

INTELBRAS Access Controllers

AC Hierarchy 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 AC hierarchy	1
Network configuration	1
Analysis	2
Restrictions and guidelines	2
Procedures	3
Configuring the central AC	3
Configuring the local AC	5
Configuring the INC server	7
Verifying the configuration	12
Configuration files	14
Related documentation	16

Introduction

The following information provides an AC hierarchy configuration example.

Prerequisites

NOTE:

Support for this configuration example varies by device model and version.

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 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 AC hierarchy, portal, WLAN access, and AP management.

Example: Configuring AC hierarchy

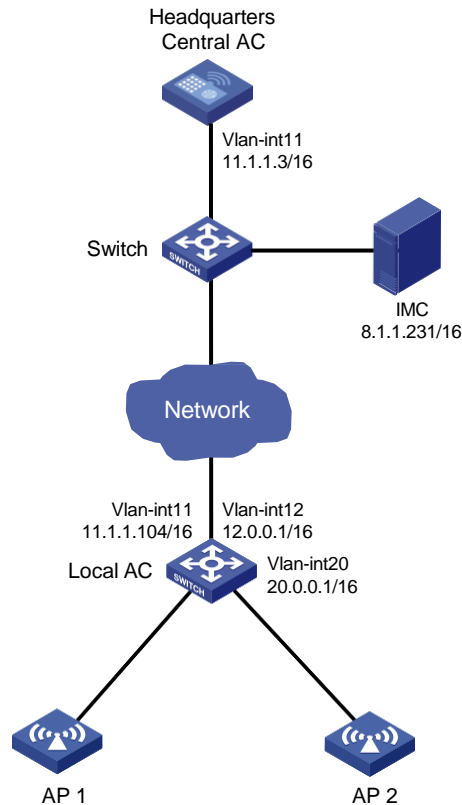
Network configuration

As shown in [Figure 1](#), the central AC is deployed at the headquarters and a local AC (a unified wired and wireless AC) is deployed at the branch. The central AC performs client authentication and the local AC forwards client traffic.

Configure network settings to meet the following requirements:

- APs obtain the IP address of the central AC through DHCP Option 43 and establish CAPWAP tunnels with the local AC after AC rediscovery.
- The INC server acts as the portal server and AAA server to perform client portal authentication.
- The local AC acts as the DHCP server to assign IP addresses to APs and clients.

Figure 1 Network diagram



Analysis

- For the AP to discover the AC across the Internet, configure Option 43 and manually specify the IP address of the AC on Router A.
- For interface GigabitEthernet1/0/1 on an AP to join the local-forwarding VLAN, use a text editor to create an AP configuration file and upload the file to the central AC.
- With AC rediscovery enabled, the APs might fail to come online through the local AC in the branch if the local AC does not have the lowest workload. For the central AC to assign the local AC to the APs at AC rediscovery, specify the local AC for APs.

Restrictions and guidelines

When you configure AC hierarchy, follow these restrictions and guidelines:

- Use the actual serial ID of an AP to uniquely identify that AP.
- Do not configure any portal settings on the local AC when portal authentication and local forwarding are used in the AC hierarchy network.
- Do not enable auto AP on the local AC, and do not create APs on the local AC if the APs are to be managed centrally by the central AC.
- Disable firmware upgrade for the local AC because the S5560 unified wired and wireless AC and the access controller module have different software versions.
- The URL of the portal Web server redirected to clients does not carry parameters by default. You must configure the parameters manually.
- Central ACs do not support IRF.

Procedures

Configuring the central AC

1. Make sure the devices can reach each other. (Details not shown.)
2. Create AP configuration file **map.txt** as follows and then upload the file to the central AC.

```
system-view
vlan 20
interface GigabitEthernet1/0/1
port link-type trunk
port trunk permit vlan 20
```
3. Create VLAN 11 and VLAN-interface 11, and assign an IP address to the VLAN interface.

```
<Central AC> system-view
[Central AC] vlan 11
[Central AC-vlan11] quit
[Central AC] interface vlan-interface 11
[Central AC-Vlan-interface11] ip address 11.1.1.3 16
[Central AC-Vlan-interface11] quit
```
4. Configure GigabitEthernet 1/0/1 that connects the central AC to the switch as a trunk port, and assign the port to VLAN 11.

```
[Central AC] interface gigabitethernet 1/0/1
[Central AC-GigabitEthernet1/0/1] port link-type trunk
[Central AC-GigabitEthernet1/0/1] port trunk permit vlan 11
[Central AC-GigabitEthernet1/0/1] quit
```
5. Create local AC **55ng-1**, and specify the serial ID of the local AC.

```
[Central AC] wlan local-ac name 55ng-1 model S5560
[Central AC-wlan-local-ac-55ng-1] serial-id 210235A1GCH147000017
[Central AC-wlan-local-ac-55ng-1] quit
```
6. Configure the RADIUS scheme for portal authentication:
Create RADIUS scheme iNC.

```
[Central AC] radius scheme iNC
```

Specify the IP address of the primary authentication server as 8.1.1.231.

```
[Central AC-radius-iNC] primary authentication 8.1.1.231
```

Specify the IP address of the primary accounting server as 8.1.1.231.

```
[Central AC-radius-iNC] primary accounting 8.1.1.231
```

Set the shared key to 12345678 in plaintext form for secure authentication communication.

```
[Central AC-radius-iNC] key authentication simple 12345678
```

Set the shared key to 12345678 in plaintext form for secure accounting communication.

```
[Central AC-radius-iNC] key accounting simple 12345678
```

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

```
[Central AC-radius-iNC] user-name-format without-domain
```

Specify IP address 11.1.1.3 as the source IP address of outgoing RADIUS packets.

```
[Central AC-radius-iNC] nas-ip 11.1.1.3
[Central AC-radius-iNC] quit
```
7. Configure the authentication domain for portal authentication:

- # Create domain **iNC** and enter its view.
- ```
[Central AC] domain iNC
```
- # Perform RADIUS authentication for portal users based on scheme **iNC**.
- ```
[Central AC-isp-iNC] authentication portal radius-scheme iNC
```
- # Perform RADIUS authorization for portal users based on scheme **iNC**.
- ```
[Central AC-isp-iNC] authorization portal radius-scheme iNC
```
- # Perform RADIUS accounting for portal users based on scheme **iNC**.
- ```
[Central AC-isp-iNC] accounting portal radius-scheme iNC
[Central AC-isp-iNC] quit
```
8. Configure the portal authentication server:
- # Create portal authentication server **iNC** and enter its view.
- ```
[Central AC] portal server iNC
```
- # Configure the IP address of the portal authentication server as **8.1.1.231** and the plaintext key as **12345678**.
- ```
[Central AC-portal-server-iNC] ip 8.1.1.231 key simple 12345678
```
9. Configure the portal Web server:
- # Create portal Web server **iNC** and enter its view.
- ```
[Central AC-portal-server-iNC] portal web-server iNC
```
- # Configure the URL for the portal Web server as **http://8.1.1.231:8080/portal**.
- ```
[Central AC-portal-server-iNC] url http://8.1.1.231:8080/portal
```
- # Configure the parameters carried in the URL of the portal Web server.
- ```
[Central AC-portal-server-iNC] url-parameter apmac ap-mac
[Central AC-portal-server-iNC] url-parameter ssid ssid
[Central AC-portal-server-iNC] url-parameter userip source-address
[Central AC-portal-server-iNC] url-parameter usermac source-mac
[Central AC-portal-server-iNC] quit
```
- # Enable validity check on wireless portal clients.
- ```
[Central AC] portal host-check enable
```
10. Configure wireless services:
- # Create service template **portal**.
- ```
[Central AC] wlan service-template portal
```
- # Set the SSID for the service template to **portal**.
- ```
[Central AC-wlan-st-portal] ssid portal
```
- # Set the AKM mode to PSK, and specify the plaintext preshared key as **12345678**.
- ```
[Central AC-wlan-st-portal] akm mode psk
[Central AC-wlan-st-portal] preshared-key pass-phrase simple 12345678
```
- # Set the cipher suite to CCMP and the security IE to RSN.
- ```
[Central AC-wlan-st-portal] cipher-suite ccmp
[Central AC-wlan-st-portal] security-ie rsn
```
- # Assign clients coming online through the service template to VLAN 20.
- ```
[Central AC-wlan-st-portal] vlan 20
```
- # Enable APs to forward client traffic. If the APs act as the client traffic forwarder by default, skip this step.
- ```
[Central AC-wlan-st-portal] client forwarding-location ap
```
- # Enable direct IPv4 portal authentication on the service template.
- ```
[Central AC-wlan-st-portal] portal enable method direct
```
- # Specify the authentication domain as **iNC** for IPv4 portal users on the service template.

```
[Central AC-wlan-st-portal] portal domain iNC
Configure the BAS-IP attribute as 11.1.1.3 for portal packets sent to the portal authentication server.
[Central AC-wlan-st-portal] portal bas-ip 11.1.1.3
Apply IPv4 portal Web server iNC on the service template for portal authentication.
[Central AC-wlan-st-portal] portal apply web-server iNC
Enable the service template.
[Central AC-wlan-st-portal] service-template enable
[Central AC-wlan-st-portal] quit
Create AP ap1 and set the serial ID to 210235A1SVC15C000028.
[Central AC] wlan ap ap1 model AP 3620
[Central AC-wlan-ap-ap1] serial-id 219801A28N819CE0002T
[Central AC-wlan-ap-ap1] quit
Create AP group group1 and configure a grouping rule by AP name to add AP ap1 to the group.
[Central AC] wlan ap-group group1
[Central AC-wlan-ap-group-group1] ap ap1
```

---

#### NOTE:

In a large-scale network, configure AP settings in AP group view instead of AP view as a best practice.

---

```
Bind service template portal to radio 1.
[Central AC-wlan-ap-group-group1] ap-model AP 3620
[Central AC-wlan-ap-group-group1-ap-model-AP 3620] radio
1
[Central AC-wlan-ap-group-group1-ap-model-AP 3620-radio-1] service-template portal
Enable radio 1.
[Central AC-wlan-ap-group-group1-ap-model-AP 3620-radio-1] radio
enable [Central AC-wlan-ap-group-group1-ap-model-AP 3620-radio-1] quit
Bind service template portal to radio 2.
[Central AC-wlan-ap-group-group1-ap-model-AP 3620] radio 2
[Central AC-wlan-ap-group-group1-ap-model-AP 3620-radio-2] service-template portal
Enable radio 2.
[Central AC-wlan-ap-group-group1-ap-model-AP 3620-radio-2] radio
enable [Central AC-wlan-ap-group-group1-ap-model-AP 3620-radio-2] quit
Deploy configuration file map.txt to AP ap1.
[Central AC-wlan-ap-group-group1-ap-model-AP 3620] map-configuration cfa0:/map.txt
[Central AC-wlan-ap-group-group1-ap-model-AP 3620] quit
Enable AC rediscovery.
[Central AC-wlan-ap-group-group1] control-address enable
Specify the local AC with IP address 11.1.1.104 for the AP.
[Central AC-wlan-ap-group-group1] control-address ip 11.1.1.104
```

## Configuring the local AC

1. Configure the local AC feature:

```
Enable the local AC feature.
```

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

```
[Local AC] wlan local-ac enable
```

# Specify the central AC with IP address **11.1.1.3** for the local AC.

```
[Local AC] wlan central-ac ip 11.1.1.3
```

# Configure the local AC to use VLAN 11 to establish a tunnel with the central AC.

```
[Local AC] wlan local-ac capwap source-vlan 11
```

## 2. Configure DHCP:

# Enable DHCP.

```
[Local AC] dhcp enable
```

# Create DHCP address pool **ap**, specify the gateway address as **12.0.0.1**, and specify the subnet for dynamic allocation as **12.0.0.0/16**.

```
[Local AC] dhcp server ip-pool ap
```

```
[Local AC-dhcp-pool-ap] gateway-list 12.0.0.1
```

```
[Local AC-dhcp-pool-ap] network 12.0.0.0 mask 255.255.0.0
```

# Configure Option 43 that specifies a DNS server address 11.1.1.3 in the DHCP address pool.

```
[Local AC-dhcp-pool-ap] option 43 hex 80070000010b010103
```

```
[Local AC-dhcp-pool-ap] quit
```

# Create DHCP address pool **client**, specify the gateway address as **20.0.0.1**, and specify the subnet for dynamic allocation as **20.0.0.0/16**.

```
[Local AC] dhcp server ip-pool client
```

```
[Local AC-dhcp-pool-ap] gateway-list 20.0.0.1
```

```
[Local AC-dhcp-pool-ap] network 20.0.0.0 mask 255.255.0.0
```

```
[Local AC-dhcp-pool-ap] quit
```

## 3. Configure VLAN interfaces:

# Create VLAN 11 and VLAN-interface 11, and assign an IP address to the interface. The local AC uses this interface to associate with the central AC.

```
[Local AC] vlan 11
```

```
[Local AC-vlan11] quit
```

```
[Local AC] interface Vlan-interface11
```

```
[Local AC-Vlan-interface11] ip address 11.1.1.104 255.255.0.0
```

```
[Local AC-Vlan-interface11] quit
```

# Create VLAN 12 and VLAN-interface 12, and assign an IP address to the interface. The local AC uses this interface to associate with APs.

```
[Local AC] vlan 12
```

```
[Local AC-vlan12] quit
```

```
[Local AC] interface Vlan-interface12
```

```
[Local AC-Vlan-interface12] ip address 12.0.0.1 255.255.0.0
```

```
[Local AC-Vlan-interface12] dhcp server apply ip-pool ap
```

```
[Local AC-Vlan-interface12] quit
```

# Create VLAN 20 and VLAN-interface 20, and assign an IP address to the interface. The local AC uses this interface to provide access to clients.

```
[Local AC] vlan 20
```

```
[Local AC-vlan20] quit
```

```
[Local AC] interface Vlan-interface20
```

```
[Local AC-Vlan-interface20] ip address 20.0.0.1 255.255.0.0
```

```
[Local AC-Vlan-interface20] dhcp server apply ip-pool client
```

```
[Local AC-Vlan-interface20] quit
```

# Configure GigabitEthernet 1/0/1 that connects the local AC to AP 1 as a trunk port, assign the port to VLAN 12 and VLAN 20, and set the PVID to 12.



```
[Local AC] interface GigabitEthernet 1/0/1
[Local AC-GigabitEthernet1/0/1] port link-type trunk
[Local AC-GigabitEthernet1/0/1] port trunk permit vlan 12 20
[Local AC-GigabitEthernet1/0/1] port trunk pvid vlan 12
[Local AC-GigabitEthernet1/0/1] quit
```

# Configure GigabitEthernet 1/0/2 that connects the local AC to AP 2 as a trunk port, assign the port to VLAN 12 and VLAN 20, and set the PVID to 12.

```
[Local AC] interface GigabitEthernet 1/0/2
[Local AC-GigabitEthernet1/0/2] port link-type trunk
[Local AC-GigabitEthernet1/0/2] port trunk permit vlan 12 20
[Local AC-GigabitEthernet1/0/2] port trunk pvid vlan 12
[Local AC-GigabitEthernet1/0/2] quit
```

# Configure GigabitEthernet 1/0/3 that connects the local AC to the headquarters as a trunk port, and assign the port to VLAN 11, VLAN 12, and VLAN 20.

```
[Local AC] interface GigabitEthernet 1/0/3
[Local AC-GigabitEthernet1/0/3] port link-type trunk
[Local AC-GigabitEthernet1/0/3] port trunk permit vlan 11 12 20
[Local AC-GigabitEthernet1/0/3] quit
```

## Configuring the INC server

This example uses the INC server to describe the RADIUS server and portal server configuration. The INC server runs on INC PLAT 7.2 (E0403p10), INC - EIA 7.2 (E0405), and INC EIP 7.2 (E0405).

To configure the INC server:

1. Log in to INC and click the **User** tab.
2. Add an access device.
  - a. In the left navigation pane, select **User Access Policy > Access Device Management > Access Device**.
  - b. Click **Add**.  
The **Add Access Device** page opens.
  - c. In the **Device List** area, click **Add Manually**, and specify the start IP address as 11.1.1.3.
  - d. In the **Access Configuration** area, configure the following parameters:
    - Enter **radius** in the **Shared Key** and **Confirm Shared Key** fields.  
The key is consistent with the shared key configured on the AC.
    - Use the default values for other parameters.
  - e. 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 Unlimited

Access Device Type ((General))

Shared Key \* \*\*\*\*\*

Access Location Group ..

Forcible Logout Type Disconnect user

Service Group Ungrouped

Confirm Shared Key \* \*\*\*\*\*

Device List

Select Add Manually Clear All

| Device Name | Device IP   | Device Model | Comments | Delete |
|-------------|-------------|--------------|----------|--------|
|             | 112.12.1.25 |              |          |        |

Total Items: 1.

OK Cancel

3. Add an access policy:
  - a. From the navigation pane, select **User Access Policy > Access Policy**.
  - b. Click **Add**.
  - c. On the **Add Access Policy** page, configure the following parameters:
    - Enter the policy name.
    - Select the service group.
    - Use the default values 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 \* qucf-porta

Service Group \* Ungrouped

Description

Authorization Information

Access Period None

Downstream Rate(Kbps)

Priority

Certificate Authentication ☒ None ☐ EAP

Certificate Type EAP-TLS Authn

Deploy VLAN

☐ Deploy User Profile

☐ Deploy ACL

Allocate IP \* No

Upstream Rate(Kbps)

☐ RSA Authentication

Deploy User Group ?

4. Add an access service:
  - a. From the navigation pane, select **User Access Policy > Access Service**.
  - b. Click **Add**.
  - c. On the **Add Access Service** page, configure the following parameters:
    - Enter the service name.
    - Use the default values for other parameters.

d. Click **OK**.

**Figure 4 Adding an access service**

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

Basic Information

Service Name \* qucf-portal Service Suffix

Service Group \* Ungrouped Default Access Policy \* qucf-portal

Default Proprietary Attribute Assignment Policy \* Do not use

Default Max. Number of Bound Endpoints \* 0 Default Max. Number of Online Endpoints \* 0

Description

☒ Available ☒ Transparent Authentication on Portal Endpoints

5. Add an access user:

a. From the navigation pane, select **Access User > Access User**.

b. Click **Add**.

c. In the **Access Information** area, add a user:

- Select a user.
- Set the password.

d. Click **OK**.

**Figure 5 Adding an access user**

User > All Access Users > Add Access User

Access Information

User Name \* adm\_office\_mac Select Add User

Account Name \*

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

Password \* Confirm Password \*

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

Start Time End Time

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

Login Message

Access Service

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

6. Create an IP group:

a. From the navigation pane, select **User Access Policy > Portal Service > IP Group**.

b. Click **Add**.

c. Configure the following parameters:

- **IP Group Name**—Enter the IP group name.
- **Start IP**—Enter the start IP address of the IP group. Make sure the client IP address is in the IP group.
- **End IP**—Enter the end IP address of the IP group. Make sure the client IP address is in the IP group.
- **Service Group**—Select a service group. This example uses the default value **Ungrouped**.
- **Action**—Select **Normal**.

d. Click **OK**.

**Figure 6 Adding an IP group**

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

Add IP Group

|                 |              |
|-----------------|--------------|
| IP Group Name * | qucf-20      |
| Start IP *      | 20.0.0.1     |
| End IP *        | 20.0.255.255 |
| Service Group   | Ungrouped ▼  |
| Action *        | Normal ▼     |

OK Cancel

7. Add a portal device:
  - a. From the navigation pane, select **User Access Policy > Portal Service > Device**.
  - b. Click **Add**.
  - c. Configure the following parameters:
    - **Device Name**—Enter the device name.
    - **Version**—Select **CMCC 1.0**.
    - **IP Address**—Enter the IP address of the AC's interface connected to the client.
    - **Support Server Heartbeat**—Select whether to support the portal server heartbeat function. In this example, select **No**.
    - **Support User Heartbeat**—Select whether to support the portal user heartbeat function. In this example, select **No**.
    - **Key**—Enter the key. The key must be the same as that configured on the AC.
    - **Access Method**—Select **layer 3**.Use the default settings for other parameters.
  - d. Click **OK**.

**Figure 7 Adding a portal device**

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

Add Device

Device Information

|                            |            |                          |           |
|----------------------------|------------|--------------------------|-----------|
| Device Name *              | central    | Service Group *          | Ungrouped |
| Version *                  | Portal 2.0 | IP Address *             | 11.1.1.3  |
| 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 *            | layer3     |                          |           |
| Device Description         |            |                          |           |

OK Cancel

8. Associate the portal device with the IP group:

- Click the **Port Group** icon  in the **Operation** field for device **NAS** to open the port group configuration page.

**Figure 8 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         | Portal 2.0 | Ungrouped     | 11.1.1.3   |                  | Not Deployed  |    |

1-1 of 1. Page 1 of 1.

<< < 1 > >> 50

b. Click **Add**.

c. Configure the following parameters:

- Port Group Name**—Enter the port group name.
- IP Group**—Select the configured IP group. The IP address used by the user to access the network must be within this IP address group.

Use the default settings for other parameters.

d. Click **OK**.

**Figure 9 Adding a port group**

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

### Add Port Group

|                               |               |                                    |         |
|-------------------------------|---------------|------------------------------------|---------|
| Port Group Name *             | central       | Language *                         | English |
| Start Port *                  | 0             | End Port *                         | zzzzzz  |
| Protocol *                    | HTTP          | Quick Authentication *             | No      |
| NAT or Not *                  | No            | Error Transparent Transmission *   | Yes     |
| Authentication Type *         | PAP           | IP Group *                         | qucf-20 |
| 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

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

### Basic Information

|                      |            |
|----------------------|------------|
| Access Policy Name * | qucf-porta |
| Service Group *      | Ungrouped  |
| Description          |            |

### Authorization Information

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

## Verifying the configuration

# Verify that the local AC is in R/M state on the central AC. This state indicates that the local AC has come online on the central AC.

```
[Central AC] display wlan local-ac name 55ng-1
```

Local AC Information

State : I = Idle, J = Join, JA = JoinAck, IL = ImageLoad  
C = Config, DC = DataCheck, R = Run

| AC name | ACID | State | Model | Serial ID            |
|---------|------|-------|-------|----------------------|
| 55ng-1  | 2    | R/M   | S5560 | 210235A1GCH147000017 |

# Verify that the AP is in R/M state on the central AC.

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

Total number of APs: 1

```

Total number of connected APs: 1
Total number of connected manual APs: 1
Total number of connected auto APs: 0
Total number of connected common APs: 1
Total number of connected WTUs: 0
Total number of inside APs: 0
Maximum supported APs: 4096
Remaining APs: 4095
Total AP licenses: 512
Local AP licenses: 512
Server AP licenses: 0
Remaining local AP licenses: 511
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     | 8    | R/M   | AP 3620 | 219801A28N819CE0002T |

#### # Verify that the AP has associated with the local AC.

```

[Central AC] display wlan ap-distribution all
Central AC
Slot : 1
Total Number of APs: 0
AP name :

```

#### Local AC

```

Name : 55ng-1
Total Number of APs: 1
AP name : ap1

```

#### # Verify that a client has come online.

```

[Central AC] display wlan client
Total number of clients: 1

```

| MAC address    | User name | AP name | RID | IP address | IPv6 address | VLAN |
|----------------|-----------|---------|-----|------------|--------------|------|
| c81e-e738-016a | N/A       | ap1     | 1   | 20.0.0.3   |              | 20   |

#### # Verify that the client has passed portal authentication.

```

[Central AC] display portal user all
Total portal users: 1
Username: qcf

```

```

AP name: ap1
Radio ID: 1
SSID: portal
Portal server: iNC
State: Online
VPN instance: N/A

```

| MAC | IP | VLAN | Interface |
|-----|----|------|-----------|
|-----|----|------|-----------|

```

c81e-e738-016a 20.0.0.3 20 WLAN-BSS1/0/10
Authorization information:
 DHCP IP pool: N/A
 User profile: N/A
 Session group profile: N/A
 ACL number: N/A
 Inbound CAR: N/A
 Outbound CAR: N/A

```

## Configuration files

- **Central AC:**

```

#
vlan 11
#
wlan service-template portal
 ssid portal
 vlan 20
 client forwarding-location ap
 akm mode psk
 preshared-key pass-phrase cipher c3$p0PjuXJ5pGfJ6Z1XDkGRsPR8JoPhrP60GyRn
 cipher-suite ccmp
 security-ie rsn
 portal enable method direct
 portal domain iNC
 portal bas-ip 11.1.1.3
 portal apply web-server iNC
 service-template enable
#
interface Vlan-interface11
 ip address 11.1.1.3 255.255.0.0
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 11
#
radius scheme iNC
 primary authentication 8.1.1.231
 primary accounting 8.1.1.231
 key authentication cipher c3$t7x0fIARso0US949SnQS2pq53eIdsgUr6z07
 key accounting cipher c3$V4YI3sDOEq0VqAIPoANjQOV3ZalvqTL05GC0
 user-name-format without-domain
 nas-ip 11.1.1.3
#
domain iNC
 authentication portal radius-scheme iNC
 authorization portal radius-scheme iNC
 accounting portal radius-scheme iNC

```



```
#
portal host-check enable
#
portal web-server iNC
url http://8.1.1.231:8080/portal
url-parameter apmac ap-mac
url-parameter ssid ssid
url-parameter userip source-address
url-parameter usermac source-mac
#
portal server iNC
ip 8.1.1.231 key cipher c3$76rxh0Qxgg0I1zWtzrlr2r0ch76JC+3IZK2A
#
wlan ap ap1 model AP 3620
serial-id 219801A28N819CE0002T
#
wlan ap-group group1
control-address enable
control-address ip 11.1.1.104
ap ap1
ap-model AP 3620
map-configuration cfa0:/map.txt
radio 1
radio enable
service-template portal
radio 2
radio enable
service-template portal
#
wlan local-ac name 55ng-1 model S5560
serial-id 210235A1GCH147000017
#
```

- **Local AC:**

```
#
dhcp enable
#
vlan 11 to 12
#
vlan 20
#
dhcp server ip-pool ap
gateway-list 12.0.0.1
network 12.0.0.0 mask 255.255.0.0
option 43 hex 80070000010b010103
#
dhcp server ip-pool client
gateway-list 20.0.0.1
network 20.0.0.0 mask 255.255.0.0
```

```

#
interface Vlan-interface11
 ip address 11.1.1.104 255.255.0.0
#
interface Vlan-interface12
 ip address 12.0.0.1 255.255.0.0
 dhcp server apply ip-pool ap
#
interface Vlan-interface20
 ip address 20.0.0.1 255.255.0.0
 dhcp server apply ip-pool client
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 12 20
 port trunk pvid vlan 12
#
interface GigabitEthernet1/0/2
 port link-type trunk
 port trunk permit vlan 12 20
 port trunk pvid vlan 12
#
interface GigabitEthernet1/0/3
 port link-type trunk
 port trunk permit vlan 11 12 20
#
 wlan local-ac enable
 wlan local-ac capwap source-vlan 11
#
 wlan central-ac ip 11.1.1.3

```

## Related documentation

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

# INTELBRAS Access Controllers

## 802.1X Authentication on an AC Hierarchy Network with Local ACs as Authenticators and Traffic Forwarders)

### 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  |
| General restrictions and guidelines .....                                                                                                     | 1  |
| Example: Configuring remote 802.1X authentication on an AC hierarchy<br>network with local ACs as authenticators and traffic forwarders ..... | 1  |
| Network configuration .....                                                                                                                   | 1  |
| Analysis .....                                                                                                                                | 2  |
| Restrictions and guidelines .....                                                                                                             | 2  |
| Prerequisites .....                                                                                                                           | 3  |
| Procedures .....                                                                                                                              | 3  |
| Configuring the central AC .....                                                                                                              | 3  |
| Configuring the local AC .....                                                                                                                | 4  |
| Configuring the RADIUS server .....                                                                                                           | 6  |
| Verifying the configuration .....                                                                                                             | 9  |
| Configuration files .....                                                                                                                     | 11 |
| Related documentation .....                                                                                                                   | 13 |

# Introduction

The following information provides an example of configuring 802.1X authentication for clients on a network that deploys an AC hierarchy, with local ACs as authenticators and traffic forwarders.

## Prerequisites

---

**NOTE:**

Support for this configuration example varies by device model and version.

---

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 AC hierarchy, 802.1X, WLAN access, and AP management features.

## General restrictions and guidelines

Central ACs on an AC hierarchy network do not support IRF.

## Example: Configuring remote 802.1X authentication on an AC hierarchy network with local ACs as authenticators and traffic forwarders

### Network configuration

As shown in [Figure 1](#):

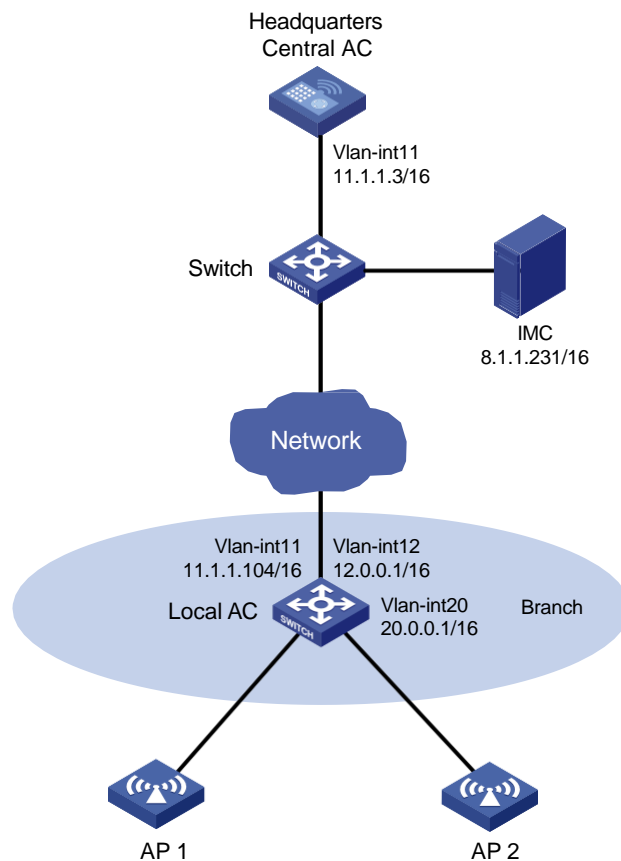
- The network deploys an AC hierarchy that contains one central AC (WX5560H in this example) and one local AC (WX3510H in this example).
- The network deploys INC to act as a RADIUS server for 802.1X authentication.
- The local AC acts as the DHCP server to assign IP addresses to APs and clients.

Configure the devices to meet the following requirements:

- The APs and clients are associated with the local AC.
  - The APs obtain the IP address of the central AC through DHCP Option 43.
  - The AC rediscovery feature is configured on the central AC for the APs to discover the local AC.

- The local AC acts as the authenticator and uses the RADIUS server to perform authentication, authorization, and accounting for the clients. 802.1X authentication is enabled in the service template through which the clients access the network.
- The local AC forwards client data traffic.
- The local AC acts as a DHCP server to assign IP addresses to the APs and the clients.

**Figure 1 Network diagram**



## Analysis

For an AP to discover the local AC and come online from the local AC, enable the AC rediscovery feature in the view of the manual AP that is created for the AP. In addition, configure the central AC to add the IP address of the local AC to the CAPWAP Control IP Address message element in the discovery responses sent to the AP. If the AC rediscovery feature is not configured for an AP, the central AC will send the IP address of the lightest loaded local AC to the AP. If the lightest loaded local AC is not the local AC in the branch, the AP cannot come online.

## Restrictions and guidelines

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

For the local AC to act as the authenticator, you must configure the authentication settings (including the RADIUS settings and domain settings) on the local AC.

On the local AC, do not enable the auto AP feature. In addition, create a manual AP for each AP in local AC view on the central AC for the central AC to manage the APs.

# Prerequisites

Make sure the devices can reach one another.

## Procedures

### Configuring the central AC

#### Configuring interfaces

# Create VLAN 11, create VLAN-interface 11, and assign an IP address to the VLAN interface. The AC will use this IP address to establish a management tunnel with the local AC.

```
<Central AC> system-view
[Central AC] vlan 11
[Central AC-vlan1] quit
[Central AC] interface vlan-interface 11
[Central AC-Vlan-interface1] ip address 11.1.1.3.16
[Central AC-Vlan-interface1] quit
```

# Configure GigabitEthernet 1/0/1 that connects the central AC to the switch as a trunk port, and assign the port to VLAN 11.

```
[Central AC] interface gigabitethernet 1/0/1
[Central AC-GigabitEthernet1/0/1] port link-type trunk
[Central AC-GigabitEthernet1/0/1] port trunk permit vlan 11
[Central AC-GigabitEthernet1/0/1] quit
```

#### Configuring a local AC for the central AC

# Create local AC **3510h-1** with model **WX3510H** and enter local AC view.

```
[Central AC] wlan local-ac name 3510h-1 model WX3510H
```

# Specify the serial ID of the local AC.

```
[Central AC-wlan-local-ac-3510h-1] serial-id 210235A1GCH147000017
[Central AC-wlan-local-ac-3510h-1] quit
```

#### Configuring a service template

# Create service template **dot1x** and set the SSID of the service template.

```
[Central AC] wlan service-template dot1x
[Central AC-wlan-st-dot1x] ssid dot1x
```

# Set the AKM mode to 802.1X.

```
[Central AC-wlan-st-dot1x] akm mode dot1x
```

# Specify the CCMP cipher suite and enable the RSN IE in beacon and probe responses.

```
[Central AC-wlan-st-dot1x] cipher-suite ccmp
[Central AC-wlan-st-dot1x] security-ie rsn
```

# Set the access authentication mode to 802.1X authentication.

```
[Central AC-wlan-st-dot1x] client-security authentication-mode dot1x
```

# Configure the AC to perform client authentication.

```
[Central AC-wlan-st-dot1x] client-security authentication-location ac
```

# Specify ISP domain **iNC** for authenticating the 802.1X client.

```
[Central AC-wlan-st-dot1x] dot1x domain iNC
```

# Configure the local ACs to forward client data traffic. If the local ACs act as the client traffic forwarder by default, skip this step.

```
[Central AC-wlan-st-dot1x] client forwarding-location ac
```

# Enable the service template.

```
[Central AC-wlan-st-dot1x] service-template enable
```

```
[Central AC-wlan-st-dot1x] quit
```

## Creating a manual AP

### NOTE:

In a large-scale network, configure AP settings in AP group view instead of AP view as a best practice.

# Create manual AP **ap1** and specify the AP model and serial ID.

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

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

```
[Central AC-wlan-ap-ap1] quit
```

# Create AP group **group1** and configure a grouping rule by AP name to add AP **ap1** to the group.

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

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

# Enable the AC rediscovery feature.

```
[Central AC-wlan-ap-group-group1] control-address enable
```

# Specify 12.0.0.1 (the IP address on the central AC) as the IP address to be carried in the CAPWAP Control IP Address message element.

```
[Central AC-wlan-ap-group-group1] control-address ip 12.0.0.1
```

# Bind service template **dot1x** to radio 1.

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

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

```
1
```

```
[Central AC-wlan-ap-group-group1-ap-model-AP 3620-radio-1] service-template dot1x vlan 2000
```

# Enable radio 1.

```
[Central AC-wlan-ap-group-group1-ap-model-AP 3620-radio-1] radio enable
```

```
[Central AC-wlan-ap-group-group1-ap-model-AP 3620-radio-1] quit
```

## Configuring the local AC

### 1. Configure the local AC feature:

# Enable the local AC feature.

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

```
[Local AC] wlan local-ac enable
```

# Specify the central AC for the local AC.

```
[Local AC] wlan central-ac ip 11.1.1.3
```

# Configure the local AC to use VLAN 11 to establish CAPWAP tunnels with the central AC.

```
[Local AC] wlan local-ac capwap source-vlan 11
```

### 2. Configure IP address pool settings:

# Enable the DHCP service.

```
[Local AC] dhcp enable
```



**# Configure DHCP address pool *ap*.** In the address pool, specify 12.0.0.1 as the gateway IP address and 12.0.0.0/16 as the subnet for dynamic allocation.

```
[Local AC] dhcp server ip-pool ap
[Local AC-dhcp-pool-ap] gateway-list 12.0.0.1
[Local AC-dhcp-pool-ap] network 12.0.0.0 mask 255.255.0.0
```

**# Configure Option 43 to specify the central AC address as the AC address in DHCP address pool *ap*.**

```
[Local AC-dhcp-pool-ap] option 43 hex 80070000010b010103
[Local AC-dhcp-pool-ap] quit
```

**# Configure DHCP address pool *client*.** In the address pool, specify 20.0.0.1 as the gateway IP address and 20.0.0.0/16 as the subnet for dynamic allocation.

```
[Local AC] dhcp server ip-pool client
[Local AC-dhcp-pool-ap] gateway-list 20.0.0.1
[Local AC-dhcp-pool-ap] network 20.0.0.0 mask 255.255.0.0
[Local AC-dhcp-pool-ap] quit
```

### 3. Configure interfaces:

**# Create VLAN 11, create VLAN-interface 11, and assign an IP address to the VLAN interface.** The local AC will use this IP address to establish CAPWAP tunnels with the central AC.

```
[Local AC] vlan 11
[Local AC-vlan11] quit
[Local AC] interface Vlan-interface11
[Local AC-Vlan-interface11] ip address 11.1.1.104 255.255.0.0
[Local AC-Vlan-interface11] quit
```

**# Create VLAN 12, create VLAN-interface 12, and assign an IP address to the VLAN interface.** The local AC assigns VLAN 12 to an AP when the AP comes online.

```
[Local AC] vlan 12
[Local AC-vlan12] quit
[Local AC] interface Vlan-interface12
[Local AC-Vlan-interface12] ip address 12.0.0.1 255.255.0.0
[Local AC-Vlan-interface12] dhcp server apply ip-pool ap
[Local AC-Vlan-interface12] quit
```

**# Create VLAN 20, create VLAN-interface 20, and assign an IP address to the VLAN interface.** The local AC assigns this VLAN to a wireless client when the client comes online.

```
[Local AC] vlan 20
[Local AC-vlan20] quit
[Local AC] interface Vlan-interface20
[Local AC-Vlan-interface20] ip address 20.0.0.1 255.255.0.0
[Local AC-Vlan-interface20] dhcp server apply ip-pool client
[Local AC-Vlan-interface20] quit
```

**# Configure GigabitEthernet 1/0/1 that connects the local AC to AP 1 as an access port, and assign the port to VLAN 12.**

```
[Local AC] interface GigabitEthernet 1/0/1
[Local AC-GigabitEthernet1/0/1] port link-type access
[Local AC-GigabitEthernet1/0/1] port access vlan 12
[Local AC-GigabitEthernet1/0/1] quit
```

**# Configure GigabitEthernet 1/0/2 that connects the local AC to AP 2 as an access port, and assign the port to VLAN 12.**

```
[Local AC] interface GigabitEthernet 1/0/2
[Local AC-GigabitEthernet1/0/2] port link-type access
[Local AC-GigabitEthernet1/0/1] port access vlan 12
```

- ```
[Local AC-GigabitEthernet1/0/2] quit
```
- # Configure GigabitEthernet 1/0/3 that connects the local AC to the headquarters as an access port, and assign the port to VLAN 11.
- ```
[Local AC] interface GigabitEthernet 1/0/3
[Local AC-GigabitEthernet1/0/3] port link-type access
[Local AC-GigabitEthernet1/0/3] port access vlan 11
[Local AC-GigabitEthernet1/0/3] quit
```
- # Configure a static route.
- ```
[Local AC] ip route-static 0.0.0.0 0.0.0.0 11.1.1.3
```
4. Specify EAP relay as the method to exchange packets with the RADIUS server.


```
[Local AC] dot1x authentication-method eap
```
 5. Configure a RADIUS scheme:

Create RADIUS scheme **iNC** and enter its view.

```
[Local AC] radius scheme iNC
```

Specify the IP address of the primary RADIUS authentication server.

```
[Local AC-radius-iNC] primary authentication 8.1.1.231
```

Specify the IP address of the primary RADIUS accounting server.

```
[Local AC-radius-iNC] primary accounting 8.1.1.231
```

Set the shared key to **12345678** in plaintext form for secure communication with the RADIUS authentication server.

```
[Local AC-radius-iNC] key authentication simple 12345678
```

Set the shared key to **12345678** in plaintext form for secure communication with the RADIUS accounting server.

```
[Local AC-radius-iNC] key accounting simple 12345678
```

Exclude the domain name from usernames sent to the servers.

```
[Local AC-radius-iNC] user-name-format without-domain
```

Specify IP address 11.1.1.104 as the source IP address for outgoing RADIUS packets.

```
[Local AC-radius-iNC] nas-ip 11.1.1.104
[Local AC-radius-iNC] quit
```
 6. Configure an authentication domain:

Create ISP domain **iNC** and enter its view.

```
[Local AC] domain iNC
```

Configure the ISP domain to use RADIUS scheme **iNC** for 802.1X user authentication.

```
[Local AC-isp-iNC] authentication lan-access radius-scheme iNC
```

Configure the ISP domain to use RADIUS scheme **iNC** for 802.1X user authorization.

```
[Local AC-isp-iNC] authorization lan-access radius-scheme iNC
```

Configure the ISP domain to use RADIUS scheme **iNC** for 802.1X user accounting.

```
[Local AC-isp-iNC] accounting lan-access radius-scheme iNC
[Local AC-isp-iNC] quit
```

Configuring the RADIUS server

Prerequisites

The RADIUS server runs INC PLAT 7.2 (E0403p10), INC INC - EIA 7.2 (E0405), and INC EIP 7.2 (E0405).

Make sure the RADIUS server has been installed with the EAP-PEAP certificate.

Adding the central AC as an access device to INC

1. Log in to INC and click the **User** tab.
2. From the navigation tree, select **User Access Policy > Access Device Management > Access Device**.
3. Click **Add**.
The **Add Access Device** page opens.
4. In the **Access Configuration** area, configure the following parameters, as shown in [Figure 2](#):
 - Enter **12345678** in the **Shared Key** and **Confirm Shared Key** fields. The shared key must be the same as the authentication and accounting shared keys configured on the central AC.
 - Use the default values for other parameters.
5. In the **Device List** area, click **Select** or **Add Manually** to add the local AC at 11.1.1.104 as an access device.
The IP address must be the source IP address specified for outgoing RADIUS packets in the RADIUS scheme on the central AC.
6. Click **OK**.

Figure 2 Adding an access device

The screenshot shows the 'Add Access Device' page in the INC management interface. The page is divided into two main sections: 'Access Configuration' and 'Device List'.

Access Configuration:

- Authentication Port: 1812
- Service Type: Unlimited
- Access Device Type: (General)
- Shared Key: 12345678
- Accounting Port: 1813
- Forcible Logout Type: Disconnect user
- Service Group: Ungrouped
- Confirm Shared Key: 12345678

Device List:

Device Name	Device IP	Device Model	Comments	Delete
Local AC	11.1.1.1			

Total Items: 1.

Buttons: Select, Add Manually, Clear All, OK, Cancel.

Adding an access policy

1. From the navigation tree, select **User Access Policy > Access Policy**.
2. Click **Add**.
3. On the **Add Access Policy** page, configure the following parameters, as shown in [Figure 3](#):
 - Enter **dot1x** in the **Access Policy Name** field.
 - Select **EAP-PEAP** from the **Preferred EAP Type** list, and select **EAP-MSCHAPv2** from the **Subtype** list.

The certificate subtype on the INC server must be the same as the identity authentication method configured on the clients.
4. Click **OK**.

Figure 3 Adding an access policy

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

Basic Information

Access Policy Name * dot1x

Service Group * Ungrouped

Description

Authorization Information

Access Period None

Downstream Rate (Kbps)

Priority

Preferred EAP Type EAP-PEAP

EAP Auto Negotiate Enable

Deploy Address Pool

☐ Deploy User Profile

☐ Deploy ACL

Offline Check Period (Hours)

Allocate IP * No

Upstream Rate (Kbps)

Deploy User Group

Subtype EAP-MSCHAPv2

Maximum Online Duration for a Logon (Minutes)

Deploy VLAN

Deploy VSI name

Authentication Password Account Password

Authentication Binding Information

User Client Configuration

OK Cancel

Adding an access service

1. From the navigation tree, select **User Access Policy > Access Service**.
2. Click **Add**.
3. On the **Add Access Service** page, configure the following parameters, as shown in [Figure 4](#):
 - o Enter **dot1x** in the **Service Name** field.
 - o Select **dot1x** from the **Default Access Policy** list.
4. Click **OK**.

Figure 4 Adding an access service

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

Basic Information

Service Name * dot1x

Service Group * Ungrouped

Default Proprietary Attribute Assignment Policy * Do not use

Default Max. Number of Online Endpoints * 0

Description

☒ Available

Service Suffix

Default Access Policy * dot1x Add

Daily Max. Online Duration * 0

Access Scenario List

Add

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

OK Cancel

Adding an access user

1. From the navigation tree, select **Access User > Access User**.
The access user list opens.
2. Click **Add**.
The **Add Access User** page opens.
3. In the **Access Information** area, configure the following parameters, as shown in [Figure 5](#):
 - a. Click **Select** or **Add User** to associate the user with INC Platform user **user**.
 - b. Enter **user** in the **Account Name** field.
 - c. Enter **dot1x** in the **Password** and **Confirm Password** fields.

4. In the **Access Service** area, select **dot1x** from the list.
5. Click **OK**.

Figure 5 Adding an access user account

Verifying the configuration

Verify that the local AC has associated with the central AC and come online. The state of the local AC changes to **R/M (Run/Master)** on the central AC after it comes up.

```
[Central AC] display wlan local-ac name 3510h-1
```

```

                                Local AC Information

State : I = Idle,           J = Join,           JA = JoinAck,       IL = ImageLoad
        C = Config,       DC = DataCheck,   R = Run

AC name          ACID  State Model          Serial ID
3510h-1          2     R/M   WX3510H             210235A1GCH147000017

```

Verify that the local AC has established a management tunnel with the central AC. The state of an AP changes to **R/M (Run/Master)** on the central AC after it comes online from the local AC.

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

```

Total number of APs: 1
Total number of connected APs: 1
Total number of connected manual APs: 1
Total number of connected auto APs: 0
Total number of connected common APs: 1
Total number of connected WTUs: 0
Total number of inside APs: 0
Maximum supported APs: 4096
Remaining APs: 4095
Total AP licenses: 512
Local AP licenses: 512
Server AP licenses: 0
Remaining AP licenses: 511
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	8	R/M	AP 3620	219801A28N819CE0002T

On the central AC, verify that the AP has associated with the local AC.

[Central AC] display wlan ap-distribution all

Central AC

Slot : 1

Total Number of APs: 0

AP name :

Local AC

Name : 3510h-1

Total Number of APs: 1

AP name : ap1

Connect a client to the wireless network to verify that the client can pass 802.1X authentication.
(Details not shown.)

On the central AC, display wireless client information to verify that the client has come online.

[Central AC] display wlan client

Total number of clients: 1

MAC address	User name	AP name	RID	IP address	VLAN
e49a-dc71-a162	N/A	ap1	1	20.0.0.3	20

On the central AC, display online 802.1X information to verify that the client has passed 802.1X authentication.

[Central AC] dis dot1x connection

Total connections: 1

User MAC address : e49a-dc71-a162

AP name : ap1

Radio ID : 1

SSID : dot1x

BSSID : 3891-d59a-7960

Username : user

Authentication domain : iNC

IPv4 address : 20.0.0.2

Authentication method : EAP

Initial VLAN : 20

Authorization VLAN : 20

Authorization ACL number : 3000

Authorization user profile : N/A

Termination action : Default

Session timeout period : 86400 s

Online from : 2019/5/22 11:31:18

Online duration : 0h 2m 12s

Configuration files

- **Central AC:**

```
#
vlan 1
#
wlan service-template dot1x
    ssid dot1x
    client forwarding-location ac
    client-security authentication-location ac
    akm mode dot1x
    cipher-suite ccmp
    security-ie rsn
    client-security authentication-mode dot1x
    dot1x domain iNC
    service-template enable
#
interface Vlan-interface1
    ip address 11.1.1.3 16
#
interface GigabitEthernet1/0/1
    port link-type trunk
    port trunk permit vlan 11
#
wlan ap ap1 model AP 3620
    serial-id 219801A28N819CE0002T
#
wlan ap-group group1
    control-address enable
    control-address ip 11.1.1.104
ap ap1
ap-model AP 3620
    map-configuration cfa0:/map.txt
    radio 1
        radio enable
        service-template dot1x vlan 20
#
wlan local-ac name 3510h-1 model WX3510H
    serial-id 210235A1JNB166000078
#
```

- **Local AC:**

```
#
    dhcp enable
#
vlan 11 to 12
#
vlan 20
#
```

```

dhcp server ip-pool ap
    gateway-list 12.0.0.1
    network 12.0.0.0 mask 255.255.0.0
    option 43 hex 80070000010b010103
#
dhcp server ip-pool client
    gateway-list 20.0.0.1
    network 20.0.0.0 mask 255.255.0.0
#
interface Vlan-interface11
    ip address 11.1.1.104 255.255.0.0
#
interface Vlan-interface12
    ip address 12.0.0.1 255.255.0.0
    dhcp server apply ip-pool ap
#
interface Vlan-interface20
    ip address 20.0.0.1 255.255.0.0
    dhcp server apply ip-pool client
#
interface GigabitEthernet1/0/1
    port link-type access
    port access vlan 12
#
interface GigabitEthernet1/0/2
    port link-type access
    port access vlan 12
#
interface GigabitEthernet1/0/3
    port link-type access
    port access vlan 11
#
    wlan local-ac enable
    wlan local-ac capwap source-vlan 11
#
    wlan central-ac ip 11.1.1.3
#
dot1x authentication-method eap
#
radius scheme iNC
    primary authentication 8.1.1.231
    primary accounting 8.1.1.231
    key authentication cipher $c$3$t7x0fIARso0US949SnQS2pq53eIdsgUr6z07
    key accounting cipher $c$3$V4YI3sDOEq0VqAIPoANjQOV3ZalvqTL05GC0
    user-name-format without-domain
    nas-ip 11.1.1.104
#
domain iNC

```


authentication lan-access radius-scheme iNC
authorization lan-access radius-scheme iNC
accounting lan-access radius-scheme iNC

Related documentation

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

INTELBRAS Access Controllers

Remote 802.1X Authentication on an AC Hierarchy Network (Central AC Authentication + AP 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
General restrictions and guidelines	1
Example: Configuring remote 802.1X authentication on an AC hierarchy network	1
Network configuration	1
Analysis	2
Restrictions and guidelines	2
Prerequisites	3
Procedures	3
Editing the AP configuration file	3
Configuring the central AC	3
Configuring the local AC	5
Configuring the RADIUS server	7
Verifying the configuration	9
Configuration files	11
Related documentation	13

Introduction

The following information provides an example of configuring remote 802.1X authentication for clients on a network that deploys an AC hierarchy.

Prerequisites

NOTE:

Support for this configuration example varies by device model and version.

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 AC hierarchy, 802.1X, WLAN access, and AP management features.

General restrictions and guidelines

Central ACs on an AC hierarchy network do not support IRF.

Example: Configuring remote 802.1X authentication on an AC hierarchy network

Network configuration

As shown in [Figure 1](#):

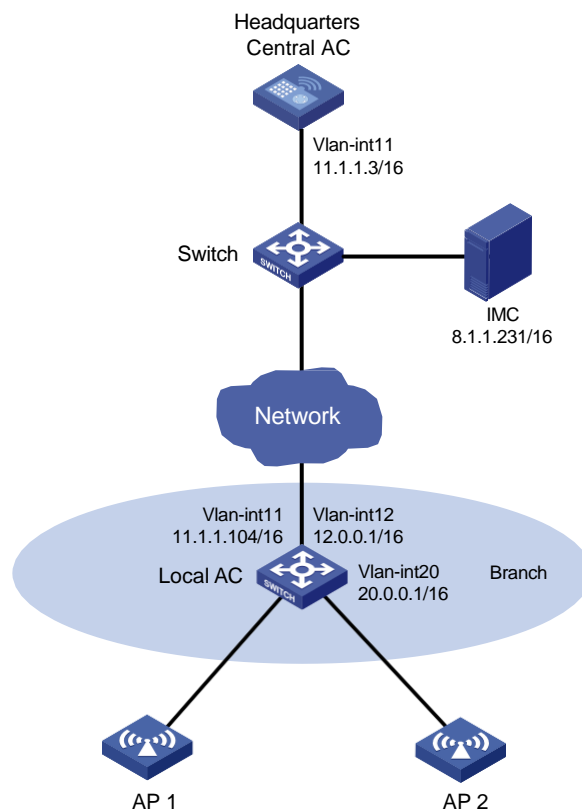
- The network deploys an AC hierarchy that contains one central AC and one local AC. The central AC is deployed at the headquarters and the local AC is a unified wired and wireless access controller. In this example, the APs are connected to the local AC through GigabitEthernet 1/0/1.
- The APs are assigned to VLAN 12 and the clients are assigned to VLAN 20.
- The network deploys a RADIUS server that runs INC for 802.1X authentication.

Configure the devices to meet the following requirements:

- The APs and clients are associated with the local AC.
 - The APs obtain the IP address of the central AC through DHCP Option 43.
 - The AC rediscovery feature is configured on the central AC for the APs to discover the local AC.

- The central AC acts as the authenticator and uses the RADIUS server to perform authentication, authorization, and accounting for the clients. 802.1X authentication is enabled in the service template through which the clients access the network.
- The AP locally forwards client data traffic in VLAN 12.
- The local AC acts as a DHCP server to assign IP addresses to the APs and the clients.

Figure 1 Network diagram



Analysis

For GigabitEthernet 1/0/1 to forward client data traffic in VLAN 12, edit a .txt configuration file and upload the file to the central AC. In the file, the port is added to VLAN 12. Because the clients are assigned to VLAN 20, add the port also to VLAN 20 for the clients to pass RADIUS-based 802.1X authentication and come online.

For an AP to discover the local AC and come online from the local AC, enable the AC rediscovery feature in the view of the manual AP that is created for the AP. In addition, configure the central AC to add the IP address of the local AC to the CAPWAP Control IP Address message element in the discovery responses sent to the AP. If the AC rediscovery feature is not configured for an AP, the central AC will send the IP address of the lightest loaded local AC to the AP. If the lightest loaded local AC is not the local AC in the branch, the AP cannot come online.

Restrictions and guidelines

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

On the local AC, do not enable the auto AP feature. In addition, create a manual AP for each AP in local AC view on the central AC for the central AC to manage the APs.

Prerequisites

Make sure the devices can reach one another.

Procedures

Editing the AP configuration file

Use a text editor to edit the APs' configuration file, and then upload the file to the central AC. In this example, the configuration file name is **map.txt**.

The following is the AP configuration for this example:

```
system-view
vlan 20
interface GigabitEthernet1/0/1
port link-type trunk
port trunk permit vlan 20
```

Configuring the central AC

Configuring interfaces

Create VLAN 11, create VLAN-interface 11, and assign an IP address to the VLAN interface. The AC will use this IP address to establish a management tunnel with the local AC.

```
<Central AC> system-view
[Central AC] vlan 11
[Central AC-vlan11] quit
[Central AC] interface vlan-interface 11
[Central AC-Vlan-interface11] ip address 11.1.1.3 16
[Central AC-Vlan-interface11] quit
```

Configure GigabitEthernet 1/0/1 that connects the central AC to the switch as a trunk port, and assign the port to VLAN 11.

```
[Central AC] interface gigabitethernet 1/0/1
[Central AC-GigabitEthernet1/0/1] port link-type trunk
[Central AC-GigabitEthernet1/0/1] port trunk permit vlan 11
[Central AC-GigabitEthernet1/0/1] quit
```

Configuring a local AC for the central AC

Create local AC **3510h-1** with model **WX3510H** and enter local AC view.

```
[Central AC] wlan local-ac name 3510h-1 model WX3510H
```

Specify the serial ID of the local AC.

```
[Central AC-wlan-local-ac-3510h-1] serial-id 210235A1GCH147000017
[Central AC-wlan-local-ac-3510h-1] quit
```

Configuring RADIUS-based 802.1X authentication

1. Configure a RADIUS scheme:

Create RADIUS scheme **iNC** and enter its view.

```
[Central-AC] radius scheme iNC
```

Specify the IP address of the primary RADIUS authentication server.

- ```
[Central AC-radius-iNC] primary authentication 8.1.1.231
```
- # Specify the IP address of the primary RADIUS accounting server.
- ```
[Central AC-radius-iNC] primary accounting 8.1.1.231
```
- # Set the shared key to **12345678** in plaintext form for secure communication with the RADIUS authentication server.
- ```
[Central AC-radius-iNC] key authentication simple 12345678
```
- # Set the shared key to **12345678** in plaintext form for secure communication with the RADIUS accounting server.
- ```
[Central AC-radius-iNC] key accounting simple 12345678
```
- # Exclude the domain name from usernames sent to the RADIUS servers.
- ```
[Central AC-radius-iNC] user-name-format without-domain
```
- # Specify IP address 11.1.1.3 as the source IP address for outgoing RADIUS packets.
- ```
[Central AC-radius-iNC] nas-ip 11.1.1.3
```
- ```
[Central AC-radius-iNC] quit
```
2. Configure an authentication domain:
 

# Create ISP domain **iNC** and enter its view.

```
[Central AC] domain iNC
```

# Configure the ISP domain to use RADIUS scheme **iNC** for 802.1X user authentication.

```
[Central AC-isp-iNC] authentication lan-access radius-scheme iNC
```

# Configure the ISP domain to use RADIUS scheme **iNC** for 802.1X user authorization.

```
[Central AC-isp-iNC] authorization lan-access radius-scheme iNC
```

# Configure the ISP domain to use RADIUS scheme **iNC** for 802.1X user accounting.

```
[Central AC-isp-iNC] accounting lan-access radius-scheme iNC
```

```
[Central AC-isp-iNC] quit
```
  3. Configure EAP relay as the method for the AC to exchange packets with the RADIUS server.
- ```
[Central AC] dot1x authentication-method eap
```

Configuring a service template

- # Create service template **dot1x** and set the SSID of the service template.
- ```
[Central AC] wlan service-template dot1x
```
- ```
[Central AC-wlan-st-dot1x] ssid dot1x
```
- # Assign VLAN 20 to the matching clients.
- ```
[Central AC-wlan-st-dot1x] vlan 20
```
- # Specify the central AC as the authenticator.
- ```
[Central AC-wlan-st-dot1x] client-security authentication-location central-ac
```
- # Configure APs to forward client data traffic from all VLANs. If the APs act as client traffic forwarder by default, skip this step.
- ```
[Central AC-wlan-st-dot1x] client forwarding-location ap
```
- # Set the AKM mode to 802.1X.
- ```
[Central AC-wlan-st-dot1x] akm mode dot1x
```
- # Specify the CCMP cipher suite and enable the RSN IE in beacon and probe responses.
- ```
[Central AC-wlan-st-dot1x] cipher-suite ccmp
```
- ```
[Central AC-wlan-st-dot1x] security-ie rsn
```
- # Set the access authentication mode to 802.1X authentication.
- ```
[Central AC-wlan-st-dot1x] client-security authentication-mode dot1x
```
- # Specify ISP domain **iNC** for authenticating the 802.1X client.

```
[Central AC-wlan-st-dot1x] dot1x domain iNC
```

# Enable the service template.

```
[Central AC-wlan-st-dot1x] service-template enable
```

```
[Central AC-wlan-st-dot1x] quit
```

## Creating a manual AP

# Create manual AP **ap1** and specify the AP model and serial ID.

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

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

```
[Central AC-wlan-ap-ap1] quit
```

# Create AP group **group1** and configure a grouping rule by AP name to add AP **ap1** to the group.

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

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

---

### NOTE:

In a large-scale network, configure AP settings in AP group view instead of AP view as a best practice.

---

# Enable the AC rediscovery feature.

```
[Central AC-wlan-ap-group-group1] control-address enable
```

# Specify 11.1.1.104 (an IP address on the local AC) as the IP address to be carried in the CAPWAP Control IP Address message element.

```
[Central AC-wlan-ap-group-group1] control-address ip 11.1.1.104
```

# Bind service template **dot1x** to radio 1 and specify VLAN 20 for radio 1.

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

```
[Central AC-wlan-ap-group-group1-ap-model-AP 3620] radio 1
```

```
[Central AC-wlan-ap-group-group1-ap-model-AP 3620-radio-1] service-template dot1x vlan 20
```

# Enable radio 1.

```
[Central AC-wlan-ap-group-group1-ap-model-AP 3620-radio-1] radio enable
```

```
[Central AC-wlan-ap-group-group1-ap-model-AP 3620-radio-1] quit
```

## Configuring the local AC

### 1. Configure the local AC feature:

# Enable the local AC feature.

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

```
[Local AC] wlan local-ac enable
```

# Specify the central AC for the local AC.

```
[Local AC] wlan central-ac ip 11.1.1.3
```

# Configure the local AC to use VLAN 11 to establish CAPWAP tunnels with the central AC.

```
[Local AC] wlan local-ac capwap source-vlan 11
```

### 2. Configure IP address pool settings:

# Enable the DHCP service.

```
[Local AC] dhcp enable
```

# Configure DHCP address pool **ap**. In the address pool, specify 12.0.0.1 as the gateway IP address and 12.0.0.0/16 as the subnet for dynamic allocation.

```
[Local AC] dhcp server ip-pool ap
```



```
[Local AC-dhcp-pool-ap] gateway-list 12.0.0.1
[Local AC-dhcp-pool-ap] network 12.0.0.0 mask 255.255.0.0
```

**# Configure Option 43 to specify the central AC address as the AC address in DHCP address pool ap.**

```
[Local AC-dhcp-pool-ap] option 43 hex 80070000010b010103
[Local AC-dhcp-pool-ap] quit
```

**# Configure DHCP address pool client. In the address pool, specify 20.0.0.1 as the gateway IP address and 20.0.0.0/16 as the subnet for dynamic allocation.**

```
[Local AC] dhcp server ip-pool client
[Local AC-dhcp-pool-client] gateway-list 20.0.0.1
[Local AC-dhcp-pool-client] network 20.0.0.0 mask 255.255.0.0
[Local AC-dhcp-pool-client] quit
```

### 3. Configure interfaces:

**# Create VLAN 11, create VLAN-interface 11, and assign an IP address to the VLAN interface. The local AC will use this IP address to establish CAPWAP tunnels with the central AC.**

```
[Local AC] vlan 11
[Local AC-vlan11] quit
[Local AC] interface vlan-interface 11
[Local AC-Vlan-interface11] ip address 11.1.1.104 255.255.0.0
[Local AC-Vlan-interface11] quit
```

**# Create VLAN 12, create VLAN-interface 12, and assign an IP address to the VLAN interface. The local AC assigns VLAN 12 to an AP when the AP comes online.**

```
[Local AC] vlan 12
[Local AC-vlan12] quit
[Local AC] interface vlan-interface 12
[Local AC-Vlan-interface12] ip address 12.0.0.1 255.255.0.0
[Local AC-Vlan-interface12] dhcp server apply ip-pool ap
[Local AC-Vlan-interface12] quit
```

**# Create VLAN 20, create VLAN-interface 20, and assign an IP address to the VLAN interface. The local AC assigns this VLAN to a wireless client when the client comes online.**

```
[Local AC] vlan 20
[Local AC-vlan20] quit
[Local AC] interface vlan-interface 20
[Local AC-Vlan-interface20] ip address 20.0.0.1 255.255.0.0
[Local AC-Vlan-interface20] dhcp server apply ip-pool client
[Local AC-Vlan-interface20] quit
```

**# Configure GigabitEthernet 1/0/1 that connects the local AC to AP 1 as a trunk port, assign the port to VLAN 12 and VLAN 20, and set the PVID to 12.**

```
[Local AC] interface GigabitEthernet 1/0/1
[Local AC-GigabitEthernet1/0/1] port link-type trunk
[Local AC-GigabitEthernet1/0/1] port trunk permit vlan 12 20
[Local AC-GigabitEthernet1/0/1] port trunk pvid vlan 12
[Local AC-GigabitEthernet1/0/1] quit
```

**# Configure GigabitEthernet 1/0/2 that connects the local AC to AP 2 as a trunk port, assign the port to VLAN 12 and VLAN 20, and set the PVID to 12.**

```
[Local AC] interface GigabitEthernet 1/0/2
[Local AC-GigabitEthernet1/0/2] port link-type trunk
[Local AC-GigabitEthernet1/0/2] port trunk permit vlan 12 20
[Local AC-GigabitEthernet1/0/2] port trunk pvid vlan 12
```

```
[Local AC-GigabitEthernet1/0/2] quit
Configure GigabitEthernet 1/0/3 that connects the local AC to the headquarters as an access
port, and assign the port to VLAN 11.
[Local AC] interface GigabitEthernet 1/0/3
[Local AC-GigabitEthernet1/0/3] port link-type access
[Local AC-GigabitEthernet1/0/3] port access vlan 11
[Local AC-GigabitEthernet1/0/3] quit
Create a static route.
[Local AC] ip route-static 0.0.0.0 0.0.0.0 11.1.1.3
```

## Configuring the RADIUS server

### Prerequisites

The RADIUS server runs INC PLAT 7.2 (E0403p10), INC INC - EIA 7.2 (E0405), and INC EIP 7.2 (E0405).

Make sure the RADIUS server has been installed with the EAP-PEAP certificate.

### Adding the central AC as an access device to INC

1. Log in to INC and click the **User** tab.
2. From the navigation tree, select **User Access Policy > Access Device Management > Access Device**.
3. Click **Add**.  
The **Add Access Device** page opens.
4. In the **Access Configuration** area, configure the following parameters, as shown in [Figure 2](#):
  - o Enter **12345678** in the **Shared Key** and **Confirm Shared Key** fields. The shared key must be the same as the authentication and accounting shared keys configured on the central AC.
  - o Use the default values for other parameters.
5. In the **Device List** area, click **Select** or **Add Manually** to add the central AC at 11.1.1.3 as an access device.

The IP address must be the source IP address specified for outgoing RADIUS packets in the RADIUS scheme on the central AC.

6. 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          | Unlimited | Forcible Logout Type | Disconnect user |
| Access Device Type    | (General) | Service Group        | Ungrouped       |
| Shared Key *          | 12345678  | Confirm Shared Key * | 12345678        |
| Access Location Group | ---       |                      |                 |

**Device List**

Select Add Manually Clear All Click OK to save your change.

| Device Name | Device IP | Device Model | Comments | Delete |
|-------------|-----------|--------------|----------|--------|
| Central AC  | 11.1.1.1  |              |          |        |

Total Items: 1.

OK Cancel

## Adding an access policy

1. From the navigation tree, select **User Access Policy > Access Policy**.
2. Click **Add**.
3. On the **Add Access Policy** page, configure the following parameters, as shown in [Figure 3](#):
  - Enter **dot1x** in the **Access Policy Name** field.
  - Select **EAP-PEAP** from the **Preferred EAP Type** list, and select **EAP-MSCHAPv2** from the **Subtype** list.

The certificate subtype on the INC server must be the same as the identity authentication method configured on the clients.

4. Click **OK**.

**Figure 3** Adding an access policy

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

Basic Information

Access Policy Name \* dot1x

Service Group \* Ungrouped

Description

Authorization Information

Access Period None

Downstream Rate (Kbps)

Priority

Preferred EAP Type EAP-PEAP

EAP Auto Negotiate Enable

Deploy Address Pool

☐ Deploy User Profile

☐ Deploy ACL

Offline Check Period (Hours)

Allocate IP \* No

Upstream Rate (Kbps)

Deploy User Group

Subtype EAP-MSCHAPv2

Maximum Online Duration for a Logon (Minutes)

Deploy VLAN

Deploy VSI name

Authentication Password Account Password

Authentication Binding Information

User Client Configuration

OK Cancel

## Adding an access service

1. From the navigation tree, select **User Access Policy > Access Service**.
2. Click **Add**.
3. On the **Add Access Service** page, configure the following parameters, as shown in [Figure 4](#):
  - Enter **dot1x** in the **Service Name** field.
  - Select **dot1x** from the **Default Access Policy** list.
4. Click **OK**.

**Figure 4 Adding an access service**

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

Basic Information

Service Name \* dot1x

Service Group \* Ungrouped

Default Proprietary Attribute Assignment Policy \* Do not use

Default Max. Number of Online Endpoints \* 0

Description

☒ Available

Service Suffix

Default Access Policy \* dot1x Add

Daily Max. Online Duration \* 0

Access Scenario List

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

OK Cancel

## Adding an access user

- From the navigation tree, select **Access User > Access User**.  
The access user list opens.
- Click **Add**.  
The **Add Access User** page opens.
- In the **Access Information** area, configure the following parameters, as shown in Figure 5:
  - Click **Select** or **Add User** to associate the user with INC Platform user **user**.
  - Enter **user** in the **Account Name** field.
  - Enter **dot1x** in the **Password** and **Confirm Password** fields.
- In the **Access Service** area, select **dot1x** from the list.
- Click **OK**.

**Figure 5 Adding an access user account**

User > All Access Users > Add Access User

Access Information

User Name \* user Select Add User

Account Name \* user

☐ Trial Account

☐ Default BYOD User

☐ MAC Authentication User

☐ Computer User

☐ Fast Access User

Password \* \*\*\*\*

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

☒ Allow User to Change Password

☐ Enable Password Strategy

☐ Modify Password at Next Login

Start Time

End Time

Max. Idle Time (Minutes)

Max. Concurrent Logins 1

Login Message

Access Service

| Service Name                              | Service Suffix | Status    | Allocate IP |
|-------------------------------------------|----------------|-----------|-------------|
| <input checked="" type="checkbox"/> dot1x |                | Available |             |

Binding Information

OK OK & Print Cancel

## Verifying the configuration

# Verify that the local AC associates with the central AC and comes online. The state of the local AC changes to **R/M (Run/Master)** on the central AC after it comes up.

```
[Central AC] display wlan local-ac name 3510h-1
```

Local AC Information

```

State : I = Idle, J = Join, JA = JoinAck, IL = ImageLoad
 C = Config, DC = DataCheck, R = Run
AC name ACID State Model Serial ID
3510h-1 2 R/M WX3510H 210235A1GCH147000017

```

**# Verify that the local AC has established a management tunnel with the central AC. The state of an AP changes to **R/M (Run/Master)** on the central AC after it comes online from the local AC.**

```

[Central AC] display wlan ap all
Total number of APs: 1
Total number of connected APs: 1
Total number of connected manual APs: 1
Total number of connected auto APs: 0
Total number of connected common APs: 1
Total number of connected WTUs: 0
Total number of inside APs: 0
Maximum supported APs: 4096
Remaining APs: 4095
Total AP licenses: 512
Local AP licenses: 512
Server AP licenses: 0
Remaining AP licenses: 511
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
apl 8 R/M AP 3620 219801A28N819CE0002T

```

**# On the central AC, verify that the AP has associated with the local AC.**

```

[Central AC] display wlan ap-distribution all
Central AC
Slot : 1
Total Number of APs: 0
AP name :

```

```

Local AC
Name : 3510h-1
Total Number of APs: 1
AP name : apl

```

**# Connect a client to the wireless network to verify that the client can pass 802.1X authentication. (Details not shown.)**

**# On the central AC, display wireless client information to verify that the client has come online.**

```

[Central AC] display wlan client
Total number of clients: 1

MAC address User name AP name RID IP address VLAN
e49a-dc71-a162 N/A apl 1 20.0.0.2 20

```

# On the central AC, display online 802.1X information to verify that the client has passed 802.1X authentication.

```
[Central AC] display dot1x connection
Total connections: 1
User MAC address : e49a-dc71-a162
AP name : ap1
Radio ID : 1
SSID : dot1x
BSSID : 3891-d59a-7960
Username : user
Authentication domain : iNC
IPv4 address : 20.0.0.2
Authentication method : EAP
Initial VLAN : 20
Authorization VLAN : 20
Authorization ACL number : N/A
Authorization user profile : N/A
Termination action : Default
Session timeout period : 86400 s
Online from : 2019/05/22 11:31:18
Online duration : 0h 2m 12s
```

## Configuration files

- Central AC:

```
#
vlan 11
#
dot1x authentication-method eap
#
wlan service-template 1
 ssid dot1x
 client forwarding-location ap
 client-security authentication-location central-ac
 akm mode dot1x
 cipher-suite ccmp
 security-ie rsn
 client-security authentication-mode dot1x
 dot1x domain iNC
 service-template enable
#
interface Vlan-interface11
 ip address 11.1.1.3 255.255.0.0
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 11
#
```

```

radius scheme iNC
 primary authentication 8.1.1.231
 primary accounting 8.1.1.231
 key authentication cipher c3$t7x0fIARso0US949SnQS2pq53eIdsgUr6z07
 key accounting cipher c3$V4YI3sDOEq0VqAIPoaNjQOV3ZalvqTL05GC0
 user-name-format without-domain
 nas-ip 11.1.1.3
#
domain iNC
 authentication lan-access radius-scheme iNC
 authorization lan-access radius-scheme iNC
 accounting lan-access radius-scheme iNC
#
wlan ap ap1 model AP 3620
 serial-id 219801A28N819CE0002T
#
wlan ap-group group1
 control-address enable
 control-address ip 11.1.1.104
ap ap1
ap-model AP 3620
 map-configuration cfa0:/map.txt
 radio 1
 radio enable
 service-template dot1x vlan 20
#
wlan local-ac name 3510h-1 model WX3510H
 serial-id 210235A1JNB166000078
#

```

- **Local AC:**

```

#
dhcp enable
#
vlan 11 to 12
#
vlan 20
#
dhcp server ip-pool ap
 gateway-list 12.0.0.1
 network 12.0.0.0 mask 255.255.0.0
 option 43 hex 80070000010b010103
#
dhcp server ip-pool client
 gateway-list 20.0.0.1
 network 20.0.0.0 mask 255.255.0.0
#
interface Vlan-interface11
 ip address 11.1.1.104 255.255.0.0

```

```

#
interface Vlan-interface12
 ip address 12.0.0.1 255.255.0.0
 dhcp server apply ip-pool ap
#
interface Vlan-interface20
 ip address 20.0.0.1 255.255.0.0
 dhcp server apply ip-pool client
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 12 20
 port trunk pvid vlan 12
#
interface GigabitEthernet1/0/2
 port link-type trunk
 port trunk permit vlan 12 20
 port trunk pvid vlan 12
#
interface GigabitEthernet1/0/3
 port link-type access
 port access vlan 11
#
 wlan local-ac enable
 wlan local-ac capwap source-vlan 11
#
 wlan central-ac ip 11.1.1.3
#
 ip route-static 0.0.0.0 0.0.0.0 11.1.1.3

```

## Related documentation

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



# INTELBRAS Access Controllers AC Hierarchy (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 AC hierarchy ..... | 1  |
| Network configuration .....             | 1  |
| Analysis .....                          | 2  |
| Restrictions and guidelines .....       | 2  |
| Procedures .....                        | 3  |
| Configuring the central AC .....        | 3  |
| Configuring the local AC .....          | 5  |
| Configuring the INC server .....        | 7  |
| Verifying the configuration .....       | 11 |
| Configuration files .....               | 13 |
| Related documentation .....             | 15 |

# Introduction

The following information provides an AC hierarchy configuration example.

## Prerequisites

---

**NOTE:**

Support for this configuration example varies by device model and version.

---

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

The following information is provided based on the assumption that you have basic knowledge of IPv6, AC hierarchy, portal, WLAN access, and AP management.

## Example: Configuring AC hierarchy

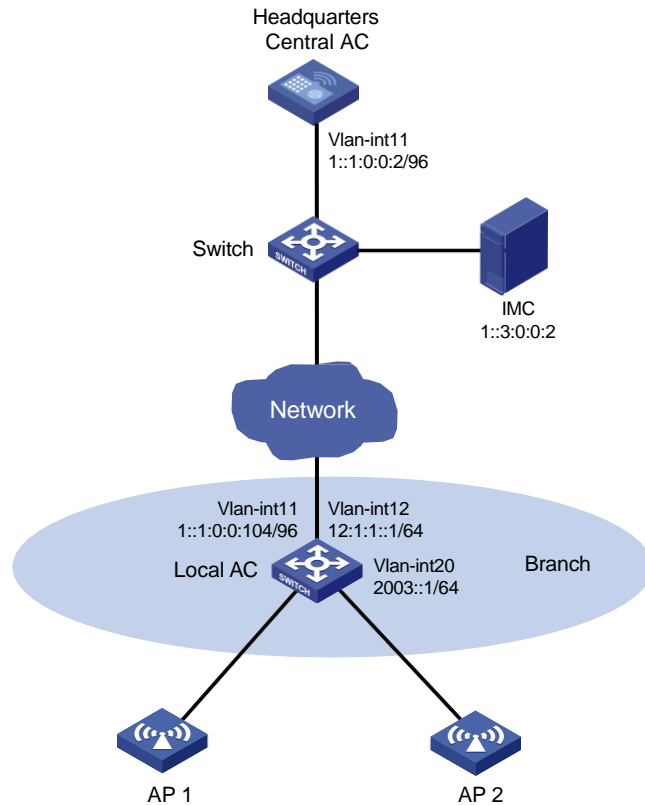
### Network configuration

As shown in [Figure 1](#), the central AC is deployed at the headquarters and a local AC (a unified wired and wireless AC) is deployed at the branch. The central AC performs client authentication and the local AC forwards client traffic.

Configure network settings to meet the following requirements:

- APs obtain the IPv6 address of the central AC through DHCPv6 and establish CAPWAP tunnels with the local AC after AC rediscovery.
- The INC server performs portal authentication as a portal server and AAA server.
- The local AC assigns IPv6 addresses to APs and clients as a DHCPv6 server.

**Figure 1 Network diagram**



## Analysis

- For interface GigabitEthernet1/0/1 on an AP to join the local-forwarding VLAN, use a text editor to create an AP configuration file and upload the file to the central AC.
- With AC rediscovery enabled, the APs might fail to come online through the local AC in the branch if the local AC is not the lowest-loaded AC. For the central AC to assign the local AC to the APs at AC rediscovery, specify the local AC for APs.

## Restrictions and guidelines

When you configure AC hierarchy, follow these restrictions and guidelines:

- Use the actual serial ID of an AP to uniquely identify that AP.
- Do not configure any portal settings on the local AC when portal authentication and local forwarding are used in the AC hierarchy network.
- Do not enable auto AP on the local AC, and do not create APs on the local AC if the APs are to be managed centrally by the central AC.
- Disable firmware upgrade for the local AC because the S5560 unified wired and wireless AC and the access controller module have different software versions.
- The URL of the portal Web server redirected to clients does not contain any parameters by default. You must configure the parameters manually.
- Central ACs do not support IRF.

# Procedures

## Configuring the central AC

1. Make sure the devices can reach each other. (Details not shown.)
2. Create AP configuration file **map.txt** as follows and then upload the file to the central AC.  

```
system-view
vlan 20
interface GigabitEthernet1/0/1
port link-type trunk
port trunk permit vlan 20
```
3. Create VLAN 11 and VLAN-interface 11, and assign an IPv6 address to the VLAN interface.  

```
<Central AC> system-view
[Central AC] vlan 11
[Central AC-vlan11] quit
[Central AC] interface vlan-interface 11
[Central AC-Vlan-interface11] ipv6 address 1::1:0:0:2/96
[Central AC-Vlan-interface11] quit
```
4. Configure GigabitEthernet 1/0/1 that connects the central AC to the switch as a trunk port, and assign the port to VLAN 11.  

```
[Central AC] interface gigabitethernet 1/0/1
[Central AC-GigabitEthernet1/0/1] port link-type trunk
[Central AC-GigabitEthernet1/0/1] port trunk permit vlan 11
[Central AC-GigabitEthernet1/0/1] quit
```
5. Create local AC **wx3540h**, and specify the serial ID of the local AC.  

```
[Central AC] wlan local-ac name wx3540h model WX3540H
[Central AC-wlan-local-ac-wx3540h] serial-id 210235A1JQB161000013
[Central AC-wlan-local-ac-wx3540h] quit
```
6. Configure the RADIUS scheme for portal authentication:  
**# Create RADIUS scheme iNC.**  

```
[Central AC] radius scheme iNC
```

**# Specify the IPv6 address of the primary authentication server as 1::3:0:0:2.**  

```
[Central AC-radius-iNC] primary ipv6 authentication 1::3:0:0:2
```

**# Specify the IPv6 address of the primary accounting server as 1::3:0:0:2.**  

```
[Central AC-radius-iNC] primary ipv6 accounting 1::3:0:0:2
```

**# Set the shared key to 12345678 in plaintext form for secure authentication communication.**  

```
[Central AC-radius-iNC] key authentication simple 12345678
```

**# Set the shared key to 12345678 in plaintext form for secure accounting communication.**  

```
[Central AC-radius-iNC] key accounting simple 12345678
```

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

```
[Central AC-radius-iNC] user-name-format without-domain
```

**# Specify IPv6 address 1::1:0:0:2 as the source IPv6 address of outgoing RADIUS packets.**  

```
[Central AC-radius-iNC] nas-ip ipv6 1::1:0:0:2
[Central AC-radius-iNC] quit
```
7. Configure the authentication domain for portal authentication:

- # Create domain **iNC** and enter its view.
- ```
[Central AC] domain iNC
```
- # Perform RADIUS authentication for portal users based on scheme **iNC**.
- ```
[Central AC-isp-iNC] authentication portal radius-scheme iNC
```
- # Perform RADIUS authorization for portal users based on scheme **iNC**.
- ```
[Central AC-isp-iNC] authorization portal radius-scheme iNC
```
- # Perform RADIUS accounting for portal users based on scheme **iNC**.
- ```
[Central AC-isp-iNC] accounting portal radius-scheme iNC
[Central AC-isp-iNC] quit
```
8. Configure the portal authentication server:
- # Create portal authentication server **iNC** and enter its view.
- ```
[Central AC] portal server iNC
```
- # Configure the IPv6 address of the portal authentication server as **1::3:0:0:2** and the plaintext key as **12345678**.
- ```
[Central AC-portal-server-iNC] ipv6 1::3:0:0:2 key simple 12345678
```
9. Configure the portal Web server:
- # Create portal Web server **iNC** and enter its view.
- ```
[Central AC-portal-server-iNC] portal web-server iNC
```
- # Configure the URL for the portal Web server as **http://[1::3:0:0:2]:8080/portal**.
- ```
[Central AC-portal-server-iNC] url http://[1::3:0:0:2]:8080/portal
```
- # Configure the parameters carried in the URL of the portal Web server.
- ```
[Central AC-portal-server-iNC] url-parameter apmac ap-mac
[Central AC-portal-server-iNC] url-parameter ssid ssid
[Central AC-portal-server-iNC] url-parameter userip source-address
[Central AC-portal-server-iNC] url-parameter usermac source-mac
[Central AC-portal-server-iNC] quit
```
10. Configure wireless services:
- # Create service template **portal**.
- ```
[Central AC] wlan service-template portal
```
- # Set the SSID for the service template to **portal**.
- ```
[Central AC-wlan-st-portal] ssid portal
```
- # Assign clients coming online through the service template to VLAN 20.
- ```
[Central AC-wlan-st-portal] vlan 20
```
- # Configure the central AC to perform client authentication.
- ```
[Central AC-wlan-st-portal] client-security authentication-location central-ac
```
- # Enable APs to forward client traffic.
- ```
[Central AC-wlan-st-portal] client forwarding-location ap
```
- # Set the AKM mode to PSK, and set the plaintext preshared key to **12345678**.
- ```
[Central AC-wlan-st-portal] akm mode psk
[Central AC-wlan-st-portal] preshared-key pass-phrase simple 12345678
```
- # Configure the CCMP cipher suite and RSN security IE.
- ```
[Central AC-wlan-st-portal] cipher-suite ccmp
[Central AC-wlan-st-portal] security-ie rsn
```
- # Enable direct IPv6 portal authentication on the service template.
- ```
[Central AC-wlan-st-portal] portal ipv6 enable method direct
```
- # Specify the authentication domain as **iNC** for IPv6 portal users on the service template.
- ```
[Central AC-wlan-st-portal] portal ipv6 domain iNC
```

# Configure the BAS-IPv6 attribute as **1::1:0:0:2** for portal packets sent to the portal authentication server.

```
[Central AC-wlan-st-portal] portal bas-ipv6 1::1:0:0:2
```

# Enable snooping ND packets and snooping DHCPv6 packets.

```
[Central AC-wlan-st-portal] client ipv6-snooping nd-learning enable
```

```
[Central AC-wlan-st-portal] client ipv6-snooping dhcpv6-learning enable
```

# Apply IPv6 portal Web server **iNC** on the service template for portal authentication.

```
[Central AC-wlan-st-portal] portal ipv6 apply web-server iNC
```

# Enable the service template.

```
[Central AC-wlan-st-portal] service-template enable
```

```
[Central AC-wlan-st-portal] quit
```

# Create AP **ap1** and set the serial ID to **219801A28N819CE0002T**.

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

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

```
[Central AC-wlan-ap-ap1] quit
```

# Create AP group **group1** and configure a grouping rule by AP name to add **ap1** to the group.

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

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

---

#### NOTE:

In a large-scale network, configure AP settings in AP group view instead of AP view as a best practice.

---

# Enable AC rediscovery.

```
[Central AC-wlan-ap-group-group1] control-address enable
```

# Specify the local AC with IPv6 address **1::1:0:0:104** for the AP.

```
[Central AC-wlan-ap-group-group1] control-address ipv6 1::1:0:0:104
```

# Bind service template **portal** to radio 1.

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

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

```
1
```

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

# Enable radio 1.

```
[Central AC-wlan-ap-group-group1-ap-model-AP 3620-radio-1] radio enable
```

```
[Central AC-wlan-ap-group-group1-ap-model-AP 3620-radio-1] quit
```

# Bind service template **portal** to radio 2.

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

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

# Enable radio 2.

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

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

# Deploy the configuration file to AP 3620 APs in the AP group.

```
[Central AC-wlan-ap-group-group1-ap-model-AP 3620] map-configuration cfa0:/map.txt
```

## Configuring the local AC

1. Configure the local AC feature:

# Enable the local AC feature.

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

```
[Local AC] wlan local-ac enable
```

# Specify the central AC with IPv6 address **1::1:0:0:2** for the local AC.

```
[Local AC] wlan central-ac ipv6 1::1:0:0:2
```

# Configure the local AC to use VLAN 11 to establish a tunnel with the central AC.

```
[Local AC] wlan local-ac capwap source-vlan 11
```

## 2. Configure DHCP:

# Enable DHCP.

```
[Local AC] dhcp enable
```

# Create DHCPv6 address pool **ap** and specify the subnet for dynamic allocation as **12:1:1::/64**.

```
[Local AC] ipv6 dhcp pool ap
```

```
[Local AC-dhcp-pool-ap] network 12:1:1::/64
```

# Configure Option 52 that specifies the AC's IPv6 address.

```
[Local AC-dhcp-pool-ap] option 52 hex 000100000000000000010000000000001
```

```
[Local AC-dhcp-pool-ap] quit
```

# Create DHCPv6 address pool **client** and specify the subnet for dynamic allocation as **2003::/64**.

```
[Local AC] ipv6 dhcp pool client
```

```
[Local AC-dhcp-pool-ap] network 2003::/64
```

```
[Local AC-dhcp-pool-ap] quit
```

## 3. Configure VLAN interfaces:

# Create VLAN 11 and VLAN-interface 11, and assign an IPv6 address to the interface. The local AC uses this interface to associate with the central AC.

```
[Local AC] vlan 11
```

```
[Local AC-vlan11] quit
```

```
[Local AC] interface Vlan-interface11
```

```
[Local AC-Vlan-interface11] ipv6 address 1::1:0:0:104/96
```

```
[Local AC-Vlan-interface11] quit
```

# Create VLAN 12 and VLAN-interface 12, and assign an IPv6 address to the interface. The local AC uses this interface to associate with APs.

```
[Local AC] vlan 12
```

```
[Local AC-vlan12] quit
```

```
[Local AC] interface Vlan-interface12
```

```
[Local AC-Vlan-interface12] ipv6 address 12:1:1::1/64
```

# Disable RA message suppression, and set both the M flag and O flag to 1 in RA advertisements to be sent.

```
[Local AC-Vlan-interface12] undo ipv6 nd ra halt
```

```
[Local AC-Vlan-interface12] ipv6 nd autoconfig managed-address-flag
```

```
[Local AC-Vlan-interface12] ipv6 nd autoconfig other-flag
```

# Enable the DHCPv6 server, and apply address pool **ap** to the VLAN-interface 12.

```
[Local AC-Vlan-interface12] ipv6 dhcp select server
```

```
[Local AC-Vlan-interface12] ipv6 dhcp server apply pool ap
```

```
[Local AC-Vlan-interface12] quit
```

# Create VLAN 20 and VLAN-interface 20, and assign an IPv6 address to the interface. The local AC uses this interface to provide access to clients.

```
[Local AC] vlan 20
```

```
[Local AC-vlan20] quit
```

```
[Local AC] interface Vlan-interface20
```

```
[Local AC-Vlan-interface20] ipv6 address 2003::1/64
```



# Disable RA message suppression, and set both the M flag and O flag to 1 in in RA advertisements to be sent.

```
[Local AC-Vlan-interface20] undo ipv6 nd ra halt
[Local AC-Vlan-interface20] ipv6 nd autoconfig managed-address-flag
[Local AC-Vlan-interface20] ipv6 nd autoconfig other-flag
```

# Enable the DHCPv6 server, and apply address pool **client** to the VLAN-interface 20.

```
[Local AC-Vlan-interface20] ipv6 dhcp select server
[Local AC-Vlan-interface20] ipv6 dhcp server apply pool client
[Local AC-Vlan-interface20] quit
```

# Configure GigabitEthernet 1/0/1 that connects the local AC to AP 1 as a trunk port, assign the port to VLAN 12 and VLAN 20, and set the PVID to 12.

```
[Local AC] interface GigabitEthernet 1/0/1
[Local AC-GigabitEthernet1/0/1] port link-type trunk
[Local AC-GigabitEthernet1/0/1] port trunk permit vlan 12 20
[Local AC-GigabitEthernet1/0/1] port trunk pvid vlan 12
[Local AC-GigabitEthernet1/0/1] quit
```

# Configure GigabitEthernet 1/0/2 that connects the local AC to AP 2 as a trunk port, assign the port to VLAN 12 and VLAN 20, and set the PVID to 12.

```
[Local AC] interface GigabitEthernet 1/0/2
[Local AC-GigabitEthernet1/0/2] port link-type trunk
[Local AC-GigabitEthernet1/0/2] port trunk permit vlan 12 20
[Local AC-GigabitEthernet1/0/2] port trunk pvid vlan 12
[Local AC-GigabitEthernet1/0/2] quit
```

# Configure GigabitEthernet 1/0/3 that connects the local AC to the headquarters as an access port, and assign the port to VLAN 11.

```
[Local AC] interface GigabitEthernet 1/0/3
[Local AC-GigabitEthernet1/0/3] port link-type access
[Local AC-GigabitEthernet1/0/3] port access vlan 11
[Local AC-GigabitEthernet1/0/3] quit
```

# Create a static route.

```
[Local AC] ipv6 route-static 0:0::0:0 0 1::1:0:0:2
```

## Configuring the INC server

This example uses the INC server to describe the RADIUS server and portal server configuration. The INC server runs on INC PLAT 7.2 (E0403p10), INC INC - EIA 7.2 (E0405), and INC EIP 7.2 (E0405).

To configure the INC server:

1. Log in to INC and click the **User** tab.
2. Add an access device.
  - a. In the left navigation pane, select **User Access Policy > Access Device Management > Access Device**.
  - b. Click **Add**.

The **Add Access Device** page opens.
  - c. In the **Device List** area, click **Add Manually**, and specify the start IP address as 1::1:0:0:2/96.
  - d. In the **Access Configuration** area, configure the following parameters:
    - Enter **radius** in the **Shared Key** and **Confirm Shared Key** fields.

The key is consistent with the shared key configured on the AC.

- Use the default values for other parameters.
- e. Click **OK**.

**Figure 2 Adding an access device**

3. Add an access policy:
- a. From the navigation pane, select **User Access Policy > Access Policy**.
  - b. Click **Add**.
  - c. On the **Add Access Policy** page, configure the following parameters:
    - Enter the policy name.
    - Select the service group.
    - Use the default values for other parameters.
  - d. Click **OK**.

**Figure 3 Adding an access policy**

4. Add an access service:
- a. From the navigation pane, select **User Access Policy > Access Service**.
  - b. Click **Add**.
  - c. On the **Add Access Service** page, configure the following parameters:

- Enter the service name.
- Use the default values for other parameters.

d. Click **OK**.

**Figure 4 Adding an access service**

The screenshot shows the 'Add Access Service' configuration page. The 'Basic Information' section includes the following fields:

- Service Name \***: qucf-portal
- Service Group \***: Ungrouped
- Default Access Policy \***: qucf-portal
- Default Proprietary Attribute Assignment Policy \***: Do not use
- Default Max. Number of Bound Endpoints \***: 0
- Default Max. Number of Online Endpoints \***: 0
- Description**: (empty)
- Available**: ☒ (checked)
- Transparent Authentication on Portal Endpoints**: ☒ (checked)

5. Add an access user:

a. From the navigation pane, select **Access User > Access User**.

b. Click **Add**.

c. In the **Access Information** area, add a user:

- Select a user.
- Set the password.

d. Click **OK**.

**Figure 5 Adding an access user**

The screenshot shows the 'Add Access User' configuration page. The 'Access Information' section includes the following fields:

- User Name \***: adm\_office\_mac (with 'Select' and 'Add User' buttons)
- Account Name \***: (empty)
- Account Type**: Trial Account, Default BYOD User, MAC Authentication User, Computer User, Fast Access User (all unchecked)
- Password \***: (masked with asterisks)
- Confirm Password \***: (masked with asterisks)
- Allow User to Change Password**: ☒ (checked)
- Enable Password Strategy**: ☐ (unchecked)
- Modify Password at Next Login**: ☐ (unchecked)
- Start Time**: (empty)
- End Time**: (empty)
- Max. Idle Time (Minutes)**: (empty)
- Max. Concurrent Logins**: 1
- Login Message**: (empty)

The 'Access Service' table at the bottom shows the following services:

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

6. Create an IP group:

a. From the navigation tree, select **User Access Policy > Portal Service > IP Group**.

b. Click **Add**.

c. Configure the following parameters:

- **IP Group Name**—Enter the IP group name.
- **Start IP**—Enter the start IP address of the IP group. Make sure the client IP address is in the IP group.
- **End IP**—Enter the end IP address of the IP group. Make sure the client IP address is in the IP group.
- **Service Group**—Select a service group. This example uses the default value **Ungrouped**.

d. Click **OK**.

**Figure 6 Adding an IP group**

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

Add IP Group

|                 |                              |
|-----------------|------------------------------|
| IP Group Name * | client                       |
| IPv6 *          | Yes                          |
| Start IP *      | 2003::0                      |
| End IP *        | 2003:0:0:0:ffff:ffff:fff:fff |
| Service Group   | Ungrouped                    |

7. Add a portal device:
  - a. From the navigation tree, select **User Access Policy > Portal Service > Device**.
  - b. Click **Add**.
  - c. Configure the following parameters:
    - **Device Name**—Enter the device name.
    - **IP Address**—Enter the IP address of the AC's interface connected to the client.
    - **Support Server Heartbeat**—Select whether to support the portal server heartbeat function. In this example, select **No**.
    - **Support User Heartbeat**—Select whether to support the portal user heartbeat function. In this example, select **No**.
    - **Key**—Enter the key. The key must be the same as that configured on the AC.
    - **Version**—Select **Portal 3.0**. Only portal 3.0 supports IPv6.
    - **Access Method**—Select **layer 3**.
  - d. Use the default settings for other parameters.
  - d. Click **OK**.

**Figure 7 Adding a portal device**

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

Add Device

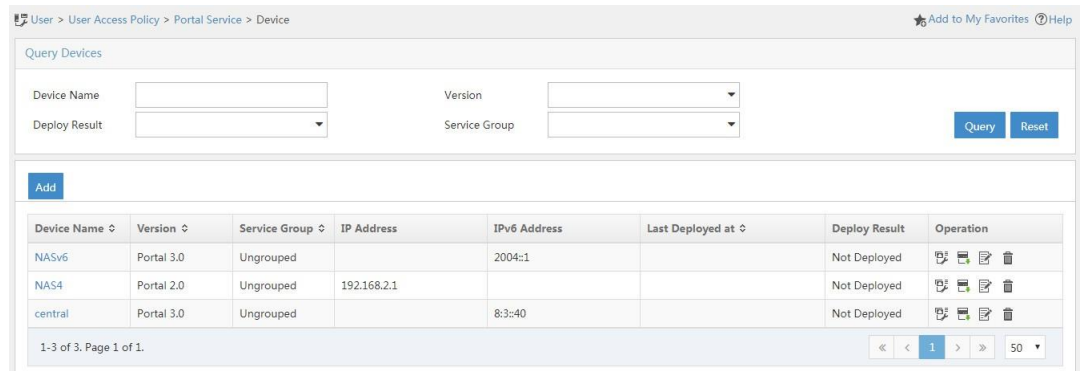
Device Information













|                            |            |                          |           |
|----------------------------|------------|--------------------------|-----------|
| Device Name *              | central    | Service Group *          | Ungrouped |
| Version *                  | Portal 2.0 | IP Address *             | 8.3.40    |
| 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 *            | Layer 3    |                          |           |
| Device Description         |            |                          |           |

8. Associate the portal device with the IP group:

- a. Click the **Port Group** icon  in the **Operation** field for device **NAS** to open the port group configuration page.

**Figure 8 Device list**

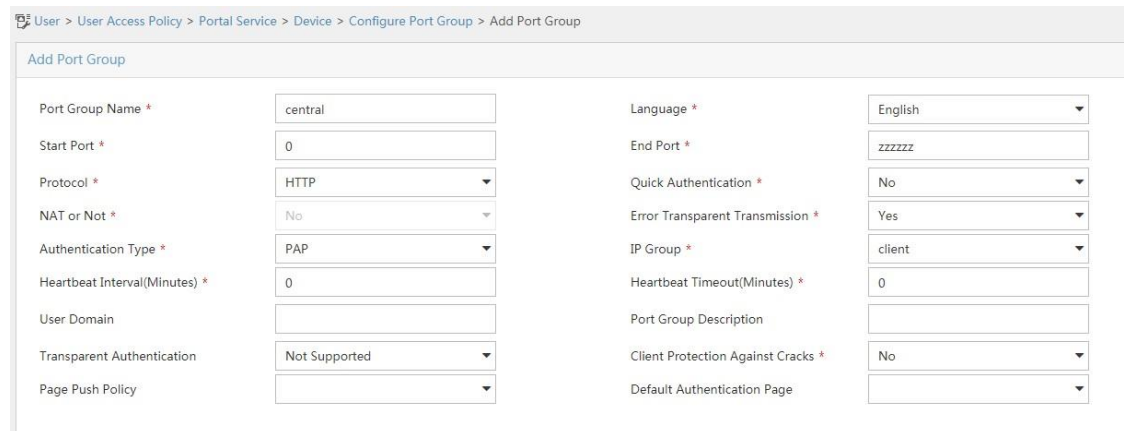


| Device Name | Version    | Service Group | IP Address  | IPv6 Address | Last Deployed at | Deploy Result | Operation                                                                                                                                                                                                                                                                                                                                       |
|-------------|------------|---------------|-------------|--------------|------------------|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| NASv6       | Portal 3.0 | Ungrouped     |             | 2004::1      |                  | Not Deployed  |     |
| NAS4        | Portal 2.0 | Ungrouped     | 192.168.2.1 |              |                  | Not Deployed  |     |
| central     | Portal 3.0 | Ungrouped     |             | 8:3:40       |                  | Not Deployed  |     |

- b. Click **Add**.
- c. Configure the following parameters:
  - **Port Group Name**—Enter the port group name.
  - **IP Group**—Select the configured IP group. The IP address used by the user to access the network must be within this IP address group.

Use the default settings for other parameters.
- d. Click **OK**.

**Figure 9 Adding a port group**



## Verifying the configuration

# Verify that the local AC is in R/M state on the central AC. This state indicates that the local AC has come online on the central AC.

```
[Central AC] display wlan local-ac all
```

```
Total number of local ACs: 1
```

```
Total number of connected local ACs: 1
```

### Local AC Information

```
State : I = Idle, J = Join, JA = JoinAck, IL = ImageLoad
 C = Config, DC = DataCheck, R = Run
```

| AC name | ACID | State | Model   | Serial ID            |
|---------|------|-------|---------|----------------------|
| wx3540h | 2    | R/M   | WX3540H | 210235A1JQB161000013 |

**# Verify that the AP is in R/M state on the central AC. This state indicates that the local AC has established a management tunnel with the central AC after AC rediscovery.**

[Central AC] display wlan ap all

```

Total number of APs: 1
Total number of connected APs: 1
Total number of connected manual APs: 1
Total number of connected auto APs: 0
Total number of connected common APs: 1
Total number of connected WTUs: 0
Total number of inside APs: 0
Maximum supported APs: 1536
Remaining APs: 1535
Total AP licenses: 1024
Local AP licenses: 1024
Server AP licenses: 0
Remaining Local AP licenses: 1023
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     | 4    | R/M   | AP 3620 | 219801A28N819CE0002T |

**# Verify that the AP has associated with the local AC.**

[Central AC] display wlan ap-distribution all

|            |        |                        |
|------------|--------|------------------------|
| Central AC | Slot 2 | Total Number of APs: 0 |
|------------|--------|------------------------|

|          |         |                        |
|----------|---------|------------------------|
| Local AC | wx3540h | Total Number of APs: 1 |
|----------|---------|------------------------|

| AP name | AP ID | AP IP     | AC IP     |
|---------|-------|-----------|-----------|
| ap1     | 4     | 12:1:1::4 | 12:1:1::1 |

**# Verify that a client has come online.**

[Central AC] display wlan client ipv6

| MAC address    | AP name | IPv6 address | VLAN |
|----------------|---------|--------------|------|
| e49a-dc71-a162 | ap1     | 2003::3      | 20   |

**# Verify that the client has passed portal authentication.**

[Central AC] display portal user all

Total portal users: 1

Username: qucf

AP name: ap1

Radio ID: 1

```

SSID: qucf-portal
Portal server: iNC
State: Online
VPN instance: N/A

```

| MAC            | IP      | VLAN | Interface     |
|----------------|---------|------|---------------|
| e49a-dc71-a162 | 2003::3 | 20   | WLAN-BSS2/0/2 |

```

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

```

## Configuration files

- Central AC:

```

#
vlan 11
#
wlan service-template portal
ssid portal
vlan 20
client forwarding-location ap
akm mode psk
preshared-key pass-phrase cipher c3$p0PjuXJ5pGfJ6Z1XDkGRsPR8JoPhrP60GyRn
cipher-suite ccmp
security-ie rsn
client ipv6-snooping nd-learning enable
client ipv6-snooping dhcpv6-learning enable
portal enable method direct
portal domain iNC
portal bas-ip 1::1:0:0:2
portal apply web-server iNC
service-template enable
#
interface Vlan-interface11
ipv6 address 1::1:0:0:2/96
#
interface GigabitEthernet1/0/1
port link-type trunk
port trunk permit vlan 11
#
radius scheme iNC
primary authentication ipv6 1::3:0:0:2
primary accounting ipv6 1::3:0:0:2
key authentication cipher c3$hpDUnHfwXg6gyIvCDstC9zAc8UJueLbLTt/i
key accounting cipher c3$UzY7a5vF6zEHedxpnfv+NBQ2UAhUEbjM+8sZ

```

```

user-name-format without-domain
nas-ip ipv6 1::1:0:0:2
#
domain iNC
authentication portal radius-scheme iNC
authorization portal radius-scheme iNC
accounting portal radius-scheme iNC
#
portal web-server iNC
url http://[1::3:0:0:2]:8080/portal
url-parameter apmac ap-mac
url-parameter ssid ssid
url-parameter userip source-address
url-parameter usermac source-mac
#
portal server iNC
ipv6 1::3:0:0:2 key cipher c3$G0fWl7UQ9AqnAdOJEnlECL+tSwqQbmV2SuRe
#
wlan ap ap1 model AP 3620
serial-id 219801A28N819CE0002T
#
wlan ap-group group1
ap ap1
ap-model AP 3620
map-configuration cfa0:/map.txt
control-address enable
control-address ipv6 1::1:0:0:104
radio 1
radio enable
service-template portal
radio 2
radio enable
service-template portal
#
wlan local-ac name wx3540h model WX3540H
serial-id 210235A1JQB161000013

```

- **Local AC:**

```

#
dhcp enable
#
vlan 11 to 12
#
vlan 20
#
ipv6 dhcp pool ap
network 12:1:1::/64
option 52 hex 00010000000000000001000000000001
#

```



```

ipv6 dhcp pool client
 network 2003::/64
#
interface Vlan-interface11
 ipv6 address 1::1:0:0:104/96
#
interface Vlan-interface12
 ipv6 dhcp select server
 ipv6 dhcp server apply pool ap
 ipv6 address 12:1:1::1/64
 ipv6 nd autoconfig managed-address-flag
 ipv6 nd autoconfig other-flag
 undo ipv6 nd ra halt
#
interface Vlan-interface20
 ipv6 dhcp select server
 ipv6 dhcp server apply pool client
 ipv6 address 2003::1/64
 ipv6 nd autoconfig managed-address-flag
 ipv6 nd autoconfig other-flag
 undo ipv6 nd ra halt
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 12 20
port trunk pvid vlan 12
#
interface GigabitEthernet1/0/2
 port link-type trunk
 port trunk permit vlan 12 20
port trunk pvid vlan 12
#
interface GigabitEthernet1/0/3
 port link-type access
 port access vlan 11
#
wlan local-ac enable
wlan local-ac capwap source-vlan 11
#
wlan central-ac ipv6 1::1:0:0:2
#
#
ipv6 route-static 0:0::0:0 0 1::1:0:0:2

```

## Related documentation

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

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