

INTELBRAS Access Controllers License Management 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: Installing AP licenses on an AC | 1 |
| Network configuration | 1 |
| Restrictions and guidelines | 1 |
| Procedures | 2 |
| Obtaining a license key | 2 |
| Identifying the license storage on the AC | 2 |
| Compressing the license storage on the AC | 2 |
| Obtaining device information from the AC | 3 |
| Requesting an activation file on INTELBRAS License Management Platform | 3 |
| Installing an activation file on the AC | 6 |
| Verifying the configuration | 6 |
| Related documentation | 7 |

Introduction

The following information provides an example of installing AP licenses.

Prerequisites

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

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

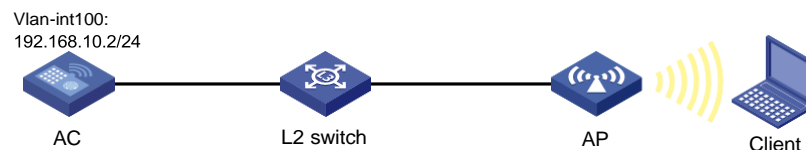
The following information is provided based on the assumption that you have basic knowledge of licensing.

Example: Installing AP licenses on an AC

Network configuration

As shown in [Figure 1](#), install AP licenses on the AC for the AC to manage the AP and for the AP to provide wireless services to the client.

Figure 1 Network diagram



Restrictions and guidelines

- Purchase licenses from INTELBRAS authorized channels.
- To identify the validity periods of the licenses that have been installed on the device, execute the **display license** command. If the license for a feature is time limited, install a new license for the feature before the old license expires.
- When you operate DID files or activation files, follow these restrictions and guidelines:
 - To avoid licensing error, do not modify the file name or edit the file content.
 - Before you install an activation file, download the activation file to the storage media of the device such as flash memory. When you install an activation file, the device automatically copies the activation file to the **license** folder in the root directory of the storage media. The **license** folder stores important files for licensing. For licensed features to function correctly, do not delete or modify the **license** folder or the files in this folder.

Procedures

Obtaining a license key

After you obtain a license key, back up it and keep the backup license key in a safe place for future use.

Obtaining a formal license key

To use a license-based feature, purchase a software license certificate for it. The authorization serial number in the software license certificate is the license key.

Obtaining a trial license key

If you need a trial license key to verify the functionality of a feature before you making a purchase decision, contact your INTELBRAS sales representative or INTELBRAS Support.

Identifying the license storage on the AC

To identify the free space of the license storage, execute the following command in any view:

```
<Sysname> display license feature
Total: 360 Usage: 0
Feature                               Licensed      State
APMGR                                 N              -
```

From the command output, view the **Total** and **Usage** fields to examine whether the remaining license storage is sufficient for installing new licenses. If the remaining license storage is not sufficient, compress the license storage.

The remaining license storage equals to the total amount of license storage minus the used amount of license storage.

Compressing the license storage on the AC

About this task

The license storage stores licensing information and has a fixed size.

You compress the license storage to delete expired and uninstalled license information to ensure sufficient storage space for installing new licenses.

Restrictions and guidelines

If uninstalled licenses or expired licenses exist on the AC, the compression operation will make the DID or DID file change. You will be unable to install the activation file obtained by using the old DID or DID file on the AC. As a best practice, install all activation files registered with the old DID or DID file before performing a compression.

Procedure

Compress the license storage.

```
<Sysname> system-view
[Sysname] license compress
```

This command will delete all data relevant to uninstalled and expired keys/licenses, including Uninstall keys, and create a new device ID for activation keys/files. Make sure you have saved the Uninstall keys so you can apply for a new activation key/file for the unexpired licenses that were covered by the uninstalled activation keys/files.

Are you sure you want to continue? [Y/N]: Y

This operation might take some time. Do not perform any other operations until the operation is completed or a failure message is displayed. Please wait...Done.

Obtaining device information from the AC

Obtain the device SN and DID file.

```
<Sysname> display license device-id
```

```
SN: 210235A1JMC166XXXXXX
```

```
SN CHECK_SUM: 2D0BF254
```

```
Device ID: flash:/license/210235A1JMC166XXXXXX.did
```

Use FTP or TFTP to upload the DID file to a local file system.

```
<Sysname> tftp 192.168.10.22 put flash:/license/210235A1JMC166XXXXXX.did
```

Press CTRL+C to abort.

| % Total | % Received | % Xferd | Average Speed | Time | Time | Time | Current |
|---------|------------|---------|---------------|--------|-------|-------|----------------------------------|
| | | | Dload | Upload | Total | Spent | Left |
| 100 | 1029 | 0 | 0 | 1029 | 0 | 43527 | --:--:-- --:--:-- --:--:-- 60529 |

```
<Sysname>
```

Requesting an activation file on INTELBRAS License Management Platform

Adding license keys

1. Access INTELBRAS License Management Platform at <http://www.intelbras.com.br/en/License>.

Figure 2 Accessing INTELBRAS License Management Platform

The screenshot shows the INTELBRAS License Management Platform interface. At the top, there are three tabs: 'License Activation Requests', 'Device License Transfer Requests', and 'Device License Uninstall Requests'. Below the tabs, there is a progress bar with four steps: 'Step 1: Enter license information' (active), 'Step 2: Bind to hardware device', 'Step 3: Enter user data', and 'Step 4: Review and activate'. On the right side of the progress bar, there are three links: 'Text Help', 'Installation guide link', and 'Access Community'. Below the progress bar, there is a section for adding license keys. It includes a text input field for the license key, a dropdown menu, and buttons for 'Search & Add', 'Import & Add', and 'Clear'. Below this section, there is a table with columns: 'No.', 'License Key', 'Software Barcode', 'Product Description', 'Product Code', 'License Key Status', and 'License Key Type'. The table is currently empty, showing 'No Data'. At the bottom of the interface, there is a 'Next' button and a footer with contact information.


2. On the **License Activation Requests** tab, add license keys.

Figure 3 Adding license keys

The screenshot shows the 'License Activation Requests' wizard. At the top, there are three tabs: 'License Activation Requests' (selected), 'Device License Transfer Requests', and 'Device License Uninstall Requests'. Below the tabs is a progress bar with four steps: 'Step 1: Enter license information' (active), 'Step 2: Bind to hardware device', 'Step 3: Enter user data', and 'Step 4: Review and activate'. A link 'Click here to view text online help' is present. The main area contains a 'License Key' input field with a search icon, and buttons for 'Search & Add', 'Import & Add', and 'Clear'. Below this is a 'Remove' button and a table with the following columns: No., License Key, Software Barcode, Product Description, Product Code, License Key Status, License Key Type, and Remaining Validity Period. The table has one row with the following data: No. 1, License Key 3130A3UK-TrVLUNf4, Software Barcode 213130A3UK021600..., Product Description SME Access Controller..., Product Code LIS-WX-4-SME, License Key Status Delivered, License Key Type Trial, and Remaining Validity Period 180. At the bottom, there is a 'Next' button and a footer with a disclaimer and recommended web browsers.

3. Select license keys to be activated, and then click **Next**.

Binding license keys to the AC

1. Click the  icon next to the empty **Device ID** box in the license key entry. In the dialog box that opens, enter the required device information, and then click **OK**.

For information about how to obtain device information, see "[Obtaining device information from the AC.](#)"

Figure 4 Entering device information

The screenshot shows the 'Enter Device Info' dialog box. It has a title bar 'Enter Device Info' with a close button. The main area contains three input fields: 'Custom Device Identifier' with the value 'NEW H3C', '* Device Info File' with the value 'license_21023...did' and a 'Select' button, and '* Device SN' with the value '21023...'. At the bottom, there are three buttons: 'Yes', 'No', and 'Reset'.

2. Review the bindings carefully. Make sure you understand the impact of the binding operation, and then select the option that explicitly states so.

Figure 5 Reviewing the bindings

The screenshot shows the 'License Activation Requests' wizard, Step 2: Bind to hardware device. The progress bar shows 'Step 2: Bind to hardware device' as the active step. A link 'Click here to view text online help' is present. The main area contains a 'Note' section with three points: 1. A Custom Device Identifier (DID) is a user-defined string that identifies a device for management purposes. It can be a combination of device information such as the device model, IP address, and location, depending on your device identifier conventions. 2. Before you import data, select license keys, export them into a file, and then import that file. 3. Import is not supported when device information contains files. Below the note is a table with the following columns: No., Custom Device Identifier, License Key, Software Barcode, Product Description, Product Code, License Key Status, and License Key Type. The table has one row with the following data: No. 1, Custom Device Identifier NEW H3C, License Key 3130A3UK-TrVLUNf4, Software Barcode 213130A3UK021600..., Product Description SME Access Controller..., Product Code LIS-WX-4-SME, License Key Status Delivered, and License Key Type Trial. At the bottom, there is a checkbox for 'I understand that a license is locked to a device once its license key is bound to that device. All information must be verified carefully to ensure a correct binding.' and buttons for 'Previous' and 'Next'.

3. Click **Next**.

Specifying customer information

Enter customer information, and then click **Next**.

Figure 6 Customer information

License Activation Requests | Device License Transfer Requests | Device License Uninstall Requests

Step 1: Enter license information | Step 2: Bind to hardware device | **Step 3: Enter user data** | Step 4: Review and activate

[Click here to view text online help](#)

* End Customer Company/Organization: ABC

* Your Company/Organization: ABC

* Contact Person: Zhangsan

* Phone Number: 12345678912

* Email Address: Zhangsan@h3c.com

Zip/Postal Code:

Address:

Project Name:

* Verification Code: w3JA

[This email address will be used to receive the activation result. Please make sure this email address is valid.](#)

[w3JA](#)

[Previous](#) [Next](#)

Reviewing information and activating the licenses

1. Review the license key and device information and then select **I accept all terms of INTELBRAS Legal Statement**.
2. Click **Confirm & Activate**.

Figure 7 Confirming and activating the licenses

License Activation Requests | Device License Transfer Requests | Device License Uninstall Requests

Step 1: Enter license information | Step 2: Bind to hardware device | Step 3: Enter user data | **Step 4: Review and activate**

[Click here to view text online help](#)

| No. | Get Activation Info | Custom Device Identifier | License Key | Software Barcode | Product Description | Product Code | License Key Status |
|-----|---------------------|--------------------------|--------------------|---------------------|--------------------------|--------------|--------------------|
| 1 | | NEW H3C | 3130A3UK-TrVLUNf4- | 213130A3UK021600... | SME Access Controller... | LIS-WX-4-SME | Delivered |

Total 1 | 10/page | [Previous](#) [Next](#) | Go to 1

☐ I accept all terms and conditions of [H3C License Service Portal Legal Statement](#)

[Previous](#) [Confirm & Activate](#)

3. Double-check the license key and device information, and then click **OK**.

Figure 8 Confirming information

Confirm

! Verify that all information provided for this activation is correct.

[Cancel](#) [OK](#)

4. Click **Get Activation Info** to download an activation file to the local disk.

Figure 9 Obtaining activation information

License Activation Requests Device License Transfer Requests Device License Uninstall Requests

Step 1: Enter license information Step 2: Bind to hardware device Step 3: Enter user data Step 4: Review and activate

[Click here to view text online help](#)

| No. | Get Activation Info | Custom Device Identifier | License Key | Software Barcode | Product Description | Product Code |
|-----|--------------------------------------|--------------------------|-------------------|---------------------|---------------------------|--------------|
| 1 | <button>Get Activation Info</button> | NEW H3C | 3130A3UK-TrvLUNf4 | 213130A3UK021600... | SME Access Controller ... | LIS-WX-4-SM |

Total 1 10/page < 1 > Go to 1

Bulk Get Activation Info Continue to Activate

☒ I accept all terms and conditions of [H3C License Service Portal Legal Statement](#)

Previous Confirm & Activate

Installing an activation file on the AC

⚠ CAUTION:

Back up an activation file before you install it. If the activation file is inadvertently deleted or becomes unavailable for some other reason, you can use the backup activation file to restore the license.

Use FTP or TFTP to upload the activation file to be installed to the AC.

```
<Sysname> tftp 192.168.10.22 get 210235A1JMC166XXXXXX1909581318505.ak
```

Press CTRL+C to abort.

| % Total | % Received | % Xferd | Average Speed | Time | Time | Time | Current |
|----------|------------|----------|---------------|----------|----------|----------|---------|
| | | | Dload | Upload | Total | Spent | Left |
| 100 | 2594 | 100 | 2594 | 0 | 0 | 42681 | 0 |
| --:--:-- | --:--:-- | --:--:-- | --:--:-- | --:--:-- | --:--:-- | --:--:-- | 48943 |

Writing file...Done.

Install the activation file.

```
<Sysname> system-view
```

```
[Sysname] license activation-file install flash:/210235A1JMC166XXXXXX1909581318505.ak
```

This operation might take some time. Do not perform any other operations until this operation is completed. Please wait...Done.

```
[Sysname]
```

Verifying the configuration

On the AC, view license information to verify that an AP license has been installed.

```
[Sysname] display license
```

```
flash:/license/210235A1JMC166XXXXXX1909581318505.ak
```

Feature: APMGR

Product Description: Enhanced Access Controller License, 8 APs, for Verticals, for V7

Registered at: 2021-05-19 17:29:14

License Type: Trial (days restricted)

Trial Time Left (days): 180

Current State: In use

Pre-installed License

Feature: APMGR

Feature Description: PreAtom This is APMGR license

Time Left (days): 0
Current State: Expired

[Sysname]

Related documentation

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

INTELBRAS Access Controllers

AP Association with the AC at Layer 2

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 an AP to associate with the AC at Layer 2 | 1 |
| Network configuration | 1 |
| Analysis | 2 |
| Restrictions and guidelines | 2 |
| Procedures | 2 |
| Configuring the Layer 3 switch | 2 |
| Configuring the AC | 4 |
| Configuring Layer 2 switch 1 | 5 |
| Configuring Layer 2 switch 2 | 6 |
| Verifying the configuration | 6 |
| Configuration files | 7 |
| Related documentation | 10 |

Introduction

The following information provides an example for configuring APs to associate with the AC at Layer 2.

Prerequisites

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

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

This document assumes that you have basic knowledge of DHCP and WLAN access.

Example: Configuring an AP to associate with the AC at Layer 2

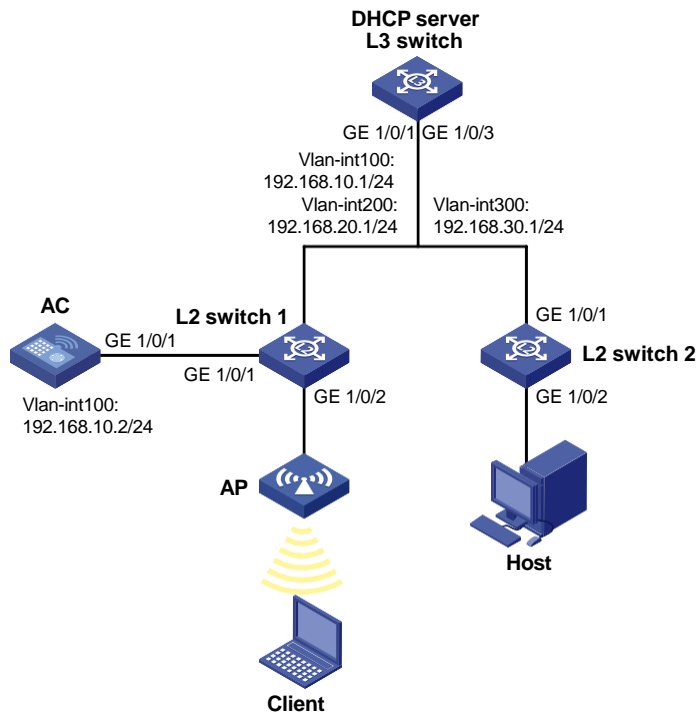
Network configuration

As shown in [Figure 1](#), the AC is attached to a Layer 2 switch, and the Layer 3 switch acts as a DHCP server to assign IP addresses to the AP, client, and host. Assume centralized forwarding is used in this example.

Configure the following settings for the client to communicate with the host:

- Configure the client to access the WLAN through VLAN 200, and the host to access the network through VLAN 300.
- Assign the AC to VLAN 100, and configure the AC to establish tunnels with the AP through a Layer 2 network.
- Configure Layer 2 switch 1 to supply power to the AP through PoE.

Figure 1 Network diagram



Analysis

- For the AP, the client, and the host to obtain IP addresses through DHCP, enable the DHCP server feature on the Layer 3 switch.
- For Layer 2 switch 1 to supply power to the AP, enable PoE on the switch.
- For the client to access the network, configure wireless services on the AC.

Restrictions and guidelines

When you configure AP's association with the AC at Layer 2, follow these restrictions and guidelines:

- Use the serial ID labeled on the AP's rear panel to specify an AP.
- Set the link type of the switch's interface that connects Layer 2 switch 1 to the AP to access. Configure the interface to deny packets from VLAN 1 in case there are too many packets in VLAN 1.

Procedures

Configuring the Layer 3 switch

1. Configure switch interfaces:
Create VLAN 100 and VLAN-interface 100, and assign IP address 192.168.10.1 to the interface. The switch will use this interface to forward traffic in CAPWAP tunnels between the AC and the AP.

```
<L3 switch> system-view
[L3 switch] vlan 100
```

```
[L3 switch-vlan100] quit
[L3 switch] interface vlan-interface 100
[L3 switch-Vlan-interface100] ip address 192.168.10.1 255.255.255.0
[L3 switch-Vlan-interface100] quit
```

Create VLAN 200 and VLAN-interface 200, and assign IP address 192.168.20.1 to the interface. The client will use this VLAN to access the WLAN.

```
[L3 switch] vlan 200
[L3 switch-vlan200] quit
[L3 switch] interface vlan-interface 200
[L3 switch-Vlan-interface200] ip address 192.168.20.1 255.255.255.0
[L3 switch-Vlan-interface200] quit
```

Create VLAN 300 and VLAN-interface 300, and assign IP address 192.168.30.1 to the interface. The host will use this VLAN to communicate with the AC.

```
[L3 switch] vlan 300
[L3 switch-vlan300] quit
[L3 switch] interface vlan-interface 300
[L3 switch-Vlan-interface300] ip address 192.168.30.1 255.255.255.0
[L3 switch-Vlan-interface300] quit
```

Set the link type of GigabitEthernet 1/0/1 that connects the switch to Layer 2 switch 1 to trunk, remove the port from VLAN 1, and assign the port to VLANs 100 and 200.

```
[L3 switch] interface gigabitEthernet 1/0/1
[L3 switch-GigabitEthernet1/0/1] port link-type trunk
[L3 switch-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[L3 switch-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[L3 switch-GigabitEthernet1/0/1] quit
```

Set the link type of GigabitEthernet 1/0/2 that connects the switch to Layer 2 switch 2 to trunk, remove the port from VLAN 1, and assign the port to VLAN 300.

```
[L3 switch] interfac gigabitEthernet 1/0/3
[L3 switch-GigabitEthernet1/0/3] port link-type trunk
[L3 switch-GigabitEthernet1/0/3] undo port trunk permit vlan 1
[L3 switch-GigabitEthernet1/0/3] port trunk permit vlan 300
[L3 switch-GigabitEthernet1/0/3] quit
```

2. Configure the DHCP server:

Enable DHCP server.

```
<L3 switch> system-view
[L3 switch] dhcp enable
```

Create DHCP address pool 1, specify subnet 192.168.10.0/24 in the address pool, and specify the gateway address as 192.168.10.1. The switch will use this address pool to assign an IP address to the AP.

```
[L3 switch] dhcp server ip-pool 1
[L3 switch-dhcp-pool-1] network 192.168.10.0 mask 255.255.255.0
[L3 switch-dhcp-pool-1] gateway-list 192.168.10.1
```

Exclude IP address 192.168.10.2 from dynamic allocation. The excluded IP address is the address of VLAN-interface 100 on the AC.

```
[L3 switch-dhcp-pool-1] forbidden-ip 192.168.10.2
[L3 switch-dhcp-pool-1] quit
```

Create DHCP address pool 2, specify subnet 192.168.20.0/24 in the address pool, specify the gateway address as 192.168.20.1, and specify the address of the DNS server. In this example,

the gateway also acts as the DNS server. The switch will use this address pool to assign an IP address to the client.

```
[L3 switch] dhcp server ip-pool 2
[L3 switch-dhcp-pool-2] network 192.168.20.0 mask 255.255.255.0
[L3 switch-dhcp-pool-2] gateway-list 192.168.20.1
[L3 switch-dhcp-pool-2] dns-list 192.168.20.1
[L3 switch-dhcp-pool-2] quit
```

Create DHCP address pool 3, specify subnet 192.168.30.0/24 in the address pool, specify the gateway address as 192.168.30.1, and specify the address of the DNS server. In this example, the gateway also acts as the DNS server. The switch will use this address pool to assign an IP address to the host.

```
[L3 switch] dhcp server ip-pool 3
[L3 switch-dhcp-pool-3] network 192.168.30.0 mask 255.255.255.0
[L3 switch-dhcp-pool-3] gateway-list 192.168.30.1
[L3 switch-dhcp-pool-3] dns-list 192.168.30.1
[L3 switch-dhcp-pool-3] quit
```

Configuring the AC

1. Configure AC interfaces:

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

```
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 192.168.10.2 255.255.255.0
[AC-Vlan-interface100] quit
```

Create VLAN 200. VLAN 200 will be used for client access.

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

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

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

2. Configure wireless services:

Create service template 1 and enter its view.

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

Configure the SSID as **service**.

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

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

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

Set the CCMP cipher suite and enable the RSE security IE.

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

Enable the AC to forward client data traffic. You can skip this step if the AC is the client traffic forwarder by default.

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

Enable the service template.

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

```
[AC-wlan-st-1] quit
```

3. Configure the AP:

NOTE:

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

Create manual AP **officeap**, and specify the AP model and serial ID.

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

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

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

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

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

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

Bind service template 1 and VLAN 200 to radio 1.

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

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

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

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

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

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

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

Configuring Layer 2 switch 1

Create VLANs 100 and 200. The switch will use VLAN 100 to forward packets between the AC and the AP. VLAN 200 will be used for client access.

```
<L2 switch 1> system-view
```

```
[L2 switch 1] vlan 100
```

```
[L2 switch 1-vlan100] quit
```

```
[L2 switch 1] vlan 200
```

```
[L2 switch 1-vlan200] quit
```

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

```
[L2 switch 1] interface gigabitEthernet 1/0/1
```

```
[L2 switch 1-GigabitEthernet1/0/1] port link-type trunk
```

```
[L2 switch 1-GigabitEthernet1/0/1] undo port trunk permit vlan 1
```

```
[L2 switch 1-GigabitEthernet1/0/1] port trunk permit vlan 100 200
```

```
[L2 switch 1-GigabitEthernet1/0/1] quit
```

Configure GigabitEthernet 1/0/2 that connects the switch to the AP as an access port, assign the port to VLAN 100, and enable PoE.

```
[L2 switch 1] interface gigabitEthernet 1/0/2
```

```
[L2 switch 1-GigabitEthernet1/0/2] port link-type access
```

```
[L2 switch 1-GigabitEthernet1/0/2] port access vlan 100
```

```
[L2 switch 1-GigabitEthernet1/0/2] poe enable
```



```
[L2 switch 1-GigabitEthernet1/0/2] quit
```

Configure GigabitEthernet 1/0/2 that connects the switch to the Layer 3 switch as a trunk port, remove the port from VLAN 1, assign the port to VLANs 100 and 200.

```
[L2 switch 1] interface gigabitEthernet 1/0/3
[L2 switch 1-GigabitEthernet1/0/3] port link-type trunk
[L2 switch 1-GigabitEthernet1/0/3] undo port trunk permit vlan 1
[L2 switch 1-GigabitEthernet1/0/3] port trunk permit vlan 100 200
[L2 switch 1-GigabitEthernet1/0/3] quit
```

Configuring Layer 2 switch 2

Create VLAN 300. The switch will use this VLAN for host access.

```
<L2 switch 2> system-view
[L2 switch 2] vlan 300
[L2 switch 2-vlan300] quit
```

Set the link type of GigabitEthernet 1/0/1 that connects the switch to the Layer 3 switch to trunk, remove the port from VLAN 1, and assign the port to VLAN 300.

```
[L2 switch 2] interface gigabitEthernet 1/0/1
[L2 switch 2-GigabitEthernet1/0/1] port link-type trunk
[L2 switch 2-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[L2 switch 2-GigabitEthernet1/0/1] port trunk permit vlan 300
[L2 switch 2-GigabitEthernet1/0/1] quit
```

Set the link type of GigabitEthernet 1/0/2 that connects the switch to the host to access, and assign the port to VLAN 300.

```
[L2 switch 2] interface gigabitEthernet 1/0/2
[L2 switch 2-GigabitEthernet1/0/2] port link-type access
[L2 switch 2-GigabitEthernet1/0/2] port access vlan 300
[L2 switch 2-GigabitEthernet1/0/2] quit
```

Verifying the configuration

Verify that the AP is in R/M state.

```
<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: 3072
Remaining APs: 3071
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           AP ID   State   Model           Serial ID
officeap          1       R/M     AP 3620          219801A28N819CE0002T

# Verify that the client is connected to radio 1 on AP officeap.
<AC> display wlan client
Total number of clients: 1

MAC address      Username   AP name      RID   IP address      IPv6 address   VLAN
109a-dd9d-fc68   N/A       officeap     1     192.168.20.4    N/A            200

# Verify that the client and the host can ping each other successfully.
C:\Users\system32>ping 192.168.20.4 -t
Pinging 192.168.20.4 with 32 bytes of data:
Reply from 192.168.20.4: bytes=32 time=8ms TTL=255
Reply from 192.168.20.4: bytes=32 time<1ms TTL=255
Reply from 192.168.20.4: bytes=32 time<1ms TTL=255
Reply from 192.168.20.4: bytes=32 time<1ms TTL=255
Reply from 192.168.20.4: bytes=32 time<1ms TTL=255
Reply from 192.168.20.4: bytes=32 time<1ms TTL=255
Reply from 192.168.20.4: bytes=32 time<1ms TTL=255
Reply from 192.168.20.4: bytes=32 time<1ms TTL=255
Reply from 192.168.20.4: bytes=32 time<1ms TTL=255
Reply from 192.168.20.4: bytes=32 time<1ms TTL=255
Reply from 192.168.20.4: bytes=32 time<1ms TTL=255
Ping statistics for 192.168.20.4:
    Packets: Sent = 11, Received = 11, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 8ms, Average = 0ms
Control-C
^C
C:\Users\system32>

```

Configuration files

- Layer 3 switch:


```

#
dhcp enable
#
vlan 1
#
vlan 100
#
vlan 200
#
vlan 300
#

```

```

dhcp server ip-pool 1
 gateway-list 192.168.10.1
 network 192.168.10.0 mask 255.255.255.0
 static-bind ip-address 192.168.10.2 mask 255.255.255.0 hardware-address
 000f-e212-3510
#

```

```

dhcp server ip-pool 2
 gateway-list 192.168.20.1
 network 192.168.20.0 mask 255.255.255.0
 dns-list 192.168.20.1
#

```

```

dhcp server ip-pool 3
 gateway-list 192.168.30.1
 network 192.168.30.0 mask 255.255.255.0
 dns-list 192.168.30.1
#

```

```

interface Vlan-interface100
 ip address 192.168.10.1 255.255.255.0
#

```

```

interface Vlan-interface200
 ip address 192.168.20.1 255.255.255.0
#

```

```

interface Vlan-interface300
 ip address 192.168.30.1 255.255.255.0
#

```

```

interface GigabitEthernet1/0/1
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100 200
#

```

```

interface GigabitEthernet1/0/3
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 300
#

```

- **AC:**

```

#
wlan service-template 1
 ssid service
 client forwarding-location ac
 akm mode psk
 preshared-key pass-phrase cipher $c$3$9tIUH$SkAUVqCH9/EPfL26ldkcEQnngexUEFj
 cipher-suite ccmp
 security-ie rsn
 service-template enable
#
interface Vlan-interface1
#

```

```

interface Vlan-interface100
 ip address 192.168.10.1 255.255.255.0
#
interface Vlan-interface200
 ip address 192.168.20.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100 200
 port trunk pvid vlan 100
#
wlan ap-group group1
 ap officeap
 ap-model AP 3620
 radio 1
 radio enable
 service-template 1 vlan 200
 radio 2
#
wlan ap officeap model AP 3620
 serial-id 219801A28N819CE0002T
#

```

- **Layer 2 switch 1:**

```

#
vlan 100
#
vlan 200
#
interface GigabitEthernet1/0/1
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100 200
#
interface GigabitEthernet1/0/2
 port link-type access
 port access vlan 100
 poe enable
#
interface GigabitEthernet1/0/3
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100 200
#

```

- **Layer 2 switch 2:**

```

#
vlan 300
#

```

```
interface GigabitEthernet1/0/1
  port link-type trunk
  undo port trunk permit vlan 1
  port trunk permit vlan 300
#
interface GigabitEthernet1/0/2
  port link-type access
  port access vlan 300
  poe enable
#
```

Related documentation

- *AP and WT Management Command Reference in INTELBRAS Access Controllers Command References*
- *AP and WT Management Configuration Guide in INTELBRAS Access Controllers Configuration Guides*
- *Network Connectivity Command Reference in INTELBRAS Access Controllers Command References*
- *Network Connectivity 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

AP Association with the AC at Layer 3

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 an AP to associate with the AC at Layer 3 | 1 |
| Network configuration | 1 |
| Analysis | 2 |
| Restrictions and guidelines | 2 |
| Procedures | 2 |
| Configuring the AC | 2 |
| Configuring the Layer 3 switch | 4 |
| Configuring Layer 2 switch 1 | 5 |
| Configuring Layer 2 switch 2 | 6 |
| Verifying the configuration | 6 |
| Configuration files | 7 |
| Related documentation | 10 |

Introduction

The following information provides an example for configuring APs to associate with the AC at Layer 3.

Prerequisites

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

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

This document assumes that you have basic knowledge of WLAN access.

Example: Configuring an AP to associate with the AC at Layer 3

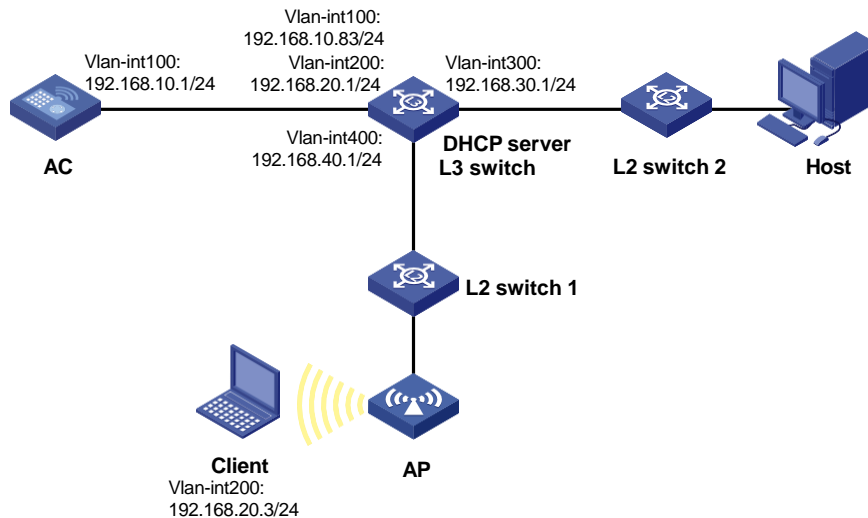
Network configuration

As shown in [Figure 1](#), the AC is attached to the Layer 3 switch and the Layer 3 switch acts as a DHCP server to assign IP addresses to the AP, client, and host. Assume centralized forwarding is used in this example.

Configure the following settings for the client to communicate with the host:

- Configure the client to access the WLAN through VLAN 200, and the host to access the network through VLAN 300.
- Assign the AC to VLAN 100 and the AP to VLAN 400, and configure the AC to establish tunnels with the AP through a Layer 3 network.
- Configure Layer 2 switch 1 to supply power to the AP through PoE.

Figure 1 Network diagram



Analysis

- For the AP, the client, and the host to obtain IP addresses through DHCP, enable the DHCP server feature on the Layer 3 switch.
- For the AC to reach the Layer 3 switch, configure a static route on the AC with the Layer 3 switch as the next hop.
- For the AP to establish tunnels with the AC, configure the DHCP server to send the AC's IP address to the AP through DHCP Option 43.
- For Layer 2 switch 1 to supply power to the AP, enable PoE on the switch.
- For the client to access the network, configure wireless services on the AC.

Restrictions and guidelines

When you configure AP's association with the AC at Layer 3, follow these restrictions and guidelines:

- Use the serial ID labeled on the AP's rear panel to specify an AP.
- Configure the switch's interface that connects Layer 2 switch 1 to the AP as an access port.

Procedures

Configuring the AC

1. Configure AC interfaces:

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

```
<AC> system-view
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface100
[AC-Vlan-interface100] ip address 192.168.10.1 255.255.255.0
```

```
[AC-Vlan-interface100] quit
```

Create VLAN 200. The AC will use VLAN 200 to forward client traffic.

```
[AC] vlan 200
```

```
[AC-vlan200] quit
```

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

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

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

```
[AC-GigabitEthernet1/0/1] undo port trunk permit vlan 1
```

```
[AC-GigabitEthernet1/0/1] port trunk permit vlan 100 200
```

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

2. Configure a static route, whose next hop is the Layer 3 switch.

```
[AC] ip route-static 0.0.0.0 0 24 192.168.10.83
```

3. Configure wireless services:

Create service template 1 and enter its view.

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

Configure the AC to forward client data traffic. You can skip this step if the AC is the client traffic forwarder by default.

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

Configure the SSID as **service**.

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

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

```
[AC-wlan-st-1] akm mode psk
```

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

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

```
[AC-wlan-st-1] cipher-suite ccmp
```

```
[AC-wlan-st-1] security-ie rsn
```

Enable the service template.

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

```
[AC-wlan-st-1] quit
```

4. Configure the AP:

NOTE:

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

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

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

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

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

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

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

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

Bind service template 1 and VLAN 200 to radio 1.

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

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

```
[AC-wlan-ap-group-group1-ap-model-AP 3620-radio-1] service-template 1 vlan 200
```

Enable radio 1.

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

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

Configuring the Layer 3 switch

1. Configure switch interfaces:

Create VLAN 100, VLAN 400, VLAN-interface 100 and VLAN-interface 400, and assign IP addresses to the VLAN interfaces. The switch will use VLAN 100 and VLAN 400 to forward packets between the AC and the AP.

```
<L3 switch> system-view
[L3 switch] vlan 100
[L3 switch-vlan100] quit
[L3 switch] interface vlan-interface 100
[L3 switch-Vlan-interface100] ip address 192.168.10.83 255.255.255.0
[L3 switch-Vlan-interface100] quit
[L3 switch] vlan 400
[L3 switch-vlan400] quit
[L3 switch] interface vlan-interface 400
[L3 switch-Vlan-interface400] ip address 192.168.40.1 255.255.255.0
[L3 switch-Vlan-interface400] quit
```

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

```
[L3 switch] vlan 200
[L3 switch-vlan200] quit
[L3 switch] interface vlan-interface 200
[L3 switch-Vlan-interface200] ip address 192.168.20.1 255.255.255.0
[L3 switch-Vlan-interface200] quit
```

Create VLAN 300 and VLAN-interface 300 and assign an IP address to the VLAN interface. This VLAN will be used for host access.

```
[L3 switch] vlan 300
[L3 switch-vlan300] quit
[L3 switch] interface vlan-interface 300
[L3 switch-Vlan-interface300] ip address 192.168.30.1 255.255.255.0
[L3 switch-Vlan-interface300] quit
```

Configure GigabitEthernet 1/0/1 that connects the switch to the AC as a trunk port, and assign the port to VLANs 100 and 200.

```
[L3 switch] interface gigabitEthernet 1/0/1
[L3 switch-GigabitEthernet1/0/1] port link-type trunk
[L3 switch-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[L3 switch-GigabitEthernet1/0/1] quit
```

Set the link type of GigabitEthernet 1/0/2 that connects the switch to Layer 2 switch 1 to trunk, remove the port from VLAN 1, and assign the port to VLAN 400.

```
[L3 switch] interface gigabitEthernet 1/0/2
[L3 switch-GigabitEthernet1/0/2] port link-type trunk
[L3 switch-GigabitEthernet1/0/2] undo port trunk permit vlan 1
[L3 switch-GigabitEthernet1/0/2] port trunk permit vlan 400
[L3 switch-GigabitEthernet1/0/2] quit
```

Set the link type of GigabitEthernet 1/0/3 that connects the switch to Layer 2 switch 2 to trunk, remove the port from VLAN 1, and assign the port to VLAN 300.

```
[L3 switch] interface gigabitEthernet 1/0/3
```

```
[L3 switch-GigabitEthernet1/0/3] port link-type trunk
[L3 switch-GigabitEthernet1/0/3] undo port trunk permit vlan 1
[L3 switch-GigabitEthernet1/0/3] port trunk permit vlan 300
[L3 switch-GigabitEthernet1/0/3] quit
```

2. Configure DHCP:

Enable DHCP.

```
[L3 switch] dhcp enable
```

Create DHCP address pool 1 to assign an IP address to the AP, and specify subnet 192.168.40.0/24 in the DHCP address pool.

```
[L3 switch] dhcp server ip-pool 1
[L3 switch-dhcp-pool-1] network 192.168.40.0 mask 255.255.255.0
```

Specify the gateway address as 192.168.40.1 in the DHCP address pool.

```
[L3 switch-dhcp-pool-1] gateway-list 192.168.40.1
```

Configure Option 43 to specify AC IP address in the hexadecimal format in DHCP address pool 1.

```
[L3 switch-dhcp-pool-1] option 43 hex 8007000001c0a80a01
[L3 switch-dhcp-pool-1] quit
```

Create DHCP address pool 2 to assign an IP address to the client, and specify subnet 192.168.20.0/24 in the DHCP address pool.

```
[L3 switch] dhcp server ip-pool 2
[L3 switch-dhcp-pool-2] network 192.168.20.0 mask 255.255.255.0
```

Specify the gateway address as 192.168.20.1 in the DHCP address pool.

```
[L3 switch-dhcp-pool-2] gateway-list 192.168.20.1
[L3 switch-dhcp-pool-2] quit
```

Create DHCP address pool 3 to assign an IP address to the host, and specify subnet 192.168.30.0/24 in the DHCP address pool.

```
[L3 switch] dhcp server ip-pool 3
[L3 switch-dhcp-pool-3] network 192.168.30.0 mask 255.255.255.0
```

Specify the gateway address as 192.168.30.1 in the DHCP address pool.

```
[L3 switch-dhcp-pool-3] gateway-list 192.168.30.1
[L3 switch-dhcp-pool-3] quit
```

Configuring Layer 2 switch 1

Create VLAN 400. The switch will use this VLAN for AP access.

```
<L2 switch 1> system-view
[L2 switch 1] vlan 400
[L2 switch 1-vlan400] quit
```

Set the link type of GigabitEthernet 1/0/1 that connects the switch to the Layer 3 switch to trunk, remove the port from VLAN 1, and assign the port to VLAN 400.

```
[L2 switch 1] interface gigabitEthernet 1/0/1
[L2 switch 1-GigabitEthernet1/0/1] port link-type trunk
[L2 switch 1-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[L2 switch 1-GigabitEthernet1/0/1] port trunk permit vlan 400
[L2 switch 1-GigabitEthernet1/0/1] quit
```

Set the link type of GigabitEthernet 1/0/2 that connects the switch to the AP to access, assign the port to VLAN 400, and enable PoE.

```
[L2 switch 1] interface gigabitEthernet 1/0/2
```

```
[L2 switch 1-GigabitEthernet1/0/2] port link-type access
[L2 switch 1-GigabitEthernet1/0/2] port access vlan 400
[L2 switch 1-GigabitEthernet1/0/2] poe enable
[L2 switch 1-GigabitEthernet1/0/2] quit
```

Configuring Layer 2 switch 2

Create VLAN 300. The switch will use this VLAN for host access.

```
<L2 switch 2> system-view
[L2 switch 2] vlan 300
[L2 switch 2-vlan300] quit
```

Set the link type of GigabitEthernet 1/0/1 that connects the switch to the Layer 3 switch to trunk, remove the port from VLAN 1, and assign the port to VLAN 300.

```
[L2 switch 2] interface gigabitEthernet 1/0/1
[L2 switch 2-GigabitEthernet1/0/1] port link-type trunk
[L2 switch 2-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[L2 switch 2-GigabitEthernet1/0/1] port trunk permit vlan 300
[L2 switch 2-GigabitEthernet1/0/1] quit
```

Set the link type of GigabitEthernet 1/0/2 that connects the switch to the host to access, and assign the port to VLAN 300.

```
[L2 switch 2] interface gigabitEthernet 1/0/2
[L2 switch 2-GigabitEthernet1/0/2] port link-type access
[L2 switch 2-GigabitEthernet1/0/2] port access vlan 300
[L2 switch 2-GigabitEthernet1/0/2] quit
```

Verifying the configuration

Verify that the AP is in R/M state.

```
<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: 399
Remaining APs: 399
Total AP licenses: 0
Local AP licenses: 0
Server AP licenses: 0
Remaining local AP licenses: 0
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 | 1 | R/M | AP 3620 | 219801A28N819CE0002T |

Verify that the client is connected to radio 1 on AP officeap.

```
<AC> display wlan client
```

```
Total number of clients: 1
```

| MAC address | User name | AP name | R IP address | VLAN |
|----------------|-----------|---------|----------------|------|
| 90b9-311a-bef6 | N/A | ap1 | 1 192.168.20.3 | 200 |

Verify that the client and the host can ping each other successfully.

```
C:\Users\system32>ping 192.168.20.3 -t
```

```
Pinging 192.168.20.3 with 32 bytes of data:
```

```
Reply from 192.168.20.3: bytes=32 time=2470ms TTL=63
```

```
Reply from 192.168.20.3: bytes=32 time=2ms TTL=63
```

```
Reply from 192.168.20.3: bytes=32 time=1427ms TTL=63
```

```
Reply from 192.168.20.3: bytes=32 time=2ms TTL=63
```

```
Reply from 192.168.20.3: bytes=32 time=86ms TTL=63
```

```
Reply from 192.168.20.3: bytes=32 time=142ms TTL=63
```

```
Reply from 192.168.20.3: bytes=32 time=561ms TTL=63
```

```
Reply from 192.168.20.3: bytes=32 time=84ms TTL=63
```

```
Reply from 192.168.20.3: bytes=32 time=465ms TTL=63
```

```
Reply from 192.168.20.3: bytes=32 time=114ms TTL=63
```

```
Reply from 192.168.20.3: bytes=32 time=124ms TTL=63
```

```
Reply from 192.168.20.3: bytes=32 time=446ms TTL=63
```

```
Ping statistics for 192.168.20.3:
```

```
Packets: Sent = 12, Received = 12, Lost = 0 (0% loss),
```

```
Approximate round trip times in milli-seconds:
```

```
Minimum = 2ms, Maximum = 2470ms, Average = 495ms
```

```
Control-C
```

```
^C
```

```
C:\Users\system32>
```

Configuration files

- AC:


```
#
vlan 100
#
vlan 200
#
interface Vlan-interface100
 ip address 192.168.10.1 255.255.255.0
#
wlan service-template 1
 client forwarding-location ac
 akm mode psk
 preshared-key pass-phrase simple 12345678
```

```

cipher-suite ccmp
security-ie rsn
ssid service
service-template enable
#
interface GigabitEthernet1/0/1
port link-type trunk
port trunk permit vlan 100 200
#
ip route-static 192.168.40.0 24 192.168.10.83
#
wlan ap ap1 model AP 3620
serial-id 219801A28N819CE0002T
#
wlan ap-group group1
ap ap1
ap-model AP 3620
radio 1
radio enable
service-template 1 vlan 200
radio 2
#

```

- **Layer 3 switch:**

```

#
dhcp enable
#
vlan 100
#
vlan 200
#
vlan 300
#
vlan 400
#
dhcp server ip-pool 1
gateway-list 192.168.40.1
network 192.168.40.0 mask 255.255.255.0
option 43 hex 8007000001c0a80a01
#
dhcp server ip-pool 2
gateway-list 192.168.20.1
network 192.168.20.0 mask 255.255.255.0
#
dhcp server ip-pool 3
gateway-list 192.168.30.1
network 192.168.30.0 mask 255.255.255.0
#
interface Vlan-interface100

```

```

ip address 192.168.10.83 255.255.255.0
#
interface Vlan-interface200
ip address 192.168.20.1 255.255.255.0
#
interface Vlan-interface300
ip address 192.168.30.1 255.255.255.0
#
interface Vlan-interface400
ip address 192.168.40.1 255.255.255.0
#
interface GigabitEthernet1/0/1
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 100 200
#
interface GigabitEthernet1/0/2
port link-type trunk
undo port trunk permit vlan 1
port trunk pvid vlan 400
#
interface GigabitEthernet1/0/3
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 300
#

```

- **Layer 2 switch 1:**

```

#
vlan 400
#
interface GigabitEthernet1/0/1
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 400
#
interface GigabitEthernet1/0/2
port link-type access
port access vlan 400
poe enable
#

```

- **Layer 2 switch 2:**

```

#
vlan 300
#
interface GigabitEthernet1/0/1
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 300

```



```
#
interface GigabitEthernet1/0/2
 port link-type access
 port access vlan 300
 poe enable
#
```

Related documentation

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

INTELBRAS Access Controllers

Local Forwarding Configuration Examples

Copyright © 2024 Intelbras S.A All rights reserved.

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

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

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

Contents

| | |
|---|---|
| Introduction | 1 |
| Prerequisites | 1 |
| Example: Configuring local forwarding | 1 |
| Network configuration | 1 |
| Restrictions and guidelines | 1 |
| Procedures | 2 |
| Configuring the configuration file | 2 |
| Configuring the AC | 2 |
| Configuring the switch | 3 |
| Verifying the configuration | 4 |
| Configuration files | 4 |
| Related documentation | 6 |

Introduction

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

Prerequisites

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

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

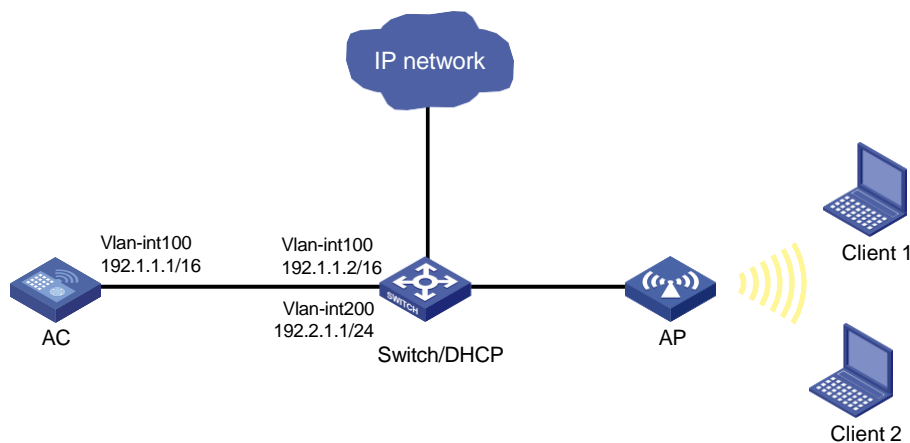
This document assumes that you have basic knowledge of WLAN local forwarding.

Example: Configuring local forwarding

Network configuration

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

Figure 1 Network diagram



Restrictions and guidelines

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

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

Procedures

Configuring the configuration file

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

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

Upload the file to the AC.

Configuring the AC

1. Configure AC interfaces:

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

```
<AC> system-view
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 192.1.1.1 16
[AC-Vlan-interface100] quit
```

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

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

2. Configure wireless services:

Create service template 1 and enter its view.

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

Configure the SSID as **service**.

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

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

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

Set the CCMP cipher suite and enable RSN security IE.

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

Enable local forwarding.

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

Enable the service template.

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

3. Configure the AP:

NOTE:

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

Create manual AP **officeap**, and specify the AP model and serial ID.

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

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

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

Bind service template 1 and VLAN 200 to radio 2.

```
[AC-wlan-ap-group-group1] ap-model AP 3620
[AC-wlan-ap-group-group1-ap-model-AP 3620] radio 2
[AC-wlan-ap-group-group1-ap-model-AP 3620-radio-2] service-template 1 vlan 200
```

Enable radio 2.

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

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

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

Configuring the switch

1. Configure switch interfaces:

Create VLAN 100 and VLAN-interface 100, and assign an IP address to the VLAN interface. The switch will use VLAN 100 to forward packets between the AC and the AP.

```
<Switch> system-view
[Switch] vlan 100
[Switch-vlan100] quit
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ip address 192.1.1.2 16
[Switch-Vlan-interface100] quit
```

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

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

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

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

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

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

Enable PoE on GigabitEthernet 1/0/2.

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

2. Configure DHCP:

Enable DHCP.

```
[Switch] dhcp enable
```

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

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

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

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

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

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

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

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

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

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

Verifying the configuration

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

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

Figure 2 ICMP packets from clients

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

Frame 27: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface 0
 Ethernet II, Src: Azurewaw_4c:b5:59 (6c:71:d9:4c:b5:59), Dst: D-LinkCo_b1:69:ae (5c:d9:98:b1:69:ae)
 802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 300
 Internet Protocol Version 4, Src: 100.1.3.3 (100.1.3.3), Dst: 100.1.3.5 (100.1.3.5)
 Internet Control Message Protocol

Configuration files

- AC:

```

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

```

- **Switch:**

```

#
    dhcp enable
#
vlan 100
#
vlan 200
#
dhcp server ip-pool vlan100
    gateway-list 192.1.1.2
    network 192.1.0.0 mask 255.255.0.0
    forbidden-ip 192.1.1.1
#
dhcp server ip-pool vlan200
    gateway-list 192.2.1.1
    network 192.2.1.0 mask 255.255.255.0
    dns-list 192.2.1.1
#

```



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

Related documentation

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

INTELBRAS Access Controllers

PSK Encryption 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 PSK encryption | 1 |
| Network configuration | 1 |
| Restrictions and guidelines | 1 |
| Procedures | 1 |
| Configuring the AC | 1 |
| Configuring the switch | 3 |
| Verifying the configuration | 4 |
| Configuration files | 5 |
| Related documentation | 6 |

Introduction

The following information provides an example for configuring PSK encryption.

Prerequisites

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

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

This document assumes that you have basic knowledge of WLAN access and WLAN security.

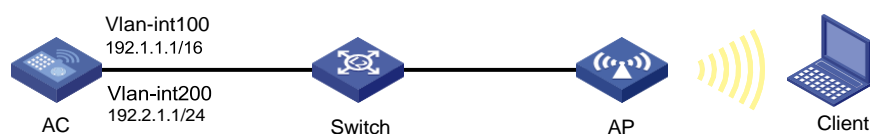
Example: Configuring PSK encryption

Network configuration

As shown in [Figure 1](#), the switch acts as a DHCP server to assign IP addresses to the AP and the client. Perform the following tasks:

- Configure PSK on the AC to enable the client to use PSK for encryption.
- Configure open system authentication and bypass authentication so that the client can access the WLAN without being authenticated.
- Configure PSK as the authentication and key management (AKM) mode.
- Set the cipher suite to CCMP.
- Set the security IE to RSN.

Figure 1 Network diagram



Restrictions and guidelines

When you configure PSK encryption, follow these restrictions and guidelines:

- Use the serial ID labeled on the AP's rear panel to specify an AP.
- Configure a pre-shared key if the AKM mode is PSK.

Procedures

Configuring the AC

1. Configure AC interfaces:

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

```
<AC> system-view
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 192.1.1.1 16
[AC-Vlan-interface100] quit
```

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

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

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

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

2. Configure wireless services:

Create service template 1 and enter its view.

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

Configure the SSID as **service**.

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

Specify VLAN 200 for clients to access the WLAN defined by the service template.

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

Set the AKM mode to PSK, and configure simple character string of 12345678 as the PSK.

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

Set the cipher suite to CCMP and set the security IE to RSN.

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

Configure the AC to forward client data traffic. You can skip this step if the AC is the client traffic forwarder by default.

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

Enable the service template.

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

3. Configure the AP:

NOTE:

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

Create manual AP **officeap**, and specify the AP model and serial ID.

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

```
[AC-wlan-ap-officeap] quit
# Create AP group group1, and add the AP to the AP group.
[AC] wlan ap-group group1
[AC-wlan-ap-group-group1] ap officeap
# Bind service template 1 to radio 2.
[AC-wlan-ap-group-group1] ap-model AP 3620
[AC-wlan-ap-group-group1-ap-model-AP 3620] radio 2
[AC-wlan-ap-group-group1-ap-model-AP 3620-radio-2] service-template 1
# Enable radio 2.
[AC-wlan-ap-group-group1-ap-model-AP 3620-radio-2] radio
enable [AC-wlan-ap-group-group1-ap-model-AP 3620-radio-2] quit
[AC-wlan-ap-group-group1-ap-model-AP 3620]
quit [AC-wlan-ap-group-group1] quit
```

Configuring the switch

1. Configure switch interfaces:

Create VLAN 100 and VLAN-interface 100, and assign an IP address to the VLAN interface. The switch will use VLAN 100 to forward packets between the AC and the AP.

```
<Switch> system-view
[Switch] vlan 100
[Switch-vlan100] quit
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ip address 192.1.1.2 16
[Switch-Vlan-interface100] quit
```

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

```
[Switch] vlan 200
[Switch-vlan200] quit
[Switch] interface vlan-interface 200
[Switch-Vlan-interface200] ip address 192.2.1.2 24
[Switch-Vlan-interface200] quit
```

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

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

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

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

Enable PoE on GigabitEthernet 1/0/2.

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

2. Configure DHCP:

Enable DHCP.

```
[Switch] dhcp enable
```

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

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

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

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

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

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

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

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

Create DHCP address pool **vlan200** to assign an IP address to the client, and specify subnet 192.2.1.0/24 in the DHCP address pool.

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

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

Exclude IP address 192.2.1.1 from dynamic allocation in the address pool.

```
[Switch-dhcp-pool-vlan200] forbidden-ip 192.2.1.1
```

Specify the gateway address as 192.2.1.2 and specify the DNS server address in the DHCP address pool. In this example, the gateway also acts as a DNS server.

```
[Switch-dhcp-pool-vlan200] gateway-list 192.2.1.2
```

```
[Switch-dhcp-pool-vlan200] dns-list 192.2.1.2
```

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

Verifying the configuration

Verify that the client has been associated with the WLAN and the AKM mode is PSK.

```
[AC] display wlan client verbose
```

```
Total number of clients: 1
```

| | |
|-----------------|---|
| MAC address | : 0024-d705-c608 |
| IPv4 address | : 192.2.1.3 |
| IPv6 address | : N/A |
| Username | : N/A |
| AID | : 1 |
| AP ID | : 2 |
| AP name | : officeap |
| Radio ID | : 2 |
| SSID | : service |
| BSSID | : 80f6-2eaf-5190 |
| VLAN ID | : 200 |
| Sleep count | : 137 |
| Wireless mode | : 802.11g |
| Supported rates | : 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps |
| QoS mode | : WMM |
| Listen interval | : 100 |
| RSSI | : 20 |

| | |
|----------------------------|------------------------------------|
| Rx/Tx rate | : 2/1 |
| Authentication method | : Open system |
| Security mode | : PRE-RSNA |
| AKM mode | : N/A |
| Security mode | : RSN |
| AKM mode | : PSK |
| Cipher suite | : CCMP |
| User authentication mode | : Bypass |
| Authorization ACL ID | : N/A |
| Authorization user profile | : N/A |
| Roam status | : N/A |
| Key derivation | : N/A |
| PMF status | : N/A |
| Forwarding policy name | : N/A |
| Online time | : 0days 0hours 21minutes 55seconds |
| FT status | : Inactive |

Configuration files

- AC:


```
#
vlan 100
#
vlan 200
#
wlan service-template 1
  ssid service
  client forwarding-location ac
  vlan 200
  akm mode psk
  preshared-key pass-phrase cipher $c$3$N//5BVbsOqdBTxi+7MJZKT6Zqh5MAMYs2ZzM
  cipher-suite ccmp
  security-ie rsn
service-template enable
#
interface Vlan-interface100
  ip address 192.1.1.1 255.255.0.0
#
interface Vlan-interface200
  ip address 192.2.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
  port link-type trunk
  undo port trunk permit vlan 1
  port trunk permit vlan 100 200
#
wlan ap-group group1
  ap officeap
```



```

ap-model AP 3620
  radio 2
    radio enable
    service-template 1
#
wlan ap officeap model AP 3620
  serial-id 219801A28N819CE0002T
#
• Switch:
#
  dhcp enable
#
vlan 100
#
vlan 200
#
dhcp server ip-pool vlan100
  gateway-list 192.1.1.2
  network 192.1.0.0 mask 255.255.0.0
  forbidden-ip 192.1.1.1
#
dhcp server ip-pool vlan200
  gateway-list 192.2.1.2
  network 192.2.1.0 mask 255.255.255.0
  dns-list 192.2.1.2
  forbidden-ip 192.2.1.1
#
interface GigabitEthernet1/0/1
  port link-type trunk
  undo port trunk permit vlan 1
  port trunk permit vlan 100 200
#
interface GigabitEthernet1/0/2
  port link-type trunk
  undo port trunk permit vlan 1
  port trunk permit vlan 100
  port trunk pvid vlan 100
poe enable
#

```

Related documentation

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

INTELBRAS Access Controllers Remote 802.1X Authentication Configuration Examples

Copyright © 2024 Intelbras S.A All rights reserved.

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

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

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

Contents

| | |
|--|----|
| Introduction | 1 |
| Prerequisites | 1 |
| Example: Configuring remote 802.1X authentication..... | 1 |
| Network configuration..... | 1 |
| Restrictions and guidelines | 2 |
| Procedures | 2 |
| Configuring the AC..... | 2 |
| Configuring the switch | 4 |
| Configuring the RADIUS server | 5 |
| Verifying the configuration | 8 |
| Configuration files..... | 10 |
| Related documentation | 12 |

Introduction

The following information provides an example for configuring remote 802.1X authentication for wireless clients.

Prerequisites

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

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

The following information is provided based on the assumption that you have basic knowledge of WLAN access, WLAN security, WLAN authentication, and 802.1X.

Example: Configuring remote 802.1X authentication

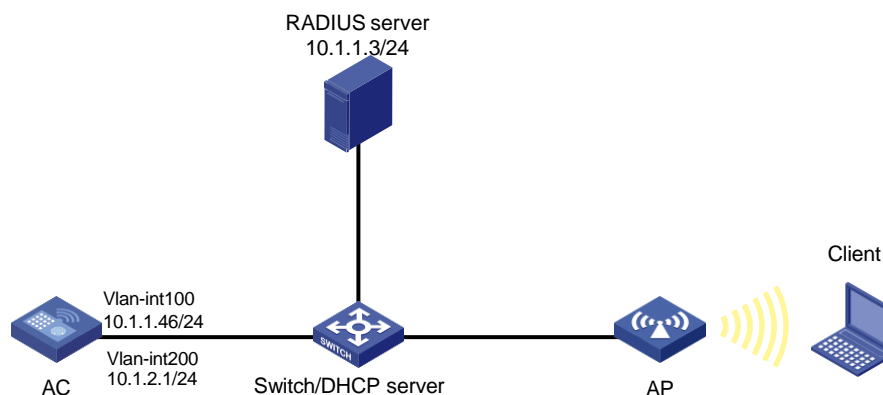
Network configuration

As shown in [Figure 1](#), the switch acts as a DHCP server to assign IP addresses to the AP and the client. The RADIUS server runs on INC.

Configure the AC, the client, the switch, and the RADIUS server to meet the following requirements:

- The AC uses the RADIUS server to perform 802.1X authentication for the wireless client.
- The AC uses the open system authentication for the client at the data link layer. This is the default authentication method.
- The AC uses the 802.1X AKM mode to secure data transmission between the client and the AP.
- The cipher suite is CCMP.

Figure 1 Network diagram



Restrictions and guidelines

When you configure remote 802.1X authentication for wireless clients, follow these restrictions and guidelines:

- Use the serial ID labeled on the AP's rear panel to specify an AP.
- For the INC server to dynamically change the client authorization information or forcibly disconnect clients, enable the RADIUS session-control feature on the AC.
- To avoid dynamic authorization failures when the client is coming online, configure the RADIUS DAE server (DAS) feature.

Procedures

Configuring the AC

1. Configure interfaces on the AC:

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

```
<AC> system-view
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 10.1.1.46 24
[AC-Vlan-interface100] quit
```

Create VLAN 200 and VLAN-interface 200, and assign an IP address to the VLAN interface. VLAN 200 will be used for client access.

```
[AC] vlan 200
[AC-vlan200] quit
[AC] interface vlan-interface 200
[AC-Vlan-interface200] ip address 10.1.2.1 24
[AC-Vlan-interface200] quit
```

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

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

2. Configure a RADIUS scheme:

Create a RADIUS scheme named **radius1** and enter its view.

```
[AC] radius scheme radius1
```

Specify the IP addresses of the primary authentication and accounting RADIUS servers.

```
[AC-radius-radius1] primary authentication 10.1.1.3
[AC-radius-radius1] primary accounting 10.1.1.3
```

Set the shared key to **12345** in plain text for secure communication with the servers.

```
[AC-radius-radius1] key authentication simple 12345
[AC-radius-radius1] key accounting simple 12345
```

Specify IP address 10.1.2.1 as the source IP address for outgoing RADIUS packets.

```
[AC-radius-radius1] nas-ip 10.1.2.1
```

```
[AC-radius-radius1] quit
```

Create an ISP domain named **dom1** and enter its view.

```
[AC] domain dom1
```

Apply RADIUS scheme **radius1** to ISP domain **dom1** for LAN user authentication, authorization, and accounting.

```
[AC-isp-dom1] authentication lan-access radius-scheme radius1
```

```
[AC-isp-dom1] authorization lan-access radius-scheme radius1
```

```
[AC-isp-dom1] accounting lan-access radius-scheme radius1
```

```
[AC-isp-dom1] quit
```

Enable the RADIUS session-control feature.

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

Enable the RADIUS DAS feature and enter RADIUS DAS view.

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

Specify the RADIUS server at 10.1.1.3 as a DAC and set the shared key to **12345** in plain text for validating DAE packets from the RADIUS server.

```
[AC-radius-da-server] client ip 10.1.1.3 key simple 12345
```

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

3. Configure the AC to use EAP relay to authenticate 802.1X clients.

```
[AC] dot1x authentication-method eap
```

4. Configure a wireless service:

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

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

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

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

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

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

Set the AKM mode to 802.1X.

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

Set the cipher suite to CCMP.

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

Enable the RSN IE in beacon and probe responses.

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

Set the authentication mode to 802.1X.

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

Specify ISP domain **dom1** for authenticating 802.1X clients.

```
[AC-wlan-st-service] dot1x domain dom1
```

Enable the AC to forward client data traffic. If the AC forwards client data traffic by default, skip this step.

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

Enable the service template.

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

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

5. Configure AP settings:

❗ **IMPORTANT:**

In a large-scale network, configure AP groups as a best practice.

Create a manual AP named **office**, and specify the AP model and serial ID

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

Create AP group **group1** and create an AP grouping rule by AP names to add AP **office** to AP group **group1**.

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

Bind service template **service** to radio 1 in AP group **group1**.

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

Enable radio 1.

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

Configuring the switch

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

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

Create VLAN 200. The switch will use this VLAN to forward packets for wireless clients.

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

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

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

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

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

Enable PoE on GigabitEthernet 1/0/2.

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

Create VLAN-interface 100, and assign an IP address to the VLAN interface.

```
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ip address 10.1.1.47 24
[Switch-Vlan-interface100] quit
```

Create VLAN-interface 200, and assign an IP address to the VLAN interface.

```
[Switch] interface vlan-interface 200
[Switch-Vlan-interface200] ip address 10.1.2.2 24
[Switch-Vlan-interface200] quit
```

Configure DHCP pool **100** to assign an IP address to the AP.

```
[Switch] dhcp server ip-pool 100
[Switch-dhcp-pool-100] network 10.1.1.0 mask 255.255.255.0
[Switch-dhcp-pool-100] gateway-list 10.1.1.46
[Switch-dhcp-pool-100] quit
```

Configure DHCP pool **200** to assign an IP address to the client. In this example, the address of the DNS server is 10.1.2.1 (the gateway address). You must replace it with the actual address of the DNS server on your network.

```
[Switch] dhcp server ip-pool 200
[Switch-dhcp-pool-200] network 10.1.2.0 mask 255.255.255.0
[Switch-dhcp-pool-200] gateway-list 10.1.2.1
[Switch-dhcp-pool-200] dns-list 10.1.2.1
[Switch-dhcp-pool-200] quit
```

Enable DHCP.

```
[Switch] dhcp enable
```

Configuring the RADIUS server

In this example, the RADIUS server runs INC PLAT 7.1(E0302) and INC UAM 7.1(E0302).

1. Add the AC to INC as an access device:
 - a. Log in to INC and click the **User** tab.
 - b. From the navigation tree, select **User Access Policy > Access Device Management > Access Device**.
 - c. Click **Add**.
The **Add Access Device** page opens.
 - d. In the **Access Configuration** area, configure the following parameters, as shown in [Figure 2](#):
 - Enter **12345** in the **Shared Key** and **Confirm Shared Key** fields.
 - Use the default values for other parameters.
 - e. In the **Device List** area, click **Select** or **Add Manually** to add the device at **10.1.2.1** as an access device.
 - f. Click **OK**.

Figure 2 Adding an access device

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

Access Configuration

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

Device List

Select Add Manually Clear All

| Device Name | Device IP | Device Model | Comments | Delete |
|-------------|-----------|--------------|----------|--------|
| | 10.1.2.1 | | | |

Total Items: 1.

OK Cancel

2. Add an access policy:
 - a. Click the **User** tab.
 - b. From the navigation tree, select **User Access Policy > Access Policy**.
 - c. Click **Add**.
 - d. On the **Add Access Policy** page, configure the following parameters, as shown in [Figure 3](#):
 - Enter **dot1x** in the **Access Policy Name** field.
 - Select **EAP** for the **Certificate Authentication** field.
 - Select **EAP-PEAP Auth** from the **Certificate Type** list, and select **MS-CHAPV2 Auth** from the **Certificate Sub-Type** list.

The certificate sub-type on the INC server must be the same as the identity authentication method configured on the client.
 - e. Click **OK**.

Figure 3 Adding an access policy

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

Basic Information

Access Policy Name *

Service Group *

Description

Authorization Information

Access Period

Allocate IP *

Downstream Rate(Kbps)

Upstream Rate(Kbps)

Priority

☐ RSA Authentication

Certificate Authentication ☐ None ☒ EAP

Certificate Type

Certificate Sub-Type

Deploy VLAN

☐ Deploy User Profile

☐ Deploy ACL

Deploy User Group

3. Add an access service:
 - a. Click the **User** tab.
 - b. From the navigation tree, select **User Access Policy > Access Service**.
 - c. Click **Add**.
 - d. On the **Add Access Service** page, configure the following parameters, as shown in [Figure 4](#):
 - Enter **dot1x** in the **Service Name** field.
 - Select **dot1x** from the **Default Access Policy** list.
 - e. Click **OK**.

Figure 4 Adding an access service

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

Basic Information

Service Name *

Service Suffix

Service Group *

Default Access Policy *

Default Proprietary Attribute Assignment Policy *

Default Max. Number of Bound Endpoints *

Default Max. Number of Online Endpoints *

Description

☒ Available ☐ Transparent Authentication on Portal Endpoints

Access Scenario List

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

4. Add an access user:
 - a. Click the **User** tab.
 - b. From the navigation tree, select **Access User > All Access Users**.

The access user list opens.

c. Click Add.

The **Add Access User** page opens.

d. In the Access Information area, configure the following parameters, as shown in Figure 5:

- Click **Select** or **Add User** to associate the user with INC Platform user **user**.
- Enter **dot1x** in the **Account Name** field.
- Enter **dot1x123** in the **Password** and **Confirm Password** fields.

e. In the Access Service area, select dot1x from the list.

f. Click OK.

Figure 5 Adding an access user account

User Name *

Account Name *

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

Password * Confirm Password *

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

Inspiration Time Expiration Time

Max. Idle Time(Minutes)

Max. Concurrent Logins

Max. Transparent Portal Bindings

Login Message

Access Service

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

Verifying the configuration

1. On the client, verify that the client can pass authentication, associate with the AP, and access the wireless network. (Details not shown.)
2. On the AC, perform the following tasks to verify that the user has passed authentication and come online:

Display detailed WLAN client information.

```
[AC] display wlan client verbose
```

```
Total number of clients: 1
```

```
MAC address           : cc3a-61a8-fb8c
IPv4 address           : 10.1.2.3
IPv6 address           : N/A
Username               : dot1x
AID                    : 1
AP ID                  : 3
AP name                : office
Radio ID               : 1
```

| | |
|----------------------------|-------------------------------------|
| SSID | : service |
| BSSID | : 741f-4ad4-1fe0 |
| VLAN ID | : 200 |
| Sleep count | : 0 |
| Wireless mode | : 802.11ac |
| Channel bandwidth | : 80MHz |
| SM power save | : Disabled |
| Short GI for 20MHz | : Supported |
| Short GI for 40MHz | : Supported |
| Short GI for 80MHz | : Supported |
| Short GI for 160/80+80MHz | : Not supported |
| STBC RX capability | : Not supported |
| STBC TX capability | : Not supported |
| LDPC RX capability | : Not supported |
| SU beamformee capability | : Not supported |
| MU beamformee capability | : Not supported |
| Beamformee STS capability | : N/A |
| Block Ack | : N/A |
| Supported VHT-MCS set | : NSS1 0, 1, 2, 3, 4, 5, 6, 7, 8, 9 |
| Supported HT MCS set | : 0, 1, 2, 3, 4, 5, 6, 7 |
| Supported rates | : 6, 9, 12, 18, 24, 36, 48, 54 Mbps |
| QoS mode | : WMM |
| Listen interval | : 10 |
| RSSI | : 0 |
| Rx/Tx rate | : 0/0 |
| Authentication method | : Open system |
| Security mode | : RSN |
| AKM mode | : 802.1X |
| Cipher suite | : CCMP |
| User authentication mode | : 802.1X |
| Authorization ACL ID | : N/A |
| Authorization user profile | : N/A |
| Roam status | : N/A |
| Key derivation | : SHA1 |
| PMF status | : N/A |
| Forwarding policy name | : N/A |
| Online time | : 0days 0hours 0minutes 15seconds |
| FT status | : Inactive |

Display online 802.1X client information.

[AC] display dot1x connection

Total connections: 1

| | |
|------------------|------------------|
| User MAC address | : cc3a-61a8-fb8c |
| AP name | : office |
| Radio ID | : 1 |
| SSID | : service |
| BSSID | : 741f-4ad4-1fe0 |
| Username | : dot1x |

```

Authentication domain      : dom1
IPv4 address               : 10.1.2.3
Authentication method      : EAP
Initial VLAN               : 200
Authorization VLAN         : 200
Authorization ACL number    : N/A
Authorization user profile  : N/A
Termination action         : Default
Session timeout period     : 36000001 s
Online from                 : 2015/12/21 11:27:11
Online duration             : 0h 1m 1s

```

Configuration files

- AC:

```

#
 dot1x authentication-method eap
#
vlan 100
#
vlan 200
#
wlan service-template service
 ssid service
 vlan 200
 client forwarding-location ac
 akm mode dot1x
 cipher-suite ccmp
 security-ie rsn
 client-security authentication-mode dot1x
 dot1x domain dom1
 service-template enable
#
interface Vlan-interface100
 ip address 10.1.1.46 255.255.255.0
#
interface Vlan-interface200
 ip address 10.1.2.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 1 100 200
#
radius scheme radius1
 primary authentication 10.1.1.3
 primary accounting 10.1.1.3
 key authentication cipher $c$3$Bb61SHV2ZsVYPJU2+RFB/8ntk0uCQkmdA==
 key accounting cipher $c$3$w03NfxnBmfDuedv9/xo7ESnoxKjowmmX9A==

```

```

nas-ip 10.1.2.1
#
radius dynamic-author server
    client ip 10.1.1.3 key cipher $c$3$AkTEB7OgMYnCqsfDeplhoAgXUek/rVrLZw==
#
radius session-control enable
#
domain dom1
    authentication lan-access radius-scheme radius1
    authorization lan-access radius-scheme radius1
    accounting lan-access radius-scheme radius1
#
wlan ap-group group1
    ap office
    ap-model AP 3620
        radio 1
            radio enable
            service-template service
        radio 2
#
wlan ap office model AP 3620
    serial-id 219801A28N819CE0002T
#

```

- **Switch:**

```

#
    dhcp enable
#
vlan 100
#
vlan 200
#
dhcp server ip-pool 100
    gateway-list 10.1.1.46
    network 10.1.1.0 mask 255.255.255.0
#
dhcp server ip-pool 200
    gateway-list 10.1.2.1
    network 10.1.2.0 mask 255.255.255.0
    dns-list 10.1.2.1
#
interface Vlan-interface100
    ip address 10.1.1.47 255.255.255.0
#
interface Vlan-interface200
    ip address 10.1.2.2 255.255.255.0
#
interface GigabitEthernet1/0/1
    port link-type trunk

```

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

Related documentation

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

INTELBRAS Access Controllers Remote Portal Authentication Configuration Examples

Copyright © 2024 Intelbras S.A All rights reserved.

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

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

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

Contents

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

Introduction

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

Prerequisites

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

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

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

Example: Configuring remote portal authentication

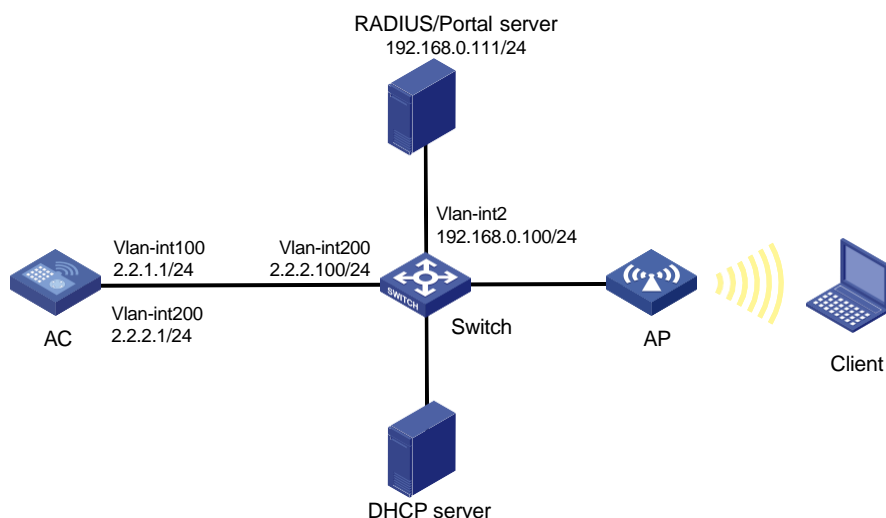
Network configuration

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

To implement remote portal authentication, perform the following tasks:

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

Figure 1 Network diagram



Analysis

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

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

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

Restrictions and guidelines

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

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

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

Procedures

Configuring INC

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

Configuring the RADIUS server

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

Figure 2 Adding an access device

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

Access Configuration

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

Device List

Select Add Manually Clear All

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

Total Items: 1.

OK Cancel

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

Figure 3 Adding an access policy

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

Basic Information

| | |
|----------------------|--------------|
| Access Policy Name * | AccessPolicy |
| Service Group * | Ungrouped |
| Description | |

Authorization Information

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

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

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

Figure 4 Adding an access service

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

Figure 5 Adding an access user

Configuring the portal server

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

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

Figure 6 Configuring the portal server

User > User Access Policy > Portal Service > Server

Portal Server

Basic Information

Log Level * Info

Portal Server

Request Timeout(Seconds) * 4 ? Server Heartbeat Interval(Seconds) * 20 ?

User Heartbeat Interval(Minutes) * 5 ? LB Device Address

Portal Web

Request Timeout(Seconds) * 15 ? Packet Code ?

Verify Endpoint Requests Yes Use Cache Yes

HTTP Heartbeat Display New Page HTTPS Heartbeat Display Original Page

Portal Page

http://192.168.0.111:8080/portal/

192.168.0.111

2. Configure the IP address group:
 - a. From the navigation tree, select **User Access Policy > Portal Service > IP Group**.
 - b. Click **Add** to open the page as shown in [Figure 7](#).
 - c. Enter the IP group name.
 - d. Enter the start IP address and end IP address of the IP group.
Make sure the client IP address is in the IP group.
 - e. Select a service group.
This example uses the default group **Ungrouped**.
 - f. Select **Normal** from the **Action** list.
 - g. Click **OK**.

Figure 7 Adding an IP address group

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

Add IP Group

IP Group Name * Portal_user

Start IP * 2.2.2.1

End IP * 2.2.2.255

Service Group Ungrouped

Action * Normal

OK Cancel

3. Add a portal device:
 - a. From the navigation tree, select **User Access Policy > Portal Service > Device**.
 - b. Click **Add** to open the page as shown in [Figure 8](#).
 - c. Enter the device name.
 - d. Select **CMCC 1.0** from the **Version** list.
 - e. Enter the IP address of the AC's interface connected to the client.
 - f. Set whether to support the portal server heartbeat and user heartbeat functions.
In this example, select **No** for both **Support Server Heartbeat** and **Support User Heartbeat**.
 - g. Enter the key, which must be the same as that configured on the AC.
 - h. Select **Directly Connected** for **Access Method**.
 - i. Use the default settings for other parameters.
 - j. Click **OK**.

Figure 8 Adding a portal device

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

Add Device

Device Information

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

OK Cancel

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

Figure 9 Device list

User > User Access Policy > Portal Service > Device

★Add to My Favorites ⓘHelp

Query Devices

Device Name Version

Deploy Result Service Group

Query Reset

Add

| Device Name | Version | Service Group | IP Address | Last Deployed at | Deploy Result | Operation |
|-------------|----------|---------------|------------|------------------|---------------|--|
| NAS | CMCC 1.0 | Ungrouped | 2.2.2.1 | | Not Deployed | <div> <div>Port Group</div> <div></div> <div></div> <div></div> </div> |

1-1 of 1. Page 1 of 1.

« < 1 > » 50

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

- d. Select the configured IP address group.

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

- e. Use the default settings for other parameters.

- f. Click **OK**.

Figure 10 Adding a port group

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

Add Port Group

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

OK Cancel

Configuring the AC

1. Configure interfaces on the AC:

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

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

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

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

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

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

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

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

3. Configure a wireless service:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Enable service template **st1**.

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

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

4. Configure the AP:

NOTE:

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

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

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

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

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

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

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

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

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

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

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

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

Enable radio 2.

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

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

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

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

5. Configure a RADIUS scheme:

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

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

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

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

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

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

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

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

Enable the RADIUS session-control feature.

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

6. Configure an authentication domain:

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

```
[AC] domain dm1
```

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

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

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

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

7. Configure portal authentication:

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

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

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

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

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

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

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

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

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

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

```

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

```

Configuring the switch

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

```

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

```

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

```

[Switch] vlan 200
[Switch-vlan200] quit

```

Create VLAN 2.

```

[Switch] vlan 2
[Switch-vlan2] quit

```

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

```

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

```

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

```

[Switch] interface gigabitethernet 1/0/2

```

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

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

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

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

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

Verifying the configuration

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

Display information about all portal users.

```
[AC] display portal user all
Total portal users: 1
Username: Client
  AP name: office
  Radio ID: 2
  SSID: service
  Portal server: newpt
  State: Online
  VPN instance: N/A
  MAC          IP          VLAN    Interface
  0021-6330-0933 2.2.2.2    200     WLAN-BSS1/0/2
Authorization information:
  DHCP IP pool: N/A
  User profile: N/A
  Session group profile: N/A
  ACL number: N/A
  Inbound CAR: N/A
  Outbound CAR: N/A
```

Configuration files

- AC:

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

```

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

```

- **Switch:**

```

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

```

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

Related documentation

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

INTELBRAS Access Controllers

Local Portal Authentication Through the LDAP Server

Configuration Examples

Copyright © 2024 Intelbras S.A All rights reserved.

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

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

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

Contents

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

Introduction

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

Prerequisites

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

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

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

Example: Configuring local portal authentication through the LDAP server

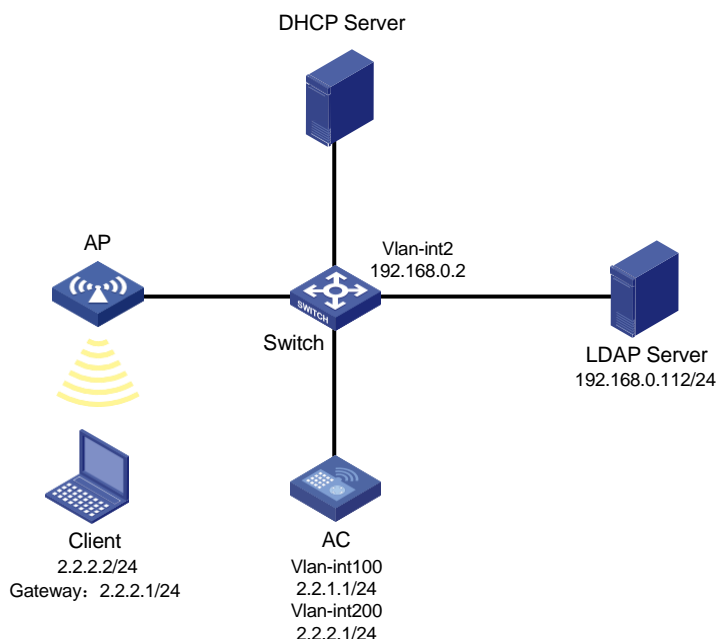
Network configuration

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

Configuration requirements are as follows:

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

Figure 1 Network diagram



Restrictions and guidelines

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

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

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

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

Procedures

Configuring the AC

1. Configuring VLANs and interfaces:

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

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

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

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

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

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

2. Configure the LDAP scheme:

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

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

Specify the administrator DN.

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

Specify the base DN for user search.

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

Specify the IP address of the LDAP server.

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

Specify the administrator password.

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

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

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

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

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

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

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

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

```
[AC] domain ldap
```

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

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

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

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

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

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

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

3. Configure portal authentication:

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

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

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

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

Create an HTTP-based local portal Web service.

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

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

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

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

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

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

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

4. Configure the wireless service:

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

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

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

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

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

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

Enable direct portal authentication on the service template.

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

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

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

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

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

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

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

5. Configure the AP:

NOTE:

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

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

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

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

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

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

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

Enable radio 2.

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

Configuring the switch

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

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

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

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

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

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

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

Assign the VLAN interface an IP address.

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

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

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

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

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

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

Enable PoE on the access port.

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

Configuring the LDAP server

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

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

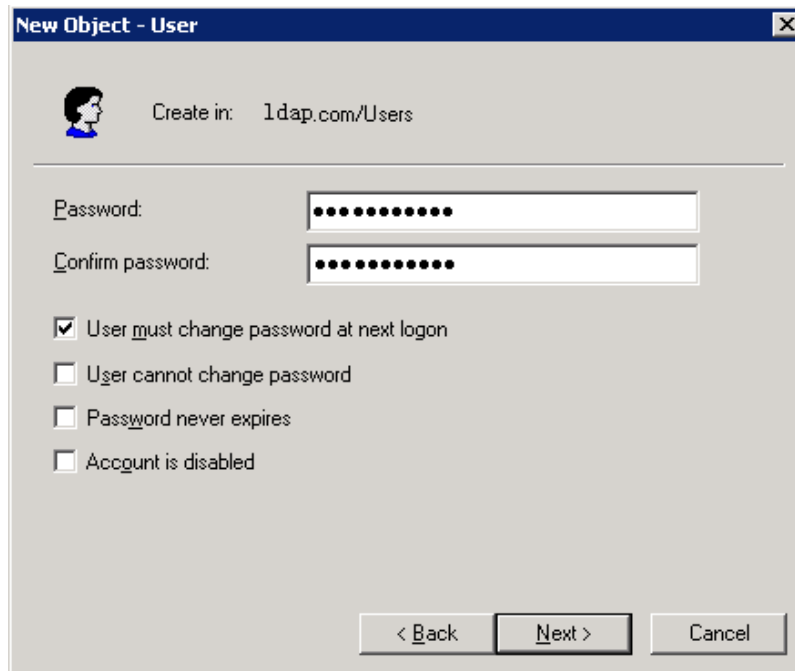
The **Active Directory Users and Computers** window opens.
 - c. From the navigation tree, click **Users** under the **ldap.com** node.
 - d. Select **Action > New > User** from the menu to open the dialog box for adding a user.
 - e. Enter logon name **aaa** and click **Next**.

Figure 2 Adding user aaa

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

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

Figure 3 Setting the user's password



New Object - User

Create in: ldap.com/Users

Password: [masked]

Confirm password: [masked]

☒ User must change password at next logon

☐ User cannot change password

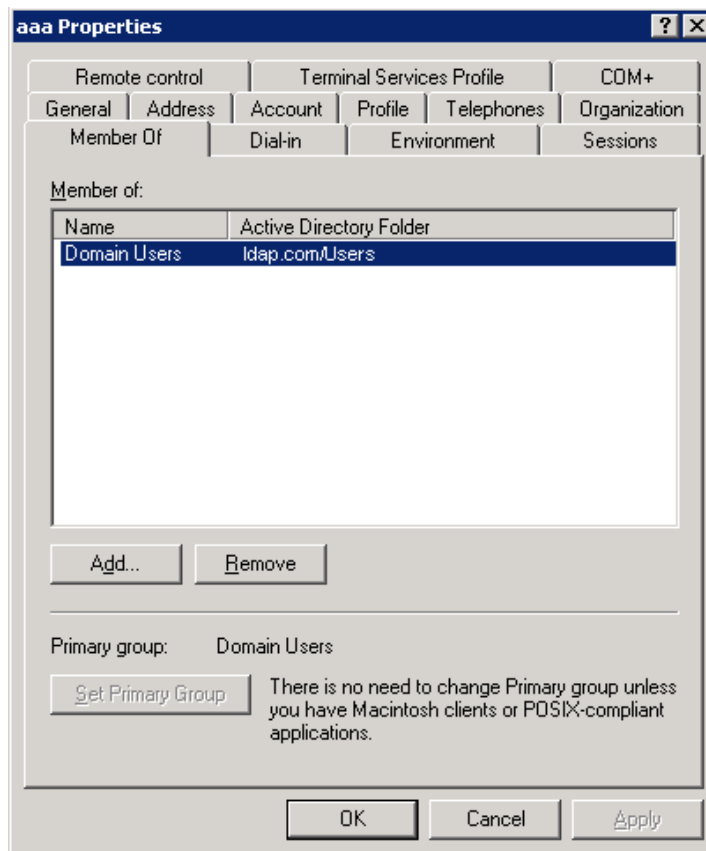
☐ Password never expires

☐ Account is disabled

< Back Next > Cancel

- g. Click **OK**.
2. Add user **aaa** to user group **Users**:
 - a. From the navigation tree, click **Users** under the **ldap.com** node.
 - b. In the right pane, right-click user **aaa** and select **Properties**.
 - c. In the dialog box, click the **Member Of** tab and click **Add**.

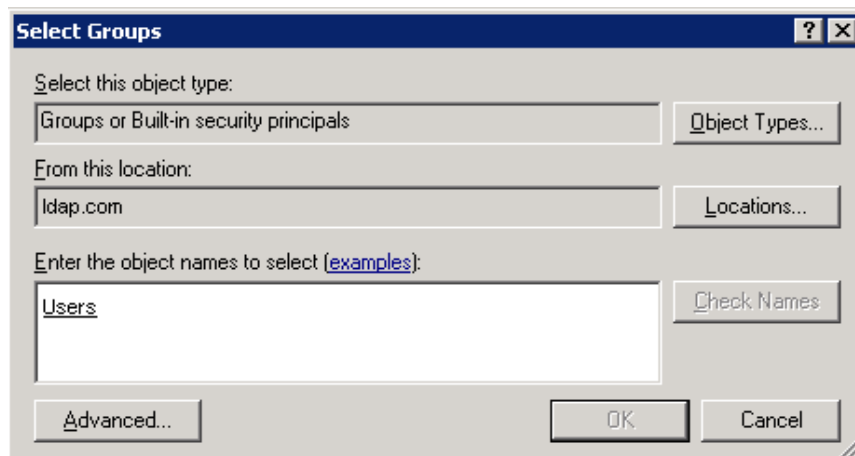
Figure 4 Modifying user properties



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

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

Figure 5 Adding user aaa to group Users



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

Verifying the configuration

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

Display online portal users on the AC.

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

Configuration files

- AC:

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

```

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

```

- **Switch:**

```

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

```

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

Related documentation

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

INTELBRAS Access Controllers

Portal MAC-Trigger Authentication

Configuration Examples

Copyright © 2024 Intelbras S.A All rights reserved.

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

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

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

Contents

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

Introduction

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

Prerequisites

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

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

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

Example: Configuring portal MAC-trigger authentication

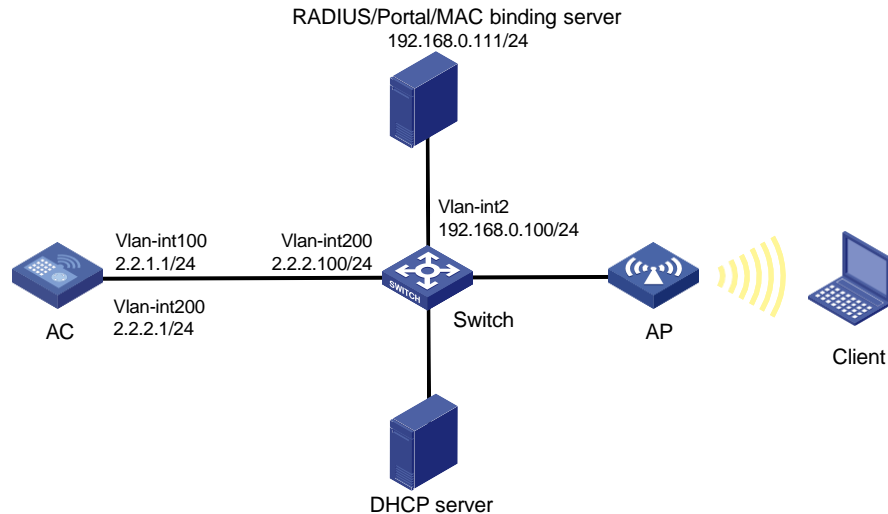
Network configuration

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

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

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

Figure 1 Network diagram



Analysis

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

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

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

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

Restrictions and guidelines

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

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

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

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

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

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

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

Procedures

Configuring INC

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

Configuring the RADIUS server

Add the AC to INC as an access device:

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

Figure 2 Adding the AC as an access device

Access Configuration

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

Device List

Select Add Manually Clear All

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

Total Items: 1.

OK Cancel

Configuring the portal server

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

Figure 3 Portal authentication server configuration

User > User Access Policy > Portal Service > Server

Portal Server

Basic Information

Log Level * Info

Portal Server

Request Timeout(Seconds) * 4 Server Heartbeat Interval(Seconds) * 20

User Heartbeat Interval(Minutes) * 5 LB Device Address

Portal Web

Request Timeout(Seconds) * 15 Packet Code

Verify Endpoint Requests Yes Use Cache Yes

HTTP Heartbeat Display New Page HTTPS Heartbeat Display Original Page

Portal Page

http://192.168.0.111:8080/portal/

192.168.0.111

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

Figure 4 Adding an IP address group

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

Add IP Group

IP Group Name * Portal_user

Start IP * 2.2.2.1

End IP * 2.2.2.255

Service Group Ungrouped

Action * Normal

OK Cancel

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

- c. Enter the device name.
- d. Select **CMCC 1.0** for **Version**.
- e. Enter the IP address of the AC's interface connected to the client.
- f. Set whether to support the portal server heartbeat and user heartbeat functions.
In this example, select **No** for both **Support Server Heartbeat** and **Support User Heartbeat**.
- g. Enter the key, which must be the same as that configured on the AC.
- h. Select **Directly Connected** from the **Access Method** list.
- i. Use the default settings for other parameters.
- j. Click **OK**.

Figure 5 Adding a portal device


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

Figure 6 Device list

- b. Click **Add** to open the page as shown in Figure 7.
- c. Enter the port group name.
- d. Select the configured IP address group.
The IP address used by the user to access the network must be within this IP address group.

- e. Select **Supported** for **Transparent Authentication**.
- f. Use the default settings for other parameters.
- g. Click **OK**.

Figure 7 Adding a port group

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

Add Port Group

| | | | |
|-------------------------------|-----------|------------------------------------|-------------|
| Port Group Name * | group | Language * | English |
| Start Port * | 0 | End Port * | zzzzzz |
| Protocol * | HTTP | Quick Authentication * | No |
| NAT or Not * | No | Error Transparent Transmission * | Yes |
| Authentication Type * | CHAP | IP Group * | Portal_user |
| Heartbeat Interval(Minutes) * | 10 | Heartbeat Timeout(Minutes) * | 30 |
| User Domain | | Port Group Description | |
| Transparent Authentication | Supported | Client Protection Against Cracks * | No |
| Page Push Policy | | Default Authentication Page | |

OK Cancel

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

Configuring the MAC binding server

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

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

Figure 8 Adding an access policy

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

Basic Information

Access Policy Name *

Service Group *

Description

Authorization Information

Access Period

Allocate IP *

Downstream Rate(Kbps)

Upstream Rate(Kbps)

Priority

☐ RSA Authentication

Certificate Authentication ☒ None ☐ EAP

Certificate Type

Deploy VLAN

☐ Deploy User Profile

Deploy User Group

☐ Deploy ACL

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

Figure 9 Adding an access service

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

Basic Information

Service Name *

Service Suffix

Service Group *

Default Access Policy *

Default Proprietary Attribute Assignment Policy *

Default Max. Number of Bound Endpoints *

Default Max. Number of Online Endpoints *

Description

☒ Available ☒ Transparent Authentication on Portal Endpoints

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

Figure 10 Adding an access user

User > All Access Users > Add Access User

Access Information

User Name * client1 Select Add User

Account Name * client ?

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

Password * ***** Confirm Password * *****

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

Start Time [] End Time []

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

Login Message []

Access Service

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

Binding Information

OK OK & Print Cancel

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

Figure 11 Configuring user endpoint settings

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

User Endpoint Settings

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

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

OK Cancel

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

Figure 12 Setting the endpoint aging time

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

Modify Endpoint Aging Time

Endpoint Aging Time(Days) * 7 ?

OK Cancel

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

Editing a configuration file for the AP

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

Enter the following content in the file.

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

Upload the file to the AC.

Configuring the AC

1. Configure interfaces on the AC:

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

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

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

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

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

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

2. Configure a static route to the INC server:

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

3. Configure a WLAN service:

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

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

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

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

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

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

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

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

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

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

4. Configure the AP:

NOTE:

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

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

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

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

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

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

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

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

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

Enable radio 2.

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

5. Configure a RADIUS scheme:

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

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

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

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

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

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

Enable RADIUS session-control.

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

Enable the RADIUS DAS feature and enter RADIUS DAS view.


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

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

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

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

6. Configure an authentication domain:

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

```
[AC] domain dm1
```

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

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

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

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

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

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

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

7. Configure portal authentication:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Enable portal roaming.

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

```

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

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

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

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

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

8. Configure portal MAC-trigger authentication:

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

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

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

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

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

```

Configuring the switch

```

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

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

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

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

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

```

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

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

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

Enable PoE.

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

Assign an IP address to VLAN-interface 200.

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

Assign an IP address to VLAN-interface 2.

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

Verifying the configuration

Display information about MAC binding server mts.

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

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

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

Display information about all portal users.

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

```

State: Online
VPN instance: N/A
MAC          IP          VLAN    Interface
0021-6330-0933  2.2.2.2    200     WLAN-BSS1/0/1
Authorization information:
  DHCP IP pool: N/A
  User profile: N/A
  Session group profile: N/A
  ACL number: N/A
  Inbound CAR: N/A
  Outbound CAR: N/A

```

Configuration files

- AC:


```

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

```

```

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

```

```

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

```

- **Switch:**

```

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

```

Related documentation

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

INTELBRAS Access Controllers

Transparent Authentication Through Remote MAC and Portal Authentication Configuration Examples

Copyright © 2024 Intelbras S.A All rights reserved.

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

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

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

Contents

| | |
|--|----|
| Introduction | 1 |
| Prerequisites | 1 |
| Example: Configuring transparent authentication through remote MAC and portal authentication | 1 |
| Network configuration | 1 |
| Analysis | 2 |
| Restrictions and guidelines | 2 |
| Procedures | 3 |
| Configuring INC | 3 |
| Configuring the AC | 9 |
| Configuring the switch | 12 |
| Verifying the configuration | 13 |
| Configuration files | 14 |
| Related documentation | 17 |

Introduction

The following information provides examples for configuring transparent authentication through remote MAC authentication and remote portal authentication.

Prerequisites

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

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

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

Example: Configuring transparent authentication through remote MAC and portal authentication

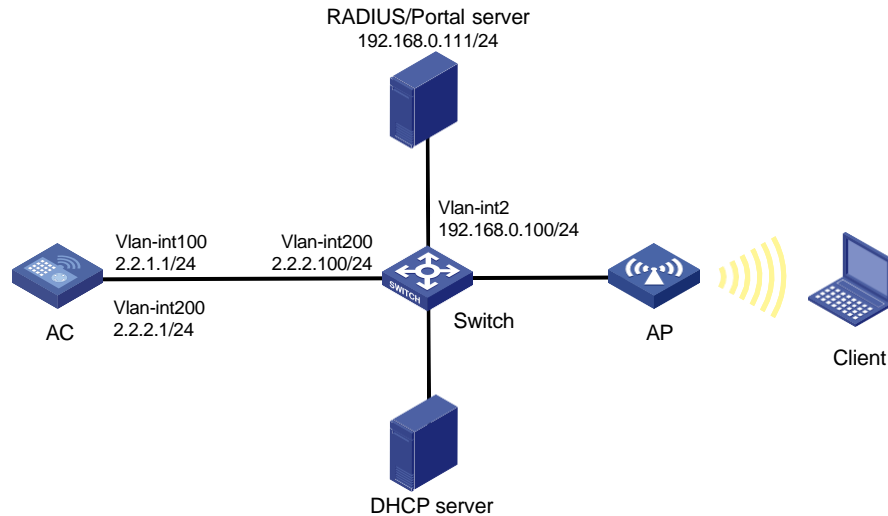
Network configuration

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

Configure the devices to meet the following requirements:

- The AC provides remote MAC authentication and direct portal authentication for the client.
- The RADIUS server can dynamically change user authorization information or forcibly disconnect users.

Figure 1 Network diagram



Analysis

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

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

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

Restrictions and guidelines

- Use the serial ID labeled on the AP's rear panel to specify an AP.
- By default, the URL of the portal Web server to which the AC redirects portal users does not carry any parameters. You can add parameters to be carried in the URL as needed.
- If portal authentication is enabled on a VLAN interface, the AC can forward client traffic. If portal authentication is enabled on a service template, both the AC and the AP can forward client traffic. (In this example, portal authentication is enabled on a service template.)
- In wireless networks where the AP forwards client traffic, the AC does not have ARP entries for clients. Therefore, the AC cannot check the validity of portal clients by using ARP entries. To ensure that valid users can perform portal authentication, enable wireless client validity check on the AC.
- If a portal client logs out and then tries to come online frequently in a short time, the client will fail portal authentication. To avoid this problem, disable the Rule ARP entry feature for portal clients.
- Some endpoints by default use random MAC addresses. For transparent authentication to take effect on such an endpoint, disable the endpoint from using a random MAC address.

Procedures

Configuring INC

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

Configuring the RADIUS server

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

Figure 2 Adding the AC as an access device

The screenshot shows the 'Add Access Device' page. The breadcrumb navigation is: User > User Access Policy > Access Device Management > Access Device > Add Access Device. The page has two main sections: 'Access Configuration' and 'Device List'.

Access Configuration:

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

Device List:

Buttons: Select, Add Manually, Clear All

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

Total Items: 1.

Buttons: OK, Cancel

2. Add an access policy:
 - a. From the navigation tree, select **User Access Policy > Access Policy**.
 - b. Click **Add** to open the page as shown in [Figure 3](#).
 - c. Enter the access policy name.
 - d. Select a service group.

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

Figure 3 Adding an access policy

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

Basic Information

Access Policy Name * AccessPolicy

Service Group * Ungrouped

Description

Authorization Information

Access Period None

Allocate IP * No

Downstream Rate(Kbps)

Upstream Rate(Kbps)

Priority

☐ RSA Authentication

Certificate Authentication ☒ None ☐ EAP

Certificate Type EAP-TLS Auth!

Deploy VLAN

☐ Deploy User Profile

Deploy User Group ?

☐ Deploy ACL

3. Add an access service:
 - a. From the navigation tree, select **User Access Policy > Access Service**.
 - b. Click **Add** to open the page as shown in Figure 4.
 - c. Enter the service name.
 - d. Select the **Transparent Authentication on Portal Endpoints** option.
 - e. Use the default settings for other parameters.
 - f. Click **OK**.

Figure 4 Adding an access service

User > User Access Policy > Access Service > Modify Access Service

Basic Information

Service Name * MAC_server

Service Suffix

Service Group * Ungrouped

Default Access Policy * AccessPolicy

Default Proprietary Attribute Assignment Policy * Do not use

Default Max. Number of Bound Endpoints * 0

Default Max. Number of Online Endpoints * 0

Description

☒ Available

☒ Transparent Authentication on Portal Endpoints

4. Add an access user:
 - a. From the navigation tree, select **Access User > Access User**.
 - b. Click **Add** to open the page as shown in Figure 5.
 - c. Select an existing access user or click **Add User** to add a new access user.
 - d. Enter the account name.
 - e. Set the password.
 - f. Select the access service.
 - g. Use the default settings for other parameters.
 - h. Click **OK**.

Figure 5 Adding an access user

User > All Access Users > Add Access User

Access Information

User Name * Client1 Select Add User

Account Name * client

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

Password * ***** Confirm Password * *****

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

Start Time [] End Time []

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

Login Message []

Access Service

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

Configuring the portal server

1. Configure the portal authentication service:
 - a. Click the **User** tab.
 - b. From the navigation tree, select **User Access Policy > Portal Service > Server** to open the portal server configuration page, as shown in [Figure 6](#).
 - c. Configure the portal server parameters as needed.
This example uses the default values.
 - d. Click **OK**.

Figure 6 Portal authentication server configuration

User > User Access Policy > Portal Service > Server

Portal Server

Basic Information

Log Level * Info

Portal Server

Request Timeout(Seconds) * 4 Server Heartbeat Interval(Seconds) * 20

User Heartbeat Interval(Minutes) * 5 LB Device Address []

Portal Web

Request Timeout(Seconds) * 15 Packet Code []

Verify Endpoint Requests Yes Use Cache Yes

HTTP Heartbeat Display New Page HTTPS Heartbeat Display Original Page

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

192.168.0.111

2. Configure an IP address group:
 - a. From the navigation tree, select **User Access Policy > Portal Service > IP Group**.
 - b. Click **Add** to open the page as shown in [Figure 7](#).
 - c. Enter the IP group name.
 - d. Enter the start IP address and end IP address of the IP group.
Make sure the client IP address is in the IP group.

- e. Select a service group.
This example uses the default value **Ungrouped**.
- f. From the **Action** list, select **Normal**.
- g. Click **OK**.

Figure 7 Adding an IP address group

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

Add IP Group

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

OK Cancel

3. Add a portal device:
 - a. From the navigation tree, select **User Access Policy > Portal Service > Device**.
 - b. Click **Add** to open the page as shown in [Figure 8](#).
 - c. Enter the device name.
 - d. Select **CMCC 1.0** for **Version**.
 - e. Enter the IP address of the AC's interface connected to the client.
 - f. Set whether to support the portal server heartbeat and user heartbeat functions.
In this example, select **No** for both **Support Server Heartbeat** and **Support User Heartbeat**.
 - g. Enter the key, which must be the same as that configured on the AC.
 - h. Select **Directly Connected** for **Access Method**.
 - i. Use the default settings for other parameters.
 - j. Click **OK**.

Figure 8 Adding a portal device

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

Add Device

Device Information

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

OK Cancel


4. Associate the portal device with the IP address group:
- As shown in Figure 9, click the **Port Group** icon  in the **Operation** field for device **NAS** to open the port group configuration page.

Figure 9 Device list

User > User Access Policy > Portal Service > Device





Query Devices

Device Name Version

Deploy Result Service Group

Query Reset

Add

| Device Name | Version | Service Group | IP Address | Last Deployed at | Deploy Result | Operation |
|-------------|----------|---------------|------------|------------------|---------------|---|
| NAS | CMCC 1.0 | Ungrouped | 2.2.2.1 | | Not Deployed |     |

1-1 of 1. Page 1 of 1.

<< < 1 > >> 50

- Click **Add** to open the page as shown in Figure 10.
- Enter the port group name.
- Select the configured IP address group.
The IP address used by the user to access the network must be within this IP address group.
- Select **Supported** for **Transparent Authentication**.
- Use the default settings for other parameters.
- Click **OK**.

Figure 10 Adding a port group

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

Add Port Group

| | | | |
|-------------------------------|-----------|------------------------------------|-------------|
| Port Group Name * | group | Language * | English |
| Start Port * | 0 | End Port * | zzzzzz |
| Protocol * | HTTP | Quick Authentication * | No |
| NAT or Not * | No | Error Transparent Transmission * | Yes |
| Authentication Type * | CHAP | IP Group * | Portal_user |
| Heartbeat Interval(Minutes) * | 10 | Heartbeat Timeout(Minutes) * | 30 |
| User Domain | | Port Group Description | |
| Transparent Authentication | Supported | Client Protection Against Cracks * | No |
| Page Push Policy | | Default Authentication Page | |

OK Cancel



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

Figure 11 Configuring user endpoint settings

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

User Endpoint Settings

| | | | |
|--------------------------------|--|-------------------------------------|----|
| Transparent MAC Authentication | Enable | Max. Device for Single Account * | 10 |
| Non-Terminal Authentication | Enable  | Log off User with Endpoint Conflict | No |

OK Cancel


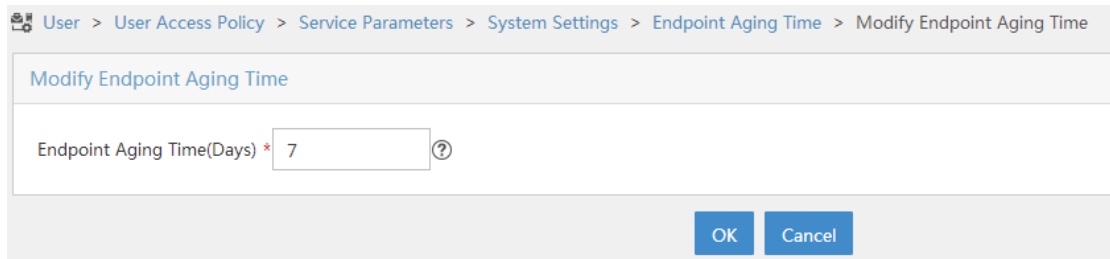
- f. Click the **Configure** icon  for **Endpoint Aging Time** to open the page as shown in [Figure 12](#).
 - g. Set the endpoint aging time as needed.
This example uses the default value.
 - h. Click **OK**.

Figure 12 Setting the endpoint aging time



7. From the navigation tree, select **User Access Policy > Service Parameters > Validate System Configuration** to make the configuration take effect.

Configuring the AC

1. Configure interfaces on the AC:

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

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

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

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

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

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

2. Configure a static route to the INC server:

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

3. Configure a WLAN service:

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

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

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

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

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

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

Set the PSK AKM mode and configure simple character string of **12345678** as the PSK.

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

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

Set the CCMP cipher suite for frame encryption and enable the RSN IE in beacon and probe responses.

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

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

Enable the AC to forward client data traffic. If the AC forwards client data traffic by default, skip this step.

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

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

4. Configure AP settings:

! IMPORTANT:

In a large-scale network, configure AP groups as a best practice.

Create an AP named **office** with model WA4320i-ACN and set its serial ID to 219801A0CNC138011454.

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

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

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

Create AP group **group1** and create an AP grouping rule by AP names to add AP **office** to AP group **group1**.

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

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

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

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

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

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

Enable radio 2.

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

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

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

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

5. Configure a RADIUS scheme:

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

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

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

```
[AC-radius-rs1] primary authentication 192.168.0.111
```

```
[AC-radius-rs1] primary accounting 192.168.0.111
```

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

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

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

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

Configure the source IP address for outgoing RADIUS packets as 2.2.2.1.

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

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

Enable RADIUS session-control.

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

Enable the RADIUS DAS feature and enter RADIUS DAS view.

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

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

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

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

6. Configure authentication domain **dm2**:

Create an ISP domain named **dm2** and enter its view.

```
[AC] domain dm2
```

Configure the authentication, authorization, and accounting scheme RADIUS scheme **rs1** for LAN access users in the ISP domain.

```
[AC-isp-dm2] authentication lan-access radius-scheme rs1
```

```
[AC-isp-dm2] authorization lan-access radius-scheme rs1
```

```
[AC-isp-dm2] accounting lan-access radius-scheme rs1
```

```
[AC-isp-dm2] quit
```

7. Configure authentication domain **dm1**:

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

```
[AC] domain dm1
```

Configure the authentication and authorization methods as RADIUS and the accounting method as none for portal users in the ISP domain.

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

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

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

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

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

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

8. Configure portal authentication:

Create a portal authentication server.

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

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

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

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

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

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

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

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

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

Configure the portal redirection URL to carry the **ssid**, **wlanuserip**, and **wlanacname** parameters, and their values are the wireless SSID, the user's IP address, and the AC's name (required by a CMCC portal Web server).

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

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

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

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

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

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

Configure a portal-free rule numbered **0** to allow portal users to access the portal Web server (whose IP address is 192.168.0.111) without authentication.

```

[AC] portal free-rule 0 destination ip 192.168.0.111 24
# Configure a portal-free rule to permit traffic from aggregate interface 1.
[AC] portal free-rule 1 source interface Bridge-Aggregation 1
# Configure destination-based portal-free rules to permit traffic destined for the DNS server.
[AC] portal free-rule 2 destination ip any udp 53
[AC] portal free-rule 3 destination ip any tcp 53
# Enable portal roaming.
[AC] portal roaming enable
# Disable the Rule ARP entry feature for portal clients.
[AC] undo portal refresh arp enable
# Enable validity check on wireless portal clients.
[AC] portal host-check enable
# Enable direct portal authentication on service template st1.
[AC] wlan service-template st1
[AC-wlan-st-st1] portal enable method direct
# Specify ISP domain dm1 as the portal authentication domain.
[AC-wlan-st-st1] portal domain dm1
# Specify portal Web server newpt on service template st1 for portal authentication.
[AC-wlan-st-st1] portal apply web-server newpt
# Configure the source IP address for outgoing portal packets as 2.2.2.1.
[AC-wlan-st-st1] portal bas-ip 2.2.2.1
[AC-wlan-st-st1] quit
9. Configure MAC authentication:
# Set the authentication mode to mac for WLAN clients on service template st1.
[AC-wlan-st-st1] client-security authentication-mode mac
# Configure the AC to ignore MAC authentication failures on service template st1.
[AC-wlan-st-st1] client-security ignore-authentication
# Specify ISP domain dm2 as the authentication domain for MAC authentication clients on service template st1.
[AC-wlan-st-st1] mac-authentication domain dm2
# Enable service template st1.
[AC-wlan-st-st1] service-template enable
[AC-wlan-st-st1] quit

```

Configuring the switch

```

# Create VLAN 100. The switch will use this VLAN to forward traffic on the CAPWAP tunnel between the AC and the AP.
<Switch> system-view
[Switch] vlan 100
[Switch-vlan100] quit
# Create VLAN 200. The switch will use this VLAN to forward client traffic.
[Switch] vlan 200
[Switch-vlan200] quit
# Create VLAN 2.
[Switch] vlan 2
[Switch-vlan2] quit

```

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

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

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

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

Enable PoE.

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

Configure GigabitEthernet 1/0/3 (the port connected to the INC server) as an access port and assign the access port to VLAN 2.

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

Assign an IP address to VLAN-interface 200.

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

Assign an IP address to VLAN-interface 2.

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

Verifying the configuration

1. Verify that the client needs to pass portal authentication when the client attempts to come online for the first time.

In this case, the RADIUS server does not have the user and its MAC address information. The AC determines that the user has failed the MAC authentication and performs portal authentication for the user.

Display information about all online portal users on the AC.

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

Total portal users: 1

Username: client

AP name: office

Radio ID: 2

SSID: service

Portal server: newpt

State: Online

VPN instance: N/A

| MAC | IP | VLAN | Interface |
|----------------|---------|------|---------------|
| 0021-6330-0933 | 2.2.2.2 | 200 | WLAN-BSS1/0/2 |

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

2. Log out then log in again.

After the client passes portal authentication, the RADIUS server records the user and MAC address information. When the client goes offline and then tries to access the network again, the AC determines that the client has passed MAC authentication and does not perform portal authentication for the client, either.

3. Verify that the client has passed MAC authentication.

Display information about online MAC authentication users on the AC.

```
[AC] display mac-authentication connection
User MAC address           : 0021-6330-0933
AP name                    : office
Radio ID                   : 2
SSID                      : service
BSSID                     : 70ba-efaf-ddb0
Username                   : 002163300933
Authentication domain      : dm2
Initial VLAN               : 200
Authorization VLAN         : 200
Authorization ACL number   : N/A
Authorization user profile : N/A
Termination action         : Default
Session timeout period     : 86401 s
Online from                : 2016/04/22 18:56:20
```

Configuration files

- **AC:**

```
#
vlan 100
#
vlan 200
#
wlan service-template st1
  ssid service
  vlan 200
  client forwarding-location ac
  akm mode psk
  preshared-key pass-phrase cipher $c$3$oLf6pOZ6bxrf25nodjOJKYEfnZ6g6ErccHyQ
  cipher-suite ccmp
  security-ie rsn
  client-security authentication-mode mac
  client-security ignore-authentication
```

```

mac-authentication domain dm2
portal enable method direct
portal domain dm1
portal bas-ip 2.2.2.1
portal apply web-server newpt
service-template enable
#
interface Vlan-interface100
 ip address 2.2.1.1 255.255.255.0
#
interface Vlan-interface200
 ip address 2.2.2.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 100 200
#
 ip route-static 192.168.0.0 16 2.2.2.100
#
 radius session-control enable
#
radius scheme rs1
 primary authentication 192.168.0.111
 primary accounting 192.168.0.111
 key authentication cipher $c$3$Sggqz7lDs4XPnethmAgyAKVlke7qwEkYbQ==
 key accounting cipher $c$3$4J/JBRGwqB4F213furJmKB6JWYXBFjWE6g==
 user-name-format without-domain
nas-ip 2.2.2.1
#
radius dynamic-author server
 client ip 192.168.0.111 key cipher $c$3$AkTEB7OgMYnCqsfDeplhoAgXUek/rVrLZw==
#
domain dm1
 authorization-attribute idle-cut 15 1024
 authentication portal radius-scheme rs1
 authorization portal radius-scheme rs1
 accounting portal none
#
domain dm2
 authorization-attribute idle-cut 15 1024
 authentication lan-access radius-scheme rs1
 authorization lan-access radius-scheme rs1
 accounting lan-access radius-scheme rs1
#
portal host-check enable
portal free-rule 0 destination ip 192.168.0.0 255.255.255.0
portal free-rule 1 source interface Bridge-Aggregation 1

```

```

portal free-rule 2 destination ip any udp 53
portal free-rule 3 destination ip any tcp 53
#
portal roaming enable
undo portal refresh arp enable
#
portal web-server newpt
url http://192.168.0.111:8080/portal
server-type cmcc
url-parameter ssid ssid
url-parameter wlanacname value AC
url-parameter wlanuserip source-address
#
portal server newpt
ip 192.168.0.111 key cipher $c$3$jiLQ5VIGG4TF7R3sHTT07bmv9rtiSQYBzQ==
server-type cmcc
#
wlan ap-group group1
ap office
ap-model AP 3620
radio 1
radio 2
radio enable
service-template st1
#
wlan ap office model AP 3620
serial-id 219801A28N819CE0002T
#

```

- **Switch:**

```

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

```



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

Related documentation

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

INTELBRAS Access Controllers

Dual-Link Backup and AP License Synchronization

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 dual-link backup and AP license synchronization | 1 |
| Network requirements | 1 |
| Restrictions and guidelines | 2 |
| Procedures | 2 |
| Configuring AC 1 | 2 |
| Configuring AC 2 | 3 |
| Configuring the switch | 4 |
| Verifying the configuration | 5 |
| Configuration files | 6 |
| Related documentation | 8 |

Introduction

The following information provides a dual-link backup and AP license synchronization configuration example.

Prerequisites

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

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

This document assumes that you have basic knowledge of AP management, WLAN high availability, and AP license synchronization features.

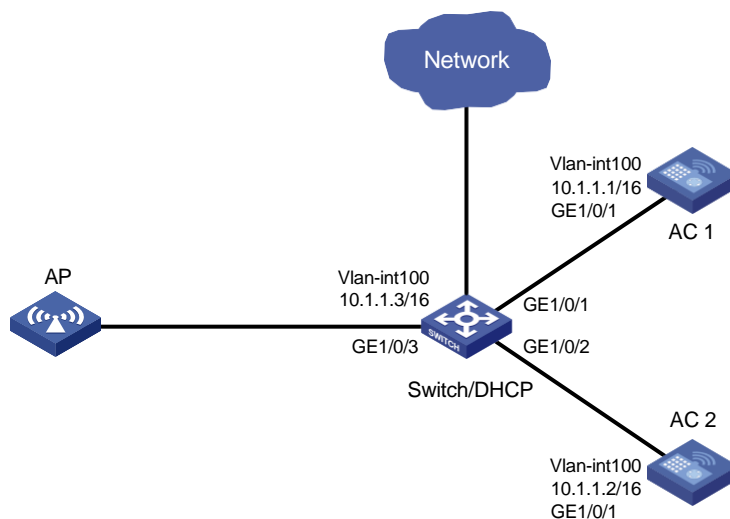
Example: Configuring dual-link backup and AP license synchronization

Network requirements

As shown in [Figure 1](#), configure AC 1 as the master AC and AC 2 as the backup AC. When AC 1 fails and AC 2 takes over, the AP can communicate through AC 2. Configure the master CAPWAP tunnel preemption feature on the two ACs so that the AP reconnects to AC 1 when AC 1 recovers.

Enable AP license synchronization on AC 1 and AC 2 for the two ACs to back up licenses for each other.

Figure 1 Network diagram



Restrictions and guidelines

When you configure dual-link backup and AP license synchronization, follow these restrictions and guidelines:

- Make sure the device model is compatible with the software version.
- Use the actual serial ID of an AP to uniquely identify that AP.
- If you use a manual AP to establish CAPWAP tunnels with the ACs, make sure the name of the AP is the same on the two ACs and either a serial ID or MAC address is configured for the AP on the two ACs.
- As a best practice, install a license on the master AC before enabling AP license synchronization.
- Before enabling AP license synchronization, you must specify IP addresses and roles for the AC and its member ACs in the AP license synchronization group.
- Configure both AC 1 and AC 2 as the master in the AP license synchronization group.
- When the master AC fails, the backup AC takes over and becomes the new master AC. The licenses synchronized to the new master AC will be valid for a 30-day grace period.
- Dual-link backup is applicable to both centralized forwarding and local forwarding. This example uses centralized forwarding.

Procedures

Configuring AC 1

Installing a license

Install a license on AC 1. (Details not shown.)

Configuring interfaces on AC 1

Configure VLAN 100 and VLAN-interface 100, and assign an IP address to the VLAN interface. AC 1 will use this IP address to establish CAPWAP tunnels with APs.

```
<AC1> system-view
[AC1] vlan 100
[AC1-vlan100] quit
[AC1] interface vlan-interface 100
[AC1-Vlan-interface100] ip address 10.1.1.1 16
[AC1-Vlan-interface100] quit
```

Configure GigabitEthernet 1/0/1 that connects AC 1 to the switch as a trunk port, and assign it to all VLANs.

```
[AC1] interface gigabitethernet 1/0/1
[AC1-GigabitEthernet1/0/1] port link-type trunk
[AC1-GigabitEthernet1/0/1] port trunk permit vlan all
[AC1-GigabitEthernet1/0/1] quit
```

Configuring dual-link backup

Create AP group **group1**, and set the connection priority to 7.

```
[AC1] wlan ap-group group1
[AC1-wlan-ap-group-group1] priority 7
```

Specify a backup AC.

```
[AC1-wlan-ap-group-group1] backup-ac ip 10.1.1.2
```

```
# Enable master CAPWAP tunnel preemption.
[AC1-wlan-ap-group-group1] wlan tunnel-preempt enable

# Create an AP grouping rule by AP names.
[AC1-wlan-ap-group-group1] ap ap1
[AC1-wlan-ap-group-group1] quit
```

Configuring AP license synchronization

```
# Enable AP license synchronization on AC 1 and configure AC 1 as the master AC.
[AC1] wlan ap-license-group
[AC1-wlan-als-group] local ip 10.1.1.1
[AC1-wlan-als-group] member ip 10.1.1.2
[AC1-wlan-als-group] ap-license-synchronization enable
[AC1-wlan-als-group] quit
```

Configuring a manual AP

```
# Create an AP named ap1, and specify the AP model and serial ID.
[AC1] wlan ap ap1 model AP 3620
[AC1-wlan-ap-ap1] serial-id 219801A28N819CE0002T
```

Configuring AC 2

(Optional.) Installing a license

```
# Install a license on AC 2. (Details not shown.)
```

Configuring interfaces on AC 2

```
# Configure VLAN 100 and VLAN-interface 100, and assign an IP address to the VLAN interface. AC 2 will use this IP address to establish CAPWAP tunnels with APs.
```

```
<AC2> system-view
[AC2] vlan 100
[AC2-vlan100] quit
[AC2] interface Vlan-interface 100
[AC2-Vlan-interface100] ip address 10.1.1.2 16
[AC2-Vlan-interface100] quit
```

```
# Configure GigabitEthernet 1/0/1 that connects AC 2 to the switch as a trunk port, and assign it to all VLANs.
```

```
[AC2] interface gigabitethernet 1/0/1
[AC2-GigabitEthernet1/0/1] port link-type trunk
[AC2-GigabitEthernet1/0/1] port trunk permit vlan all
[AC2-GigabitEthernet1/0/1] quit
```

Configuring dual-link backup

```
# Create AP group group1, and specify a backup AC. Use the default setting for the connection priority.
```

```
[AC2] wlan ap-group group1
[AC2-wlan-ap-group-group1] backup-ac ip 10.1.1.1
```

```
# Create an AP grouping rule by AP names.
```

```
[AC2-wlan-ap-group-group1] ap ap1
[AC2-wlan-ap-group-group1] quit
```

Configuring AP license synchronization

Enable AP license synchronization on AC 1 and configure AC 1 as the master AC.

```
[AC2] wlan ap-license-group
[AC2-wlan-als-group] local ip 10.1.1.2
[AC2-wlan-als-group] member ip 10.1.1.1
[AC2-wlan-als-group] ap-license-synchronization enable
[AC2-wlan-als-group] quit
```

Configuring a manual AP

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

```
[AC2] wlan ap ap1 model AP 3620
[AC2-wlan-ap-ap1] serial-id 219801A28N819CE0002T
```

Configuring the switch

Configuring interfaces on the switch

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

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

Create VLAN interface 100, and assign it an IP address.

```
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ip address 10.1.1.3 16
[Switch-Vlan-interface100] quit
```

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

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

Configure GigabitEthernet 1/0/2 that connects the switch to AC 2 as a trunk port, and assign the port to all VLANs.

```
[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] port link-type trunk
[Switch-GigabitEthernet1/0/2] port trunk permit vlan all
[Switch-GigabitEthernet1/0/2] quit
```

Configure GigabitEthernet 1/0/3 that connects the switch to the AP as an access port, and assign the port to VLAN 100.

```
[Switch] interface gigabitethernet 1/0/3
[Switch-GigabitEthernet1/0/3] port link-type access
[Switch-GigabitEthernet1/0/3] port access vlan 100
```

Enable the PoE feature.

```
[Switch-GigabitEthernet1/0/3] poe enable
[Switch-GigabitEthernet1/0/3] quit
```

Configuring DHCP

Create DHCP address pool 100. Specify the 10.1.0.0/16 subnet for the pool.

```
[Switch] dhcp server ip-pool 100
[Switch-dhcp-pool-100] network 10.1.0.0 mask 255.255.0.0
[Switch-dhcp-pool-100] quit

# Enable DHCP.
[Switch] dhcp enable
```

Verifying the configuration

Display AP license synchronization group information on AC 1 to verify that the number of licenses in the group is the sum of licenses installed on AC 1 and AC 2.

```
<AC1> display wlan ap-license-group
Group total licenses: 256
Group used licenses: 1
AP license synchronization: Enabled
Local IP: 10.1.1.1
Local role: Master
Member information: 1
```

| IP address | Total | Used | Member role | State | Online duration |
|------------|-------|------|-------------|-------|-----------------|
| 10.1.1.2 | 0 | 0 | Master | UP | 00hr 1min 51sec |

Verify that the AP state is R/M on AC 1.

```
<AC1> 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: 384
Remaining APs: 383
Total AP licenses: 256
Local AP licenses: 256
Server AP licenses: 0
Remaining local AP licenses: 255
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 | 1 | R/M | AP 3620 | 219801A28N819CE0002T |

Verify that the AP state is R/M on AC 1 and R/B on AC 2, and the number of licenses is 256.

```
<AC2> 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: 384
Remaining APs: 383
Total AP licenses: 256
Local AP licenses: 256
Server AP licenses: 0
Remaining local AP licenses: 256
Sync AP licenses: 256

```

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 | 1 | R/B | AP 3620 | 219801A28N819CE0002T |

Shut down VLAN-interface 1 on AC 2 and wait for no longer than 30 seconds, during which service interruption occurs. Verify that the AP is in R/M state.

```
<AC2> 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: 384
Remaining APs: 383
Total AP licenses: 256
Local AP licenses: 256
Server AP licenses: 0
Remaining local AP licenses: 255
Sync AP licenses: 256

```

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 | 1 | R/M | AP 3620 | 219801A28N819CE0002T |

Bring up VLAN-interface 1 on AC 1. Verify that the AP state is R/M on AC 1 and R/B on AC 2. (Details not shown.)

Configuration files

- AC 1:
#

```

vlan 100
#
interface Vlan-interface100
 ip address 10.1.1.1 255.255.0.0
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan all
#
wlan ap-group group1
 priority 7
 wlan tunnel-preempt enable
 backup-ac ip 10.1.1.2
 ap ap1
#
wlan ap ap1 model AP 3620
 serial-id 219801A28N819CE0002T
#
wlan ap-license-group
 local ip 10.1.1.1
 member ip 10.1.1.2
 ap-license-synchronization enable
#

```

- **AC 2:**

```

#
vlan 100
#
interface Vlan-interface100
 ip address 10.1.1.2 255.255.0.0
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan all
#
wlan ap-group group1
 backup-ac ip 10.1.1.1
 ap ap1
#
wlan ap ap1 model AP 3620
 serial-id 219801A28N819CE0002T
#
wlan ap-license-group
 local ip 10.1.1.2
 member ip 10.1.1.1
 ap-license-synchronization enable
#

```

- **Switch**

```

#

```

```

    dhcp enable
#
vlan 100
#
dhcp server ip-pool 100
    network 10.1.0.0 mask 255.255.0.0
#
interface Vlan-interface100
    ip address 10.1.1.3 255.255.0.0
#
#
interface GigabitEthernet1/0/1
    port link-type trunk
    port trunk permit vlan all
#
interface GigabitEthernet1/0/2
    port link-type trunk
    port trunk permit vlan all
#
interface GigabitEthernet1/0/3
    port link-type access
    port access vlan 100
    poe enable
#

```

Related documentation

- *AP License Synchronization Command Reference in INTELBRAS Access Controllers Command References*
- *AP License Synchronization Configuration Guide in INTELBRAS Access Controllers Configuration Guides*
- *AP Management Command Reference in INTELBRAS Access Controllers Command References*
- *AP Management Configuration Guide in INTELBRAS Access Controllers Configuration Guides*
- *WLAN High Availability Command Reference in INTELBRAS Access Controllers Command References*
- *WLAN High Availability Configuration Guide in INTELBRAS Access Controllers Configuration Guides*

INTELBRAS Access Controllers

Auto-DFS and Auto-TPC 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 |
| Restrictions and guidelines | 1 |
| Example: Configuring auto-DFS and auto-TPC | 1 |
| Network configuration | 1 |
| Procedures | 2 |
| Configuring the AC | 2 |
| Configure the switch | 3 |
| Verifying the configuration | 4 |
| Configuration files | 7 |
| Related documentation | 9 |

Introduction

The following information provides an example for configuring auto dynamic frequency selection (DFS) and auto transmit power control (TPC).

Prerequisites

The following information applies to Comware-based access controllers and access points with a software version of 5439 or later (5411 or later for the AP 7000 series access points). Procedures and information in the examples might be slightly different depending on the software or hardware version of the access controllers and access points.

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

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

Restrictions and guidelines

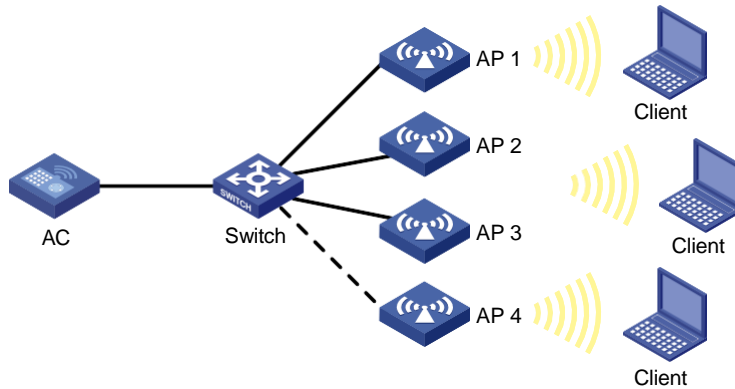
- Auto-DFS and auto-TPC are not supported in the following scenarios or devices:
 - Scenarios where the working channels and powers are not allowed to change.
 - Unified wired and wireless access controller.
 - WTU420, WTU420H, and X-share series access points.
- As a best practice, do not enable Auto-DFS or auto-TPC when CUPID location is enabled.
- Use the serial ID labeled on the AP to specify an AP.
- Do not manually specify a working channel, because it has a higher priority than the automatically selected channel.
- Make sure power lock is disabled.
- As a best practice, set the bandwidth mode for the 5 GHz radio to 40 MHz or 20 MHz.
- To enable auto-DFS or auto-TPC only for an AP or AP group, use the following commands:
 - `calibrate-channel self-decisive enable`
 - `calibrate-power self-decisive enable`

Example: Configuring auto-DFS and auto-TPC

Network configuration

As shown in [Figure 1](#), in centralized forwarding mode, the AC is connected to the switch, and the switch assigns an IP address to the AP and clients as a DHCP server. Configure auto-DFS and auto-TPC for the AP to change the working channel and transmit power automatically based on the wireless environment.

Figure 1 Network diagram



Procedures

Configuring the AC

1. Configure interfaces on the AC:

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

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

Create VLAN 200 and VLAN-interface 200, and assign an IP address to the VLAN interface. VLAN 200 will be used for client access.

```
[AC] vlan 200
[AC-vlan200] quit
[AC] interface vlan-interface 200
[AC-Vlan-interface200] ip address 192.2.0.1 24
[AC-Vlan-interface200] quit
```

Configure GigabitEthernet 1/0/1 that connects the switch to the AC as a trunk port, and assign the trunk port to VLAN1, VLAN 100, and VLAN 200.

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

2. Configure a wireless service:

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

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

Configure the SSID as **service**.

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

Specify VLAN 200 in the service template.

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

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

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

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

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

Configure the AC to forward client data traffic. You can skip this step if the AC is the client traffic forwarder by default.

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

Enable the service template.

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

3. Configure an AP:

Create a manual AP named **ap1**, and specify the AP model and serial ID.

```
[AC] wlan ap ap1 model AP 5630
[AC-wlan-ap-ap1] serial-id 219801A23V8192E00021
```

Create AP group **group1**, add the AP to the AP group, and specify the AP model.

```
[AC] wlan ap-group group1
[AC-wlan-ap-group-group1] ap ap1
[AC-wlan-ap-group-group1] ap-model AP 5630
```

Enter the view of radio 1.

```
[AC-wlan-ap-group-group1-ap-model-AP 5630] radio 1
```

Set the bandwidth mode to **40 MHz**.

```
[AC-wlan-ap-group-group1-ap-model-AP 5630-radio-1] channel band-width 40
```

Bind WLAN service template **service** to radio 1 and enable the radio.

```
[AC-wlan-ap-group-group1-ap-model-AP 5630-radio-1] service-template
service [AC-wlan-ap-group-group1-ap-model-AP 5630-radio-1] radio enable
[AC-wlan-ap-group-group1-ap-model-AP 5630-radio-1]
quit [AC-wlan-ap-group-group1-ap-model-AP 5630] quit
[AC-wlan-ap-group-group1] quit
```

Configure AP 2, AP 3, and AP 4 in the same way AP 1 is configured.

4. Configure auto-DFS and auto-TPC:

Enter global configuration view.

```
[AC] wlan global-configuration
```

Enable auto-TPC.

```
[AC-wlan-global-configuration] calibrate-power self-decisive enable all
```

Enable auto-DFS.

```
[AC-wlan-global-configuration] calibrate-channel self-decisive enable all
[AC-wlan-global-configuration] quit
[AC] quit
```

Configure the switch

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

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



```
[Switch-vlan100] quit
```

Create VLAN 200. The switch will use this VLAN to forward packets for wireless clients.

```
[Switch] vlan 200
```

```
[Switch-vlan200] quit
```

Configure GigabitEthernet 1/0/1 that connects the switch to the AC as a trunk port, and assign the trunk port to VLAN1, VLAN 100, and VLAN 200.

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

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

```
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 1 100 200
```

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

Configure GigabitEthernet 1/0/2 that connects the switch to the APs as an access port, and assign the access port to VLAN 100.

```
[Switch] interface range gigabitethernet 1/0/2 to gigabitethernet 1/0/5
```

```
[Switch-if-range] port link-type access
```

```
[Switch-if-range] port access vlan 100
```

Enable the PoE feature.

```
[Switch-if-range] poe enable
```

```
[Switch-if-range] quit
```

Specify an IP address for VLAN-interface 100.

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

```
[Switch-Vlan-interface100] ip address 192.1.0.2 16
```

```
[Switch-Vlan-interface100] quit
```

Specify an IP address for VLAN-interface 200.

```
[Switch] interface vlan-interface 200
```

```
[Switch-Vlan-interface200] ip address 192.2.0.2 24
```

```
[Switch-Vlan-interface200] quit
```

Enable DHCP.

```
[Switch] dhcp enable
```

Create DHCP address pool 100. Specify the 192.1.0.0/16 subnet and the 192.1.0.1 gateway for the pool.

```
[Switch] dhcp server ip-pool 100
```

```
[Switch-dhcp-pool-100] network 192.1.0.0 mask 255.255.0.0
```

```
[Switch-dhcp-pool-100] gateway-list 192.1.0.1
```

```
[Switch-dhcp-pool-100] quit
```

Create DHCP address pool 200. Specify the 192.2.0.0/16 subnet and the 192.2.0.1 gateway for the pool.

```
[Switch] dhcp server ip-pool 200
```

```
[Switch-dhcp-pool-200] network 192.2.0.0 mask 255.255.255.0
```

```
[Switch-dhcp-pool-200] gateway-list 192.2.0.1
```

```
[Switch-dhcp-pool-200] quit
```

Verifying the configuration

1. View AP registration information on the AC:

Verify that the APs have been associated with the AC. If the APs are in R/M state, the APs have been associated with the AC.

```
<AC> display wlan ap all
```

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 | 1 | R/M | AP 5630 | 219801A23V8192E00021 |
| ap2 | 2 | R/M | AP 5630 | 219801A23V8192E00022 |
| ap3 | 3 | R/M | AP 5630 | 219801A23V8192E00023 |
| ap4 | 4 | R/M | AP 5630 | 219801A23V8192E00024 |

2. View history and detailed RRM information on the AC.

Display DFS and TPC information for radio 1 of AP 1 on the AC to verify that the channel and power have been changed.

<AC> display wlan rrm-history ap name ap1

AP RRM History

Flags : I - Interference, P - Packets discarded, F - Retransmission,
R - Radar, C - Coverage, B - Channelbusy,
M - Manual O - Others

AP RRM History : ap1

Radio : 1 Basic BSSID : 7848-59f3-df80

| | Ch | Power (dBm) | Load (%) | Util (%) | Intf (%) | PER (%) | Retry (%) | Reason | Date (yyyy-mm-dd) | Time (hh:mm:ss) |
|--------|----|----------------|-------------|-------------|-------------|------------|--------------|----------|----------------------|--------------------|
| Before | 36 | 20 | 21 | 0 | 11 | 0 | 1 | ----C--- | 2021-02-25 | 15:12:56 |
| After | 36 | 17 | 21 | 0 | 11 | 0 | 1 | - | - | - |
| Before | 36 | 17 | 21 | 0 | 12 | 0 | 0 | ----C--- | 2021-02-25 | 15:15:56 |
| After | 36 | 14 | 21 | 0 | 12 | 0 | 0 | - | - | - |
| Before | 36 | 14 | 21 | 0 | 12 | 0 | 0 | ----C--- | 2021-02-25 | 15:18:56 |
| After | 36 | 11 | 21 | 0 | 12 | 0 | 0 | - | - | - |
| Before | 36 | 11 | 18 | 0 | 11 | 0 | 10 | - ---B-- | 2021-02-25 | 15:25:21 |
| After | 40 | 11 | 16 | 0 | 10 | 0 | 8 | - | - | - |

Display detailed DFS and TPC information for radio 1 of AP 1 on the AC.

<AC> display wlan rrm-status ap name ap1

AP RRM Profile : ap1

Radio : 1 Basic BSSID : 7848-59f3-df80
Channel : 40 Tx Power (dBm) : 14

| Ch | Nbrs | Load | Util | Intf | PER | Retry | Radar | Last Detected At |
|----|------|------|------|------|-----|-------|-------|------------------|
|----|------|------|------|------|-----|-------|-------|------------------|

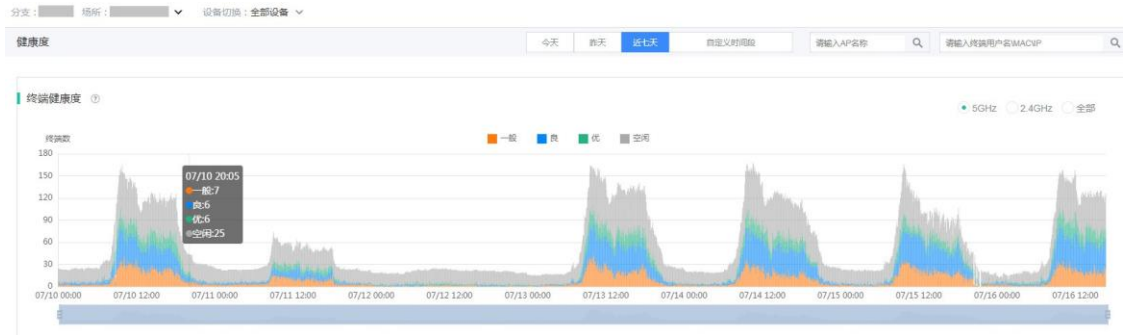
| | | (%) | (%) | (%) | (%) | (%) | | |
|-----|----|-----|-----|-----|-----|-----|---|---------------------|
| 36 | 44 | 23 | 0 | 16 | 0 | 0 | - | 2021-02-26 15:30:32 |
| 40 | 3 | 9 | - | 1 | 0 | - | - | 2021-02-26 15:30:32 |
| 44 | 11 | 18 | - | 6 | 0 | - | - | 2021-02-26 15:30:32 |
| 48 | 8 | 30 | - | 10 | 0 | - | - | 2021-02-26 15:30:32 |
| 52 | 25 | 17 | - | 12 | 0 | - | - | 2021-02-26 15:30:32 |
| 56 | 0 | 7 | - | 0 | 0 | - | - | 2021-02-26 15:30:32 |
| 60 | 4 | 8 | - | 1 | 0 | - | - | 2021-02-26 15:30:32 |
| 64 | 7 | 7 | - | 0 | 0 | - | - | 2021-02-26 15:30:32 |
| 149 | 30 | 32 | - | 24 | 0 | - | - | 2021-02-26 15:30:32 |
| 153 | 12 | 10 | - | 3 | 0 | - | - | 2021-02-26 15:30:32 |
| 157 | 12 | 14 | - | 4 | 0 | - | - | 2021-02-26 15:30:32 |
| 161 | 5 | 8 | - | 2 | 0 | - | - | 2021-02-26 15:30:32 |
| 165 | 5 | 7 | - | 1 | 0 | - | - | 2021-02-26 15:30:32 |

| Nbr-MACAddress | Ch | Intf (%) | SignalStr (dBm) | Type | Last Detected At |
|----------------|-----|-------------|--------------------|-----------|---------------------|
| 0023-89e2-ed80 | 36 | 0 | -29 | Unmanaged | 2021-02-26 15:30:40 |
| 0023-ee00-1168 | 52 | 0 | -88 | Unmanaged | 2021-02-26 15:30:40 |
| 04d7-a537-8540 | 149 | 0 | -68 | Unmanaged | 2021-02-26 15:30:40 |
| 1019-651b-d682 | 36 | 0 | -7 | Unmanaged | 2021-02-26 15:30:40 |
| 1019-651b-d691 | 149 | 2 | -52 | Unmanaged | 2021-02-26 15:30:40 |
| 346b-5b6c-1e00 | 36 | 0 | -47 | Unmanaged | 2021-02-26 15:30:40 |
| 346b-5b6c-1e01 | 36 | 0 | -53 | Unmanaged | 2021-02-26 15:30:40 |
| 346b-5b76-1d20 | 36 | 0 | -35 | Managed | 2021-02-26 15:30:40 |
| 346b-5b76-1d22 | 36 | 0 | -23 | Managed | 2021-02-26 15:30:40 |
| 346b-5b76-1d23 | 36 | 0 | -17 | Managed | 2021-02-26 15:30:40 |
| 346b-5b76-1d24 | 36 | 0 | -20 | Managed | 2021-02-26 15:30:40 |
| 3891-d502-be60 | 52 | 0 | -60 | Managed | 2021-02-26 15:30:40 |
| 3891-d502-be61 | 52 | 0 | -61 | Managed | 2021-02-26 15:30:40 |
| 3891-d58a-8f80 | 44 | 0 | -75 | Unmanaged | 2021-02-26 15:30:40 |
| 3891-d58a-8f81 | 44 | 0 | -76 | Unmanaged | 2021-02-26 15:30:40 |
| 3891-d58a-8f82 | 44 | 0 | -75 | Unmanaged | 2021-02-26 15:30:40 |
| 3891-d58a-8f90 | 161 | 0 | -94 | Unmanaged | 2021-02-26 15:30:40 |
| 3891-d58d-6d41 | 52 | 0 | -45 | Unmanaged | 2021-02-26 15:30:40 |
| 3897-d618-90e0 | 36 | 0 | -32 | Unmanaged | 2021-02-26 15:30:40 |
| 3897-d6e0-e860 | 36 | 0 | -38 | Unmanaged | 2021-02-26 15:30:40 |

3. (Optional.) Connect the AC to the Cloudnet platform to view AP and client statistics.

View the health status of clients to identify whether the number of clients with a health score of excellent and good has increased.

Figure 2 Client health status



View the health status of APs to identify whether the number of APs with a health score of excellent and good has increased.

Figure 3 AP health status



Configuration files

- Switch:

```
#
dhcp enable

#
vlan 100
#
vlan 200
#
dhcp server ip-pool 100
gateway-list 192.1.0.1
network 192.1.0.0 mask 255.255.0.0
#
dhcp server ip-pool 200
gateway-list 192.2.0.1
network 192.2.0.0 mask 255.255.255.0
#
interface Vlan-interface100
ip address 192.1.0.2 255.255.0.0
#
interface Vlan-interface200
ip address 192.2.0.2 255.255.255.0
```

```
#
interface GigabitEthernet1/0/1
  port link-type trunk
  port trunk permit vlan 1 100 200
#
interface GigabitEthernet1/0/2
  port link-type access
  port access vlan 100
  poe enable
#
interface GigabitEthernet1/0/3
  port link-type access
  port access vlan 100
  poe enable
#
interface GigabitEthernet1/0/4
  port link-type access
  port access vlan 100
  poe enable
#
interface GigabitEthernet1/0/5
  port link-type access
  port access vlan 100
  poe enable
#
```

- **AC:**

```
#
wlan global-configuration
  calibrate-channel self-decisive enable all
  calibrate-power self-decisive enable all
#
vlan 100
#
vlan 200
#
wlan service-template service
  ssid service
  vlan 200
  client forwarding-location ap
  akm mode psk
  preshared-key pass-phrase cipher $c$3$HOaHaYA7Aazh6+V0xH8AvnFdV1xTZew0uBZs
  cipher-suite ccmp
  security-ie rsn
service-template enable
#
interface Vlan-interface100
  ip address 192.1.0.1 255.255.0.0
#
```

```

interface Vlan-interface200
 ip address 192.2.0.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 1 100 200
#
wlan ap-group group1
 vlan 1
 ap ap1
 ap-model AP 5630
 radio 1
 radio enable
 channel band-width 40
 service-template service
#
wlan ap ap1 model AP 5630
 serial-id 219801A23V8192E00021
#
wlan ap ap2 model AP 5630
 serial-id 219801A23V8192E00022
#
wlan ap ap3 model AP 5630
 serial-id 219801A23V8192E00023
#
wlan ap ap4 model AP 5630
 serial-id 219801A23V8192E00024
#

```

Related documentation

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