wt] quit
```

# Configure DHCP address pool **host** and specify subnet 161.157.1.0/24 and gateway address 161.157.1.2 in the address pool.

```
[AC] dhcp server ip-pool host
[AC-dhcp-pool-host] network 161.157.1.0 mask 255.255.255.0
[AC-dhcp-pool-host] gateway-list 161.157.1.2
[AC-dhcp-pool-host] quit
```

## 3. Configure WT and WTU:

# Create an AP named **ap1** with model **WT1024-X-EI**, and set its serial ID to **219801A1ARC178000322**.

```
[AC] wlan ap ap1 model WT1024-X-EI
[AC-wlan-ap-ap1] serial-id 219801A1ARC178000322
[AC-wlan-ap-ap1] map-configuration map.txt
[AC-wlan-ap-ap1] quit
```

# Create an AP named **ap2** with model **WTU420H**, and set its serial ID to **219801A0WA916BQ20133**.

```
[AC] wlan ap ap2 model WTU420H
[AC-wlan-ap-ap2] serial-id 219801A0WA916BQ20133
[AC-wlan-ap-ap2] quit
```

## 4. Configure the switch:

# Create VLAN 156 and assign an IP address to VLAN-interface 156. The VLAN will be used to forward traffic in the CAPWAP tunnels between the AC and the WT.

```
<Switch> system-view
[Switch] vlan 156
[Switch-vlan156] quit
[Switch] interface vlan-interface 156
[Switch-Vlan-interface156] ip address 161.156.1.2 24
```

```
[Switch-Vlan-interface156] quit
```

**# Create VLAN 157 and assign an IP address to VLAN-interface 157. The VLAN will be used to forward client traffic.**

```
[Switch] vlan 157
```

```
[Switch-vlan157] quit
```

```
[Switch] interface vlan-interface 157
```

```
[Switch-Vlan-interface157] ip address 161.157.1.2 24
```

```
[Switch-Vlan-interface157] quit
```

**# Configure GigabitEthernet 1/0/1 that connects the switch to the AC as a trunk port, and assign the port to VLANs 156 and 157.**

```
[Switch] interface gigabitethernet 1/0/1
```

```
[Switch-GigabitEthernet1/0/1] port link-type trunk
```

```
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 156 157
```

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

**# Configure GigabitEthernet 1/0/2 that connects the switch to the WT as a trunk port, assign the port to VLANs 156 and 157, and set the PVID to 156.**

```
[Switch] interface gigabitethernet 1/0/2
```

```
[Switch-GigabitEthernet1/0/2] port link-type trunk
```

```
[Switch-GigabitEthernet1/0/2] port trunk permit vlan 156 157
```

```
[Switch-GigabitEthernet1/0/2] port trunk pvid vlan 156
```

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

#### 5. Edit the WT configuration file:

**# Edit the WT configuration file `map.txt` and upload it to the AC storage medium via FTP or TFTP. The content and format of the configuration file are as follows:**

```
vlan 157
```

```
interface Ten-GigabitEthernet 1/0/1
```

```
port link-type trunk
```

```
port trunk permit vlan 157
```

**# Enable WT preprovisioning to issue the settings to the WTU.**

```
slot 1
```

```
provision model WTU420H
```

```
interface range Ethernet 1/1/1 to Ethernet 1/1/4
```

```
port access vlan 157
```

## Verifying the configuration

**# Verify that you can see the following information:**

- The WT and WTU obtain the IP address of the AC through DHCP.
- The WT, WTU, and the AC have established a CAPWAP tunnel.
- The WT and WTU are in Run state.

```
[AC] display wlan ap all
```

```
Total number of APs: 2
```

```
Total number of connected APs: 2
```

```
Total number of connected manual APs: 2
```

```
Total number of connected auto APs: 0
```

```
Total number of connected common APs: 0
```

```
Total number of connected WTUs: 1
```

```
Total number of inside APs: 0
```

```

Maximum supported APs: 3072
Remaining APs: 3071
Total AP licenses: 640
Local AP licenses: 640
Server AP licenses: 0
Remaining Local AP licenses: 639.75
Sync AP licenses: 0

```

```

                                AP information
State : I = Idle,           J = Join,           JA = JoinAck,       IL = ImageLoad
        C = Config,        DC = DataCheck,    R = Run,           M = Master,       B = Backup

```

| AP name | APID | State | Model       | Serial ID            |
|---------|------|-------|-------------|----------------------|
| ap1     | 7    | R/M   | WT1024-X-EI | 219801A1ARC178000322 |
| ap2     | 145  | R/M   | WTU420H     | 219801A0WA916BQ20133 |

#### # On the AC, display the IP addresses assigned to the clients.

```

[AC] display dhcp server ip-in-use pool 157
IP address      Client identifier/      Lease expiration      Type
                  Hardware address
161.157.1.3     01f0-921c-ef67-49         Apr 10 15:16:57 2018  Auto(C)

```

#### # Verify that the AC and the WTU can reach each other.

```

[AC] ping 161.157.1.3
Ping 161.157.1.3 (161.157.1.3): 56 data bytes, press CTRL_C to break
56 bytes from 161.157.1.3: icmp_seq=0 ttl=128 time=1.883 ms
56 bytes from 161.157.1.3: icmp_seq=1 ttl=128 time=0.826 ms
56 bytes from 161.157.1.3: icmp_seq=2 ttl=128 time=0.846 ms
56 bytes from 161.157.1.3: icmp_seq=3 ttl=128 time=1.039 ms
56 bytes from 161.157.1.3: icmp_seq=4 ttl=128 time=1.046 ms

--- Ping statistics for 161.157.1.3 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 0.826/1.128/1.883/0.389 ms

```

# INTELBRAS Access Controllers

## Remote AP 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 .....              | 1 |
| Network configuration .....                       | 1 |
| Restrictions and guidelines .....                 | 1 |
| Procedures .....                                  | 2 |
| Configuring the AC .....                          | 2 |
| Configuring the switch .....                      | 3 |
| Configuring AP configuration file apcfg.txt ..... | 4 |
| Verifying the configuration .....                 | 4 |
| Configuration files .....                         | 4 |
| Related documentation .....                       | 6 |

# Introduction

The following information provides an example for configuring remote AP.

## 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.

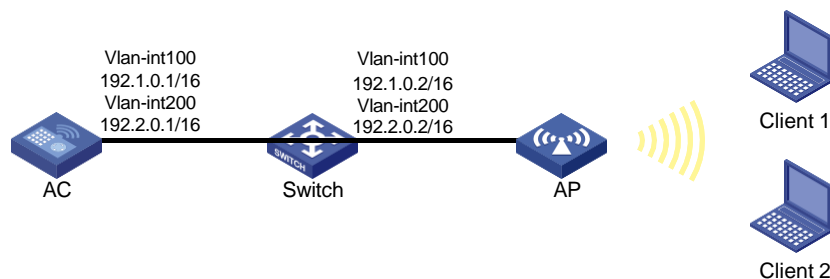
This document assumes that you have basic knowledge of remote AP.

## Example: Configuring remote AP

### Network configuration

As shown in [Figure 1](#), the switch acts as a DHCP server to assign IP addresses to the AP and the clients. Configure remote AP on the AC so that the AP can still provide services for clients when the tunnel between the AP and the AC is disconnected.

**Figure 1 Network diagram**



## Restrictions and guidelines

When you configure remote AP, follow these restrictions and guidelines:

- Use the actual serial ID of an AP to uniquely identify that AP.
- For also new clients to come online, make sure the clients are associated with and authenticated at APs. In this case, use simple text or PSK encryption as a best practice.
- Remote AP takes effect only on an AP that operates in local forwarding mode.
- For GigabitEthernet 1/0/1 on the AP to join VLAN 200, edit the AP configuration file, and upload it to the storage media of the AC.

# 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 APs.

```
<AC> system-view
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 192.1.0.1 16
[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 192.2.0.1 16
[AC-Vlan-interface200] quit
```

# Configure GigabitEthernet 1/0/1 that connects the AC and the switch as a trunk port, 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] port trunk permit vlan 100 200
[AC-GigabitEthernet1/0/1] quit
```

### 2. Configure wireless services:

# 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
```

# Set the PSK AKM mode and specify plaintext string **12345678** as the preshared key.

```
[AC-wlan-st-1] akm mode psk
[AC-wlan-st-1] preshared-key pass-phrase simple 12345678
```

# Set the CCMP cipher suite and enable RSN security IE.

```
[AC-wlan-st-1] cipher-suite ccmp
[AC-wlan-st-1] security-ie rsn
```

# Specify APs as the client traffic forwarder.

```
[AC-wlan-st-1] client forwarding-location ap
```

# To ensure that new clients can come online, enable client authentication and association on APs.

```
[AC-wlan-st-1] client-security authentication-location ap
[AC-wlan-st-1] client association-location ap
```

# Enable the service template.

```
[AC-wlan-st-1] service-template enable
[AC-wlan-st-1] quit
```

### 3. Configure the AP:

---

**NOTE:**

In a large-scale network, configure AP groups instead of single APs 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
```

# Create AP group **group1**, and add the AP to the AP group.

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

# Bind service template **1** and VLAN **200** 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 1 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
```

# Deploy configuration file **apcfg.txt** to the AP.

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

# Enable remote AP.

```
[AC-wlan-ap-group-group1] hybrid-remote-ap enable
[AC-wlan-ap-group-group1] quit
```

## 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 VLAN **100** to forward the traffic on the CAPWAP tunnel between the AC and AP.

```
<Switch> system-view
[Switch] vlan 100
[Switch-vlan100] quit
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ip address 192.1.0.2 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 VLAN **200** to forward client traffic.

```
[Switch] vlan 200
[Switch-vlan200] quit
[Switch] interface vlan-interface 200
[Switch-Vlan-interface200] ip address 192.2.0.2 16
[Switch-Vlan-interface200] quit
```

# Configure GigabitEthernet **1/0/1** that connects the switch and 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 that connects the switch and the AP as a trunk port, remove the port from VLAN 1, and assign the trunk port to VLANs 100 and 200.

```
[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 100 200
```

# Set the PVID of GigabitEthernet 1/0/2 to VLAN 100.

```
[Switch-GigabitEthernet1/0/2] port trunk pvid vlan 100
[Switch-GigabitEthernet1/0/2] quit
```

## 2. Configure DHCP services:

# Enable DHCP.

```
[Switch] dhcp enable
```

# Create a DHCP address pool named **vlan100** to assign an IP address to the AP.

```
[Switch] dhcp server ip-pool vlan100
```

# In DHCP address pool **vlan100**, specify subnet 192.1.0.0/16 for dynamic allocation, exclude 192.1.0.1 from dynamic allocation, and specify gateway IP address 192.1.0.2.

```
[Switch-dhcp-pool-vlan100] network 192.1.0.0 mask 255.255.0.0
[Switch-dhcp-pool-vlan100] forbidden-ip 192.1.0.1
[Switch-dhcp-pool-vlan100] gateway-list 192.1.0.2
[Switch-dhcp-pool-vlan100] quit
```

# Create a DHCP address pool named **vlan200** to assign IP address to clients.

```
[Switch] dhcp server ip-pool vlan200
```

# In DHCP address pool **vlan200**, specify subnet 192.2.0.0/16 for dynamic allocation, and exclude 192.2.0.1 from dynamic allocation. Specify gateway IP address 192.2.0.2, and specify the DNS server address. In this example, the gateway also acts as a DNS server.

```
[Switch-dhcp-pool-vlan200] network 192.2.0.0 mask 255.255.0.0
[Switch-dhcp-pool-vlan200] forbidden-ip 192.2.0.1
[Switch-dhcp-pool-vlan200] gateway-list 192.2.0.2
[Switch-dhcp-pool-vlan200] dns-list 192.2.0.2
[Switch-dhcp-pool-vlan200] quit
```

## Configuring AP configuration file apcfg.txt

# Copy the following text to a text file and upload the file to the AC.

```
system-view
vlan 200
interface GigabitEthernet 1/0/1
port link-type trunk
port trunk permit vlan 200
```

## Verifying the configuration

# Verify that clients remain online and the AP can still forward client traffic when the tunnel between the AP and the AC is disconnected. (Details not shown.)

## Configuration files

- AC:

```

#
vlan 100
#
vlan 200
#
wlan service-template 1
    ssid service
    client forwarding-location ap
    akm mode psk
    preshared-key pass-phrase cipher $c$3$N//5BVbsOqdBTxi+7MJZKT6Zqh5MAMys2ZzM
    cipher-suite ccmp
    security-ie rsn
    client-security authentication-location ap
    client association-location ap
    service-template enable
#
interface Vlan-interface100
    ip address 192.1.0.1 255.255.0.0
#
interface Vlan-interface200
    ip address 192.2.0.1 255.255.0.0
#
wlan ap-group group1
    hybrid-remote-ap enable
    ap officeap
    ap-model AP 3620
    radio 2
        radio enable
        service-template 1 vlan 200
        map-configuration flash:/apcfg.txt
#
wlan ap officeap model AP 3620
serial-id 219801A28N819CE0002T
    gigabitethernet 1
    gigabitethernet 2
#

```

- **apcfg.txt:**

```

system-view
vlan 200
quit
interface GigabitEthernet 1/0/1
port link-type trunk
port trunk permit vlan 200

```

- **Switch:**

```

#
dhcp enable
#
vlan 100

```

```

#
vlan 200
#
dhcp server ip-pool vlan100
    gateway-list 192.1.0.2
    network 192.1.0.0 mask 255.255.0.0
    forbidden-ip 192.1.0.1
#
dhcp server ip-pool vlan200
    gateway-list 192.2.0.2
    network 192.2.0.0 mask 255.255.0.0
    dns-list 192.2.0.2
    forbidden-ip 192.2.0.1
#
interface Vlan-interface100
    ip address 192.1.0.2 255.255.0.0
#
interface Vlan-interface200
    ip address 192.2.0.2 255.255.0.0
#
interface GigabitEthernet1/0/1
    port link-type trunk
    port trunk permit vlan 100 200
    port trunk pvid vlan 100
#
interface GigabitEthernet1/0/2
    port link-type trunk
    undo port trunk permit vlan 1
    port trunk permit vlan 100 200
    port trunk pvid vlan 100
#

```

## 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*
- *Network Connectivity Command Reference in INTELBRAS Access Controllers Command References*
- *Network Connectivity Configuration Guide in INTELBRAS Access Controllers Configuration Guides*

# INTELBRAS Access Controllers

## Downlink VLAN Management for Fit-Mode APs

### 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 downlink VLAN management for fit-mode APs ..... | 1 |
| Network configuration .....                                          | 1 |
| Analysis .....                                                       | 2 |
| Restrictions and guidelines .....                                    | 2 |
| Procedures .....                                                     | 2 |
| Configuring the AC .....                                             | 2 |
| Configuring the switch .....                                         | 4 |
| Verifying the configuration .....                                    | 6 |
| Configuration files .....                                            | 6 |
| Related documentation .....                                          | 8 |

# Introduction

The following information provides a downlink VLAN management configuration example for fit-mode APs.

## 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 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 AP management, radio management, WLAN access, VLAN, and local forwarding.

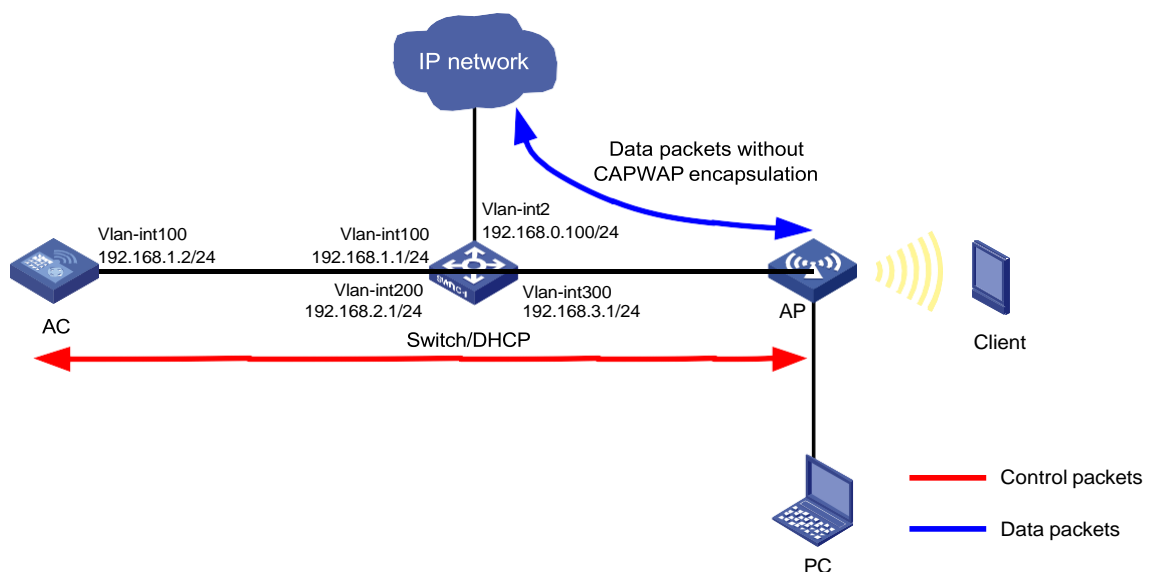
## Example: Configuring downlink VLAN management for fit-mode APs

### Network configuration

As shown in [Figure 1](#), the switch acts as the DHCP server to assign IP addresses to the AP, the client, and the PC. The AP and the AC use VLAN 100 to establish a CAPWAP tunnel, the client uses VLAN 200 to access the wireless network, and the PC uses VLAN 300 to access the wired network.

- Configure local forwarding on the AC for the AP to directly forward client traffic.
- Connect the PC to a downlink Ethernet interface on the AP and make sure the PC can visit the external network.

**Figure 1 Network diagram**



# Analysis

For the configuration to be deployed to the AP, configure remote configuration synchronization or deploy the map file.

## Restrictions and guidelines

- For configuration to be deployed correctly, do not attach Tab characters or spaces to the end of command lines in the map file.
- Use the actual AP model and serial ID to configure the AP.
- If a backup AC is configured, make sure the backup AC is also uploaded with the map file.

## Procedures

### Configuring the AC

1. Configure the interfaces of the AC:

# Create VLAN 100 and VLAN-interface 100, and assign an IP address to the 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 192.168.1.2 24
[AC-Vlan-interface100] quit
```

# Configure GigabitEthernet 1/0/1 that connects the AC to the switch as a trunk port, and assign the port to VLAN 100.

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

2. Configure a wireless service:

# Create service template 1 and enter its view.

```
[AC] wlan service-template 1
```

# Set the SSID to **service**.

```
[AC-wlan-st-1] ssid service
```

# Set the VLAN to VLAN 200.

```
[AC-wlan-st-1] vlan 200
```

# Specify PSK as the AKM mode and specify **12345678** as the plaintext key.

```
[AC-wlan-st-1] akm mode psk
[AC-wlan-st-1] preshared-key pass-phrase simple 12345678
```

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

```
[AC-wlan-st-1] cipher-suite ccmp
[AC-wlan-st-1] security-ie rsn
```

# Configure the AP to forward client data traffic.

```
[AC-wlan-st-1] client forwarding-location ap
```

# Enable the service template.

```
[AC-wlan-st-1] service-template enable
[AC-wlan-st-1] quit
```

### 3. Configure AP settings:

---

#### NOTE:

To simplify AP configuration on a large-scale network, configure AP settings on a per AP group basis as a best practice.

---

# Create manual AP **ap1**.

```
[AC] wlan ap ap1 model AP 3620H
```

# Specify the AP serial ID.

```
[AC-wlan-ap-ap1] serial-id 219801A28N819CE0002T
[AC-wlan-ap-ap1] quit
```

# Create AP group **group1** and configure **ap1** as the AP grouping rule.

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

# Bind service template 1 to radio 2 for AP group **group1**.

```
[AC-wlan-ap-group-group1] ap-model AP 3620H
[AC-wlan-ap-group-group1-ap-model-AP 3620H] radio 2
[AC-wlan-ap-group-group1-ap-model-AP 3620H-radio-2] service-template 1
```

# Enable radio 2.

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

### 4. To deploy configuration through remote configuration synchronization:

# Create VLANs 200 and 300 in AP group **group1**.

```
[AC-wlan-ap-group-group1] vlan 200
[AC-wlan-ap-group-group1-vlan200] quit
[AC-wlan-ap-group-group1] vlan 300
[AC-wlan-ap-group-group1-vlan300] quit
```

# Specify uplink Ethernet interface **GE1/0/1** that connects the AP to the switch as a trunk port, assign the port to all VLANs, set the PVID to 1, and disable port isolation.

```
[AC-wlan-ap-group-group1] ap-model AP 3620H
[AC-wlan-ap-group-group1-ap-model-AP 3620H] gigabitethernet 1
[AC-wlan-ap-group-group1-ap-model-AP 3620H-gigabitethernet-1] port-isolate
disable [AC-wlan-ap-group-group1-ap-model-AP 3620H-gigabitethernet-1] port link-
type trunk
[AC-wlan-ap-group-group1-ap-model-AP 3620H-gigabitethernet-1] port trunk permit
vlan all
[AC-wlan-ap-group-group1-ap-model-AP 3620H-gigabitethernet-1] port trunk pvid vlan
1 [AC-wlan-ap-group-group1-ap-model-AP 3620H-gigabitethernet-1] quit
```

# Specify all downlink Ethernet interfaces that connect the AP to the PC as access ports, assign the ports to VLAN 300, and disable port isolation. This step uses GE 1/0/2 as an example.

```
[AC-wlan-ap-group-group1-ap-model-AP 3620H] gigabitethernet 2
[AC-wlan-ap-group-group1-ap-model-AP 3620H-gigabitethernet-2] port-isolate
disable [AC-wlan-ap-group-group1-ap-model-AP 3620H-gigabitethernet-2] port access
vlan 300 [AC-wlan-ap-group-group1-ap-model-AP 3620H-gigabitethernet-2] quit
[AC-wlan-ap-group-group1-ap-model-AP 3620H] quit
```

# Enable remote configuration synchronization.

```
[AC-wlan-ap-group-group1] remote-configuration enable
```

# Synchronize the configuration to the AP.

```
[AC-wlan-ap-group-group1] remote-configuration synchronize
```

5. To deploy configuration through a map configuration file:

---

**NOTE:**

- Use a text editor to edit the content of the apcfg.txt file in the configuration order, and upload the file to the AC. After the AP associates with the AC, use the **map-configuration** command to deploy the file to the AP for the configuration to take effect on the AP.
  - Specify all downlink Ethernet interfaces that connect the AP to the PC as access ports, assign the ports to VLAN 300, and disable port isolation. This step uses GE 1/0/2 as an example.
- 

# Edit the apcfg.txt file.

```
system-view
vlan 200
quit
vlan 300
quit
interface GigabitEthernet 1/0/1
undo port-isolate enable
port link-type trunk
port trunk permit vlan all
quit
interface GigabitEthernet 1/0/2
undo port-isolate enable
port access vlan 300
quit
```

# Specify the AP configuration file as apcfg.txt in the AP group's AP model view.

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

## Configuring the switch

1. Configure switch interfaces:

# Create VLAN 2, VLAN 100, VLAN 200, VLAN 300, and the VLAN interfaces, and assign IP addresses to the VLAN interfaces. The switch will use VLAN 2 as the egress to the external network, VLAN 100 to forward packets between AC and AP, VLAN 200 to forward client traffic, and VLAN 300 for wired network access of the PC.

```
<Switch> system-view
[Switch] vlan 2
[Switch-vlan2] quit
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] ip address 192.168.0.100 24
[Switch-Vlan-interface2] quit
[Switch] vlan 100
[Switch-vlan100] quit
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ip address 192.168.1.1 24
```

```
[Switch-Vlan-interface100] quit
[Switch] vlan 200
[Switch-vlan200] quit
[Switch] interface vlan-interface 200
[Switch-Vlan-interface200] ip address 192.168.2.1 24
[Switch-Vlan-interface200] quit
[Switch] vlan 300
[Switch-vlan300] quit
[Switch] interface vlan-interface 300
[Switch-Vlan-interface300] ip address 192.168.3.1 24
[Switch-Vlan-interface300] quit
```

**# Specify GigabitEthernet 1/0/1 that connects the switch to the AC as a trunk port, and assign the port to VLAN 100.**

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

**# Specify GigabitEthernet 1/0/2 that connects the switch to the AP as a trunk port, assign the port to all VLANs, 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 all
[Switch-GigabitEthernet1/0/2] port trunk pvid vlan 100
```

**# Enable PoE on GigabitEthernet 1/0/2 that connects the switch to the AP.**

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

**# Specify GigabitEthernet 1/0/3 that connects the switch to the external network as an access port, and configure the port to permit traffic from 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
```

## 2. Configure DHCP:

**# Enable DHCP.**

```
[Switch] dhcp enable
```

**# Create DHCP address pool **vlan100** to assign an IP address to the AP, and specify subnet 192.168.1.0/24 in the DHCP address pool.**

```
[Switch] dhcp server ip-pool vlan100
[Switch-dhcp-pool-vlan100] network 192.168.1.0 mask 255.255.255.0
[Switch-dhcp-pool-vlan100] forbidden-ip 192.168.1.2
[Switch-dhcp-pool-vlan100] gateway-list 192.168.1.1
[Switch-dhcp-pool-vlan100] quit
```

**# Create DHCP address pool **vlan200** to assign an IP address to the client, specify subnet 192.168.2.0/24 in the DHCP address pool, and specify the gateway address as 192.168.2.1. Set the DNS server address according to the actual networking planning.**

```
[Switch] dhcp server ip-pool vlan200
[Switch-dhcp-pool-vlan200] network 192.168.2.0 mask 255.255.255.0
[Switch-dhcp-pool-vlan200] gateway-list 192.168.2.1
[Switch-dhcp-pool-vlan200] dns-list 192.168.2.1
```

```
[Switch-dhcp-pool-vlan200] quit
```

# Create DHCP address pool **vlan300** to assign an IP address to the PC, specify subnet 192.168.3.0/24 in the DHCP address pool, and specify the gateway address as 192.168.3.1. Set the DNS server address according to the actual networking planning.

```
[Switch] dhcp server ip-pool vlan300
```

```
[Switch-dhcp-pool-vlan300] network 192.168.3.0 mask 255.255.255.0
```

```
[Switch-dhcp-pool-vlan300] gateway-list 192.168.3.1
```

```
[Switch-dhcp-pool-vlan300] dns-list 192.168.3.1
```

```
[Switch-dhcp-pool-vlan300] quit
```

3. Configure default routes for the switch to visit the external IP network. (Details not shown.)

## Verifying the configuration

# Verify that the IP address of the client is 192.168.2.2, the IP address of the PC is 192.168.3.2, and both the client and the PC can visit the external network.

## Configuration files

- AC:

```
#
```

```
Vlan 100
```

```
#
```

```
wlan service-template 1
```

```
ssid service
```

```
vlan 200
```

```
client forwarding-location ap
```

```
akm mode psk
```

```
preshared-key pass-phrase cipher $c$3$N//5BVbsOqdBTxi+7MJZKT6Zqh5MAMys2ZzM
```

```
cipher-suite ccmp
```

```
security-ie rsn
```

```
service-template enable
```

```
#
```

```
interface Vlan-interface100
```

```
ip address 192.168.1.2 255.255.255.0
```

```
#
```

```
interface GigabitEthernet1/0/1
```

```
port link-type trunk
```

```
port trunk permit vlan 1 100
```

```
#
```

```
wlan ap-group group1
```

```
ap ap1
```

```
ap-model AP 3620H
```

```
map-configuration flash:/apcfg.txt
```

```
radio 1
```

```
radio 2
```

```
radio enable
```

```
service-template 1
```

```
#
```

```

wlan ap ap1 model AP 3620H
    serial-id 219801A28N819CE0002T
#
• Switch:
#
    dhcp enable
#
vlan 2
#
vlan 100
#
vlan 200
#
vlan 300
#
dhcp server ip-pool vlan100
    gateway-list 192.168.1.1
    network 192.168.1.0 mask 255.255.255.0
    forbidden-ip 192.168.1.2
#
dhcp server ip-pool vlan200
    gateway-list 192.168.2.1
    network 192.168.2.0 mask 255.255.255.0
    dns-list 192.168.2.1
#
dhcp server ip-pool vlan300
    gateway-list 192.168.3.1
    network 192.168.3.0 mask 255.255.255.0
    dns-list 192.168.3.1
#
interface Vlan-interface2
    ip address 192.168.0.100 255.255.255.0
#
interface Vlan-interface100
    ip address 192.168.1.1 255.255.255.0
#
interface Vlan-interface200
    ip address 192.168.2.1 255.255.255.0
#
interface Vlan-interface300
    ip address 192.168.3.1 255.255.255.0
#
interface GigabitEthernet1/0/1
    port link-mode bridge
    port link-type trunk
    port trunk permit vlan 1 100
#
interface GigabitEthernet1/0/2

```



```
port link-mode bridge
port link-type trunk
port trunk permit vlan all
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*
- *WLAN Access Command Reference in INTELBRAS Access Controllers Command References*
- *WLAN Access Configuration Guide in INTELBRAS Access Controllers Configuration Guides*

# INTELBRAS Access Controllers

## Downlink VLAN Management for Fit-Mode APs and Cloud-Mode APs

### 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 downlink VLAN management for fit-mode APs and<br>cloud-mode APs..... | 1  |
| Network configuration.....                                                                | 1  |
| Analysis .....                                                                            | 2  |
| Restrictions and guidelines.....                                                          | 2  |
| Procedures .....                                                                          | 2  |
| Configuring the AC.....                                                                   | 2  |
| Configuring the cloud-managed AP.....                                                     | 5  |
| Configuring the switch .....                                                              | 6  |
| Verifying the configuration .....                                                         | 7  |
| Configuration files.....                                                                  | 8  |
| Related documentation .....                                                               | 10 |

# Introduction

The following information provides a downlink VLAN management configuration example for fit-mode APs and cloud-mode APs.

## 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 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 AP management, radio management, WLAN access, VLAN, and local forwarding.

## Example: Configuring downlink VLAN management for fit-mode APs and cloud-mode APs

### Network configuration

As shown in [Figure 1](#), the switch acts as the DHCP server to assign IP addresses to the APs, the clients, and the PCs. The fit AP and the AC use VLAN 100 to establish a CAPWAP tunnel, the clients use VLAN 200 to access the wireless network, and the PCs use VLAN 300 to access the wired network.

- Configure local forwarding on the AC for the fit AP to directly forward the data traffic of Client 1.
- Connect PC 1 and PC 2 to downlink Ethernet interfaces on the fit AP and the cloud-managed AP, respectively. Make sure the PCs can visit the external network.

The diagram illustrates a network topology for a Cloud Managed Network (CMN) scenario. A central **Switch/DHCP** is connected to three access points: **AC**, **FI AP**, and **Cloud AP**. The **AC** and **FI AP** are connected to an **IP network**. The **Cloud AP** is connected to **PC 1** and **PC 2**. **Client 1** is connected to the **FI AP**, and **Client 2** is connected to the **Cloud AP**.

The **Switch/DHCP** has the following interfaces and configurations:

- GE1/0/1**: Vlan-int100, 192.168.1.2/24 (connected to AC)
- GE1/0/1**: Vlan-int100, 192.168.1.1/24 (connected to IP network)
- Vlan-int200**: 192.168.2.1/24 (connected to Cloud AP)
- GE1/0/2**: Vlan-int300, 192.168.3.1/24 (connected to FI AP)
- GE1/0/4**: (connected to IP network)

The **AC** has the following configuration:

- GE1/0/1**: Vlan-int100, 192.168.1.2/24

The **FI AP** has the following configuration:

- GE1/0/3**: Vlan-int2, 192.168.0.100/24
- GE1/0/2**: (connected to Switch/DHCP)

The **Cloud AP** has the following configuration:

- GE1/0/1**: (connected to Switch/DHCP)

The **IP network** is represented by a cloud icon. A red arrow indicates the path for **Control packets** from the IP network to the AC. A blue arrow indicates the path for **Data packets** from the IP network to the FI AP, labeled "Data packets without CAPWAP encapsulation".

For the configuration to be deployed to the AP, configure remote configuration synchronization or deploy the map file.

- For configuration to be deployed correctly, do not attach Tab characters or spaces to the end of command lines in the map file.
- Use the actual AP models and serial IDs to configure the APs.
- If a backup AC is configured, make sure the backup AC is also uploaded with the map file.

## Configuring the AC

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

```
<AC> system-view
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 192.168.1.2 24
[AC-Vlan-interface100] quit
```

# Configure GigabitEthernet 1/0/1 that connects the AC to the switch as a trunk port, and assign the port to VLAN 100.

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

2. Configure a wireless service:

# Create service template 1 and enter its view.

```
[AC] wlan service-template 1
```

# Set the SSID to **service**.

```
[AC-wlan-st-1] ssid service
```

# Set the VLAN to VLAN 200.

```
[AC-wlan-st-1] vlan 200
```

# Specify PSK as the AKM mode and specify **12345678** as the plaintext key.

```
[AC-wlan-st-1] akm mode psk
[AC-wlan-st-1] preshared-key pass-phrase simple 12345678
```

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

```
[AC-wlan-st-1] cipher-suite ccmp
[AC-wlan-st-1] security-ie rsn
```

# Configure the AP to forward client data traffic.

```
[AC-wlan-st-1] client forwarding-location ap
```

# Enable the service template.

```
[AC-wlan-st-1] service-template enable
[AC-wlan-st-1] quit
```

3. Configure the fit AP:

---

**NOTE:**

To simplify AP configuration on a large-scale network, configure AP settings on a per AP group basis as a best practice.

---

# Create manual AP **ap1**.

```
[AC] wlan ap ap1 model AP 3620H
```

# Specify the AP serial ID.

```
[AC-wlan-ap-ap1] serial-id 219801A28N819CE0002T
[AC-wlan-ap-ap1] quit
```

# Create AP group **group1** and configure **ap1** as the AP grouping rule.

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

# Bind service template 1 to radio 2 for AP group **group1**.

```
[AC-wlan-ap-group-group1] ap-model AP 3620H
[AC-wlan-ap-group-group1-ap-model-AP 3620H] radio 2
[AC-wlan-ap-group-group1-ap-model-AP 3620H-radio-2] service-template 1
```

# Enable radio 2.

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

4. To deploy configuration through remote configuration synchronization:

# Create VLANs 200 and 300 in AP group **group1**.

```
[AC-wlan-ap-group-group1] vlan 200
[AC-wlan-ap-group-group1-vlan200] quit
[AC-wlan-ap-group-group1] vlan 300
[AC-wlan-ap-group-group1-vlan300] quit
```

**# Specify uplink Ethernet interface GE1/0/1 that connects the AP to the switch as a trunk port, assign the port to all VLANs, set the PVID to 1, and disable port isolation.**

```
[AC-wlan-ap-group-group1] ap-model AP 3620H
[AC-wlan-ap-group-group1-ap-model-AP 3620H] gigabitethernet 1
[AC-wlan-ap-group-group1-ap-model-AP 3620H-gigabitethernet-1] port-isolate
disable [AC-wlan-ap-group-group1-ap-model-AP 3620H-gigabitethernet-1] port link-
type trunk
[AC-wlan-ap-group-group1-ap-model-AP 3620H-gigabitethernet-1] port trunk permit
vlan all
[AC-wlan-ap-group-group1-ap-model-AP 3620H-gigabitethernet-1] port trunk pvid vlan
1 [AC-wlan-ap-group-group1-ap-model-AP 3620H-gigabitethernet-1] quit
```

**# Specify all downlink Ethernet interfaces that connect the AP to the PC 1 as access ports, assign the ports to VLAN 300, and disable port isolation. This step uses GE 1/0/2 as an example.**

```
[AC-wlan-ap-group-group1-ap-model-AP 3620H] gigabitethernet 2
[AC-wlan-ap-group-group1-ap-model-AP 3620H-gigabitethernet-2] port-isolate
disable [AC-wlan-ap-group-group1-ap-model-AP 3620H-gigabitethernet-2] port access
vlan 300 [AC-wlan-ap-group-group1-ap-model-AP 3620H-gigabitethernet-2] quit
[AC-wlan-ap-group-group1-ap-model-AP 3620H] quit
```

**# Enable remote configuration synchronization.**

```
[AC-wlan-ap-group-group1] remote-configuration enable
```

**# Synchronize the configuration to the AP.**

```
[AC-wlan-ap-group-group1] remote-configuration synchronize
```

## 5. To deploy configuration through a map configuration file:

---

### NOTE:

- Use a text editor to edit the content of the apcfg.txt file in the configuration order, and upload the file to the AC. After the AP associates with the AC, use the **map-configuration** command to deploy the file to the AP for the configuration to take effect on the AP.
  - Specify all downlink Ethernet interfaces that connect the AP to the PC 1 as access ports, assign the ports to VLAN 300, and disable port isolation. This step uses GE 1/0/2 as an example.
- 

**# Edit the apcfg.txt file.**

```
system-view
vlan 200
quit
vlan 300
quit
interface GigabitEthernet 1/0/1
undo port-isolate enable
port link-type trunk
port trunk permit vlan all
quit
interface GigabitEthernet 1/0/2
undo port-isolate enable
port access vlan 300
quit
```

```
# Specify the AP configuration file as apcfg.txt in the AP group's AP model view.
[AC] wlan ap-group group1
[AC-wlan-ap-group-group1] ap-model AP 3620H
[AC-wlan-ap-group-group1-ap-model-AP 3620H] map-configuration apcfg.txt
```

## Configuring the cloud-managed AP

### 1. Configure the AP interfaces:

# Create VLAN 200 and VLAN 300. The AP will use VLAN 200 to forward wireless traffic of Client 2 and use VLAN 300 for the wired network access of PC 2.

```
<AP> system-view
[AP] vlan 200
[AP-vlan200] quit
[AP] vlan 300
[AP-vlan300] quit
```

# Specify GigabitEthernet 1/0/1 that connects the AP to the switch as a trunk port, assign the port to all VLANs, and disable port isolation.

```
[AP] interface gigabitethernet 1/0/1
[AP-GigabitEthernet1/0/1] undo port-isolate enable
[AP-GigabitEthernet1/0/1] port link-type trunk
[AP-GigabitEthernet1/0/1] port trunk permit vlan all
[AP-GigabitEthernet1/0/1] quit
```

# Specify all downlink Ethernet interfaces that connect the Cloud AP to the PC 2 as access ports, assign the ports to VLAN 300, and disable port isolation. This step uses GE 1/0/2 as an example.

```
[AP] interface gigabitethernet 1/0/2
[AP-GigabitEthernet1/0/2] undo port-isolate enable
[AP-GigabitEthernet1/0/2] port link-type access
[AP-GigabitEthernet1/0/2] port access vlan 300
[AP-GigabitEthernet1/0/2] quit
```

### 2. Configure a wireless service:

# Create service template **service1** and enter its view.

```
[AP] wlan service-template service1
```

# Set the SSID to **service**.

```
[AP-wlan-st-service1] ssid service
```

# Set the VLAN to VLAN 200.

```
[AP-wlan-st-service1] vlan 200
```

# Specify PSK as the AKM mode and specify **12345678** as the plaintext key.

```
[AP-wlan-st-service1] akm mode psk
[AP-wlan-st-service1] preshared-key pass-phrase simple 12345678
```

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

```
[AP-wlan-st-service1] cipher-suite ccmp
[AP-wlan-st-service1] security-ie rsn
```

# Enable the service template.

```
[AP-wlan-st-service1] service-template enable
[AP-wlan-st-service1] quit
```

### 3. Bind service template **service1** to interface WLAN-Radio 1/0/1.

```
[AP] interface WLAN-Radio 1/0/1
```



```
[AP-WLAN-Radiol/0/1] undo shutdown
[AP-WLAN-Radiol/0/1] service-template service1
[AP-WLAN-Radiol/0/1] quit
```

## Configuring the switch

### 1. Configure switch interfaces:

**# Create VLAN 2, VLAN 100, VLAN 200, VLAN 300, and the VLAN interfaces, and assign IP addresses to the VLAN interfaces. The switch will use VLAN 2 as the egress to the external network, VLAN 100 to forward packets between AC and AP, VLAN 200 to forward client traffic, and VLAN 300 for wired network access of the PCs.**

```
<Switch> system-view
[Switch] vlan 2
[Switch-vlan2] quit
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] ip address 192.168.0.100 24
[Switch-Vlan-interface2] quit
[Switch] vlan 100
[Switch-vlan100] quit
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ip address 192.168.1.1 24
[Switch-Vlan-interface100] quit
[Switch] vlan 200
[Switch-vlan200] quit
[Switch] interface vlan-interface 200
[Switch-Vlan-interface200] ip address 192.168.2.1 24
[Switch-Vlan-interface200] quit
[Switch] vlan 300
[Switch-vlan300] quit
[Switch] interface vlan-interface 300
[Switch-Vlan-interface300] ip address 192.168.3.1 24
[Switch-Vlan-interface300] quit
```

**# Specify GigabitEthernet 1/0/1 that connects the switch to the AC as a trunk port, and assign the port to VLAN 100.**

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

**# Specify GigabitEthernet 1/0/2 that connects the switch to the AP as a trunk port, assign the port to all VLANs, 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 all
[Switch-GigabitEthernet1/0/2] port trunk pvid vlan 100
```

**# Enable PoE on GigabitEthernet 1/0/2 that connects the switch to the fit AP.**

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

**# Specify GigabitEthernet 1/0/3 that connects the switch to the external network as an access port, and configure the port to permit traffic from 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

# Specify GigabitEthernet 1/0/4 that connects the switch to the cloud-managed AP as a trunk
port, assign the port to all VLANs, and set the PVID to 100.
[Switch] interface GigabitEthernet 1/0/4
[Switch-GigabitEthernet1/0/4] port link-type trunk
[Switch-GigabitEthernet1/0/4] port trunk permit vlan all
[Switch-GigabitEthernet1/0/4] port trunk pvid vlan 100

# Enable PoE on GigabitEthernet 1/0/4 that connects the switch to the cloud-managed AP.
[Switch-GigabitEthernet1/0/4] poe enable
[Switch-GigabitEthernet1/0/4] quit
```

## 2. Configure DHCP:

# Enable DHCP.

```
[Switch] dhcp enable
```

# Create DHCP address pool **vlan100** to assign IP addresses to the APs, and specify subnet 192.168.1.0/24 in the DHCP address pool.

```
[Switch] dhcp server ip-pool vlan100
[Switch-dhcp-pool-vlan100] network 192.168.1.0 mask 255.255.255.0
[Switch-dhcp-pool-vlan100] forbidden-ip 192.168.1.2
[Switch-dhcp-pool-vlan100] gateway-list 192.168.1.1
[Switch-dhcp-pool-vlan100] quit
```

# Create DHCP address pool **vlan200** to assign IP addresses to the clients, specify subnet 192.168.2.0/24 in the DHCP address pool, and specify the gateway address as 192.168.2.1. Set the DNS server address according to the actual networking planning.

```
[Switch] dhcp server ip-pool vlan200
[Switch-dhcp-pool-vlan200] network 192.168.2.0 mask 255.255.255.0
[Switch-dhcp-pool-vlan200] gateway-list 192.168.2.1
[Switch-dhcp-pool-vlan200] dns-list 192.168.2.1
[Switch-dhcp-pool-vlan200] quit
```

# Create DHCP address pool **vlan300** to assign IP addresses to the PCs, specify subnet 192.168.3.0/24 in the DHCP address pool, and specify the gateway address as 192.168.3.1. Set the DNS server address according to the actual networking planning.

```
[Switch] dhcp server ip-pool vlan300
[Switch-dhcp-pool-vlan300] network 192.168.3.0 mask 255.255.255.0
[Switch-dhcp-pool-vlan300] gateway-list 192.168.3.1
[Switch-dhcp-pool-vlan300] dns-list 192.168.3.1
[Switch-dhcp-pool-vlan300] quit
```

## 3. Configure default routes for the switch to visit the external IP network. (Details not shown.)

# Verifying the configuration

# Verify that the IP addresses obtained by Client 1, PC 1, Client 2, and PC 2 are 192.168.2.2, 192.168.3.2, 192.168.2.3, and 192.168.3.3, respectively, and all the clients and PCs can visit the external network.

# Configuration files

- **AC:**

```
#
Vlan 100
#
wlan service-template 1
    ssid service
    vlan 200
    client forwarding-location ap
akm mode psk
    preshared-key pass-phrase cipher $c$3$N//5BVbsOqdBTxi+7MJZKT6Zqh5MAMys2ZzM
    cipher-suite ccmp
    security-ie rsn
    service-template enable
#
interface Vlan-interface100
    ip address 192.168.1.2 255.255.255.0
#
interface GigabitEthernet1/0/1
    port link-type trunk
    port trunk permit vlan 1 100
#
wlan ap-group group1
    ap ap1
    ap-model AP 3620H
map-configuration flash:/apcfg.txt
radio 1
    radio 2
    radio enable
    service-template 1
#
wlan ap ap1 model AP 3620H
    serial-id 219801A28N819CE0002T
#
```

- **Cloud-managed AP:**

```
#
vlan 200
#
vlan 300
#
wlan service-template service1
    ssid service
    vlan 200
akm mode psk
    preshared-key pass-phrase cipher $c$3$N//5BVbsOqdBTxi+7MJZKT6Zqh5MAMys2ZzM
    cipher-suite ccmp
    security-ie rsn
```

```

service-template enable
#
interface WLAN-Radio1/0/1
service-template service1
#
interface GigabitEthernet1/0/1
port link-mode bridge
port link-type trunk
port trunk permit vlan all
#
interface GigabitEthernet1/0/2
port link-type access
port access vlan 300
#

```

- **Switch:**

```

#
dhcp enable
#
vlan 2
#
vlan 100
#
vlan 200
#
vlan 300
#
dhcp server ip-pool vlan100
gateway-list 192.168.1.1
network 192.168.1.0 mask 255.255.255.0
forbidden-ip 192.168.1.2
#
dhcp server ip-pool vlan200
gateway-list 192.168.2.1
network 192.168.2.0 mask 255.255.255.0
dns-list 192.168.2.1
#
dhcp server ip-pool vlan300
gateway-list 192.168.3.1
network 192.168.3.0 mask 255.255.255.0
dns-list 192.168.3.1
#
interface Vlan-interface2
ip address 192.168.0.100 255.255.255.0
#
interface Vlan-interface100
ip address 192.168.1.1 255.255.255.0
#
interface Vlan-interface200

```

```

ip address 192.168.2.1 255.255.255.0
#
interface Vlan-interface300
ip address 192.168.3.1 255.255.255.0
#
interface GigabitEthernet1/0/1
port link-mode bridge
port link-type trunk
port trunk permit vlan 1 100
#
interface GigabitEthernet1/0/2
port link-mode bridge
port link-type trunk
port trunk permit vlan all
port trunk pvid vlan 100
poe enable
#
interface GigabitEthernet1/0/3
port link-type access
port access vlan 2
#
interface GigabitEthernet1/0/4
port link-mode bridge
port link-type trunk
port trunk permit vlan all
port trunk pvid vlan 100
poe enable
#

```

## 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*
- *WLAN Access Command Reference in INTELBRAS Access Controllers Command References*
- *WLAN Access Configuration Guide in INTELBRAS Access Controllers Configuration Guides*