

INTELBRAS Access Controllers

WEP 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 WEP 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 WEP 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.

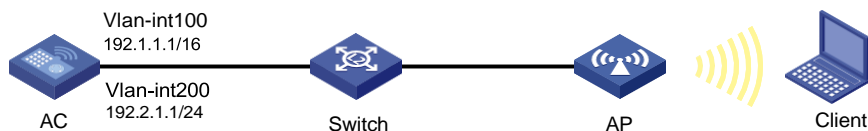
This document assumes that you have basic knowledge of WLAN access and WEP encryption.

Example: Configuring WEP 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. Configure WEP on the AC to enable the client to use WEP for encryption.

Figure 1 Network diagram



Restrictions and guidelines

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

- Use the actual serial ID of an AP to uniquely identify that AP.
- Make sure the WEP key IDs configured on the client and the AC are the same. As a best practice, set the key ID to 1 on the AC because some clients only support key ID 1.

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 WEP40 cipher suite for frame encryption, and configure plain text **12345 as WEP key 1.**

```
[AC-wlan-st-1] cipher-suite wep40
[AC-wlan-st-1] wep key 1 wep40 pass-phrase simple 12345
[AC-wlan-st-1] wep key-id 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
```

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 the 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 by using the WEP40 cipher suite.

```
[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
Cipher suite	: WEP40
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
  cipher-suite wep40
  wep key 1 wep40 pass-phrase cipher $c$3$3biXGrrILUAd5QTBAPer4VkW7KlrLoGn
  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-mode bridge
    port link-type trunk
    undo port trunk permit vlan 1
    port trunk permit vlan 100 200
#
interface GigabitEthernet1/0/2
    port link-mode bridge
    port link-type trunk
    undo port trunk permit vlan 1
    port trunk permit vlan 100
    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.

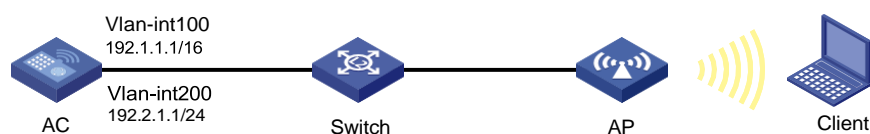
Example: Configuring PSK encryption

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 WPA3-SAE 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 with the WPA3-SAE security mode	1
Network configuration	1
Restrictions and guidelines	1
Procedures	2
Configuring the AC	2
Configuring the switch	3
Verifying the configuration	4
Configuration files	6
Related documentation	7

Introduction

The following information provides an example for configuring PSK encryption with the WPA3-SAE security mode.

Prerequisites

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

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

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

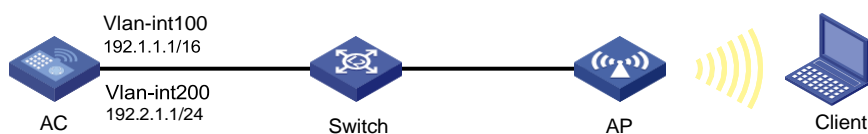
Example: Configuring PSK encryption with the WPA3-SAE security mode

Network configuration

As shown in [Figure 1](#), the switch acts as a DHCP server to assign IP addresses to the AP and the client. 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.
- Set the security mode to WPA3-SAE.

Figure 1 Network diagram



Restrictions and guidelines

When you configure PSK encryption with the WPA3-SAE security mode, follow these restrictions and guidelines:

- Use the actual serial ID of an AP to uniquely identify that 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 **wpa3_personal** and enter its view.

```
[AC] wlan service-template wpa3_personal
```

Configure the SSID as **wpa3_personal**.

```
[AC-wlan-st-wpa3_personal] ssid wpa3_personal
```

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

```
[AC-wlan-st-wpa3_personal] vlan 200
```

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

```
[AC-wlan-st-wpa3_personal] akm mode psk
[AC-wlan-st-wpa3_personal] preshared-key pass-phrase simple 12345678
```

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

```
[AC-wlan-st-wpa3_personal] cipher-suite ccmp
[AC-wlan-st-wpa3_personal] security-ie rsn
```

Set the WPA3 security mode to personal (WPA3-SAE) and specify the mandatory mode.

```
[AC-wlan-st-wpa3_personal] wpa3 personal mandatory
```

Enable mandatory management frame protection.

```
[AC-wlan-st-wpa3_personal] pmf mandatory
```

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-wpa3_personal] client forwarding-location ac
```

Enable the service template.

```
[AC-wlan-st-wpa3_personal] service-template enable
[AC-wlan-st-wpa3_personal] 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 *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 add the AP to the AP group.

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

Bind service template *wpa3_personal* 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 wpa3_personal
```

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 100 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 an access port, and assign the port to VLAN 100.

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

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

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

Enable PoE on GigabitEthernet 1/0/2.

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

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

2. Configure DHCP:

Enable DHCP.

```
[Switch] dhcp enable
```

Create DHCP address pool **vlan100 to assign an IP address to the AP, specify subnet 192.1.0.0/16 in the DHCP address pool, and specify the gateway address as 192.1.1.2.**

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

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

```
[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 AP, and specify subnet 192.2.1.0/24 in the DHCP address pool. 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 the DNS server.**

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

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

```
[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	: ccc9-5de2-512d
IPv4 address	: 192.2.1.3
IPv6 address	: N/A
Username	: N/A
AID	: 1
AP ID	: 1
AP name	: office
Radio ID	: 2
Channel	: 149
SSID	: wpa3_personal
BSSID	: f474-8879-ea70
VLAN ID	: 200
Sleep count	: 0
Wireless mode	: 802.11ax

Channel bandwidth	: 80MHz
SM power save	: Disabled
Short GI for 20MHz	: Supported
Short GI for 40MHz	: Supported
Short GI for 80MHz	: Supported
Short GI for 160/80+80MHz	: Not supported
STBC RX capability	: Not supported
STBC TX capability	: Not supported
LDPC RX capability	: Supported
Beamformee STS capability	: N/A
Number of Sounding Dimensions	: N/A
SU beamformee capability	: Not supported
MU beamformee capability	: Not supported
Block Ack	: N/A
Supported VHT-MCS set	: NSS1 0, 1, 2, 3, 4, 5, 6, 7, 8, 9 NSS2 0, 1, 2, 3, 4, 5, 6, 7, 8, 9
Supported HT MCS set	: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15
Supported rates	: 6, 9, 12, 18, 24, 36, 48, 54 Mbps
5G 40And80MHz Channel bandwidth	: Supported
5G 160MHz Channel bandwidth	: Not Supported
5G 8080MHz Channel bandwidth	: Not Supported
OFDMA random access RUs	: Not supported
Supported HE-MCS set	: NSS1 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11 NSS2 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11
TWT scheduled	: no
QoS mode	: WMM
Listen interval	: 20
RSSI	: 0
Rx/Tx rate	: 0/0 Mbps
Speed	: N/A
Authentication method	: SAE
Security mode	: RSN
AKM mode	: PSK
Cipher suite	: CCMP
User authentication mode	: Bypass
WPA3 status	: Enabled
Authorization CAR	: N/A
Authorization ACL ID	: N/A
Authorization user profile	: N/A
Roam status	: N/A
Key derivation	: SHA256
PMF status	: Enabled
Forwarding policy name	: Not configured
Online time	: 0days 0hours 0minutes 10seconds
FT status	: Inactive

Configuration files

- AC:

```
#
vlan 100
#
vlan 200
#
wlan service-template wpa3_personal
    ssid wpa3_personal
client forwarding-location ac
vlan 200
akm mode psk
    preshared-key pass-phrase cipher $c$3$N//5BVbsOqdBTxi+7MJZKT6Zqh5MAMys2ZzM
    cipher-suite ccmp
    wpa3 personal mandatory
    pmf mandatory
    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 office
    ap-model AP 3620
    radio 2
        radio enable
        service-template wpa3_personal
gigabitethernet 1
ten-gigabitethernet 1
#
wlan ap office 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
#
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
#
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
#

```

Related documentation

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

INTELBRAS Access Controllers WLAN Access (IPv6) Configuration Examples

Copyright © 2024 Intelbras S.A All rights reserved.

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

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

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

Contents

Introduction	1
Prerequisites	1
Example: Configuring IPv6 WLAN access	1
Network configuration	1
Restrictions and guidelines	1
Procedures	2
Configuring the AC	2
Configuring the switch	4
Verifying the configuration	6
Configuration files	6
Related documentation	8

Introduction

The following information provides an IPv6 access configuration example.

Prerequisites

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

The configuration examples 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.

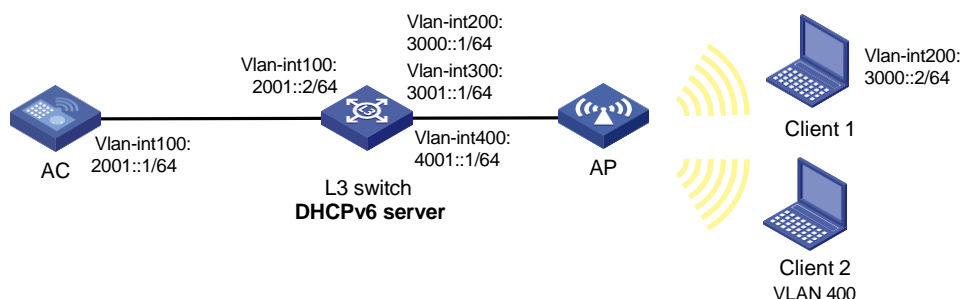
This document assumes that you have basic knowledge of IPv6 basics and WLAN access.

Example: Configuring IPv6 WLAN access

Network configuration

As shown in [Figure 1](#), the Layer 3 switch acts as a DHCP server to assign IPv6 addresses to the AP and Client 1 and assign an IPv6 prefix to Client 2. Configure wireless services to ensure that the WLAN uses IPv6 addresses and Client 1 and Client 2 can access the WLAN. Assume that centralized forwarding is used in this example.

Figure 1 Network diagram



Restrictions and guidelines

When you configure IPv6 access, follow these restrictions and guidelines:

- Use the actual serial ID of an AP to uniquely identify that AP.
- To prevent too many packets from entering VLAN 1, configure the switch's interface that connects the switch to the AP to deny packets from VLAN 1.

Procedures

Configuring the AC

1. Configure the interfaces of the AC:

Create VLAN 100 and VLAN-interface 100, and assign the interface an IPv6 address. The AC will use this IPv6 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] ipv6 address 2001::1 64
[AC-Vlan-interface100] quit
```

Create VLAN 200 and VLAN 400. The AC uses the VLANs to forward client traffic.

```
[AC] vlan 200
[AC-vlan200] quit
[AC] vlan 400
[AC-vlan400] 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, 200, and 400.

```
[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 100 200 400
[AC-GigabitEthernet1/0/1] quit
```

2. Configure IPv6 static routes.

```
[AC] ipv6 route-static 3001::0 64 2001::2
[AC] ipv6 route-static 4001::0 64 2001::2
```

3. Configure wireless services:

Create service template 1 and enter its view.

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

Set the SSID to **service1**.

```
[AC-wlan-st-1] ssid service1
```

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

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

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

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

Configure the AC to forward client data traffic. If the default client data traffic forwarder is AC, skip this step.

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

Enable service template 1.

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

Enable snooping DHCPv6 and ND packets.

```
[AC-wlan-st-2] client ipv6-snooping dhcpv6-learning enable
[AC-wlan-st-2] client ipv6-snooping nd-learning enable
```

```
[AC-wlan-st-2] quit
# Create service template 2 and enter its view.
[AC] wlan service-template 2
# Set the SSID to service2.
[AC-wlan-st-2] ssid service2
# Specify PSK as the AKM mode and specify 12345678 as the plaintext key.
[AC-wlan-st-2] akm mode psk
[AC-wlan-st-2] preshared-key pass-phrase simple 12345678
# Specify CCMP as the cipher suite and specify RSN as the security IE.
[AC-wlan-st-2] cipher-suite ccmp
[AC-wlan-st-2] security-ie rsn
# Configure the AC to forward client data traffic. If the default client data traffic forwarder is AC,
skip this step.
[AC-wlan-st-2] client forwarding-location ac
# Enable service template 2.
[AC-wlan-st-2] service-template enable
# Enable snooping DHCPv6 and ND packets.
[AC-wlan-st-2] client ipv6-snooping dhcpv6-learning enable
[AC-wlan-st-2] client ipv6-snooping nd-learning enable
[AC-wlan-st-2] quit
```

4. Configure AP settings:

NOTE:

To simply AP configuration on a large-scale network, configure AP settings on a per AP group basis 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
# Create AP group group1 and configure officeap as the AP grouping rule.
[AC] wlan ap-group group1
[AC-wlan-ap-group-group1] ap officeap
# Bind service template 1 and VLAN 200 to radio 1 for AP group group1.
[AC-wlan-ap-group-group1] ap-model AP 3620
[AC-wlan-ap-group-group1-ap-model-AP 3620] radio 1
[AC-wlan-ap-group-group1-ap-model-AP 3620-radio-1] service-template 1 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] quit
# Bind service template 2 and VLAN 400 to radio 2 for 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 2 vlan 400
# 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

1. Configure switch interfaces:

Create VLAN 100, VLAN 300, VLAN-interface 100, and VLAN-interface 300, and assign IPv6 addresses to the VLAN interfaces. The switch will use VLAN 100 and VLAN 300 to forward packets between AC and AP.

```
<L3 switch> system-view
[L3 switch] vlan 100
[L3 switch-vlan100] quit
[L3 switch] interface vlan-interface 100
[L3 switch-Vlan-interface100] ipv6 address 2001::2/64
[L3 switch-Vlan-interface100] quit
[L3 switch] vlan 300
[L3 switch-vlan300] quit
[L3 switch] interface vlan-interface 300
[L3 switch-Vlan-interface300] ipv6 address 3001::1/64
[L3 switch-Vlan-interface300] quit
```

Create VLAN 200 and VLAN-interface 200 and assign an IPv6 address to the VLAN interface. Client 1 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] ipv6 address 3000::1/64
[L3 switch-Vlan-interface200] quit
```

Create VLAN 400 and VLAN-interface 400 and assign an IPv6 address to the VLAN interface. Client 2 will use this VLAN to access the WLAN.

```
[L3 switch] vlan 400
[L3 switch-vlan400] quit
[L3 switch] interface vlan-interface 400
[L3 switch-Vlan-interface400] ipv6 address 4000::1/64
[L3 switch-Vlan-interface400] 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, 200, and 400.

```
[L3 Switch] interface gigabitEthernet 1/0/1
[L3 Switch-GigabitEthernet1/0/1] port link-type trunk
[L3 switch-GigabitEthernet1/0/2] undo port trunk permit vlan 1
[L3 Switch-GigabitEthernet1/0/1] port trunk permit vlan 100 200 400
[L3 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, configure the PVID as VLAN 300, and assign the port to VLANs 300.

```
[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 300
[L3 switch-GigabitEthernet1/0/2] port trunk pvid vlan 300
[L3 switch-GigabitEthernet1/0/2] quit
```

2. Configure DHCPv6:

Enable the DHCPv6 server on VLAN-interface 200, VLAN-interface 300, and VLAN-interface 400, respectively.

Disable RA message suppression, set both the managed address configuration flag (M) and the other stateful configuration flag (O) to 1 in RA advertisements to be sent for the created VLAN interfaces.

Create DHCPv6 address pool 1 to assign an IPv6 address to Client 1, and specify subnet 3000::0/64 in the DHCP address pool.

Create DHCPv6 address pool 2 to assign an IPv6 address to the AP, specify subnet 3001::0/64 in the DHCP address pool, and configure Option 52 that specifies AC IPv6 address 2001:1 in the address pool.

```
# Create a prefix pool and specify the prefix and the assigned prefix length for the pool.
```

Create DHCPv6 address pool 3 to assign an IPv6 address to Client 2, and specify subnet 4001::0/64 in the DHCP address pool.

5

Apply prefix pool 1 to DHCPv6 address pool 3, so the DHCPv6 server can dynamically select a prefix from the prefix pool for a client.

```
[L3 switch-dhcp6-pool-3] prefix-pool 1
```

```
[L3 switch-dhcp6-pool-3] quit
```

Verifying the configuration

Verify that Client 1 and Client 2 have connected to the network successfully.

```
[AC] display wlan client ipv6
```

MAC address	AP name	IPv6 address	VLAN
0000-000f-1211	officeap	3000::2	200
0000-000f-1212	officeap	4001::3	400

Configuration files

- AC:

```
#
vlan 100
#
vlan 200
#
vlan 400
#
interface Vlan-interface100
  ipv6 address 2001::1/64
#
wlan service-template 1
  ssid service
  client forwarding-location ac
  client ipv6-snooping dhcpv6-learning enable
  client ipv6-snooping nd-learning enable
  akm mode psk
  preshared-key pass-phrase cipher $c$3$N//5BVbsOqdBTxi+7MJZKT6Zqh5MAmYs2ZzM
  cipher-suite ccmp
  security-ie rsn
  service-template enable
#
interface GigabitEthernet1/0/1
  port link-type trunk
  undo port trunk permit vlan 1
  port trunk permit vlan 100 200 400
#
ipv6 route-static 3001::0 64 2001::2
ipv6 route-static 4001::0 64 2001::2
#
wlan ap-group group1
  ap officeap
  ap-model AP 3620
```

- Layer 3 switch:

7

```

ipv6 dhcp select server
ipv6 address 3001::1/64
ipv6 nd autoconfig managed-address-flag
ipv6 nd autoconfig other-flag
undo ipv6 nd ra halt
#
interface Vlan-interface400
    ipv6 dhcp select server
    ipv6 address 4001::1/64
    ipv6 nd autoconfig managed-address-flag
    ipv6 nd autoconfig other-flag
    undo ipv6 nd ra halt
#
interface GigabitEthernet1/0/1
    port link-type trunk
    undo port trunk permit vlan 1
    port trunk permit vlan 100 200 400
#
interface GigabitEthernet1/0/2
    port link-type trunk
    undo port trunk permit vlan 1
    port trunk permit vlan 300
    port trunk pvid vlan 300
#

```

Related documentation

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

INTELBRAS Access Controllers

Policy-Based Forwarding with Dual Gateways

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 policy-based forwarding with dual gateways	1
Network configuration	1
Analysis	2
Restrictions and guidelines	2
Procedures	2
Configuring Router A	2
Configuring Router B	3
Configuring the AC	3
Verifying the configuration	6
Configuration files	11
Related documentation	13

Introduction

The following information provides a configuration example for configuring policy-based forwarding with dual gateways.

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

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

Example: Configuring policy-based forwarding with dual gateways

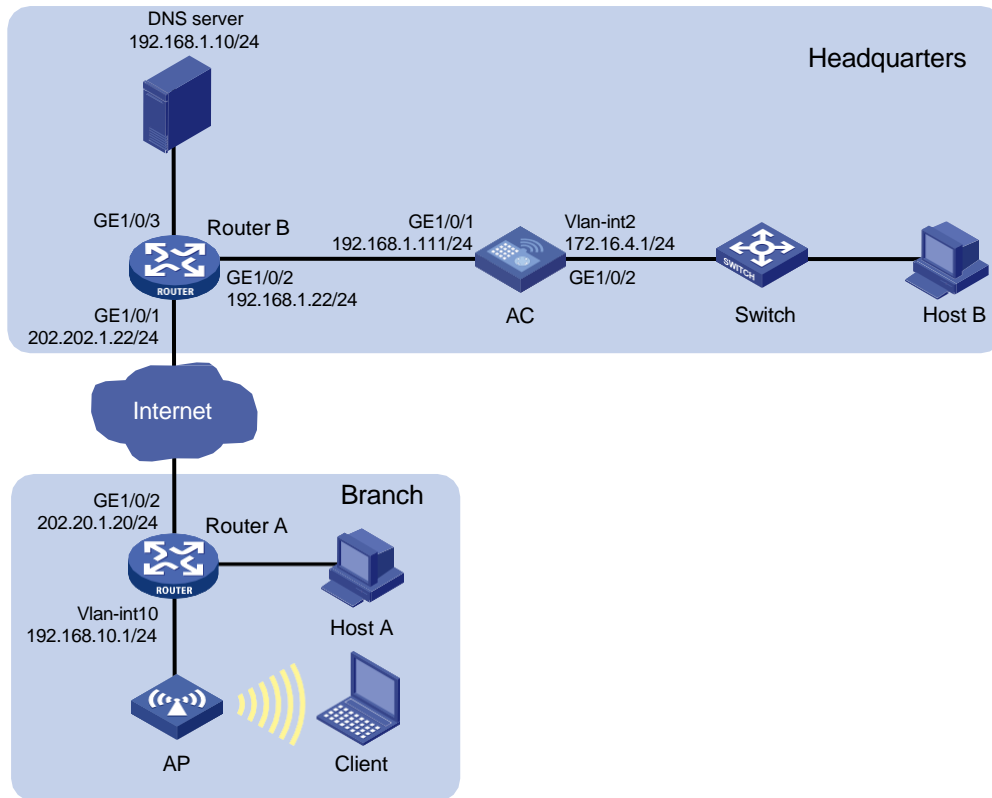
Network configuration

As shown in [Figure 1](#), the AC is deployed at the headquarters and an AP is deployed at the branch. Router A and Router B act as the gateways for the branch and the headquarters, respectively. The AP associates with the AC across the Internet.

Configure network settings to meet the following requirements:

- Packets destined to the headquarters are forwarded by the AC and packets destined to the branch or Internet are forwarded by the AP.
- The AP obtains IP addresses from Router A and the client obtains IP addresses from the AC.

Figure 1 Network diagram



Analysis

- For the AP to discover the AC through the Internet, configure Option 43 and manually specify the IP address of the AC on Router A.
- For the AP to communicate with the AC, configure NAT on both Router A and Router B.
- To simplify configurations when a large number of APs are deployed at branches, enable auto AP and auto AP conversion on the AC.
- For both the AP and the AC to forward packets, configure policy-based forwarding on the AC.
- For the AP to obtain configurations automatically from the AC, use a text editor to create an AP configuration file and upload the file to the AC.

Restrictions and guidelines

Make sure devices in the network can reach each other.

Procedures

Configuring Router A

1. Configure DHCP:
Enable DHCP.
<RouterA> system-view

```
[RouterA] dhcp enable
```

Create DHCP address pool **ap**, specify the subnet for dynamic allocation as **192.168.10.0/24**, specify the gateway address as **192.168.10.1**.

```
[RouterA] dhcp server ip-pool ap
```

```
[RouterA-dhcp-pool-ap] network 192.168.10.0 mask 255.255.255.0
```

```
[RouterA-dhcp-pool-ap] gateway-list 192.168.10.1
```

Configure Option 43 that specifies the Router B's IP address **202.202.1.22/24**.

```
[RouterA-dhcp-pool-ap] option 43 hex 8007000001CACA0116
```

```
[RouterA-dhcp-pool-ap] quit
```

2. Configure NAT:

Create NAT address group **0**, and add address **202.20.1.20** to the group.

```
[RouterA] nat address-group 0
```

```
[RouterA-address-group-0] address 202.20.1.20 202.20.1.20
```

```
[RouterA-address-group-0] quit
```

Create IPv4 basic ACL 2000 to permit only packets from source IP subnet 192.168.10.0/24.

```
[RouterA] acl basic 2000
```

```
[RouterA-acl-ipv4-basic-2000] rule permit source 192.168.10.0 0.0.0.255
```

```
[RouterA-acl-ipv4-basic-2000] quit
```

Configure interface GigabitEthernet1/0/2 to translate the source addresses of outgoing packets permitted by ACL 2000 into the addresses in address group **0**.

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

```
[RouterA-GigabitEthernet1/0/2] nat outbound 2000 address-group 0
```

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

```
[RouterA] quit
```

Configuring Router B

1. Configure NAT:

Create IPv4 ACL 3000 to permit only packets from 202.20.1.0/24 to 202.202.1.22.

```
<RouterB> system-view
```

```
[RouterB] acl advanced 3000
```

```
[RouterB-acl-ipv4-adv-3000] rule 0 permit ip source 202.20.1.0 0.0.0.255 destination 202.202.1.22 0
```

```
[RouterB-acl-ipv4-adv-3000] quit
```

Configure interface GigabitEthernet1/0/1 to allow users permitted by ACL 3000 to access the internal server at 192.168.1.111.

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

```
[RouterB-GigabitEthernet1/0/1] nat server global 3000 inside 192.168.1.111
```

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

```
[RouterB] quit
```

Configuring the AC

1. Create AP configuration file **map-OnAP.txt** as follows and then upload the file to the AC.

```
vlan 2
```

```
interface Vlan-interface1
```

```
    nat outbound 3000
```

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



```

port link-type trunk
port trunk permit vlan 1
interface Vlan-interface2
ip address 172.16.4.3 255.255.255.0
acl advanced 3000
rule 0 permit ip source 172.16.4.0 0.0.0.255

```

2. Configure basic AC functions:

Configure interface IP addresses. (Details not shown.)

Create VLAN 2 and VLAN-interface 2, and assign an IP address to the VLAN interface.

```

<AC> system-view
[AC] vlan 2
[AC-vlan2] quit
[AC] interface vlan-interface 2
[AC-Vlan-interface2] ip address 172.16.4.1 255.255.255.0
[AC-Vlan-interface2] quit

```

Configure interface GigabitEthernet1/0/2 to operate in Layer 2 mode, set the port link type to **trunk**, remove the port from VLAN 1, and add the port to VLAN 2.

```

[AC] interface gigabitethernet 1/0/2
[AC-GigabitEthernet1/0/2] port link-mode bridge
[AC-GigabitEthernet1/0/2] port link-type trunk
[AC-GigabitEthernet1/0/2] undo port trunk permit vlan 1
[AC-GigabitEthernet1/0/2] port trunk permit vlan 2
[AC-GigabitEthernet1/0/2] quit

```

Configure static routes to GigabitEthernet1/0/2 of Router A, GigabitEthernet1/0/1 of Router B, and headquarters' network segment 172.16.5.0/24.

```

[AC] ip route-static 202.20.1.0 24 192.168.1.22
[AC] ip route-static 202.202.1.0 24 192.168.1.22
[AC] ip route-static 172.16.5.0 24 172.16.4.2

```

3. Configure DHCP:

Enable DHCP.

```
[AC] dhcp enable
```

Create DHCP address pool **sta**, specify the subnet for dynamic allocation as **172.16.4.0/24**, and specify the gateway address as **172.16.4.1**.

```

[AC] dhcp server ip-pool sta
[AC-dhcp-pool-sta] network 172.16.4.0 mask 255.255.255.0
[AC-dhcp-pool-sta] gateway-list 172.16.4.1

```

Specify the DNS server address as **192.168.1.10**.

```
[AC-dhcp-pool-sta] dns-list 192.168.1.10
```

Exclude IP addresses **172.16.4.1** and **172.16.4.3** from dynamic allocation in DHCP address pool **sta**.

```

[AC-dhcp-pool-sta] forbidden-ip 172.16.4.1 172.16.4.3
[AC-dhcp-pool-sta] quit

```

4. Enable auto AP and auto AP conversion.

```

[AC] wlan auto-ap enable
[AC] wlan auto-persistent enable

```

5. Configure policy-based forwarding:

Create IPv4 advanced ACL 3001, and configure ACL rules to permit DNS, BOOTPC, and BOOTPS packets and packets from 172.16.4.0/24 to 172.16.4.0/24 or 172.16.5.0/24.

```
[AC] acl advanced 3001
[AC-acl-ipv4-adv-3001] rule 0 permit udp source-port eq dns
[AC-acl-ipv4-adv-3001] rule 1 permit udp destination-port eq dns
[AC-acl-ipv4-adv-3001] rule 2 permit udp source-port eq bootpc
[AC-acl-ipv4-adv-3001] rule 3 permit udp destination-port eq bootps
[AC-acl-ipv4-adv-3001] rule 4 permit ip source 172.16.4.0 0.0.0.255 destination
172.16.4.0 0.0.0.255
[AC-acl-ipv4-adv-3001] rule 5 permit ip source 172.16.4.0 0.0.0.255 destination
172.16.5.0 0.0.0.255
[AC-acl-ipv4-adv-3001] quit
```

Create forwarding policy *remote*, and configure the forwarding policy to perform centralized forwarding on packets that match ACL 3001.

```
[AC] wlan forwarding-policy remote
[AC-wlan-fp-remote] classifier acl 3001 behavior remote
[AC-wlan-fp-remote] quit
```

Create service template *chn*, set the SSID to **CHN, and assign clients coming online through the service template to VLAN 2.**

```
[AC] wlan service-template chn
[AC-wlan-st-chn] ssid CHN
[AC-wlan-st-chn] vlan 2
```

Enable APs to forward client traffic, apply forwarding policy *remote* to the service template, and enable the forwarding policy.

```
[AC-wlan-st-chn] client forwarding-location ap
[AC-wlan-st-chn] client forwarding-policy-name remote
[AC-wlan-st-chn] client forwarding-policy enable
```

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

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

Set the CCMP cipher suite and enable RSN security IE.

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

Enable the service template.

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

Deploy configuration file **map-OnAP.txt to AP 3620 APs in the default AP group.**

```
[AC] wlan ap-group default-group
[AC-wlan-ap-group-default-group] ap-model AP 3620
[AC-wlan-ap-group-default-group-ap-model-AP 3620] map-
configuration flash:/map-OnAP.txt
```

Bind service template *chn* to radio 1 and enable radio 1.

```
[AC-wlan-ap-group-default-group-ap-model-AP 3620] radio 1
[AC-wlan-ap-group-default-group-ap-model-AP 3620-radio-1] service-template
chn [AC-wlan-ap-group-default-group-ap-model-AP 3620-radio-1] radio enable
[AC-wlan-ap-group-default-group-ap-model-AP 3620-radio-1]
quit [AC-wlan-ap-group-default-group-ap-model-AP 3620] quit
[AC-wlan-ap-group-default-group] quit
```

Verifying the configuration

Verify that the AP has associated with the AC.

```
[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: 2048
Remaining APs: 2047
Total AP licenses: 32
Local AP licenses: 32
Server AP licenses: 0
Remaining local AP licenses: 31
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
0015-005e-9348	2	R/M	AP 3620	219801A28N819CE0002T

Verify that the AP is in Run state, the discovery type is DHCP, and the AP's IP address is 202.20.1.20.

```
[AC] display wlan ap name 0015-005e-9348 verbose
AP name : 0015-005e-9348
AP ID : 2
AP group name : default-group
State : Run
Backup type : Master
Online time : 1 days 5 hours 25 minutes 22 seconds
System up time : 1 days 6 hours 30 minutes 4 seconds
Model : AP 3620
Region code : CN
Region code lock : Disabled
Serial ID : 219801A28N819CE0002T
MAC address : 70f9-6dd3-61e0
IP address : 202.20.1.20
UDP control port number : 1099
UDP data port number : 1102
H/W version : Ver.C
S/W version : R2215
Boot version : 7.10
USB state : N/A
Power Level : N/A
```

PowerInfo : N/A
Description : Not configured
Priority : 4
Echo interval : 10 seconds
Echo count : 3 counts
Keepalive interval : 10 seconds
Statistics report interval : 50 seconds
Fragment size (data) : 1500
Fragment size (control) : 1450
MAC type : Local MAC & Split MAC
Tunnel mode : Local Bridging & 802.3 Frame & Native Frame
Discovery type : DHCP
Retransmission count : 3
Retransmission interval : 5 seconds
Firmware upgrade : Enabled
Sent control packets : 34001
Received control packets : 34001
Echo requests : 10591
Lost echo responses : 3
Average echo delay : 3
Last reboot reason : User soft reboot
Latest IP address : 202.20.1.20
Tunnel down reason : Processed join request in Run state
Connection count : 15
Backup Ipv4 : Not configured
Backup Ipv6 : Not configured
Tunnel encryption : Disabled
LED mode : Normal
Remote configuration : Disabled
Radio 1:
 Basic BSSID : 70f9-6dd3-61e0
 Admin state : Up
 Radio type : 802.11ac
 Antenna type : internal
 Client dot11ac-only : Disabled
 Client dot11n-only : Disabled
 Channel band-width : 20/40/80MHz
 Active band-width : 20/40/80MHz
 Secondary channel offset : SCA
 Short GI for 20MHz : Supported
 Short GI for 40MHz : Supported
 Short GI for 80MHz : Supported
 Short GI for 160MHz : Not supported
 A-MSDU : Enabled
 A-MPDU : Enabled
 LDPC : Not Supported
 STBC : Supported
 Operational VHT-MCS Set:

```

Mandatory : Not configured
Supported : NSS1 0,1,2,3,4,5,6,7,8,9
              NSS2 0,1,2,3,4,5,6,7,8,9
Multicast : Not configured
Operational HT MCS Set:
Mandatory : Not configured
Supported : 0, 1, 2, 3, 4, 5, 6, 7, 8, 9,
              10, 11, 12, 13, 14, 15
Multicast : Not configured
Channel : 149(auto)
Channel usage(%) : 0
Max power : 20 dBm
Operational rate:
Mandatory : 6, 12, 24 Mbps
Multicast : Auto
Supported : 9, 18, 36, 48, 54 Mbps
Disabled : Not configured
Distance : 1 km
ANI : Enabled
Fragmentation threshold : 2346 bytes
Beacon interval : 100 TU
Protection threshold : 2346 bytes
Long retry threshold : 4
Short retry threshold : 7
Maximum rx duration : 2000 ms
Noise floor : -105 dBm
Smart antenna : Enabled
Smart antenna policy : Auto
Protection mode : cts-to-self
Continuous mode : N/A
HT protection mode : No protection
Radio 2:
Basic BSSID : 70f9-6dd3-61f0
Admin state : Down
Radio type : 802.11n(2.4GHz)
Antenna type : internal
Client dot11n-only : Disabled
Channel band-width : 20MHz
Active band-width : 20MHz
Secondary channel offset : SCN
Short GI for 20MHz : Supported
Short GI for 40MHz : Supported
A-MSDU : Enabled
A-MPDU : Enabled
LDPC : Not Supported
STBC : Supported
Operational HT MCS Set:
Mandatory : Not configured

```

```

Supported : 0, 1, 2, 3, 4, 5, 6, 7, 8, 9,
            10, 11, 12, 13, 14, 15
Multicast : Not configured
Channel : 6(auto)
Channel usage(%) : 0
Max power : 20 dBm
Preamble type : Short
Operational rate:
    Mandatory : 1, 2, 5.5, 11 Mbps
    Multicast : Auto
    Supported : 6, 9, 12, 18, 24, 36, 48, 54 Mbps
    Disabled : Not configured
Distance : 1 km
ANI : Enabled
Fragmentation threshold : 2346 bytes
Beacon interval : 100 TU
Protection threshold : 2346 bytes
Long retry threshold : 4
Short retry threshold : 7
Maximum rx duration : 2000 ms
Noise floor : 0 dBm
Smart antenna : Enabled
Smart antenna policy : Auto
Protection mode : cts-to-self
Continuous mode : N/A
HT protection mode : No protection

```

Verify that the client has come online with an IP address in subnet 172.16.4.0/24, and the forwarding policy is remote.

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

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

MAC address	User name	AP name	RID	IP address	VLAN
0015-005e-9348	N/A	0015-005e-9348	1	172.16.4.11	2

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

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

```
MAC address : 0015-005e-9348
```

```
IPv4 address : 172.16.4.11
```

```
IPv6 address : N/A
```

```
Username : N/A
```

```
AID : 1
```

```
AP ID : 2
```

```
AP name : 0015-005e-9348
```

```
Radio ID : 1
```

```
SSID : CHN
```

```
BSSID : 70f9-6dd3-61e0
```

```
VLAN ID : 2
```

```
Sleep count : 0
```

```

Wireless mode : 802.11an
Channel bandwidth : 40MHz
20/40 BSS Coexistence Management : Not supported
SM power save : Disabled
Short GI for 20MHz : Supported
Short GI for 40MHz : Supported
STBC RX capability : Supported
STBC TX capability : Not supported
LDPC RX capability : Not supported
Block Ack : N/A
Supported HT MCS set : 0, 1, 2, 3, 4, 5, 6, 7,
                        8, 9, 10, 11, 12, 13, 14,
                        15
Supported rates : 6, 9, 12, 18, 24, 36,
                  48, 54 Mbps

QoS mode : WMM
Listen interval : 100
RSSI : 0
Rx/Tx rate : 0/0
Authentication method : Open system
Security mode : PRE-RSNA
AKM mode : N/A
Cipher suite : N/A
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 : remote
Online time : 0days 0hours 0minutes 33seconds
FT status : Inactive

```

Verify that IP addresses (172.16.4.2, 172.16.5.1, and 172.16.5.2) in the headquarters' network can be pinged successfully.

```
C:\Users\intelbras>ping 172.16.4.2
```

```

Pinging 172.16.4.2 with 32 bytes of data:
Reply from 172.16.4.2: bytes=32 time=6ms TTL=255
Reply from 172.16.4.2: bytes=32 time=3ms TTL=255
Reply from 172.16.4.2: bytes=32 time=6ms TTL=255
Reply from 172.16.4.2: bytes=32 time=1ms TTL=255

```

```

Ping statistics for 172.16.4.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 6ms, Average = 4ms

```

```
C:\Users\intelbras>ping 172.16.5.1
```

```

Pinging 172.16.5.1 with 32 bytes of data:
Reply from 172.16.5.1: bytes=32 time=9ms TTL=255
Reply from 172.16.5.1: bytes=32 time=1ms TTL=255
Reply from 172.16.5.1: bytes=32 time=5ms TTL=255
Reply from 172.16.5.1: bytes=32 time=1ms TTL=255

Ping statistics for 172.16.5.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 9ms, Average = 4ms

```

```
C:\Users\intelbras>ping 172.16.5.2
```

```

Pinging 172.16.5.2 with 32 bytes of data:
Reply from 172.16.5.2: bytes=32 time=8ms TTL=255
Reply from 172.16.5.2: bytes=32 time=2ms TTL=255
Reply from 172.16.5.2: bytes=32 time=5ms TTL=255
Reply from 172.16.5.2: bytes=32 time=3ms TTL=255

```

```

Ping statistics for 172.16.5.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 8ms, Average = 4ms

```

Verify that a website on the Internet (for example, www.baidu.com) can be pinged successfully.

```
C:\Users\intelbras>ping www.baidu.com
```

```

Pinging www.baidu.com [202.202.1.188] with 32 bytes of data:
Reply from 202.202.1.188: bytes=32 time=7ms TTL=255
Reply from 202.202.1.188: bytes=32 time=3ms TTL=255
Reply from 202.202.1.188: bytes=32 time=3ms TTL=255
Reply from 202.202.1.188: bytes=32 time=2ms TTL=255

```

```

Ping statistics for 202.202.1.188:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 7ms, Average = 3ms

```

Configuration files

- Router A:


```

#
nat address-group 0
    address 202.20.1.20 202.20.1.20
#
    dhcp enable
#
    dhcp server ip-pool ap

```



```

gateway-list 192.168.10.1
network 192.168.10.0 mask 255.255.255.0
option 43 hex 8007000001caca0116
#
interface GigabitEthernet1/0/2
  nat outbound 2000 address-group 0
#
acl basic 2000
  rule 0 permit source 192.168.10.0 0.0.0.255
#

```

- **Router B:**

```

#
interface GigabitEthernet1/0/1
  nat server global 3000 inside 192.168.1.111
#
acl advanced 3000
  rule 0 permit ip source 202.20.1.0 0.0.0.255 destination 202.202.1.22 0
#

```

- **AC:**

```

#
  dhcp enable
#
vlan 2
#
dhcp server ip-pool sta
  gateway-list 172.16.4.1
  network 172.16.4.0 mask 255.255.255.0
  dns-list 192.168.1.10
  forbidden-ip 172.16.4.1
  forbidden-ip 172.16.4.3
#
wlan forwarding-policy remote
  classifier acl 3001 behavior remote
#
wlan service-template chn
  ssid CHN
  vlan 2
  client forwarding-location ap
  client forwarding-policy-name remote
  client forwarding-policy enable
  akm mode psk
  preshared-key pass-phrase cipher $c$3$4T2hQpGTY8qC3U4KL3G2sMgv9RNfRZdZfDqY
  cipher-suite ccmp
  security-ie rsn
  service-template enable
#
interface Vlan-interface2
  ip address 172.16.4.1 255.255.255.0

```

```

#
interface GigabitEthernet1/0/2
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 2
#
 ip route-static 172.16.5.0 24 172.16.4.2
 ip route-static 202.20.1.0 24 192.168.1.22
 ip route-static 202.202.1.0 24 192.168.1.22
#
acl advanced 3001
 rule 0 permit udp source-port eq dns
 rule 1 permit udp destination-port eq dns
 rule 2 permit udp source-port eq bootpc
 rule 3 permit udp destination-port eq bootps
 rule 4 permit ip source 172.16.4.0 0.0.0.255 destination 172.16.4.0 0.0.0.255
 rule 5 permit ip source 172.16.4.0 0.0.0.255 destination 172.16.5.0 0.0.0.255
#
 wlan auto-ap enable
 wlan auto-persistent enable
#
 wlan ap-group default-group
 ap-model AP 3620
  radio 1
   radio enable
   service-template chn
  radio 2
   gigabitethernet 1
   gigabitethernet 2
#

```

Related documentation

- *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

Scheduled Configuration Deployment by AP Group

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 scheduled configuration deployment by AP group.....	1
Network configuration.....	1
Analysis	1
Restrictions and guidelines	2
Procedures	2
Configuring the AC.....	2
Configuring the Layer 2 switch.....	4
Verifying the configuration	5
Configuration files.....	8
Related documentation	10

Introduction

The following information provides an example for configuring scheduled configuration deployment by AP group.

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.

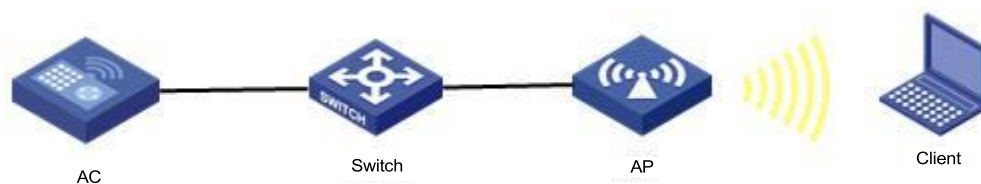
Example: Configuring scheduled configuration deployment by AP group

Network configuration

As shown in [Figure 1](#), the AP connects to the AC through a Layer 2 switch and the Layer 2 switch supplies power to the AP through PoE. The AC acts as a DHCP server to assign IP addresses to the AP and the client.

Configure a schedule to enable radio 1 on the AP at 8:00 and disable the radio at 20:00 every day.

Figure 1 Network diagram



Analysis

For the AC to act as a DHCP server, enable the DHCP server feature on the AC.

For the Layer 2 switch to supply power to the AP, enable the PoE feature on the switch.

Restrictions and guidelines

When you configure scheduled configuration deployment by AP group, follow these restrictions and guidelines:

- Use the actual serial ID of an AP to uniquely identify that AP.
- To prevent packets from accumulating in VLAN 1, configure the switch's interface that connects the switch to the AP to deny packets from VLAN 1.

Procedures

Configuring the AC

1. Configure the DHCP server:

Enable DHCP server.

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

```
[AC] dhcp enable
```

Create DHCP address pool 1, specify subnet 192.168.201.0/24 in the address pool, and specify the gateway address as 192.168.201.1.

```
[AC] dhcp server ip-pool 1
```

```
[AC-dhcp-pool-1] network 192.168.201.0 mask 255.255.255.0
```

```
[AC-dhcp-pool-1] gateway-list 192.168.201.1
```

```
[AC-dhcp-pool-1] quit
```

Create DHCP address pool 2 and specify subnet 192.168.202.0/24 in the address pool. Specify the gateway address as 192.168.202.1, and specify the address of the DNS server. In this example, the gateway also acts as the DNS server.

```
[AC] dhcp server ip-pool 2
```

```
[AC-dhcp-pool-2] network 192.168.202.0 mask 255.255.255.0
```

```
[AC-dhcp-pool-2] gateway-list 192.168.202.1
```

```
[AC-dhcp-pool-2] dns-list 192.168.202.1
```

```
[AC-dhcp-pool-2] quit
```

2. Configure AC interfaces:

Create VLAN 100 and VLAN-interface 100, and assign IP address 192.168.201.1 to the interface. The AC will use this IP address to establish CAPWAP tunnels with the AP.

```
[AC] vlan 100
```

```
[AC-vlan100] quit
```

```
[AC] interface vlan-interface 100
```

```
[AC-Vlan-interface100] ip address 192.168.201.1 255.255.255.0
```

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

Create VLAN 200 and VLAN-interface 200, and assign IP address 192.168.202.1 to the interface. Clients will use this VLAN to access the WLAN.

```
[AC] vlan 200
```

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

```
[AC] interface vlan-interface 200
```

```
[AC-Vlan-interface200] ip address 192.168.202.1 24
```

```
[AC-Vlan-interface200] quit
```

Set the link type of GigabitEthernet 1/0/1 that connects the AC to the switch to trunk. 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
```

Create job `radio_disable` to disable radio 1 of AP 3620 APs in AP group `group1`.

```
[AC] scheduler job radio_disable
[AC-job-radio_disable] command 1 system-view
[AC-job-radio_disable] command 2 wlan ap-group group1
[AC-job-radio_disable] command 3 ap-model AP 3620
[AC-job-radio_disable] command 4 radio 1
[AC-job-radio_disable] command 5 radio disable
[AC-job-radio_disable] quit
```

Create schedule `stop_radio`, assign job `radio_disable` to the schedule, and configure the AC to execute the schedule at 20:00 every day.

```
[AC] scheduler schedule stop_radio
[AC-schedule-stop_radio] job radio_disable
[AC-schedule-stop_radio] time repeating at 20:00
[AC-schedule-stop_radio] quit
```

Create job `radio_enable` to enable radio 1 of AP 3620 APs in AP group `group1`.

```
[AC] scheduler job radio_enable
[AC-job-radio_enable] command 1 system-view
[AC-job-radio_enable] command 2 wlan ap-group group1
[AC-job-radio_enable] command 3 ap-model AP 3620
[AC-job-radio_enable] command 4 radio 1
[AC-job-radio_enable] command 5 radio enable
[AC-job-radio_enable] quit
```

Create schedule `start_radio`, assign job `radio_enable` to the schedule, and configure the AC to execute the schedule at 8:00 every day.

```
[AC] scheduler schedule start_radio
[AC-schedule-start_radio] job radio_enable
[AC-schedule-start_radio] time repeating at 8:00
[AC-schedule-start_radio] quit
```

3. Configure wireless services:

Create service template 1.

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

Set the SSID to `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
```

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
```

4. Configure AP settings:

NOTE:

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

Create 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
```

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 2 switch

Create VLAN 100 and VLAN 200. The switch will use VLAN 100 to forward CAPWAP tunnel traffic and use VLAN 200 for client access.

```
<L2 switch> system-view
[L2 switch] vlan 100
[L2 switch-vlan100] quit
[L2 switch] vlan 200
[L2 switch-vlan200] quit
```

Set the link type of GigabitEthernet 1/0/1 that connects the switch to the AC to trunk and assign the port to VLANs 100 and 200.

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

Set the link type of GigabitEthernet 1/0/2 that connects the switch to the AP to trunk. Remove the port from VLAN 1, assign the port to VLAN 100, and enable PoE.

```
[L2 switch] interface gigabitEthernet 1/0/2
[L2 switch-GigabitEthernet1/0/2] port link-type trunk
[L2 switch-GigabitEthernet1/0/2] undo port trunk permit vlan 1
[L2 switch-GigabitEthernet1/0/2] port trunk permit vlan 100
[L2 switch-GigabitEthernet1/0/2] port trunk pvid vlan 100
[L2 switch-GigabitEthernet1/0/2] poe enable
[L2 switch-GigabitEthernet1/0/2] quit
```


Verifying the configuration

Use the **display wlan ap name officeap verbose** command to view the admin state of radio 1 on the AP. Verify that the state is UP from 8:00 to 20:00 and is DOWN at any other time.

```
<Sysname> display wlan ap name officeap verbose
```

```
AP name                : officeap
AP ID                  : 1
AP group name          : group1
State                  : Run
Backup type            : Master
Online time            : 0 days 1 hours 25 minutes 12 seconds
System uptime          : 0 days 2 hours 22 minutes 12 seconds
Model                  : AP 3620
Region code            : CN
Region code lock       : Disable
Serial ID              : 219801A28N819CE0002T
MAC address            : 0AFB-423B-893C
IP address              : 192.168.1.50
UDP control port number : 18313
UDP data port number   : N/A
H/W version            : Ver.C
S/W version            : E2321
Boot version           : 1.01
USB state              : N/A
Power level            : N/A
Power info             : N/A
Description            : wtp1
Priority                : 4
Echo interval          : 10 seconds
Echo count             : 3 counts
Keepalive interval     : 10 seconds
Discovery-response wait-time : 2 seconds
Statistics report interval : 50 seconds
Fragment size (data)   : 1500
Fragment size (control) : 1450
MAC type               : Local MAC & Split MAC
Tunnel mode            : Local Bridging & 802.3 Frame & Native Frame
CWPCAP data-tunnel status : Down
Discovery type         : Static Configuration
Retransmission count   : 3
Retransmission interval : 5 seconds
Firmware upgrade       : Enabled
Sent control packets   : 1
Received control packets : 1
Echo requests          : 147
Lost echo responses    : 0
Average echo delay     : 3
Last reboot reason     : User soft reboot
```

```

Last reboot reason (AP check) : The radio physical status was down
Last reboot reason (AC check) : The radio physical status was down
Latest IP address              : 10.1.0.2
Current AC IP                  : 192.168.1.1
Tunnel down reason             : Request wait timer expired
Connection count               : 1
Backup IPv4                    : Not configured
Backup IPv6                    : Not configured
Ctrl-tunnel encryption         : Disabled
Ctrl-tunnel encryption state   : Not encrypted
Data-tunnel encryption         : Disabled
Data-tunnel encryption state   : Not encrypted
LED mode                       : Normal
Remote configuration           : Enabled
Radio 1:
    Basic BSSID                 : 7848-59f6-3940
    Admin state                 : Up
    Radio type                  : 802.11ac
    Antenna type                : internal
    Client dot11ac-only        : Disabled
    Client dot11n-only         : Disabled
    Channel band-width          : 20/40/80MHz
    Active band-width           : 20/40/80MHz
    Secondary channel offset    : SCB
    Short GI for 20MHz          : Supported
    Short GI for 40MHz          : Supported
    Short GI for 80MHz          : Supported
    Short GI for 160MHz         : Not supported
    mimo                        : Not Config
    Green-Energy-Management     : Disabled
    A-MSDU                     : Enabled
    A-MPDU                     : Enabled
    LDPC                       : Not Supported
    STBC                       : Supported
    Operational VHT-MCS Set:
        Mandatory               : Not configured
        Supported               : NSS1 0,1,2,3,4,5,6,7,8,9
                                NSS2 0,1,2,3,4,5,6,7,8,9
        Multicast               : Not configured
    Operational HT MCS Set:
        Mandatory               : Not configured
        Supported               : 0, 1, 2, 3, 4, 5, 6, 7, 8, 9,
                                10, 11, 12, 13, 14, 15
        Multicast               : Not configured
    Channel                     : 44(auto)
    Channel usage(%)            : 15
    Max power                   : -102 dBm
    Operational rate:

```

Mandatory	: 6, 12, 24 Mbps
Multicast	: Auto
Supported	: 9, 18, 36, 48, 54 Mbps
Disabled	: Not configured
Distance	: 1 km
ANI	: Enabled
Fragmentation threshold	: 2346 bytes
Beacon interval	: 100 TU
Protection threshold	: 2346 bytes
Long retry threshold	: 4
Short retry threshold	: 7
Maximum rx duration	: 2000 ms
Noise Floor	: 5 dBm
Smart antenna	: Enabled
Smart antenna policy	: Auto
Protection mode	: rts-cts
Continuous mode	: N/A
HT protection mode	: No protection
Radio 2:	
Basic BSSID	: 7848-59f6-3950
Admin state	: Down
Radio type	: 802.11b
Antenna type	: internal
Client dot11n-only	: Disabled
Channel band-width	: 20MHz
Active band-width	: 20MHz
Secondary channel offset	: SCN
Short GI for 20MHz	: Supported
Short GI for 40MHz	: Supported
A-MSDU	: Enabled
A-MPDU	: Enabled
LDPC	: Not Supported
STBC	: Supported
Operational HT MCS Set:	
Mandatory	: Not configured
Supported	: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15
Multicast	: Not configured
Channel	: 5(auto)
Channel usage(%)	: 0
Max power	: 20 dBm
Preamble type	: Short
Operational rate:	
Mandatory	: 1, 2, 5.5, 11 Mbps
Multicast	: Auto
Supported	: 6, 9, 12, 18, 24, 36, 48, 54 Mbps
Disabled	: Not configured
Distance	: 1 km

ANI	: Enabled
Fragmentation threshold	: 2346 bytes
Beacon interval	: 100 TU
Protection threshold	: 2346 bytes
Long retry threshold	: 4
Short retry threshold	: 7
Maximum rx duration	: 2000 ms
Noise Floor	: 0 dBm
Smart antenna	: Enabled
Smart antenna policy	: Auto
Protection mode	: rts-cts
Continuous mode	: N/A
HT protection mode	: No protection

Configuration files

- AC:

```
#
dhcp enable
#
vlan 1
#
vlan 100
#
vlan 200
#
dhcp server ip-pool 1
gateway-list 192.168.201.1
network 192.168.201.0 mask 255.255.255.0
#
dhcp server ip-pool 2
gateway-list 192.168.202.1
network 192.168.202.0 mask 255.255.255.0
dns-list 192.168.202.1
#
wlan service-template 1
ssid service
client forwarding-location ac
akm mode psk
preshared-key pass-phrase cipher $c$3$YK66aAPo8bx6QnCsN0hjad6l1SzB6n4H3UZ4
cipher-suite ccmp
security-ie rsn
service-template enable
#
interface Vlan-interface1
#
interface Vlan-interface100
ip address 192.168.201.1 255.255.255.0
```

```

#
interface Vlan-interface200
 ip address 192.168.202.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100 200
#
wlan ap-group group1
 vlan 1
 ap officeap
 ap-model AP
 3620 radio 1
 radio enable
 service-template 1 vlan 200
 radio 2
 gigabitethernet 1
#
wlan ap officeap model AP 3620
 serial-id 219801A28N819CE0002T
vlan 1
 radio 1
 radio 2
 gigabitethernet 1
#
scheduler job radio_disable
 command 1 system-view
 command 2 wlan ap-group group1
 command 3 ap-model AP 3620
 command 4 radio 1
 command 5 radio disable
#
scheduler job radio_enable
 command 1 system-view
 command 2 wlan ap-group group1
 command 3 ap-model AP 3620
 command 4 radio 1
 command 5 radio enable
#
scheduler schedule start_radio
 user-role network-admin
 job radio_enable
 time repeating at 08:00
#
scheduler schedule stop_radio
 user-role network-admin
 job radio_disable

```

- ```
time repeating at 20:00
#
```
- **Layer 2 switch:**

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

- *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

## Inter-AC Roaming with Static Client VLAN Allocation

### 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 inter-AC roaming with static client VLAN allocation ..... | 1  |
| Network configuration .....                                                    | 1  |
| Restrictions and guidelines .....                                              | 2  |
| Procedures .....                                                               | 2  |
| Configuring AC 1 .....                                                         | 2  |
| Configuring AC 2 .....                                                         | 4  |
| Configuring the switch .....                                                   | 6  |
| Verifying the configuration .....                                              | 7  |
| Configuration files .....                                                      | 8  |
| Related documentation .....                                                    | 11 |



# Introduction

The following information provides an example for configuring inter-AC roaming with client VLAN unchanged.

## Prerequisites

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

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

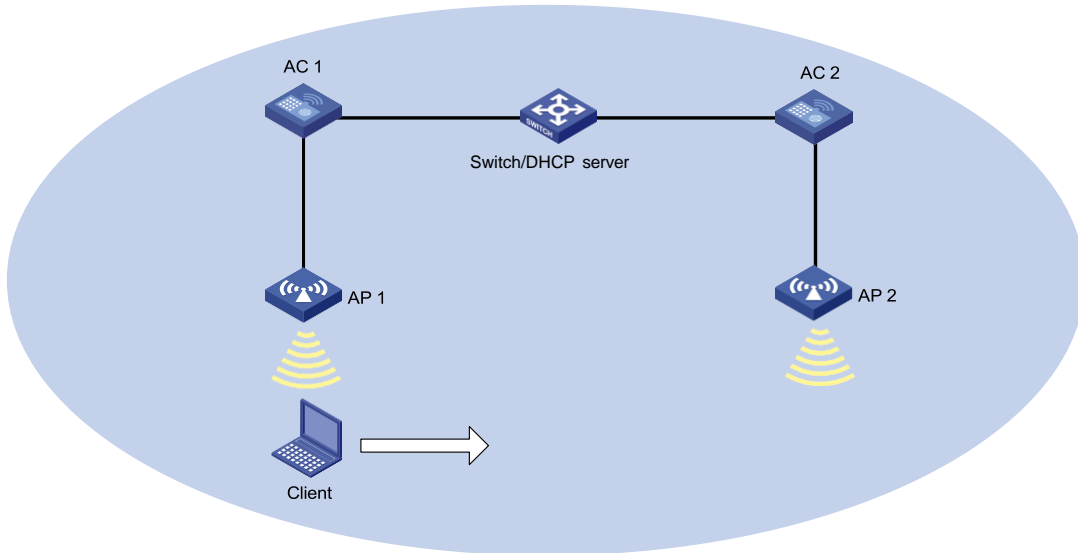
The following information is provided based on the assumption that you have basic knowledge of WLAN access and WLAN roaming.

## Example: Configuring inter-AC roaming with static client VLAN allocation

### Network configuration

As shown in [Figure 1](#), deploy two ACs connected through a switch to provide wireless services. The switch acts as a DHCP server to assign IP addresses to APs and clients. Specify the same VLAN group for each AP to enable clients to roam between the two ACs without changing client VLANs.

**Figure 1 Network diagram**



| Device | Interface   | IP address   |
|--------|-------------|--------------|
| AC 1   | Vlan-int100 | 192.1.0.2/16 |
|        | Vlan-int200 | 192.2.0.2/16 |
| AC 2   | Vlan-int100 | 192.1.0.3/16 |
|        | Vlan-int400 | 192.4.0.2/16 |
| Switch | Vlan-int100 | 192.1.0.1/16 |
|        | Vlan-int200 | 192.2.0.1/16 |
|        | Vlan-int400 | 192.4.0.1/16 |

## Restrictions and guidelines

When you configure inter-AC roaming with static client VLAN allocation, follow these restrictions and guidelines:

- Make sure the configured SSID, authentication and key management (AKM) mode, and cipher suite are the same on APs for wireless roaming.
- Use the actual serial ID of an AP to uniquely identify that AP.

## Procedures

### Configuring AC 1

1. Configure AC interfaces:

# Create VLAN 100 and VLAN-interface 100, and assign IP address 192.1.0.2/16 to the interface. The AC 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 192.1.0.2 16
[AC1-Vlan-interface100] quit
```

# Create VLAN 200 and VLAN-interface 200, and assign IP address 192.2.0.2/16 to the interface. The AC will use this interface to communicate with clients.

```
[AC1] vlan 200
[AC1-vlan200] quit
[AC1] interface vlan-interface 200
[AC1-Vlan-interface200] ip address 192.2.0.2 16
[AC1-Vlan-interface200] quit
```

# Create VLAN 400. The AC will use this VLAN to forward traffic of clients roamed from AC 2.

```
[AC1] vlan 400
[AC1-vlan400] quit
```

# Set the link type of GigabitEthernet 1/0/1 to trunk and assign the port to VLANs 100, 200, and 400.

```
[AC1] interface gigabitethernet 1/0/1
[AC1-GigabitEthernet1/0/1] port link-type trunk
[AC1-GigabitEthernet1/0/1] port trunk permit vlan 100 200 400
[AC1-GigabitEthernet1/0/1] quit
```

# Set the link type of GigabitEthernet 1/0/2 to access and assign the port to VLAN 100.

```
[AC1] interface gigabitethernet 1/0/2
[AC1-GigabitEthernet1/0/2] port link-type access
[AC1-GigabitEthernet1/0/2] port access vlan 100
[AC1-GigabitEthernet1/0/2] quit
```

2. Create VLAN group **roam**, and add VLANs 200 and 400 to the group.

```
[AC1] vlan-group roam
[AC1-vlan-group-roam] vlan-list 200 400
```

3. Configure wireless services:

# Create service template 1.

```
[AC1] wlan service-template 1
```

# Set the SSID to **service**.

```
[AC1-wlan-st-1] ssid service
```

# Set the VLAN allocation method for clients to static.

```
[AC1-wlan-st-1] client vlan-alloc static
```

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

```
[AC1-wlan-st-1] akm mode psk
[AC1-wlan-st-1] preshared-key pass-phrase simple 12345678
```

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

```
[AC1-wlan-st-1] cipher-suite ccmp
[AC1-wlan-st-1] security-ie rsn
```

# Configure the AC to forward client data traffic. If the default client data traffic forwarder is AC, skip this step.

```
[AC1-wlan-st-1] client forwarding-location ac
```

# Enable service template 1.

```
[AC1-wlan-st-1] service-template enable
[AC1-wlan-st-1] quit
```

4. Configure AP settings:

---

**NOTE:**

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

---

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

```
[AC1] wlan ap ap1 model AP 3620
[AC1-wlan-ap-ap1] serial-id 219801A28N819CE0002T
[AC1-wlan-ap-ap1] quit
```

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

```
[AC1] wlan ap-group group1
[AC1-wlan-ap-group-group1] ap ap1
```

**# Bind service template 1 and VLAN group roam to radio 1 for AP group group1.**

```
[AC1-wlan-ap-group-group1] ap-model AP 3620
[AC1-wlan-ap-group-group1-ap-model-AP 3620] radio 1
[AC1-wlan-ap-group-group1-ap-model-AP 3620-radio-1] service-template 1 vlan-group
roam
```

**# Enable radio 1.**

```
[AC1-wlan-ap-group-group1-ap-model-AP 3620-radio-1] radio
enable [AC1-wlan-ap-group-group1-ap-model-AP 3620-radio-1] quit
[AC1-wlan-ap-group-group1-ap-model-AP 3620]
quit [AC1-wlan-ap-group-group1] quit
```

**5. Configure wireless roaming:**

**# Create mobility group 1 and enter its view.**

```
[AC1] wlan mobility group 1
```

**# Specify the source IPv4 address for establishing IADTP tunnels as 192.1.0.2.**

```
[AC1-wlan-mg-1] source ip 192.1.0.2
```

**# Add AC 2 as a mobility group member.**

```
[AC1-wlan-mg-1] member ip 192.1.0.3
```

**# Enable mobility group 1.**

```
[AC1-wlan-mg-1] group enable
[AC1-wlan-mg-1] quit
```

**6. Configure a static route, whose next hop address is 192.1.0.1.**

```
[AC1] ip route-static 0.0.0.0 0.0.0.0 192.1.0.1
```

## Configuring AC 2

**1. Configure AC interfaces:**

**# Create VLAN 100 and VLAN-interface 100, and assign IP address 192.1.0.3/16 to the interface. The AC 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 192.1.0.3 16
[AC2-Vlan-interface100] quit
```

**# Create VLAN 200. The AC will use this VLAN to forward traffic of clients roamed from AC 1.**

```
<AC2> system-view
[AC2] vlan 200
[AC2-vlan200] quit
```

**# Create VLAN 400 and VLAN-interface 400, and assign IP address 192.4.0.2/16. The AC will use this interface to communicate with clients.**

```
[AC2] vlan 400
[AC2-vlan400] quit
[AC2] interface vlan-interface 400
[AC2-Vlan-interface400] ip address 192.4.0.2 16
[AC2-Vlan-interface400] quit
```

**# Set the link type of GigabitEthernet 1/0/1 to trunk and assign the port to VLANs 100, 200, and 400.**

```
[AC2] interface gigabitethernet 1/0/1
[AC2-GigabitEthernet1/0/1] port link-type trunk
[AC2-GigabitEthernet1/0/1] port trunk permit vlan 100 200 400
[AC2-GigabitEthernet1/0/1] quit
```

**# Set the link type of GigabitEthernet 1/0/2 to access and assign the port to VLAN 100.**

```
[AC2] interface gigabitethernet 1/0/2
[AC2-GigabitEthernet1/0/2] port link-type access
[AC2-GigabitEthernet1/0/2] port access vlan 100
[AC2-GigabitEthernet1/0/2] quit
```

**2. Create VLAN group **roam**, and add VLANs 200 and 400 to the group.**

```
[AC2] vlan-group roam
[AC2-vlan-group-roam] vlan-list 200 400
```

**3. Configure wireless services:**

**# Create service template 1.**

```
[AC2] wlan service-template 1
```

**# Set the SSID to **service**.**

```
[AC2-wlan-st-1] ssid service
```

**# Set the VLAN allocation method for clients to static.**

```
[AC2-wlan-st-1] client vlan-alloc static
```

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

```
[AC2-wlan-st-1] akm mode psk
```

```
[AC2-wlan-st-1] preshared-key pass-phrase simple 12345678
```

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

```
[AC2-wlan-st-1] cipher-suite ccmp
```

```
[AC2-wlan-st-1] security-ie rsn
```

**# Configure the AC to forward client data traffic. If the default client data traffic forwarder is AC, skip this step.**

```
[AC2-wlan-st-1] client forwarding-location ac
```

**# Enable service template 1.**

```
[AC2-wlan-st-1] service-template enable
```

```
[AC2-wlan-st-1] quit
```

**4. Configure AP settings:**

---

**NOTE:**

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

---

**# Create AP **ap2**, and specify the AP model and serial ID.**

```
[AC2] wlan ap ap2 model AP 3620
```

```
[AC2-wlan-ap-ap2] serial-id 219801A28N819CE0003T
```

**# Create AP group **group1** and configure **ap2** as the AP grouping rule.**

```
[AC2] wlan ap-group group1
[AC2-wlan-ap-group-group1] ap ap2
Bind service template 1 and VLAN group roam to radio 1 for AP group group1.
[AC2-wlan-ap-group-group1] ap-model AP 3620
[AC2-wlan-ap-group-group1-ap-model-AP 3620] radio 1
[AC2-wlan-ap-group-group1-ap-model-AP 3620-radio-1] service-template 1 vlan-group
roam
Enable radio 1.
[AC2-wlan-ap-group-group1-ap-model-AP 3620-radio-1] radio
enable [AC2-wlan-ap-group-group1-ap-model-AP 3620-radio-1] quit
[AC2-wlan-ap-group-group1-ap-model-AP 3620]
quit [AC2-wlan-ap-group-group1] quit
```

**5. Configure wireless roaming:**

**# Create mobility group 1 and enter its view.**

```
[AC2] wlan mobility group 1
```

**# Specify the source IPv4 address for establishing IADTP tunnels as 192.1.0.3.**

```
[AC2-wlan-mg-1] source ip 192.1.0.3
```

**# Add AC 1 as a mobility group member.**

```
[AC2-wlan-mg-1] member ip 192.1.0.2
```

**# Enable mobility group 1.**

```
[AC2-wlan-mg-1] group enable
[AC2-wlan-mg-1] quit
```

**6. Configure a static route, whose next hop address is 192.1.0.1.**

```
[AC2] ip route-static 0.0.0.0 0.0.0.0 192.1.0.1
```

## Configuring the switch

- Configure AC interfaces:
 

**# Create VLAN 100 and VLAN-interface 100, and assign IP address 192.1.0.1/16 to the interface. The switch will use this interface to communicate with AC 1 and AC 2.**

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

**# Create VLAN 200 and VLAN-interface 200, and assign IP address 192.2.0.1/16 to the interface. The switch will use this interface to communicate with clients associated with AC 1.**

```
[Switch] vlan 200
[Switch-vlan200] quit
[Switch] interface vlan-interface 200
[Switch-Vlan-interface200] ip address 192.2.0.1 16
[Switch-Vlan-interface200] quit
```

**# Create VLAN 400 and VLAN-interface 400, and assign IP address 192.4.0.1/16. The AC will use this interface to communicate with clients associated with AC 2.**

```
[Switch] vlan 400
[Switch-vlan400] quit
[Switch] interface vlan-interface 400
```

```
[Switch-Vlan-interface400] ip address 192.4.0.1 16
[Switch-Vlan-interface400] quit
```

**# Set the link type of GigabitEthernet 1/0/1 to trunk and assign the port to VLANs 100, 200, and 400.**

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100 200 400
[Switch-GigabitEthernet1/0/1] quit
```

**# Set the link type of GigabitEthernet 1/0/2 to access and assign the port to VLANs 100, 200, 400.**

```
[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] port link-type trunk
[Switch-GigabitEthernet1/0/2] port trunk permit vlan 100 200 400
[Switch-GigabitEthernet1/0/2] quit
```

## 2. Configure the DHCP server:

**# Enable DHCP.**

```
[Switch] dhcp enable
```

**# Create DHCP address pool **vlan100**, specify subnet 192.1.0.0/16 in the address pool, exclude IP addresses 192.1.0.2 and 192.1.0.3 from dynamic allocation, and specify the gateway IP address as 192.1.0.1.**

```
[Switch] dhcp server ip-pool vlan100
[Switch-dhcp-pool-vlan100] network 192.1.0.0 mask 255.255.0.0
[Switch-dhcp-pool-vlan100] forbidden-ip 192.1.0.2 192.1.0.3
[Switch-dhcp-pool-vlan100] gateway-list 192.1.0.1
[Switch-dhcp-pool-vlan100] quit
```

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

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

**# Create DHCP address pool **vlan400**, specify subnet 192.4.0.0/16 in the address pool, and exclude 192.4.0.2 from dynamic allocation. Specify the gateway address as 192.4.0.1, and specify the address of the DNS server. In this example, the gateway also acts as the DNS server.**

```
[Switch] dhcp server ip-pool vlan400
[Switch-dhcp-pool-vlan400] network 192.4.0.0 mask 255.255.0.0
[Switch-dhcp-pool-vlan400] forbidden-ip 192.4.0.2
[Switch-dhcp-pool-vlan400] gateway-list 192.4.0.1
[Switch-dhcp-pool-vlan400] dns-list 192.4.0.1
[Switch-dhcp-pool-vlan400] quit
```

## Verifying the configuration

**# Make a client come online from AC 1.**

# Use the **display wlan client** command to view the client's VLAN and IP address from AC 1.

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

Total number of clients: 1

| MAC address    | User name | AP name | R IP address | VLAN |
|----------------|-----------|---------|--------------|------|
| 68db-ca64-23fd | N/A       | ap1     | 1 192.2.0.3  | 200  |

# Make the client roam to AC 2.

# Use the **display wlan client** command to view the client's VLAN and IP address from AC 2.  
Verify that the client's VLAN and IP address are not changed after roaming.

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

Total number of clients: 1

| MAC address    | User name | AP name | R IP address | VLAN |
|----------------|-----------|---------|--------------|------|
| 68db-ca64-23fd | N/A       | ap2     | 1 192.2.0.3  | 200  |

## Configuration files

- Switch:

```
#
dhcp enable
#
vlan 100
#
vlan 200
#
vlan 400
#
dhcp server ip-pool vlan100
gateway-list 192.1.0.1
network 192.1.0.0 mask 255.255.0.0
forbidden-ip 192.1.0.2
forbidden-ip 192.1.0.3
#
dhcp server ip-pool vlan200
gateway-list 192.2.0.1
network 192.2.0.0 mask 255.255.0.0
dns-list 192.2.0.1
forbidden-ip 192.2.0.2
#
dhcp server ip-pool vlan400
gateway-list 192.4.0.1
network 192.4.0.0 mask 255.255.0.0
dns-list 192.4.0.1
forbidden-ip 192.4.0.2
#
interface Vlan-interface100
ip address 192.1.0.1 255.255.0.0
#
```



```

interface Vlan-interface200
 ip address 192.2.0.1 255.255.0.0
#
interface Vlan-interface400
 ip address 192.4.0.1 255.255.0.0
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 100 200 400
#
interface GigabitEthernet1/0/2
 port link-type trunk
 port trunk permit vlan 100 200 400
#

```

- **AC 1:**

```

#
vlan 100
#
vlan 200
#
vlan 400
#
vlan-group roam
 vlan-list 200 400
#
wlan service-template 1
 ssid service
 client forwarding-location ac
 client vlan-alloc static
 akm mode psk
 preshared-key pass-phrase cipher c3$0Lf6pOZ6bxrf25nodjOJKYEfnZ6g6ErccHyQ
 cipher-suite ccmp
 security-ie rsn
 service-template enable
#
interface Vlan-interface100
 ip address 192.1.0.2 255.255.0.0
#
interface Vlan-interface200
 ip address 192.2.0.2 255.255.0.0
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 100 200 400
#
interface GigabitEthernet1/0/2
 port link-type access
 port access vlan 100

```

```

#
ip route-static 0.0.0.0 0.0.0.0 192.1.0.1
#
wlan ap-group group1
 ap ap1
 ap-model AP 3620
 radio 1
 radio enable
 service-template 1 vlan-group roam
 radio 2
#
wlan ap ap1 model AP 3620
 serial-id 219801A28N819CE0002T
#
wlan mobility group 1
 source ip 192.1.0.2
 member ip 192.1.0.3
 group enable
#
• AC 2:
#
vlan 100
#
vlan 200
#
vlan 400
#
vlan-group roam
 vlan-list 200 400
#
wlan service-template 1
 ssid service
 client forwarding-location ac
 client vlan-alloc static
 akm mode psk
 preshared-key pass-phrase cipher c3$0Lf6pOZ6bxrf25nodjOJKYEfnZ6g6ErccHyQ
 cipher-suite ccmp
 security-ie rsn
 service-template enable
#
interface Vlan-interface100
 ip address 192.1.0.3 255.255.0.0
#
interface Vlan-interface400
 ip address 192.4.0.2 255.255.0.0
#
interface GigabitEthernet1/0/1
 port link-type trunk

```

```

port trunk permit vlan 100 200 400
#
interface GigabitEthernet1/0/2
port link-type access
port access vlan 100
#
ip route-static 0.0.0.0 0.0.0.0 192.1.0.1
#
wlan ap-group group1
ap ap2
ap-model AP 3620
radio 1
radio enable
service-template 1 vlan-group roam
radio 2
#
wlan ap ap2 model AP 3620
serial-id 219801A28N819CE0003T
#
wlan mobility group 1
source ip 192.1.0.3
member ip 192.1.0.2
group 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*
- *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

## Service Template and Radio Binding

## 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: Binding service templates with different SSIDs to radios ..... | 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 .....                                      | 6  |
| Configuring Layer 2 switch 2 .....                                      | 7  |
| Verifying the configuration .....                                       | 7  |
| Configuration files .....                                               | 8  |
| Related documentation .....                                             | 11 |

# Introduction

The following information provides an example for binding a service template to a radio.

## 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 DHCP and WLAN access.

## Example: Binding service templates with different SSIDs to radios

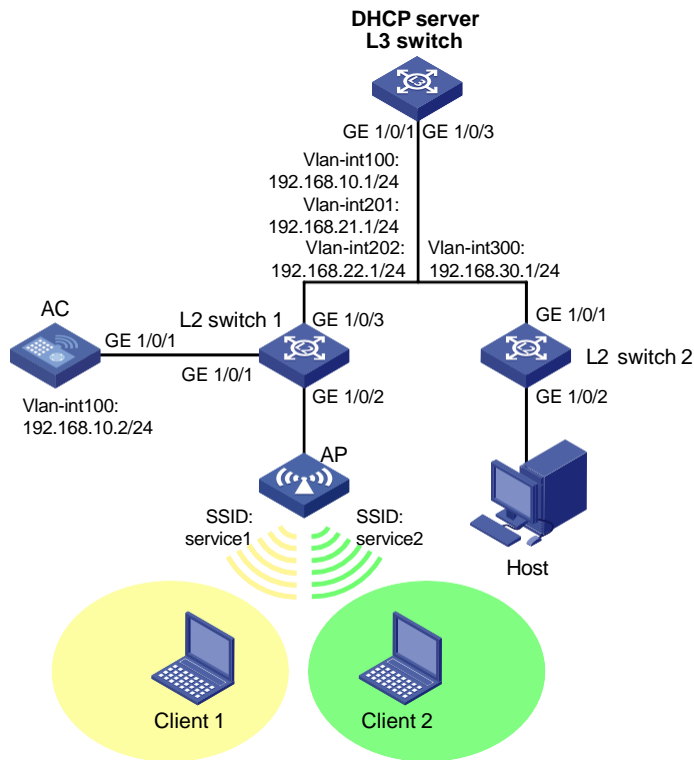
### Network configuration

As shown in [Figure 1](#), the AC connects to Layer 2 switch 1 and the Layer 3 switch acts as a DHCP server to assign IP addresses to the AP, the host, and the clients. Radio 1 and radio 2 of the AP operates at 5GHz band and 2.4 GHz band, respectively.

Configure network settings to meet the following requirements:

- Client 1 accesses WLAN service1 over VLAN 201.
- Client 2 accesses WLAN service2 over VLAN 202.
- The host accesses the network over VLAN 300.
- The AC and the AP communicate with each other over VLAN 100.
- Layer 2 switch 1 supplies power to the AP through PoE.

Figure 1 Network diagram



## Analysis

- For the Layer 3 switch to act as a DHCP server, enable the DHCP server feature on the switch.
- For Layer 2 switch 1 to supply power to the AP, enable the PoE feature on the switch.
- For the clients to ping the host through different WLANs, configure service templates with different SSIDs on the AC.

## Restrictions and guidelines

When you configure a serial ID for the AP, use the actual serial ID of an AP to uniquely identify that AP.

## Procedures

### Configuring the Layer 3 switch

1. Configure Layer 3 switch interfaces:  
# Create VLAN 100 and VLAN-interface 100, and assign IP address 192.168.10.1 to the interface. The switch communicates with the AC over VLAN 100.

```
<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 201 and VLAN-interface 201, and assign IP address 192.168.21.1 to the interface. Client 1 will use this VLAN to access the WLAN.**

```
[L3 switch] vlan 201
[L3 switch-vlan201] quit
[L3 switch] interface vlan-interface 201
[L3 switch-Vlan-interface201] ip address 192.168.21.1 255.255.255.0
[L3 switch-Vlan-interface201] quit
```

**# Create VLAN 202 and VLAN-interface 202, and assign IP address 192.168.22.1 to the interface. Client 2 will use this VLAN to access the WLAN.**

```
[L3 switch] vlan 202
[L3 switch-vlan202] quit
[L3 switch] interface vlan-interface 202
[L3 switch-Vlan-interface202] ip address 192.168.22.1 255.255.255.0
[L3 switch-Vlan-interface202] 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 access the WLAN.**

```
[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, 201, and 202.**

```
[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 100 201 202
[L3 switch-GigabitEthernet1/0/1] 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 the DHCP server feature:**

**# Enable DHCP server.**

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

**# Create DHCP address pool 1 for dynamic IP allocation to the AP. Specify 192.168.10.0/24 as the subnet and 192.168.10.1 as the gateway address in the address pool.**

```
[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 the IP address of VLAN-interface 100 on the AC from dynamic IP allocation in DHCP address pool 1.**

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



**# Create DHCP address pool 2 for dynamic IP allocation to Client 1. Specify 192.168.21.0/24 as the subnet and 192.168.21.1 as the gateway address in the address pool, and then specify the address of the DNS server. In this example, the gateway also acts as the DNS server.**

```
[L3 switch] dhcp server ip-pool 2
[L3 switch-dhcp-pool-2] network 192.168.21.0 mask 255.255.255.0
[L3 switch-dhcp-pool-2] gateway-list 192.168.21.1
[L3 switch-dhcp-pool-2] dns-list 192.168.21.1
[L3 switch-dhcp-pool-2] quit
```

**# Create DHCP address pool 3 for dynamic IP allocation to Client 2. Specify 192.168.22.0/24 as the subnet and 192.168.22.1 as the gateway address in the address pool, and then specify the address of the DNS server. In this example, the gateway also acts as the DNS server.**

```
[L3 switch] dhcp server ip-pool 3
[L3 switch-dhcp-pool-3] network 192.168.22.0 mask 255.255.255.0
[L3 switch-dhcp-pool-3] gateway-list 192.168.22.1
[L3 switch-dhcp-pool-3] dns-list 192.168.22.1
[L3 switch-dhcp-pool-3] quit
```

**# Create DHCP address pool 4 for dynamic IP allocation to the host. Specify 192.168.30.0/24 as the subnet and 192.168.30.1 as the gateway address in the address pool, and then specify the address of the DNS server. In this example, the gateway also acts as the DNS server.**

```
[L3 switch] dhcp server ip-pool 4
[L3 switch-dhcp-pool-4] network 192.168.30.0 mask 255.255.255.0
[L3 switch-dhcp-pool-4] gateway-list 192.168.30.1
[L3 switch-dhcp-pool-4] dns-list 192.168.30.1
[L3 switch-dhcp-pool-4] quit
```

## Configuring the AC

### 1. Configure AC interfaces:

**# Create VLAN 100 and VLAN-interface 100, and assign IP address 192.168.10.2 to the interface. The AC will establish a CAPWAP tunnel with the AP in this VLAN.**

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

**# Create VLAN 201. Client 1 will use this VLAN to access the WLAN.**

```
[AC] vlan 201
[AC-vlan201] quit
```

**# Create VLAN 202. Client 2 will use this VLAN to access the WLAN.**

```
[AC] vlan 202
[AC-vlan202] quit
```

**# Set the link type of GigabitEthernet 1/0/1 that connects the AC to Layer 2 switch 1 to trunk. Remove the port from VLAN 1 and assign the port to VLANs 100, 201, and 202.**

```
[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 100 201 202
[AC-GigabitEthernet1/0/1] quit
```

## 2. Configure wireless services:

# Create service template 1 and enter its view.

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

# Set the SSID to **service1**.

```
[AC-wlan-st-1] ssid service1
```

# Specify the AKM mode as PSK, 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
```

# Specify the cipher suite as CCMP and the security IE as 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 service template 1.

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

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

# Create service template 2 and enter its view.

```
[AC] wlan service-template 2
```

# Set the SSID to **service2**.

```
[AC-wlan-st-2] ssid service2
```

# Specify the AKM mode as PSK for service template 2, and specify plaintext string **abcdefgh** as the preshared key.

```
[AC-wlan-st-2] akm mode psk
```

```
[AC-wlan-st-2] preshared-key pass-phrase simple abcdefgh
```

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

```
[AC-wlan-st-2] cipher-suite ccmp
```

```
[AC-wlan-st-2] 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-2] client forwarding-location ac
```

# Enable service template 2.

```
[AC-wlan-st-2] service-template enable
```

```
[AC-wlan-st-2] quit
```

## 3. Configure AP settings:

---

### NOTE:

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

---

# Create 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 201 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 201
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
Bind service template 2 and VLAN 202 to radio 2.
[AC-wlan-ap-group-group1-ap-model-AP 3620] radio 2
[AC-wlan-ap-group-group1-ap-model-AP 3620-radio-2] service-template 2 vlan 202
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 Layer 2 switch 1

**# Create VLAN 100, VLAN 201, and VLAN 202. The switch will use VLAN 100 to forward traffic between the AC and other devices. Client 1 will use VLAN 201 to access the WLAN and Client 2 will use VLAN 202 to access the WLAN.**

```
<L2 switch 1> system-view
[L2 switch 1] vlan 100
[L2 switch 1-vlan100] quit
[L2 switch 1] vlan 201
[L2 switch 1-vlan201] quit
[L2 switch 1] vlan 202
[L2 switch 1-vlan202] quit
```

**# Set the link type of GigabitEthernet 1/0/1 that connects the switch to the AC to trunk. Remove the port from VLAN 1 and assign the port to VLANs 100, 201, and 202.**

```
[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 100 201 202
[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 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
```

**# Set the link type of GigabitEthernet 1/0/3 that connects the switch to the Layer 3 switch to trunk. Remove the port from VLAN 1 and assign the port to VLANs 100, 201, and 202.**

```
[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 100 201 202
[L2 switch 1-GigabitEthernet1/0/3] quit
```

## Configuring Layer 2 switch 2

# Create VLAN 300. The host will use VLAN 300 to access the network.

```
<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. 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

# Use the **display wlan ap all** command to view AP information on the AC. If the AP has connected to the AC, the state of the AP is R/M.

```
<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  | APID | State | Model   | Serial ID            |
|----------|------|-------|---------|----------------------|
| officeap | 1    | R/M   | AP 3620 | 219801A28N819CE0002T |

# Use the **display wlan client** command to view client information on the AC. Client 1 has connected to radio 1 of the AP and Client 2 has connected to radio 2 of the AP.

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

Total number of clients: 2

| MAC address    | User name | AP name  | R IP address   | VLAN |
|----------------|-----------|----------|----------------|------|
| 109a-dd9d-fc68 | N/A       | officeap | 1 192.168.21.2 | 201  |
| 109a-dd9d-fc69 | N/A       | officeap | 2 192.168.22.2 | 202  |

**# After Client 1 obtains IP address 192.168.21.2 from the DHCP server, the host and Client 1 can ping each other successfully.**

```
C:\Users\system32>ping 192.168.21.2 -t
```

Pinging 192.168.21.2 with 32 bytes of data:

```
Reply from 192.168.21.2: bytes=32 time=8ms TTL=255
Reply from 192.168.21.2: bytes=32 time<1ms TTL=255
Reply from 192.168.21.2: bytes=32 time<1ms TTL=255
Reply from 192.168.21.2: bytes=32 time<1ms TTL=255
Reply from 192.168.21.2: bytes=32 time<1ms TTL=255
Reply from 192.168.21.2: bytes=32 time<1ms TTL=255
Reply from 192.168.21.2: bytes=32 time<1ms TTL=255
Reply from 192.168.21.2: bytes=32 time<1ms TTL=255
Reply from 192.168.21.2: bytes=32 time<1ms TTL=255
Reply from 192.168.21.2: bytes=32 time<1ms TTL=255
Reply from 192.168.21.2: bytes=32 time<1ms TTL=255
```

Ping statistics for 192.168.21.2:

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

- L3 switch

```
#
dhcp enable
#
vlan 1
#
vlan 100
#
vlan 201
#
vlan 202
#
vlan 300
#
dhcp server ip-pool 1
gateway-list 192.168.10.1
```

```

network 192.168.10.0 mask 255.255.255.0
forbidden-ip 192.168.10.2
#
dhcp server ip-pool 2
gateway-list 192.168.21.1
network 192.168.21.0 mask 255.255.255.0
dns-list 192.168.21.1
#
dhcp server ip-pool 3
gateway-list 192.168.22.1
network 192.168.22.0 mask 255.255.255.0
dns-list 192.168.22.1
#
dhcp server ip-pool 4
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 100 201 202
#
interface GigabitEthernet1/0/3
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 300
#
• AC
#
vlan 100
#
vlan 201
#
vlan 202
#
wlan service-template 1
ssid service1
client forwarding-location ac

```

```

akm mode psk
preshared-key pass-phrase cipher c3$EGdeMZ4taNF5ifpRCaOKOoDAjSMh+WKIhH3+
cipher-suite ccmp
security-ie rsn
service-template enable
#
wlan service-template 2
ssid service2
client forwarding-location ac
akm mode psk
preshared-key pass-phrase cipher c3$s/vZYild4fsFquikaZVkJGR5qdDX/50oME5
cipher-suite ccmp
security-ie rsn
service-template enable
#
interface Vlan-interface1
#
interface Vlan-interface100
ip address 192.168.10.2 255.255.255.0
#
interface GigabitEthernet1/0/1
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 100 201 202
#
wlan ap-group group1
vlan 1
ap officeap
ap-model AP 3620
radio 1
radio enable
service-template 1 vlan 201
radio 2
radio enable
service-template 2 vlan 202
gigabitethernet 1
#
wlan ap officeap model AP 3620
serial-id 219801A28N819CE0002T
#

```

- **L2 switch 1**

```

#
vlan 100
#
vlan 201
#
vlan 202
#

```

```

interface GigabitEthernet1/0/1
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100 201 202
#
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 100 201 202
#

```

- **L2 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

## Scheduled WLAN Access Services

### 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 scheduled WLAN access services..... | 1 |
| Network configuration.....                               | 1 |
| Analysis .....                                           | 1 |
| Restrictions and guidelines .....                        | 2 |
| Procedures .....                                         | 2 |
| Configuring the Layer 3 switch.....                      | 2 |
| Configuring the AC.....                                  | 3 |
| Configuring the Layer 2 switch.....                      | 5 |
| Verifying the configuration .....                        | 5 |
| Configuration files.....                                 | 6 |
| Related documentation .....                              | 9 |

# Introduction

The following information provides an example for configuring scheduled WLAN access services.

## 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 DHCP and WLAN access.

## Example: Configuring scheduled WLAN access services

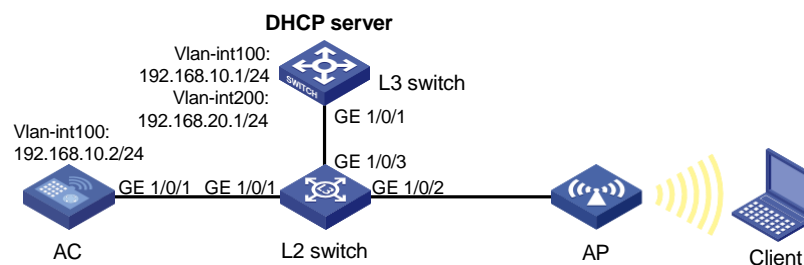
### Network configuration

As shown in [Figure 1](#), the AC connects to the Layer 2 switch and the Layer 3 switch acts as a DHCP server to assign IP addresses to the AP and the client.

Configure network settings to meet the following requirements:

- The client accesses the WLAN over VLAN 200.
- The AC and the AP communicate with each other over VLAN 100.
- The Layer 2 switch supplies power to the AP through PoE.
- The AP provides WLAN access services only from 8:00 to 20:00 every day.

**Figure 1 Network diagram**



### Analysis

- For the Layer 3 switch to act as a DHCP server, enable the DHCP server feature on the switch.
- For the Layer 2 switch to supply power to the AP, enable the PoE feature on the switch.
- Create two schedules to enable and disable the WLAN service template on the AC at specific time points.

# Restrictions and guidelines

When you configure a serial ID for the AP, use the actual serial ID of an AP to uniquely identify that AP.

## Procedures

### Configuring the Layer 3 switch

1. Configure Layer 3 switch interfaces:

# Create VLAN 100 and VLAN-interface 100, and assign IP address 192.168.10.1 to the interface. The switch communicates with the AC over VLAN 100.

```
<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
```

# Set the link type of GigabitEthernet 1/0/1 that connects the switch to the Layer 2 switch to trunk. Remove the port from VLAN 1 and assign the port to VLAN 100 and VLAN 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
```

2. Configure the DHCP server feature:

# Enable DHCP server.

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

# Create DHCP address pool 1 for dynamic IP allocation to the AP. Specify 192.168.10.0/24 as the subnet and 192.168.10.1 as the gateway address in the address pool.

```
[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 the IP address of VLAN-interface 100 on the AC from dynamic IP allocation in DHCP address pool 1.

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

# Create DHCP address pool 2 for dynamic IP allocation to the client. Specify 192.168.20.0/24 as the subnet and 192.168.20.1 as the gateway address in the address pool, and then specify the address of the DNS server. In this example, the gateway also acts as the DNS server.

```
[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
```

## Configuring the AC

### 1. Configure AC interfaces:

# Create VLAN 100 and VLAN-interface 100, and assign IP address 192.168.10.2 to the interface. The AC will establish a CAPWAP tunnel with the AP in this VLAN.

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

# Create VLAN 200. The client will use this VLAN to access the WLAN.

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

# Set the link type of GigabitEthernet 1/0/1 that connects the AC to the Layer 2 switch to trunk. Remove the port from VLAN 1 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] undo port trunk permit vlan 1
[AC-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[AC-GigabitEthernet1/0/1] quit
```

### 2. Configure a wireless service:

# Create service template 1 and enter its view.

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

# Set the SSID to **service1**.

```
[AC-wlan-st-1] ssid service1
```

# Specify the AKM mode as PSK, 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
```

# Specify the cipher suite as CCMP and the security IE as 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 service template 1.

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

### 3. Configure AP settings:

---

#### NOTE:

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

---

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

```
[AC] wlan ap officeap model AP 3620
[AC-wlan-ap-officeap] serial-id 209801A28N819CE0002T
[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 in `group1`.**

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

**4. Configure the AC to enable service template 1 at a specific time point.**

**# Create job `officeap_service_enable` to enable service template 1.**

```
[AC] scheduler job officeap_service_enable
[AC-job-officeap_service_enable] command 1 system-view
[AC-job-officeap_service_enable] command 2 wlan service-template 1
[AC-job-officeap_service_enable] command 3 service-template enable
[AC-job-officeap_service_enable] command 4 quit
[AC-job-officeap_service_enable] quit
```

**# Create schedule `officeap_service_enable` and assign job `officeap_service_enable` to the schedule. The AC will enable service template 1 at 8:00 a.m. every day.**

```
[AC] scheduler schedule officeap_service_enable
[AC-schedule-officeap_service_enable] job officeap_service_enable
[AC-schedule-officeap_service_enable] time repeating at 08:00
[AC-schedule-officeap_service_enable] quit
```

**5. Configure the AC to disable service template 1 at a specific time point.**

**# Create job `officeap_service_disable` to disable service template 1.**

```
[AC] scheduler job officeap_service_disable
[AC-job-officeap_service_disable] command 1 system-view
[AC-job-officeap_service_disable] command 2 wlan service-template 1
[AC-job-officeap_service_disable] command 3 undo service-template enable
[AC-job-officeap_service_disable] command 4 quit
[AC-job-officeap_service_disable] quit
```

**# Create schedule `officeap_service_disable` and assign job `officeap_service_disable` to the schedule. The AC will disable service template 1 at 20:00 every day.**

```
[AC] scheduler schedule officeap_service_disable
[AC-schedule-officeap_service_disable] job officeap_service_disable
[AC-schedule-officeap_service_disable] time repeating at 20:00
[AC-schedule-officeap_service_disable] quit
[AC] quit
```

## Configuring the Layer 2 switch

# Create VLAN 100 and VLAN 200. The switch will use VLAN 100 to forward traffic between the AC and other devices. The client will use VLAN 200 to access the WLAN.

```
<L2 switch> system-view
[L2 switch] vlan 100
[L2 switch-vlan100] quit
[L2 switch] vlan 200
[L2 switch-vlan200] quit
```

# Set the link type of GigabitEthernet 1/0/1 that connects the switch to the AC to trunk. Remove the port from VLAN 1 and assign the port to VLAN 100 and VLAN 200.

```
[L2 switch] interface gigabitEthernet 1/0/1
[L2 switch-GigabitEthernet1/0/1] port link-type trunk
[L2 switch-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[L2 switch-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[L2 switch-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 100 and enable PoE.

```
[L2 switch] interface gigabitEthernet 1/0/2
[L2 switch-GigabitEthernet1/0/2] port link-type access
[L2 switch-GigabitEthernet1/0/2] port access vlan 100
[L2 switch-GigabitEthernet1/0/2] poe enable
[L2 switch-GigabitEthernet1/0/2] quit
```

# Set the link type of GigabitEthernet 1/0/3 that connects the switch to the Layer 3 switch to trunk. Remove the port from VLAN 1 and assign the port to VLAN 100 and VLAN 200.

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

## Verifying the configuration

# Use the **display wlan ap all** command to view AP information on the AC. If the AP has connected to the AC, the state of the AP is R/M.

```
<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  | APID | State | Model   | Serial ID            |
|----------|------|-------|---------|----------------------|
| officeap | 1    | R/M   | AP 3620 | 209801A28N819CE0002T |

# During the period when the AC is scheduled to provide WLAN services, use the **display wlan service-template** command to view service template information on the AC. Service template 1 is enabled.

```
<AC> display wlan service-template 1
```

| Service template name | SSID     | Status  |
|-----------------------|----------|---------|
| 1                     | service1 | Enabled |

# During the period when the AC is scheduled to provide WLAN services, use the **display wlan client** command to view client information on the AC. The client has connected to radio 1 of the AP.

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

Total number of clients: 1

| MAC address    | User name | AP name  | R IP address   | VLAN |
|----------------|-----------|----------|----------------|------|
| 109a-dd9d-fc68 | N/A       | officeap | 1 192.168.20.2 | 200  |

# During the period when the AC is scheduled to not provide WLAN services, use the **display wlan service-template** command to view service template information on the AC. Service template 1 is disabled.

```
<AC> display wlan service-template 1
```

| Service template name | SSID     | Status   |
|-----------------------|----------|----------|
| 1                     | service1 | Disabled |

# During the period when the AC is scheduled to not provide WLAN services, use the **display wlan client** command to view client information on the AC. No client is online because service template 1 is disabled.

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

```
<AC>
```

## Configuration files

- L3 switch

```
#
dhcp enable
#
vlan 1
#
vlan 100
#
vlan 200
#
dhcp server ip-pool 1
gateway-list 192.168.10.1
network 192.168.10.0 mask 255.255.255.0
```



```

 forbidden-ip 192.168.10.2
#
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
#
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
#
• AC
#
vlan 100
#
vlan 200
#
wlan service-template 1
 ssid service1
 client forwarding-location ac
 akm mode psk
 preshared-key pass-phrase cipher c3$0Lf6p0Z6bxrf25nodj0JKYEfnZ6g6ErccHyQ
 cipher-suite ccmp
 security-ie rsn
 service-template enable
#
interface Vlan-interface1
#
interface Vlan-interface100
 ip address 192.168.10.2 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100 200
#
scheduler job officeap_service_disable
 command 1 system-view
 command 2 wlan service-template 1
 command 3 undo service-template enable
 command 4 quit

```

```

#
scheduler job officeap_service_enable
 command 1 system-view
 command 2 wlan service-template 1
 command 3 service-template enable
 command 4 quit
#
scheduler schedule officeap_service_disable
 user-role network-operator
 user-role network-admin
 job officeap_service_disable
 time repeating at 20:00
#
scheduler schedule officeap_service_enable
 user-role network-operator
 user-role network-admin
 job officeap_service_enable
 time repeating at 08:00
#
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 209801A28N819CE0002T
#
• L2 switch
#
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
#
```

## 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*