

INTELBRAS Access Controllers

WLAN Probe 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 WLAN probe	1
Network configuration	1
Procedures	2
Configuring the AC	2
Configuring the switch	4
Verifying the configuration	5
Configuration files	5
Related documentation	7

Introduction

The following information provides examples for configuring WLAN probe.

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 WIPS.

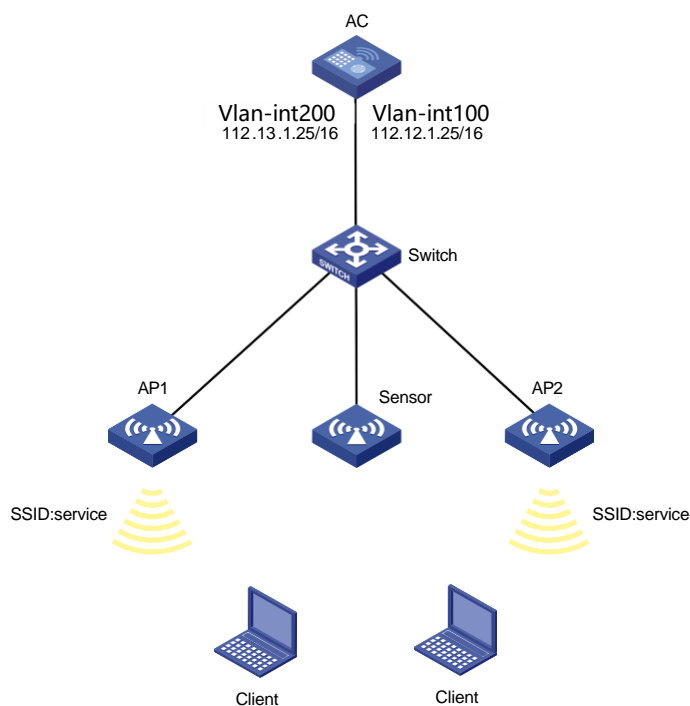
Example: Configuring WLAN probe

Network configuration

As shown in [Figure 1](#), AP 1 and AP 2 provide wireless services for clients through SSID **service**.

Enable WLAN probe on the sensor, and configure the sensor to report the received wireless device information to the AC.

Figure 1 Network diagram



Procedures

Configuring the AC

1. Configure interfaces on the AC:

Configure VLAN-interface 100 and assign it an IP address. The AC will use this IP address to establish CAPWAP tunnels with APs.

```
<AC> system-view
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 112.12.1.25 16
[AC-Vlan-interface100] quit
```

Configure VLAN-interface 200 and assign it an IP address. The AC will use VLAN 200 for client access.

```
[AC] vlan 200
[AC-vlan200] quit
[AC] interface vlan-interface 200
[AC-Vlan-interface200] ip address 112.13.1.25 16
[AC-Vlan-interface200] quit
```

Configure GigabitEthernet 1/0/1 that connects the AC to the switch as a trunk port.

```
[AC] interface gigabitethernet1/0/1
[AC-GigabitEthernet1/0/1] port link-type trunk
```

Remove the trunk port from VLAN 1, and assign the port to VLANs 100 and 200.

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

2. Configure DHCP:

Enable DHCP.

```
[AC] dhcp enable
```

Create DHCP address pool **vlan100** to assign IP addresses for APs, and specify the IP address range for the DHCP address pool.

```
[AC] dhcp server ip-pool vlan100
[AC-dhcp-pool-vlan100] network 112.12.0.0 mask 255.255.0.0
```

Specify gateway IP address 112.12.1.25 in the DHCP address pool.

```
[AC-dhcp-pool-vlan100] gateway-list 112.12.1.25
[AC-dhcp-pool-vlan100] quit
```

Create DHCP address pool **vlan200** to assign IP addresses for clients, and specify the IP address range for the DHCP address pool.

```
[AC] dhcp server ip-pool vlan200
[AC-dhcp-pool-vlan200] network 112.13.0.0 mask 255.255.0.0
```

Specify gateway IP address 112.13.1.25 in the DHCP address pool.

```
[AC-dhcp-pool-vlan200] gateway-list 112.13.1.25
```

Configure the DNS server according to the actual network plan. In this example, the gateway is specified as the DNS server.

```
[AC-dhcp-pool-vlan200] dns-list 112.13.1.25
[AC-dhcp-pool-vlan200] quit
```

3. Configure the AP:

NOTE:

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

Create a service template named **service**.

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

Set the SSID to **service**.

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

Assign the service template to VLAN 200.

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

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

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

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

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

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

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

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

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

Enable the service template.

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

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

Create AP group **group1**, add the APs to the AP group, and specify the AP model.

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

```
[AC-wlan-ap-group-group1] ap ap1 ap2
```

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

Bind the service template to the radio interface.

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

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

```
service [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
```

Create AP **ap1**, and specify its model and serial ID.

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

```
[AC-wlan-ap-ap1] serial-id 219801A28N819CE0002X
```

Create AP **ap2**, and specify its model and serial ID.

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

```
[AC-wlan-ap-ap2] serial-id 219801A28N819CE0002T
```

Create AP **sensor** and specify its model and serial ID.

```
[AC] wlan ap sensor model AP 5630
```

```
[AC-wlan-ap-sensor] serial-id 219801A23V8192E00021
```

Enable WLAN probe for the radio.

```
[AC-wlan-ap-sensor] radio 1
```

```
[AC-wlan-ap-sensor-radio-1] scan scan-time 100
```

```
[AC-wlan-ap-sensor-radio-1] client-proximity-sensor enable
```

```
[AC-wlan-ap-sensor-radio-1] radio enable
```

```
[AC-wlan-ap-sensor-radio-1] quit
[AC-wlan-ap-sensor] return
```

Configuring the switch

Create VLANs 100 and 200. The switch will use VLAN 100 to forward the traffic on CAPWAP tunnels between the AC and APs, and use VLAN 200 to forward client traffic.

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

Configure GigabitEthernet 1/0/1 that connects the switch to the AC as a trunk port.

```
[Switch] interface gigabitEthernet1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
```

Remove the trunk port from VLAN 1, and assign the port to VLAN 100 and VLAN 200.

```
[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 as an access port and assign the port to VLAN 100.

```
[Switch] interface gigabitEthernet1/0/2
[Switch-GigabitEthernet1/0/2] port link-type access
[Switch-GigabitEthernet1/0/2] port access vlan 100
```

Enable PoE.

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

Configure GigabitEthernet 1/0/3 that connects the switch to the AP 1 as a trunk port.

```
[Switch] interface gigabitEthernet 1/0/3
[Switch-GigabitEthernet1/0/3] port link-type trunk
```

Remove the trunk port from VLAN 1, and assign the port to VLAN 100.

```
[Switch-GigabitEthernet1/0/3] undo port trunk permit vlan 1
[Switch-GigabitEthernet1/0/3] port trunk permit vlan 100
```

Specify the PVID of the trunk port as VLAN 100.

```
[Switch-GigabitEthernet1/0/3] port trunk pvid vlan 100
```

Enable PoE.

```
[Switch-GigabitEthernet1/0/3] poe enable
[Switch-GigabitEthernet1/0/3] quit
```

Configure GigabitEthernet 1/0/4 that connects the switch to the AP 2 as a trunk port.

```
[Switch] interface gigabitEthernet 1/0/4
[Switch-GigabitEthernet1/0/4] port link-type trunk
```

Remove the trunk port from VLAN 1, and assign the port to VLAN 100.

```
[Switch-GigabitEthernet1/0/4] undo port trunk permit vlan 1
[Switch-GigabitEthernet1/0/4] port trunk permit vlan 100
```

Specify the PVID of the trunk port as VLAN 100.

```
[Switch-GigabitEthernet1/0/4] port trunk pvid vlan 100
```

Enable PoE.

```
[Switch-GigabitEthernet1/0/4] poe enable
[Switch-GigabitEthernet1/0/4] quit
```

Verifying the configuration

Display wireless device information detected by the sensor

```
<Sysname> display client-proximity-sensor device
```

Total 3 detected devices

MAC address	Type	Duration	Sensors	Channel	Status
0AFB-423B-893C	AP	00h 10m 46s 1	11		Active
0AFB-423B-893D	AP	00h 10m 46s 1	6		Active
0AFB-423B-893E	AP	00h 10m 46s 1	1		Active

Configuration files

- AC:

```
#
dhcp enable
#
vlan 100
#
vlan 200
#
dhcp server ip-pool vlan100
gateway-list 112.12.1.25
network 112.12.0.0 mask 255.255.0.0
#
dhcp server ip-pool vlan200
gateway-list 112.13.1.25
network 112.13.0.0 mask 255.255.0.0
dns-list 112.13.1.25
#
wlan service-template service
ssid service
vlan 200
akm mode psk
preshared-key pass-phrase simple 12345678
cipher-suite ccmp
security-ie rsn
client forwarding-location ac
service-template enable
#
interface Vlan-interface100
ip address 112.12.1.25 255.255.0.0
#
interface Vlan-interface200
ip address 112.13.1.25 255.255.0.0
```

```

#
interface GigabitEthernet1/0/1
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100 200
#
wlan ap-group group1
ap ap1 ap2
ap-model AP 3620
radio 1
service-template service
radio enable
#
wlan ap ap1 model AP 3620
serial-id 219801A28N819CE0002X
#
wlan ap ap2 model AP 3620
serial-id 219801A28N819CE0002T
#
wlan ap sensor model AP 5630
serial-id 219801A23V8192E00021
radio 1
scan scan-time 100
client-proximity-sensor enable
radio enable

```

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

```



```
interface GigabitEthernet1/0/4
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 Advanced Features Command Reference in INTELBRAS Access Controllers Command References*
- *WLAN Advanced Features Configuration Guide in INTELBRAS Access Controllers Configuration Guides*

INTELBRAS Access Controllers

Multicast Optimization 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 multicast optimization	1
Network configuration	1
Procedures	1
Configuring the AC	1
Configuring the switch	4
Verifying the configuration	5
Configuration files	6
Related documentation	7

Introduction

The following information provides examples for configuring multicast optimization.

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 multicast optimization.

Example: Configuring multicast optimization

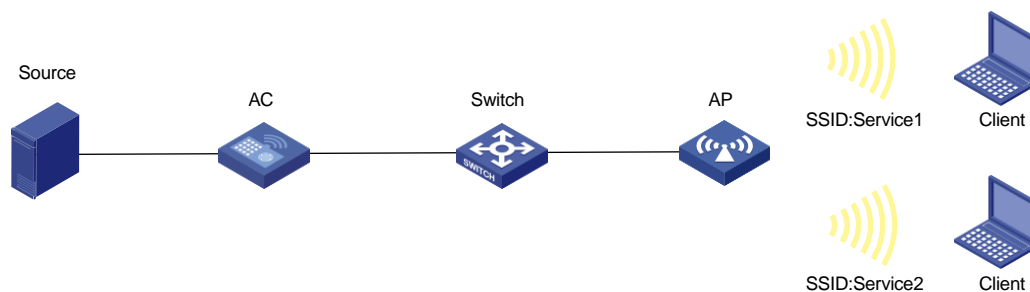
Network configuration

As shown in [Figure 1](#):

- The AC acts as a DHCP server to assign IP addresses to the AP and clients.
- The AP provides wireless services **service1** and **service2** for Client 1 and Client 2, respectively.
- The AC forwards client traffic.

Configure multicast optimization so that Client 1 can receive video stream for multicast group 224.1.1.1 and Client 2 cannot receive the video stream.

Figure 1 Network diagram



Procedures

Configuring the AC

1. Configure interfaces on the AC:

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

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

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

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

Configure GigabitEthernet 1/0/1 as a trunk port. Remove the port from VLAN 1, assign the port to VLAN 100 and VLAN 200, and set the PVID to 100.

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

2. Configure DHCP:

Enable DHCP.

```
[AC] dhcp enable
```

Configure DHCP address pool **vlan100** and specify subnet 112.12.0.0/16 and gateway address 112.12.1.25 in the address pool.

```
[AC] dhcp server ip-pool vlan100
[AC-dhcp-pool-vlan100] network 112.12.0.0 mask 255.255.0.0
[AC-dhcp-pool-vlan100] gateway-list 112.12.1.25
[AC-dhcp-pool-vlan100] quit
```

Configure a DHCP address pool **vlan200**, specify subnet 112.13.0.0/16 and gateway address 112.13.1.25 in this address pool, and specify the gateway as the DNS server. Configure the DNS server according to the actual network plan.

```
[AC] dhcp server ip-pool vlan200
[AC-dhcp-pool-vlan200] network 112.13.0.0 mask 255.255.0.0
[AC-dhcp-pool-vlan200] gateway-list 112.13.1.25
[AC-dhcp-pool-vlan200] dns-list 112.13.1.25
[AC-dhcp-pool-vlan200] quit
```

3. Configure the AP:

NOTE:

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

Create an AP named **ap1**, and specify its model and serial ID.

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

4. Configure wireless services:

Create a service template named **service1**.

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

Set the SSID to **service1**.

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

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

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

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

```
[AC-wlan-st-service1] akm mode psk
```

```
[AC-wlan-st-service1] preshared-key pass-phrase simple 12345678
```

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

```
[AC-wlan-st-service1] cipher-suite ccmp
```

```
[AC-wlan-st-service1] security-ie rsn
```

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

```
[AC-wlan-st-service1] client forwarding-location ac
```

Enable WLAN multicast optimization.

```
[AC-wlan-st-service1] multicast-optimization enable
```

Enable the service template.

```
[AC-wlan-st-service1] service-template enable
```

```
[AC-wlan-st-service1] quit
```

Create a service template named **service2**.

```
[AC] wlan service-template service2
```

Set the SSID to **service2**.

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

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

```
[AC-wlan-st-service2] vlan 200
```

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

```
[AC-wlan-st-service2] akm mode psk
```

```
[AC-wlan-st-service2] preshared-key pass-phrase simple 12345678
```

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

```
[AC-wlan-st-service2] cipher-suite ccmp
```

```
[AC-wlan-st-service2] 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-service2] client forwarding-location ac
```

Enable the service template.

```
[AC-wlan-st-service2] service-template enable
```

```
[AC-wlan-st-service2] quit
```

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

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

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

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

Bind service template **service1** to radio 1.

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

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

```
service1 [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 service2 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
service2 [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
```

5. Configure multicast optimization:

Enable IGMP snooping globally.

```
[AC] igmp-snooping
[AC-igmp-snooping] quit
```

Enable IGMP snooping and then enable dropping unknown multicast data packets for VLAN 200.

```
[AC] vlan 200
[AC-vlan200] igmp-snooping enable
[AC-vlan200] igmp-snooping drop-unknown
[AC-vlan200] quit
```

Set the aging time to 300 seconds for IPv4 multicast optimization entries.

```
[AC] wlan multicast-optimization aging-time 300
```

Configure the AP to receive a maximum of 100 IGMP packets from clients every 60 seconds.

```
[AC] wlan multicast-optimization packet-rate-limit interval 60 threshold 100
```

Set the limit for IPv4 multicast optimization entries to 100.

```
[AC] wlan multicast-optimization global entry-limit 100
```

Set the limit for multicast optimization entries per client to 8.

```
[AC] wlan multicast-optimization client entry-limit 8
```

Set the maximum number of clients that WLAN multicast optimization supports to 10, and configure the AP to drop multicast packets when the number of clients reaches the threshold.

```
[AC] wlan multicast-optimization entry client-limit 10 drop
```

Configuring the switch

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

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

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

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

Configure GigabitEthernet 1/0/1 as a trunk port. Remove the port from VLAN 1, assign the port to VLAN 100, and set the PVID to VLAN 100.

```
[Switch] interface gigabitEthernet1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[Switch-GigabitEthernet1/0/1] port trunk pvid vlan 100
[Switch-GigabitEthernet1/0/1] quit
```

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

```
[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] port link-type access
[Switch-GigabitEthernet1/0/2] port access vlan 100
# Enable PoE.
[Switch-GigabitEthernet1/0/2] poe enable
[Switch-GigabitEthernet1/0/2] quit
```

Verifying the configuration

1. Connect Client 1 and Client 2 to wireless services **service1** and **service2**, respectively. (Details not shown.)

2. Verify that Client 1 can successfully associate with **service1**.

```
[AC] display wlan client service-template service1
Total number of clients: 1
```

MAC address	Username	AP name	RID	IP address	IPv6 address	VLAN
0024-d705-c600	N/A	ap1	1	112.13.1.26	N/A	200

3. Verify that Client 2 can successfully associate with **service2**.

```
[AC] display wlan client service-template service2
Total number of clients: 1
```

MAC address	Username	AP name	RID	IP address	IPv6 address	VLAN
0024-d710-18a4	N/A	ap1	2	112.13.1.27	N/A	200

4. Verify that Client 1 can successfully receive demanded video stream.

Demand video stream of multicast group 224.1.1.1 from Client 1. (Details not shown.)

Send video stream from the source to multicast group 224.1.1.1. (Details not shown.)

Display IGMP snooping group entries on the AC.

```
[AC] display igmp-snooping group
Total 1 entries.
```

VLAN 200: Total 1 entries.

(0.0.0.0, 224.1.1.1)

Host slots (0 in total):

Host ports (2 in total):

WLAN-BSS1/0/1

(00:02:45)

The output shows that WLAN-BSS 1/0/1 (connected to Client 1) is a member port of multicast group 224.1.1.1.

Display Layer 2 multicast fast forwarding entries on the AC.

```
[AC] display l2-multicast fast-forwarding cache
```

Total 1 entries, 1 matched

(1.1.1.100,224.1.1.1)

Status : Enable

VLAN : 200

Source port : 63

Destination port: 63

Protocol : 17

Flag : 0x2

Ingress port: GigabitEthernet1/0/1

List of 1 egress ports:

WLAN-BSS1/0/1

Status: Enable

Flag: 0x10

The output shows that only Client 1 can receive video stream of multicast group 224.1.1.1.

Configuration files

- AC:

```
#
igmp-snooping
#
dhcp enable
#
vlan 100
#
vlan 200
#
dhcp server ip-pool vlan100
    gateway-list 112.12.1.25
    network 112.12.0.0 mask 255.255.0.0
#
dhcp server ip-pool vlan200
    gateway-list 112.13.1.25
    network 112.13.0.0 mask 255.255.0.0
    dns-list 112.13.1.25
#
vlan 200
    igmp-snooping enable
    igmp-snooping drop-unknown
#
wlan service-template service1
    ssid service1
    vlan 200
    akm mode psk
    preshared-key pass-phrase simple 12345678
    cipher-suite ccmp
    security-ie rsn
    client forwarding-location ac
    multicast-optimization
    service-template enable
#
wlan service-template service2
    ssid service2
    vlan 200
    akm mode psk
    preshared-key pass-phrase simple 12345678
    cipher-suite ccmp
    security-ie rsn
    client forwarding-location ac
    service-template enable
```

```

#
interface Vlan-interface100
 ip address 112.12.1.25 255.255.0.0
#
interface Vlan-interface200
 ip address 112.13.1.25 255.255.0.0
#
wlan ap ap1 model AP 3620
 serial-id 219801A28N819CE0002T
#
wlan ap-group group1
 ap ap1
 ap-model AP 3620
 radio 1
 service-template service1
 radio enable
 radio 2
 service-template service2
 radio enable
#
wlan multicast-optimization aging-time 300
 wlan multicast-optimization client entry-limit 8
 wlan multicast-optimization entry client-limit 10 drop
 wlan multicast-optimization global entry-limit 100
 wlan multicast-optimization packet-rate-limit
#

```

- **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
 port trunk pvid vlan 100
#
interface GigabitEthernet1/0/2
 port access vlan 100
 poe enable
#

```

Related documentation

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

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

INTELBRAS Access Controllers

Client Rate Limiting 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 client rate limiting	1
Network configuration	1
Restrictions and guidelines	1
Procedures	1
Configuring the AC	1
Configuring the switch	3
Verifying the configuration	4
Configuration files	4
Related documentation	5

Introduction

The following information provides an example for configuring client rate limiting.

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.

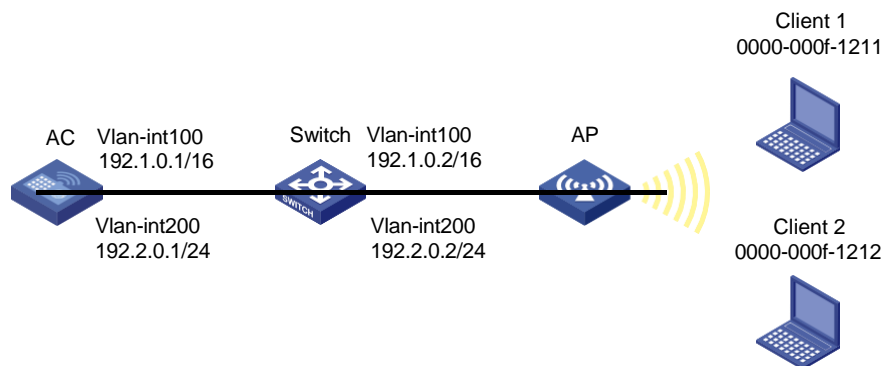
This document assumes that you have basic knowledge of client rate limiting.

Example: Configuring client rate limiting

Network configuration

As shown in [Figure 1](#), the switch acts as a DHCP server to assign IP addresses to the AP and the clients. The AC forwards client traffic. Configure service-template-based client rate limiting to limit both the incoming and outgoing traffic rates to 6000 Kbps in dynamic mode.

Figure 1 Network diagram



Restrictions and guidelines

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

Procedures

Configuring the AC

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

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

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

```
[AC] vlan 200
[AC-vlan200] quit
[AC] interface vlan-interface 200
[AC-Vlan-interface200] ip address 192.2.0.1 24
[AC-Vlan-interface200] quit
```

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

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

2. Configure wireless services:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Limit the client traffic rate in both directions to 6000 Kbps in dynamic mode, and enable client rate limiting for service template **service.**

```
[AC-wlan-st-service] client-rate-limit inbound mode dynamic cir 6000
```

```
[AC-wlan-st-service] client-rate-limit outbound mode dynamic cir 6000
```

Enable the service template.

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

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

3. Configure the AP:

NOTE:

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

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

```
[AC] wlan ap officeap model AP 3620
[AC-wlan-ap-officeap] serial-id 219801A28N819CE0002T
# Create AP group group1, add the AP to the AP group, and specify the AP model.
[AC] wlan ap-group group1
[AC-wlan-ap-group-group1] ap officeap
[AC-wlan-ap-group-group1] ap-model AP 3620
# Enter the view of radio 1.
[AC-wlan-ap-group-group1-ap-model-AP 3620] radio 1
# Bind service template service to radio 1, and enable radio 1.
[AC-wlan-ap-group-group1-ap-model-AP 3620-radio-1] service-template
service [AC-wlan-ap-group-group1-ap-model-AP 3620-radio-1] radio enable
[AC-wlan-ap-group-group1-ap-model-AP 3620-radio-1]
quit [AC-wlan-ap-group-group1-ap-model-AP 3620] quit
[AC-wlan-ap-group-group1] quit
```

Configuring the switch

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

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

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

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

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

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

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

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

Enable PoE on GigabitEthernet 1/0/2.

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

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

```
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ip address 192.1.0.2 16
[Switch-Vlan-interface100] quit
```

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

```
[Switch] interface vlan-interface 200
[Switch-Vlan-interface200] ip address 192.2.0.2 24
[Switch-Vlan-interface200] quit
```


Enable DHCP.

```
[Switch] dhcp enable
```

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

```
[Switch] dhcp server ip-pool 100
```

```
[Switch-dhcp-pool-100] network 192.1.0.0 mask 255.255.0.0
```

```
[Switch-dhcp-pool-100] gateway-list 192.1.0.1
```

```
[Switch-dhcp-pool-100] quit
```

Configure DHCP pool **200** to assign an IP address to clients. Specify the gateway address and DNS server address. In this example, the gateway also acts as a DNS server.

```
[Switch] dhcp server ip-pool 200
```

```
[Switch-dhcp-pool-200] network 192.2.0.0 mask 255.255.255.0
```

```
[Switch-dhcp-pool-200] gateway-list 192.2.0.1
```

```
[Switch-dhcp-pool-200] dns-list 192.2.0.1
```

```
[Switch-dhcp-pool-200] quit
```

Verifying the configuration

Verify that the incoming and outgoing traffic rates of client 1 and client 2 are both limited within 3000 Kbps. (Details not shown.)

Configuration files

- AC:

```
#
```

```
vlan 100
```

```
#
```

```
vlan 200
```

```
#
```

```
wlan service-template service
```

```
ssid service
```

```
vlan 200
```

```
akm mode psk
```

```
preshared-key pass-phrase simple 12345678
```

```
cipher-suite ccmp
```

```
security-ie rsn
```

```
client forwarding-location ac
```

```
client-rate-limit inbound mode dynamic cir 6000
```

```
client-rate-limit outbound mode dynamic cir 6000
```

```
service-template enable
```

```
#
```

```
interface Vlan-interface100
```

```
ip address 192.1.0.1 255.255.0.0
```

```
#
```

```
interface Vlan-interface200
```

```
ip address 192.2.0.1 255.255.255.0
```

```
#
```

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

```
port link-type trunk
```

```

port trunk permit vlan 1 100 200
#
wlan ap officeap model AP 3620
serial-id 219801A28N819CE0002T
#
wlan ap-group group1
ap officeap
ap-model AP 3620
radio 1
service-template service
radio enable
#

```

- **Switch:**

```

#
vlan 100
#
vlan 200
#
dhcp server ip-pool 100
gateway-list 192.1.0.1
network 192.1.0.0 mask 255.255.0.0
#
dhcp server ip-pool 200
gateway-list 192.2.0.1
network 192.2.0.0 mask 255.255.255.0
dns-list 192.2.0.1
#
interface Vlan-interface100
ip address 192.1.0.2 255.255.0.0
#
interface Vlan-interface200
ip address 192.2.0.2 255.255.255.0
#
interface GigabitEthernet1/0/1
port link-type trunk
port trunk permit vlan 1 100 200
#
interface GigabitEthernet1/0/2
port link-type access
port access permit vlan 100
poe enable
#

```

Related documentation

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

INTELBRAS Access Controllers Inter-AC Roaming 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.....	1
Network requirements	1
Configuration restrictions and guidelines.....	2
Configuration procedures	2
Configuring AC 1	2
Configuring AC 2	5
Configuring the switch	7
Configuring the RADIUS server	9
Verifying the configuration	12
Configuration files.....	14
Related documentation	18

Introduction

The following information provides an inter-AC roaming configuration example.

Prerequisites

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

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

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

Example: Configuring inter-AC roaming

Network requirements

As shown in [Figure 1](#), AP 1 and AP 2 are managed by AC 1 and AC 2, respectively. Clients associated with AC 1 belong to VLAN 200. Clients associated with AC 2 belong to VLAN 400.

Complete the following tasks:

- Configure inter-AC roaming to enable clients to roam between AP 1 and AP 2.
- Configure VLAN-based user isolation to improve user security and reduce radio resources consumption caused by multicast and broadcast packets.

Figure 1 Network diagram

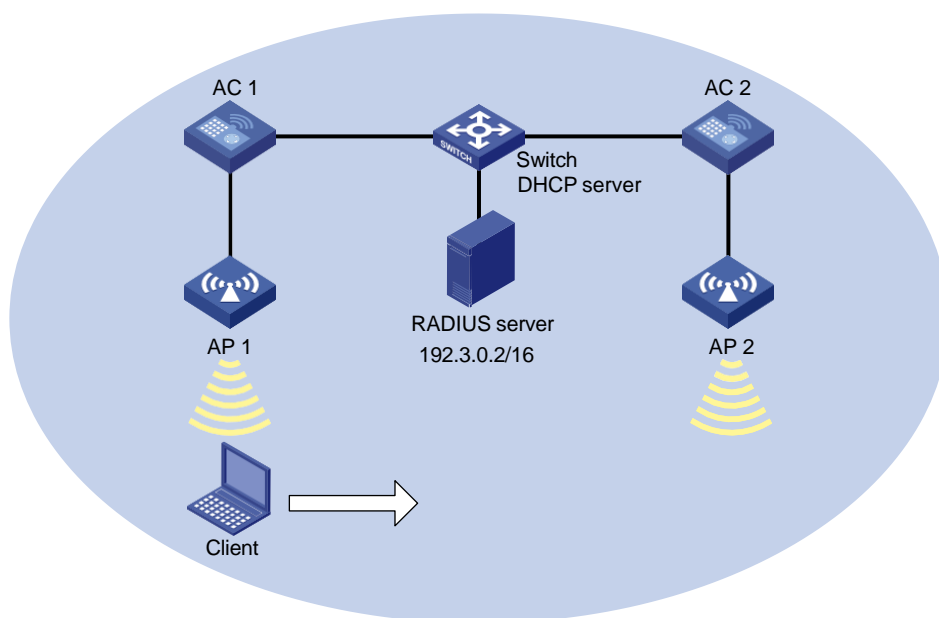


Table 1 Interface and IP address assignment

Device	Interface	IP address	Device	Interface	IP address
AC 1	VLAN-interface 100	192.1.0.2/16	Switch	VLAN-interface 100	192.1.0.1/16
	VLAN-interface 200	192.2.0.2/16		VLAN-interface 200	192.2.0.1/16
AC 2	VLAN-interface 100	192.1.0.3/16		VLAN-interface 300	192.3.0.1/16
	VLAN-interface 400	192.4.0.2/16		VLAN-interface 400	192.4.0.1/16

Configuration restrictions and guidelines

When you configure inter-AC roaming, follow these restrictions and guidelines:

- Configure the same SSID, authentication mode, AKE mode, and cipher suite for the service templates to be bound to the APs that are used during WLAN roaming.
- To implement fast roaming, configure RSN + 802.1X authentication for clients.
- Add the two ACs to the same mobility group.
- Use the actual serial ID of an AP to uniquely identify that AP.

Configuration procedures

Configuring AC 1

1. Configure interfaces on AC 1:

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

```
<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 an IP address to the VLAN interface. The AC will use VLAN 200 for client access.

```
[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 VLAN 400 to forward data of the client after the client roams from AP 2 to AP 1.

```
<AC1> system-view
[AC1] vlan 400
[AC1-vlan400] quit
```

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

Configure the interface that is connected to AP 1 as an access port, 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. Configure 802.1X authentication:

Set the EAP message handling method to EAP.

```
[AC1] dot1x authentication-method eap
```

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

```
[AC1] radius scheme office
```

Specify the server at 192.3.0.2 as the primary authentication server.

```
[AC1-radius-office] primary authentication 192.3.0.2
```

Specify the server at 192.3.0.2 as the primary accounting server.

```
[AC1-radius-office] primary accounting 192.3.0.2
```

Set the shared key to **12345678** for secure communication with the primary authentication server and accounting server.

```
[AC1-radius-office] key authentication simple 12345678
```

```
[AC1-radius-office] key accounting simple 12345678
```

Set the source IP address to 192.1.0.2 for outgoing RADIUS packets.

```
[AC1-radius-office] nas-ip 192.1.0.2
```

```
[AC1-radius-office] quit
```

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

```
[AC1] domain office
```

Configure the ISP domain to use RADIUS scheme **office** for authentication, authorization, and accounting of LAN users.

```
[AC1-isp-office] authentication lan-access radius-scheme office
```

```
[AC1-isp-office] authorization lan-access radius-scheme office
```

```
[AC1-isp-office] accounting lan-access radius-scheme office
```

```
[AC1-isp-office] quit
```

3. Configure the wireless service:

Create service template 1 and enter its view.

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

Set the SSID to **service**.

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

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

```
[AC1-wlan-st-1] vlan 200
```

Use the AC to forward client traffic.

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

Set the AKE mode to 802.1X.

```
[AC1-wlan-st-1] akm mode dot1x
```

Set the authentication mode to 802.1X for wireless clients.

```
[AC1-wlan-st-1] client-security authentication-mode dot1x
```

Specify ISP domain **office** as the authentication domain for 802.1X clients.

```
[AC1-wlan-st-1] dot1x domain office
```

Specify AES-CCMP as the cipher suite used for frame encryption.

```
[AC1-wlan-st-1] cipher-suite ccmp
```

Enable the RSN IE in beacon and probe responses.

```
[AC1-wlan-st-1] security-ie rsn
```

Enable the service template.

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

```
[AC1-wlan-st-1] quit
```

4. Configure an AP:

NOTE:

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

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

```
[AC1] wlan ap ap1 model AP 3620
```

```
[AC1-wlan-ap-ap1] serial-id 219801A28N819CE0002X
```

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

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

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

```
[AC1-wlan-ap-group-group1] ap-model AP 3620
```

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

```
[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 [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 WLAN roaming:

Create mobility group 1.

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

Set the source IP address for establishing IACTP tunnels to 192.1.0.2.

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

Add AC 2 to the mobility group.

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

Enable the mobility group.

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

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

6. Configure user isolation:

Enable user isolation for VLAN 200.

```
[AC1] user-isolation vlan 200 enable
```

Specify the MAC address of the gateway for VLAN 200 as a permitted MAC address for VLAN 200.

```
[AC1] user-isolation vlan 200 permit-mac 000f-e212-7788
```

7. Configure a default route:

Configure a default route for AC 1. Set the next hop to 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 interfaces on AC 2:

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

```
<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 VLAN 200 to forward data of the client after the client roams from AP 1 to AP 2.

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

Create VLAN 400 and VLAN-interface 400, and assign an IP address to the VLAN interface. The AC will use VLAN 400 for client access.

```
[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
```

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

Configure the interface that is connected to AP 2 as an access port, 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. Configure 802.1X authentication:

Set the EAP message handling method to EAP.

```
[AC2] dot1x authentication-method eap
```

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

```
[AC2] radius scheme office
```

Specify the server at 192.3.0.2 as the primary authentication server.

```
[AC2-radius-office] primary authentication 192.3.0.2
```

Specify the server at 192.3.0.2 as the primary accounting server.

```
[AC2-radius-office] primary accounting 192.3.0.2
```

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

```
[AC2-radius-office] key authentication simple 12345678
```

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

```
[AC2-radius-office] key accounting simple 12345678
```

Set the source IP address to 192.1.0.3 for outgoing RADIUS packets.

```
[AC2-radius-office] nas-ip 192.1.0.3
```

```
[AC2-radius-office] quit
```

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

```
[AC2] domain office
```

Configure the ISP domain to use RADIUS scheme **office** for authentication, authorization, and accounting of LAN users.

```
[AC2-isp-office] authentication lan-access radius-scheme office
```

```
[AC2-isp-office] authorization lan-access radius-scheme office
```

```
[AC2-isp-office] accounting lan-access radius-scheme office
```

```
[AC2-isp-office] quit
```

3. Configure the wireless service:

Create service template 1 and enter its view.

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

Set the SSID to **service**.

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

Assign clients coming online through the service template to VLAN 400.

```
[AC2-wlan-st-1] vlan 400
```

Use the AC to forward client traffic.

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

Set the AKE mode to 802.1X.

```
[AC2-wlan-st-1] akm mode dot1x
```

Set the authentication mode to 802.1X for wireless clients.

```
[AC2-wlan-st-1] client-security authentication-mode dot1x
```

Specify ISP domain **office** as the authentication domain for 802.1X clients.

```
[AC2-wlan-st-1] dot1x domain office
```

Specify AES-CCMP as the cipher suite used for frame encryption.

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

Enable the RSN IE in beacon and probe responses.

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

Enable the service template.

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

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

4. Configure an AP:

NOTE:

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

Create an AP named **ap2**, and specify its model and the serial ID.

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

```
[AC2-wlan-ap-ap2] serial-id 219801A28N819CE0002T
```

Create AP group named **group2**, and add a grouping rule by AP name to add AP **ap2** to the group.

```
[AC2] wlan ap-group group2
```

```
[AC2-wlan-ap-group-group2] ap ap2
```

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

```
[AC2-wlan-ap-group-group2] ap-model AP 3620
```

```
[AC2-wlan-ap-group-group2-ap-model-AP 3620] radio 1
[AC2-wlan-ap-group-group2-ap-model-AP 3620-radio-1] service-template
1 [AC2-wlan-ap-group-group2-ap-model-AP 3620-radio-1] radio enable
[AC2-wlan-ap-group-group2-ap-model-AP 3620-radio-1]
quit [AC2-wlan-ap-group-group2-ap-model-AP 3620] quit
[AC2-wlan-ap-group-group2] quit
```

5. Configure WLAN roaming:

Create mobility group 1.

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

Set the source IP address for establishing IACTP tunnels to 192.1.0.3.

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

Add AC 1 to the mobility group.

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

Enable the mobility group.

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

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

6. Configure user isolation:

Enable user isolation for VLAN 400.

```
[AC2] user-isolation vlan 400 enable
```

Specify the MAC address of the gateway for VLAN 400 as a permitted MAC address for VLAN 400.

```
[AC2] user-isolation vlan 400 permit-mac 000f-eeee-1212
```

7. Configure a default route:

Configure a default route for AC 2. Set the next hop to 192.1.0.1.

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

Configuring the switch

1. Configure interfaces on the switch:

Create VLAN 100 and VLAN-interface 100, and assign an IP address to the VLAN interface. The switch will use VLAN 100 to forward the traffic on CAPWAP tunnels between the AC and APs.

```
<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 an IP address to the VLAN interface. The switch will use VLAN 200 to forward client traffic of 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 an IP address to the VLAN interface. The switch will use VLAN 400 to forward client traffic of 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
```

Create VLAN 300 and VLAN-interface 300, and assign an IP address to the VLAN interface. The switch will use VLAN 300 to forward traffic to the RADIUS server.

```
[Switch] vlan 300
[Switch-vlan300] quit
[Switch] interface vlan-interface 300
[Switch-Vlan-interface300] ip address 192.3.0.1 16
[Switch-Vlan-interface300] quit
```

Configure the interface that is connected to AC 1 as a trunk port, and assign the port to VLAN 100, VLAN 200, and VLAN 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
```

Configure the interface that is connected to AC 2 as a trunk port, and assign the port to VLAN 100, VLAN 200, and VLAN 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
```

Configure the interface that is connected to the RADIUS server as an access port, and assign the port to VLAN 300.

```
[Switch] interface gigabitethernet 1/0/3
[Switch-GigabitEthernet1/0/3] port link-type access
[Switch-GigabitEthernet1/0/3] port access vlan 300
[Switch-GigabitEthernet1/0/3] quit
```

2. Configure the DHCP server:

Enable the DHCP service.

```
[Switch] dhcp enable
```

Create a DHCP address pool named **vlan100 for the APs. Specify the 192.1.0.0/16 subnet for the pool and exclude IP addresses 192.1.0.2 and 192.1.0.3 from dynamic allocation. Set the gateway IP address to 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 a DHCP address pool named **vlan200 for the clients. Specify the 192.2.0.0/16 subnet for the pool and exclude IP address 192.2.0.2 from dynamic allocation. Set the gateway IP address to 192.2.0.1 and specify the DNS server address. In this example, the gateway also acts as a 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 a DHCP address pool named **vlan400** for the clients. Specify the 192.4.0.0/16 subnet for the pool and exclude IP address 192.4.0.2 from dynamic allocation. Set the gateway IP address to 192.4.0.1 and specify the DNS server address. In this example, the gateway also acts as a 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
```

Configuring the RADIUS server

NOTE:

In this example, the RADIUS server runs on iNC PLAT 7.2 (E0403P06) and iNC INC - EIA 7.2 (E0409).

1. Add the ACs to the INC Platform as access devices:
 - a. Log in to INC.
 - b. Click the **User** tab.
 - c. From the navigation tree, select **User Access Policy > Access Device Management > Access Device**.
 - d. Click **Add** to add AC 1 as an access device.
 - e. Configure the following parameters:
 - Enter **192.1.0.2** for AC 1 and **192.1.0.3** for AC 2 in the **Device IP** field.
 - Enter **12345678** in the **Shared Key** field.
 - Use the default settings for other parameters.
 - f. Click **OK**.
 - g. Use the same procedure to add AC 2 as an access device.

Figure 2 Adding an access device

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

Access Configuration

Authentication Port *

1812

Accounting Port *

1813

Service Type

LAN Access Service

Forcible Logout Type

Disconnect user

Access Device Type

H3C (General)

Service Group

Ungrouped

Shared Key *

12345678

Access Device Group

--

Device List

Select

Add Manually

Add IPv6 Dev

Clear All

Device Name	Device IP	Device Model	Comments	Delete
	192.1.0.2			
	192.1.0.3			

Total Items: 2.

OK

Cancel

2. Add an access policy:
 - a. Click the **User** tab.
 - b. From the navigation tree, select **User Access Policy > Access Policy**.
 - c. Click **Add** to add an access policy that uses the following settings:
 - **Access Policy Name**—dot1x.
 - **Preferred EAP Type**—EAP-PEAP.
 - **Subtype**—EAP-MSCHAPv2. The subtype must match the client authentication method.

Figure 3 Adding an access policy

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

Basic Information

Access Policy Name *

Service Group *

Description

Authorization Information

Access Period	<input type="text" value="None"/>	Allocate IP *	<input type="text" value="No"/>
Downstream Rate (Kbps)	<input type="text"/>	Upstream Rate (Kbps)	<input type="text"/>
Priority	<input type="text"/>	Deploy User Group	<input type="text"/>
Preferred EAP Type	<input type="text" value="EAP-PEAP"/>	Subtype	<input type="text" value="EAP-MSCHAPv2"/>
EAP Auto Negotiate	<input type="text" value="Enable"/>	Maximum Online Duration for a Logon (Minutes)	<input type="text"/>
Deploy Address Pool	<input type="text"/>	Deploy VLAN	<input type="text"/>
<input type="checkbox"/> Deploy User Profile	<input type="text"/>		
<input type="checkbox"/> Deploy ACL			

3. Add an access service:
 - a. Click the **User** tab.
 - b. From the navigation tree, select **User Access Policy > Access Service**.
 - c. Click **Add** to add an access service that uses the following settings:
 - **Service Name**—dot1x.
 - **Default Access Policy**—dot1x.

Figure 4 Adding an access service

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

Basic Information

Service Name *

dot1x

Service Suffix

Service Group *

Ungrouped

Default Access Policy *

dot1x

Default Security Policy *

Do not use

Default Internet Access Policy *

Do not use

Default Proprietary Attribute Assignment Policy *

Do not use

Default Max. Devices for Single Account *

0

Default Max. Number of Online Endpoints *

0

Description

☒ Available

☐ Transparent Authentication

Access Scenario List

Add

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

OK Cancel

4. Add an access user:
 - a. Click the **User** tab.
 - b. From the navigation tree, select **All Access Users**.
 - c. Click **Add** to add an access user that uses the following settings:
 - **User Name**—user.
 - **Account Name**—dot1x.
 - **Password**—dot1x.
 - d. Select the **dot1x** service for the user.

Figure 5 Adding an access user

User > All Access Users > Add Access User Help

Access Information

User Name *

user

Select

Add User

Account Name *

dot1x

☐ Trial Account

☐ Default BYOD User

☐ MAC Authentication User

☐ Computer User

☐ Fast Access User

Password *

.....

Confirm Password *

.....

☒ Allow User to Change Password

☐ Enable Password Strategy

☐ Modify Password at Next Login

Start Time

End Time

Max. Idle Time (Minutes)

Max. Concurrent Logins

1

Login Message

Access Service

	Service Name	Service Suffix	Default Security Policy	Status	Allocate IP
<input checked="" type="checkbox"/>	dot1x		Do not use	Available	
<input type="checkbox"/>	manyou	emo2012b	Do not use	Available	
<input type="checkbox"/>	nodomain		Do not use	Available	
<input type="checkbox"/>	serv	system	Security PolicySecurity PolicySe	Available	

Verifying the configuration

Enable the client to come online from AP 1. (Details not shown.)

On AC 1, verify that the client is associated with AP 1.

```
<AC1> display wlan client verbose
```

Total number of clients: 1

MAC address	: 0015-00ba-0428
IPv4 address	: 192.2.0.3
IPv6 address	: N/A
Username	: dot1x
AID	: 1
AP ID	: 1
AP name	: ap1
Radio ID	: 1
SSID	: service
BSSID	: 5866-ba71-3960
VLAN ID	: 200
Sleep count	: 0
Wireless mode	: 802.11ac
Channel bandwidth	: 40MHz
SM power save	: Disabled
Short GI for 20MHz	: Supported
Short GI for 40MHz	: Supported
STBC RX capability	: Supported
STBC TX capability	: Not supported
LDPC RX capability	: Not supported
Block Ack	: N/A
Supported HT MCS set	: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15
Supported rates	: 6, 9, 12, 18, 24, 36, 48, 54 Mbps
QoS mode	: WMM
Listen interval	: 250
RSSI	: 0
Rx/Tx rate	: 0/0
Authentication method	: Open system
Security mode	: RSN
AKM mode	: 802.1X
Cipher suite	: CCMP
User authentication mode	: 802.1X
Authorization ACL ID	: N/A
Authorization user profile	: N/A
Roam status	: N/A
Key derivation	: SHA1
PMF status	: N/A
Forwarding policy name	: N/A

Online time : 0days 0hours 0minutes 17seconds
FT status : Inactive

Enable the client to roam to AP 2.

On AC 2, verify that the client is associated with AP 2.

<AC2> display wlan client verbose

Total number of clients: 1

MAC address	: 0015-00ba-0428
IPv4 address	: 192.2.0.3
IPv6 address	: N/A
Username	: dot1x
AID	: 1
AP ID	: 1
AP name	: ap2
Radio ID	: 1
SSID	: service
BSSID	: 5860-ba71-3960
VLAN ID	: 200
Sleep count	: 0
Wireless mode	: 802.11ac
Channel bandwidth	: 40MHz
SM power save	: Disabled
Short GI for 20MHz	: Supported
Short GI for 40MHz	: Supported
STBC RX capability	: Supported
STBC TX capability	: Not supported
LDPC RX capability	: Not supported
Block Ack	: N/A
Supported HT MCS set	: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15
Supported rates	: 6, 9, 12, 18, 24, 36, 48, 54 Mbps
QoS mode	: WMM
Listen interval	: 250
RSSI	: 0
Rx/Tx rate	: 0/0
Authentication method	: Open system
Security mode	: RSN
AKM mode	: 802.1X
Cipher suite	: CCMP
User authentication mode	: 802.1X
Authorization ACL ID	: N/A
Authorization user profile	: N/A
Roam status	: Inter-AC roam
Key derivation	: SHA1
PMF status	: N/A
Forwarding policy name	: N/A

Online time : 0days 0hours 0minutes 17seconds
FT status : Inactive

Verify that clients in VLAN 200 and VLAN 400 can access the Internet but cannot access a client in the same VLAN. (Details not shown.)

Configuration files

- Switch:

```
#
dhcp enable
#
vlan 100
#
vlan 200
#
vlan 300
#
vlan 400
#
dhcp server ip-pool vlan100
network 192.1.0.0 mask 255.255.0.0
gateway-list 192.1.0.1
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-interface300
ip address 192.3.0.1 255.255.0.0
#
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
#
interface GigabitEthernet1/0/3
 port access vlan 300
#
• AC 1:
#
dot1x authentication-method eap
#
vlan 100
#
vlan 200
#
vlan 400
#
wlan service-template 1
 ssid service
 vlan 200
 akm mode dot1x
 cipher-suite ccmp
 security-ie rsn
 client-security authentication-mode dot1x
 dot1x domain office
 service-template enable
#
interface Vlan-interface100
 ip address 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
#

```

```

radius scheme office
 primary authentication 192.3.0.2
 primary accounting 192.3.0.2
 key authentication simple 12345678
 key accounting simple 12345678
 nas-ip 192.1.0.2
#
domain office
 authentication lan-access radius-scheme office
 authorization lan-access radius-scheme office
 accounting lan-access radius-scheme office
#
user-isolation vlan 200 enable
user-isolation vlan 200 permit-mac 000f-e212-7788
#
wlan ap ap1 model AP 3620
 serial-id 219801A28N819CE0002X
#
wlan ap-group group1
 ap ap1
 ap-model AP 3620
 radio 1
 service-template 1
 radio enable
#
wlan mobility group 1
 source ip 192.1.0.2
 member ip 192.1.0.3
 group enable

```

- **AC 2:**

```

#
dot1x authentication-method eap
#
vlan 100
#
vlan 200
#
vlan 400
#
wlan service-template 1
 ssid service
 vlan 400
 akm mode dot1x
 cipher-suite ccmp
 security-ie rsn
 client-security authentication-mode dot1x
 dot1x domain office
 service-template enable

```

```

#
interface Vlan-interface100
 ip address 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
#
radius scheme office
 primary authentication 192.3.0.2
 primary accounting 192.3.0.2
 key authentication simple 12345678
 key accounting simple 12345678
 nas-ip 192.1.0.3
#
domain office
 authentication lan-access radius-scheme office
 authorization lan-access radius-scheme office
 accounting lan-access radius-scheme office
#
user-isolation vlan 400 enable
user-isolation vlan 400 permit-mac 000f-eeee-1212
#
wlan ap ap2 model AP 3620
 serial-id 219801A28N819CE0002T
#
wlan ap-group group2
 ap ap2
 ap-model AP 3620
 radio 1
 service-template 1
 radio enable
#
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*
- *WLAN Roaming Command Reference in INTELBRAS Access Controllers Command References*
- *WLAN Roaming Configuration Guide in INTELBRAS Access Controllers Configuration Guides*

INTELBRAS Access Controllers Inter-AC Roaming (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 inter-AC roaming.....	1
Network configuration.....	1
Restrictions and guidelines	2
Procedures	2
Configuring AC 1	2
Configuring AC 2	5
Configuring the switch	7
Configuring the RADIUS server	9
Verifying the configuration	11
Configuration files.....	14
Related documentation	18

Introduction

The following information provides an inter-AC roaming configuration example.

Prerequisites

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

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

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

Example: Configuring inter-AC roaming

Network configuration

As shown in [Figure 1](#), AP 1 and AP 2 are managed by AC 1 and AC 2, respectively. Clients associated with AC 1 belong to VLAN 200. Clients associated with AC 2 belong to VLAN 400.

Complete the following tasks:

- Configure all devices to use IPv6 addresses.
- Configure inter-AC roaming to enable clients to roam between AP 1 and AP 2.
- Configure VLAN-based user isolation to improve user security and reduce radio resources consumption caused by multicast and broadcast packets.

Figure 1 Network diagram

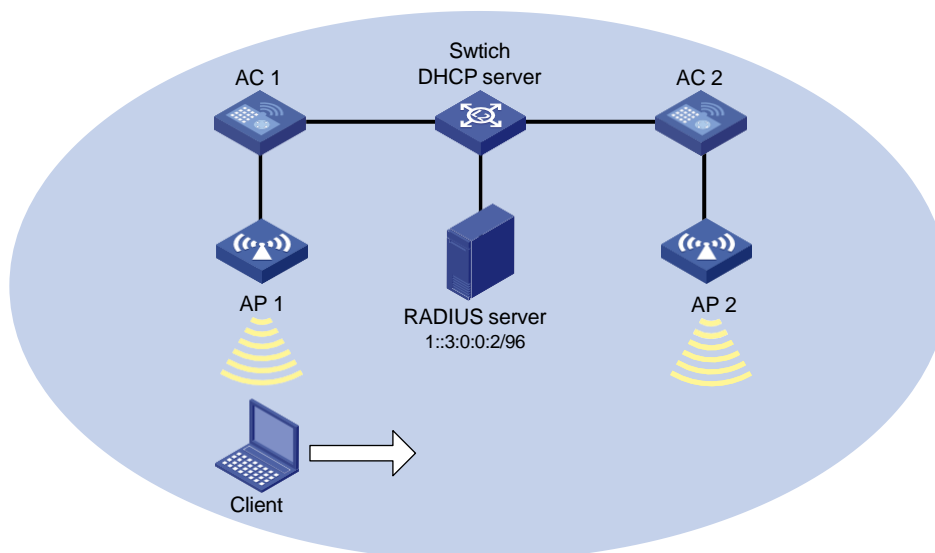


Table 1 Interface and IPv6 address assignment

Device	Interface	IPv6 address
AC 1	VLAN-interface 100	1::1:0:0:2/96
	VLAN-interface 200	1::2:0:0:2/96
AC 2	VLAN-interface 100	1::1:0:0:3/96
	VLAN-interface 400	1::4:0:0:2/96
Switch	VLAN-interface 100	1::1:0:0:1/96
	VLAN-interface 200	1::2:0:0:1/96
	VLAN-interface 300	1::3:0:0:1/96
	VLAN-interface 400	1::4:0:0:1/96

Restrictions and guidelines

When you configure inter-AC roaming, follow these restrictions and guidelines:

- Configure the same SSID, authentication mode, AKE mode, and cipher suite for the service templates to be bound to the APs that are used during WLAN roaming.
- For successful fast roaming, configure RSN + 802.1X authentication for clients.
- Add the two ACs to the same mobility group.
- Use the actual serial ID of an AP to uniquely identify that AP.

Procedures

Configuring AC 1

1. Configure interfaces on AC 1:

Create VLAN 100 and VLAN-interface 100, and assign an IPv6 address to the VLAN interface. The AC will use this IPv6 address to establish CAPWAP tunnels with APs.

```
<AC1> system-view
[AC1] vlan 100
[AC1-vlan100] quit
[AC1] interface vlan-interface 100
[AC1-Vlan-interface100] ipv6 address 1::1:0:0:2/96
[AC1-Vlan-interface100] quit
```

Create VLAN 200 and VLAN-interface 200, and assign an IPv6 address to the VLAN interface. The AC will use VLAN 200 for client access.

```
[AC1] vlan 200
[AC1-vlan200] quit
[AC1] interface vlan-interface 200
[AC1-Vlan-interface200] ipv6 address 1::2:0:0:2/96
[AC1-Vlan-interface200] quit
```

Create VLAN 400. The AC will use VLAN 400 to forward data of the client after the client roams from AP 2 to AP 1.

```
<AC1> system-view
[AC1] vlan 400
```

```
[AC1-vlan400] quit
```

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

Configure the interface that is connected to AP 1 as an access port, 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. Configure 802.1X authentication:

Set the EAP message handling method to EAP.

```
[AC1] dot1x authentication-method eap
```

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

```
[AC1] radius scheme office
```

Specify the server at 1::3:0:0:2 as the primary authentication server.

```
[AC1-radius-office] primary authentication ipv6 1::3:0:0:2
```

Specify the server at 1::3:0:0:2 as the primary accounting server.

```
[AC1-radius-office] primary accounting ipv6 1::3:0:0:2
```

Set the shared key to **12345678** for secure communication with the primary authentication server and accounting server.

```
[AC1-radius-office] key authentication simple 12345678
```

```
[AC1-radius-office] key accounting simple 12345678
```

Set the source IPv6 address to 1::1:0:0:2 for outgoing RADIUS packets.

```
[AC1-radius-office] nas-ip ipv6 1::1:0:0:2
```

```
[AC1-radius-office] quit
```

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

```
[AC1] domain office
```

Configure the ISP domain to use RADIUS scheme **office** for authentication, authorization, and accounting of LAN users.

```
[AC1-isp-office] authentication lan-access radius-scheme office
```

```
[AC1-isp-office] authorization lan-access radius-scheme office
```

```
[AC1-isp-office] accounting lan-access radius-scheme office
```

```
[AC1-isp-office] quit
```

3. Configure the wireless service:

Create service template 1 and enter its view.

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

Set the SSID to **service**.

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

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

```
[AC1-wlan-st-1] vlan 200
```

Use the AC to forward client traffic.

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

Set the AKE mode to 802.1X.

```
[AC1-wlan-st-1] akm mode dot1x
# Set the authentication mode to 802.1X for wireless clients.
[AC1-wlan-st-1] client-security authentication-mode dot1x
# Specify ISP domain office as the authentication domain for 802.1X clients.
[AC1-wlan-st-1] dot1x domain office
# Specify AES-CCMP as the cipher suite used for frame encryption.
[AC1-wlan-st-1] cipher-suite ccmp
# Enable the RSN IE in beacon and probe responses.
[AC1-wlan-st-1] security-ie rsn
# Enable the service template.
[AC1-wlan-st-1] service-template enable
# Enable snooping DHCPv6 and ND packets.
[AC1-wlan-st-1] client ipv6-snooping dhcpv6-learning enable
[AC1-wlan-st-1] client ipv6-snooping nd-learning enable
[AC1-wlan-st-1] quit
```

4. Configure an AP:

NOTE:

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

```
# Create an AP named ap1, and specify its model and the serial ID.
[AC1] wlan ap ap1 model AP 3620
[AC1-wlan-ap-ap1] serial-id 219801A28N819CE0002T
# Create AP group group1, and configure a grouping rule by AP name to add AP ap1 to the group.
[AC1] wlan ap-group group1
[AC1-wlan-ap-group-group1] ap ap1
# Bind service template 1 to radio 1, and enable radio 1.
[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 [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
```

5. Configure WLAN roaming:

```
# Create mobility group 1.
[AC1] wlan mobility group 1
# Set the source IPv6 address for establishing IACTP tunnels to 1::1:0:0:2.
[AC1-wlan-mg-1] source ipv6 1::1:0:0:2
# Add AC 2 to the mobility group.
[AC1-wlan-mg-1] member ipv6 1::1:0:0:3
# Specify the IP address type as IPv6 for IACTP tunnels.
[AC1-wlan-mg-1] tunnel-type ipv6
# Enable the mobility group.
[AC1-wlan-mg-1] group enable
[AC1-wlan-mg-1] quit
```

6. Configure user isolation:

Enable user isolation for VLAN 200.

```
[AC1] user-isolation vlan 200 enable
```

Specify the MAC address of the gateway for VLAN 200 as a permitted MAC address for VLAN 200.

```
[AC1] user-isolation vlan 200 permit-mac 000f-e212-7788
```

7. Configure a default route:

Configure a default route for AC 1. Set the next hop to 1::1:0:0:1.

```
[AC1] ipv6 route-static 0::0 96 1::1:0:0:1
```

Configuring AC 2

1. Configure interfaces on AC 2:

Create VLAN 100 and VLAN-interface 100, and assign an IPv6 address to the VLAN interface. The AC will use this IPv6 address to establish CAPWAP tunnels with APs.

```
<AC2> system-view
```

```
[AC2] vlan 100
```

```
[AC2-vlan100] quit
```

```
[AC2] interface vlan-interface 100
```

```
[AC2-Vlan-interface100] ipv6 address 1::1:0:0:3/96
```

```
[AC2-Vlan-interface100] quit
```

Create VLAN 200. The AC will use VLAN 200 to forward data of the client after the client roams from AP 1 to AP 2.

```
<AC2> system-view
```

```
[AC2] vlan 200
```

```
[AC2-vlan200] quit
```

Create VLAN 400 and VLAN-interface 400, and assign an IPv6 address to the VLAN interface. The AC will use VLAN 400 for client access.

```
[AC2] vlan 400
```

```
[AC2-vlan400] quit
```

```
[AC2] interface vlan-interface 400
```

```
[AC2-Vlan-interface400] ipv6 address 1::4:0:0:2/96
```

```
[AC2-Vlan-interface400] quit
```

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

Configure the interface that is connected to AP 2 as an access port, 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. Configure 802.1X authentication:

Set the EAP message handling method to EAP.

```
[AC2] dot1x authentication-method eap
```

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

```
[AC2] radius scheme office
# Specify the server at 1::3:0:0:2 as the primary authentication server.
[AC2-radius-office] primary authentication ipv6 1::3:0:0:2
# Specify the server at 1::3:0:0:2 as the primary accounting server.
[AC2-radius-office] primary accounting ipv6 1::3:0:0:2
# Set the shared key to 12345678 in plaintext form for secure authentication communication.
[AC2-radius-office] key authentication simple 12345678
# Set the shared key to 12345678 in plaintext form for secure accounting communication.
[AC2-radius-office] key accounting simple 12345678
# Set the source IPv6 address to 1::1:0:0:3 for outgoing RADIUS packets.
[AC2-radius-office] nas-ip ipv6 1::1:0:0:3
[AC2-radius-office] quit
# Create an ISP domain named office and enter its view.
[AC2] domain office
# Configure the ISP domain to use RADIUS scheme office for authentication, authorization,
and accounting of LAN users.
[AC2-isp-office] authentication lan-access radius-scheme office
[AC2-isp-office] authorization lan-access radius-scheme office
[AC2-isp-office] accounting lan-access radius-scheme office
[AC2-isp-office] quit
```

3. Configure the wireless service:

```
# Create service template 1 and enter its view.
[AC2] wlan service-template 1
# Set the SSID to service.
[AC2-wlan-st-1] ssid service
# Assign clients coming online through the service template to VLAN 400.
[AC2-wlan-st-1] vlan 400
# Use the AC to forward client traffic.
[AC1-wlan-st-1] client forwarding-location ac
# Set the AKE mode to 802.1X.
[AC2-wlan-st-1] akm mode dot1x
# Set the authentication mode to 802.1X for wireless clients.
[AC2-wlan-st-1] client-security authentication-mode dot1x
# Specify ISP domain office as the authentication domain for 802.1X clients.
[AC2-wlan-st-1] dot1x domain office
# Specify AES-CCMP as the cipher suite used for frame encryption.
[AC2-wlan-st-1] cipher-suite ccmp
# Enable the RSN IE in beacon and probe responses.
[AC2-wlan-st-1] security-ie rsn
# Enable the service template.
[AC2-wlan-st-1] service-template enable
# Enable snooping DHCPv6 and ND packets.
[AC2-wlan-st-1] client ipv6-snooping dhcpv6-learning enable
[AC2-wlan-st-1] client ipv6-snooping nd-learning enable
[AC2-wlan-st-1] quit
```

4. Configure an AP:

NOTE:

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

Create an AP named **ap2**, and specify its model and the serial ID.

```
[AC2] wlan ap ap2 model AP 3620
[AC2-wlan-ap-ap2] serial-id 219801A28N819CE0002T
```

Create AP group **group2**, and configure a grouping rule by AP name to add AP **ap2** to the group.

```
[AC2] wlan ap-group group2
[AC2-wlan-ap-group-group2] ap ap2
```

Bind service template 1 to radio 1, and enable radio 1.

```
[AC2-wlan-ap-group-group2] ap-model AP 3620
[AC2-wlan-ap-group-group2-ap-model-AP 3620] radio 1
[AC2-wlan-ap-group-group2-ap-model-AP 3620-radio-1] service-template
1 [AC2-wlan-ap-group-group2-ap-model-AP 3620-radio-1] radio enable
[AC2-wlan-ap-group-group2-ap-model-AP 3620-radio-1]
quit [AC2-wlan-ap-group-group2-ap-model-AP 3620] quit
```

5. Configure WLAN roaming:

Create mobility group 1.

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

Set the source IPv6 address for establishing IACTP tunnels to 1::1:0:0:3.

```
[AC2-wlan-mg-1] source ipv6 1::1:0:0:3
```

Add AC 1 to the mobility group.

```
[AC2-wlan-mg-1] member ipv6 1::1:0:0:2
```

Specify the IP address type as IPv6 for IACTP tunnels.

```
[AC1-wlan-mg-1] tunnel-type ipv6
```

Enable the mobility group.

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

6. Configure user isolation:

Enable user isolation for VLAN 400.

```
[AC2] user-isolation vlan 400 enable
```

Specify the MAC address of the gateway for VLAN 400 as a permitted MAC address for VLAN 400.

```
[AC2] user-isolation vlan 400 permit-mac 000f-eeee-1212
```

7. Configure a default route:

Configure a default route for AC 2. Set the next hop to 1::1:0:0:1.

```
[AC2] ipv6 route-static 0::0 96 1::1:0:0:1
```

Configuring the switch

1. Configure interfaces on the switch:

Create VLAN 100 and VLAN-interface 100, and assign an IPv6 address to the VLAN interface. The switch will use VLAN 100 to forward the traffic on CAPWAP tunnels between the AC and APs.

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

```
[Switch-vlan100] quit
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ipv6 address 1::1:0:0:1/96
[Switch-Vlan-interface100] quit
```

Create VLAN 200 and VLAN-interface 200, and assign an IPv6 address to the VLAN interface. The switch will use VLAN 200 to forward client traffic of AC 1.

```
[Switch] vlan 200
[Switch-vlan200] quit
[Switch] interface vlan-interface 200
[Switch-Vlan-interface200] ipv6 address 1::2:0:0:1/96
[Switch-Vlan-interface200] quit
```

Create VLAN 400 and VLAN-interface 400, and assign an IPv6 address to the VLAN interface. The switch will use VLAN 400 to forward client traffic of AC 2.

```
[Switch] vlan 400
[Switch-vlan400] quit
[Switch] interface vlan-interface 400
[Switch-Vlan-interface400] ipv6 address 1::4:0:0:1/96
[Switch-Vlan-interface400] quit
```

Create VLAN 300 and VLAN-interface 300, and assign an IPv6 address to the VLAN interface. The switch will use VLAN 300 to forward traffic to the RADIUS server.

```
[Switch] vlan 300
[Switch-vlan300] quit
[Switch] interface vlan-interface 300
[Switch-Vlan-interface300] ipv6 address 1::3:0:0:1/96
[Switch-Vlan-interface300] quit
```

Configure the interface that is connected to AC 1 as a trunk port, and assign the port to VLAN 100, VLAN 200, and VLAN 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
```

Configure the interface that is connected to AC 2 as a trunk port, and assign the port to VLAN 100, VLAN 200, and VLAN 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
```

Configure the interface that is connected to the RADIUS server as an access port, and assign the port to VLAN 300.

```
[Switch] interface gigabitethernet 1/0/3
[Switch-GigabitEthernet1/0/3] port link-type access
[Switch-GigabitEthernet1/0/3] port access vlan 300
[Switch-GigabitEthernet1/0/3] quit
```

2. Configure the DHCPv6 server:

Enable the DHCPv6 server on VLAN-interface 100, VLAN-interface 200, and VLAN-interface 300, and apply DHCPv6 address pools to the interfaces.

```
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ipv6 dhcp select server
[Switch-Vlan-interface100] ipv6 dhcp server apply pool 1
```



```
[Switch-Vlan-interface100] quit
[Switch] interface vlan-interface 200
[Switch-Vlan-interface200] ipv6 dhcp select server
[Switch-Vlan-interface200] ipv6 dhcp server apply pool 2
[Switch-Vlan-interface200] quit
[Switch] interface vlan-interface 400
[Switch-Vlan-interface400] ipv6 dhcp select server
[Switch-Vlan-interface400] ipv6 dhcp server apply pool 3
[Switch-Vlan-interface400] quit
```

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

```
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] undo ipv6 nd ra halt
[Switch-Vlan-interface100] ipv6 nd autoconfig managed-address-flag
[Switch-Vlan-interface100] ipv6 nd autoconfig other-flag
[Switch-Vlan-interface100] quit
[Switch] interface vlan-interface 200
[Switch-Vlan-interface200] undo ipv6 nd ra halt
[Switch-Vlan-interface200] ipv6 nd autoconfig managed-address-flag
[Switch-Vlan-interface200] ipv6 nd autoconfig other-flag
[Switch-Vlan-interface200] quit
[Switch] interface vlan-interface 400
[Switch-Vlan-interface400] undo ipv6 nd ra halt
[Switch-Vlan-interface400] ipv6 nd autoconfig managed-address-flag
[Switch-Vlan-interface400] ipv6 nd autoconfig other-flag
[Switch-Vlan-interface400] quit
```

Configure DHCPv6 address pool 1. Specify the subnet 1::1:0:0/96 and configure Option 52.

```
[Switch] ipv6 dhcp pool 1
[Switch-dhcp6-pool-1] network 1::1:0:0/96
[Switch-dhcp6-pool-1] option 52 hex 00010000000000000001000000000010
[Switch-dhcp6-pool-1] quit
```

Configure DHCPv6 address pool 2. Specify the subnet 1::2:0:0/96 and configure Option 52.

```
[Switch] ipv6 dhcp pool 2
[Switch-dhcp6-pool-2] network 1::2:0:0/96
[Switch-dhcp6-pool-1] option 52 hex 00010000000000000001000000000011
[Switch-dhcp6-pool-2] quit
```

Configure DHCPv6 address pool 3. Specify the subnet 1::4:0:0/96.

```
[Switch] ipv6 dhcp pool 3
[Switch-dhcp6-pool-3] network 1::4:0:0/96
[Switch-dhcp6-pool-3] quit
```

Configuring the RADIUS server

NOTE:

In this example, the RADIUS server runs on iNC PLAT 7.1 and iNC INC - EIA 7.1.

1. Add the ACs to the INC Platform as access devices:
 - a. Log in to INC.
 - b. Click the **User** tab.

- c. From the navigation tree, select **User Access Policy > Access Device Management > Access Device**.
- d. Click **Add** and perform the following tasks:
 - Enter **12345678** in the **Shared Key** field.
 - Add IPv6 addresses **1::1:0:0:2** and **1::1:0:0:3** to the **Device List**.
 - Use the default settings for other parameters.
- e. Click **OK**.

Figure 2 Adding access devices

Access Configuration

Authentication Port * 1812 Accounting Port * 1813

Service Type LAN Access Service

Access Device Type (General)

Shared Key * ***** Service Group Ungrouped

Confirm Shared Key * *****

Access Device Group --

Certificate Authentication ☒ None ☐ EAP

Certificate Type EAP-TLS Authn

Device List

Select Add Manually Add IPv6 Dev Clear All

Device Name	Device IP	Device Model	Comments	Delete
	0001:0000:0000:0000:0001:0000:0000:0002			
	0001:0000:0000:0000:0001:0000:0000:0003			

2. Add an access policy:
 - a. From the navigation tree, select **User Access Policy > Access Policy**.
 - b. Click **Add** to add an access policy that uses the following settings:
 - **Access Policy Name**—dot1x.
 - **Preferred EAP Type**—EAP-PEAP.
 - **Subtype**—EAP-MSCHAPv2. The subtype must match the client authentication method.

Figure 3 Adding an access policy

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

Basic Information

Access Policy Name * dot1x

Service Group * Ungrouped

Description

Authorization Information

Access Period None Allocate IP * No

Downstream Rate (Kbps) Upstream Rate (Kbps)

Priority Deploy User Group

Preferred EAP Type EAP-PEAP Subtype EAP-MSCHAPv2

EAP Auto Negotiate Enable Maximum Online Duration for a Logon (Minutes)

Deploy Address Pool Deploy VLAN

☐ Deploy User Profile

☐ Deploy ACL

3. Add an access service:
 - a. From the navigation tree, select **User Access Policy > Access Service**.
 - b. Click **Add** to add an access service that uses the following settings:
 - **Service Name**—dot1x.
 - **Default Access Policy**—dot1x.

Figure 4 Adding an access service

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

Basic Information

Service Name * dot1x Service Suffix

Service Group * Ungrouped Default Access Policy * dot1x

Default Proprietary Attribute Assignment Policy * Do not use

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

Description

☒ Available ☐ Transparent Authentication

4. Add an access user:
 - a. From the navigation tree, select **All Access Users**.
 - b. Click **Add** and perform the following tasks:
 - Click **Add User** to add a user with username **user**.
 - Set the **Account Name** to **dot1x**.
 - Set the **Password** to **dot1x**.
 - Select the **dot1x** service.

Figure 5 Adding an access user

User > All Access Users > Add Access User

Access Information

User Name * user Select Add User

Account Name * dot1x

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

Password * Password Confirm Password * Password

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

Start Time End Time

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

Login Message

Access Service

	Service Name	Service Suffix	Default Security Policy	Status	Allocate IP
<input checked="" type="checkbox"/>	dot1x		Do not use	Available	
<input type="checkbox"/>	manyou	emo2012b	Do not use	Available	
<input type="checkbox"/>	nodomain		Do not use	Available	
<input type="checkbox"/>	serv	system	Security PolicySecurity PolicySe	Available	

Verifying the configuration

- # Enable the client to come online from AP 1. (Details not shown.)
- # On AC 1, verify that the client is associated with AP 1.

<AC1> display wlan client verbose

Total number of clients: 1

MAC address	: 0015-00ba-0428
IPv4 address	: N/A
IPv6 address	: 1::2:0:0:2
Username	: dot1x
AID	: 1
AP ID	: 1
AP name	: ap1
Radio ID	: 1
SSID	: service
BSSID	: 5866-ba71-3960
VLAN ID	: 200
Sleep count	: 0
Wireless mode	: 802.11ac
Channel bandwidth	: 40MHz
SM power save	: Disabled
Short GI for 20MHz	: Supported
Short GI for 40MHz	: Supported
STBC RX capability	: Supported
STBC TX capability	: Not supported
LDPC RX capability	: Not supported
Beamformee STS capability	: 2
Number of Sounding Dimensions	: 1
SU beamformee capability	: Supported
MU beamformee capability	: Not supported
Block Ack	: N/A
Supported HT MCS set	: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15
Supported rates	: 6, 9, 12, 18, 24, 36, 48, 54 Mbps
QoS mode	: WMM
Listen interval	: 250
RSSI	: 0
Rx/Tx rate	: 0/0
Authentication method	: Open system
Security mode	: RSN
AKM mode	: 802.1X
Cipher suite	: CCMP
User authentication mode	: 802.1X
Authorization ACL ID	: N/A
Authorization user profile	: N/A
Roam status	: N/A
Key derivation	: SHA1
PMF status	: N/A
Forwarding policy name	: N/A

Online time : 0days 0hours 0minutes 17seconds
FT status : Inactive

Move the client toward AP 2 for the client to roam to AP 2.

On AC 2, verify that the client is associated with AP 2.

<AC2> display wlan client verbose

Total number of clients: 1

MAC address	: 0015-00ba-0428
IPv4 address	: N/A
IPv6 address	: 1::2:0:0:2
Username	: dot1x
AID	: 1
AP ID	: 1
AP name	: ap2
Radio ID	: 1
SSID	: service
BSSID	: 5860-ba71-3960
VLAN ID	: 200
Sleep count	: 0
Wireless mode	: 802.11ac
Channel bandwidth	: 40MHz
SM power save	: Disabled
Short GI for 20MHz	: Supported
Short GI for 40MHz	: Supported
STBC RX capability	: Supported
STBC TX capability	: Not supported
LDPC RX capability	: Not supported
Beamformee STS capability	: 2
Number of Sounding Dimensions	: 1
SU beamformee capability	: Supported
MU beamformee capability	: Not supported
Block Ack	: N/A
Supported HT MCS set	: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15
Supported rates	: 6, 9, 12, 18, 24, 36, 48, 54 Mbps
QoS mode	: WMM
Listen interval	: 250
RSSI	: 0
Rx/Tx rate	: 0/0
Authentication method	: Open system
Security mode	: RSN
AKM mode	: 802.1X
Cipher suite	: CCMP
User authentication mode	: 802.1X
Authorization ACL ID	: N/A
Authorization user profile	: N/A

Roam status	: Inter-AC roam
Key derivation	: SHA1
PMF status	: N/A
Forwarding policy name	: N/A
Online time	: 0days 0hours 0minutes 17seconds
FT status	: Inactive

Verify that clients in VLAN 200 and VLAN 400 can access the Internet but cannot access a client in the same VLAN. (Details not shown.)

Configuration files

- Switch:

```
#
dhcp enable
#
vlan 100
#
vlan 200
#
vlan 300
#
vlan 400
#
ipv6 dhcp pool 1
 network 1::1:0:0/96
 option 52 hex 00010000000000000001000000000010
#
ipv6 dhcp pool 2
 network 1::2:0:0/96
 option 52 hex 00010000000000000001000000000011
#
ipv6 dhcp pool 3
 network 1::4:0:0/96
#
interface Vlan-interface100
 ipv6 dhcp select server
 ipv6 dhcp server apply pool 1
 ipv6 address 1::1:0:0:1/96
 ipv6 nd autoconfig managed-address-flag
 ipv6 nd autoconfig other-flag
 undo ipv6 nd ra halt
#
interface Vlan-interface200
 ipv6 dhcp select server
 ipv6 dhcp server apply pool 2
 ipv6 address 1::2:0:0:1/96
 ipv6 nd autoconfig managed-address-flag
 ipv6 nd autoconfig other-flag
```

```

undo ipv6 nd ra halt
#
interface Vlan-interface300
  ipv6 address 1::3:0:0:1/96
#
interface Vlan-interface400
  ipv6 dhcp select server
  ipv6 dhcp server apply pool 3
  ipv6 address 1::4:0:0:1/96
  ipv6 nd autoconfig managed-address-flag
  ipv6 nd autoconfig other-flag
  undo ipv6 nd ra halt
#
interface GigabitEthernet1/0/1
  port link-type trunk
  port trunk permit vlan 100 200 400
#
interface GigabitEthernet1/0/2
  port link-type trunk
  port trunk permit vlan 100 200 400
#
interface GigabitEthernet1/0/3
  port access vlan 300
#

```

- **AC 1:**

```

#
dot1x authentication-method eap
#
vlan 100
#
vlan 200
#
vlan 400
#
wlan service-template 1
  ssid service
  client ipv6-snooping nd-learning enable
  client ipv6-snooping dhcpv6-learning enable
  vlan 200
  akm mode dot1x
  cipher-suite ccmp
  security-ie rsn
client-security authentication-mode dot1x
  dot1x domain office
  service-template enable
#
interface Vlan-interface100
  ipv6 address 1::1:0:0:2/96

```

```

#
interface Vlan-interface200
  ipv6 address 1::2:0:0:2/96
#
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
#
ipv6 route-static 0::0 96 1::1:0:0:1
#
radius scheme office
  primary authentication ipv6 1::3:0:0:2
  primary accounting ipv6 1::3:0:0:2
  key authentication simple 12345678
  key accounting simple 12345678
  nas-ip ipv6 1::1:0:0:2
#
domain office
  authentication lan-access radius-scheme office
  authorization lan-access radius-scheme office
  accounting lan-access radius-scheme office
#
user-isolation vlan 200 enable
user-isolation vlan 200 permit-mac 000f-e212-7788
#
wlan ap ap1 model AP 3620
  serial-id 219801A28N819CE0002T
#
wlan ap-group group1
  ap ap1
  ap-model AP 3620
  radio 1
  service-template 1
  radio enable
#
wlan mobility group 1
  tunnel-type ipv6
  source ipv6 1::1:0:0:2
  member ipv6 1::1:0:0:3
  group enable

```

- **AC 2:**

```

#
dot1x authentication-method eap
#

```



```

vlan 100
#
vlan 200
#
vlan 400
#
wlan service-template 1
    ssid service
    client ipv6-snooping nd-learning enable
    client ipv6-snooping dhcpv6-learning enable
    vlan 400
    akm mode dot1x
    cipher-suite ccmp
    security-ie rsn

    client-security authentication-mode dot1x
    dot1x domain office
    service-template enable
#
interface Vlan-interface100
    ipv6 address 1::1:0:0:3/96
#
interface Vlan-interface400
    ipv6 address 1::4:0:0:2/96
#
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
#
ipv6 route-static 0::0 96 1::1:0:0:1
#
radius scheme office
    primary authentication ipv6 1::3:0:0:2
    primary accounting ipv6 1::3:0:0:2
    key authentication simple 12345678
    key accounting simple 12345678
    nas-ip ipv6 1::1:0:0:3
#
domain office
    authentication lan-access radius-scheme office
    authorization lan-access radius-scheme office
    accounting lan-access radius-scheme office
#
user-isolation vlan 400 enable

```

```
user-isolation vlan 400 permit-mac 000f-eeee-1212
#
wlan ap ap2 model AP 3620
    serial-id 219801A28N819CE0002T
#
wlan ap-group group2
ap ap2
ap-model AP 3620
radio 1
service-template 1
radio enable
#
wlan mobility group 1
    tunnel-type ipv6
    source ipv6 1::1:0:0:3
    member ipv6 1::1:0:0:2
    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*

INTELBRAS Access Controllers

Inter-AC Roaming in Local Forwarding Mode

Configuration Examples

Copyright © 2024 Intelbras S.A All rights reserved.

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

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

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

Contents

Introduction	1
Prerequisites	1
Example: Configuring inter-AC roaming in local forwarding mode.....	1
Network configuration.....	1
Analysis	2
Restrictions and guidelines	2
Procedures	3
Configuring the configuration files.....	3
Configuring AC 1	3
Configuring AC 2.....	5
Configuring switch 1	8
Configuring switch 2.....	8
Configuring switch 3.....	9
Configuring the RADIUS server	11
Verifying the configuration	13
Configuration files.....	15
Related documentation	19

Introduction

The following information provides an example for configuring inter-AC roaming in local forwarding 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 roaming.

Example: Configuring inter-AC roaming in local forwarding mode

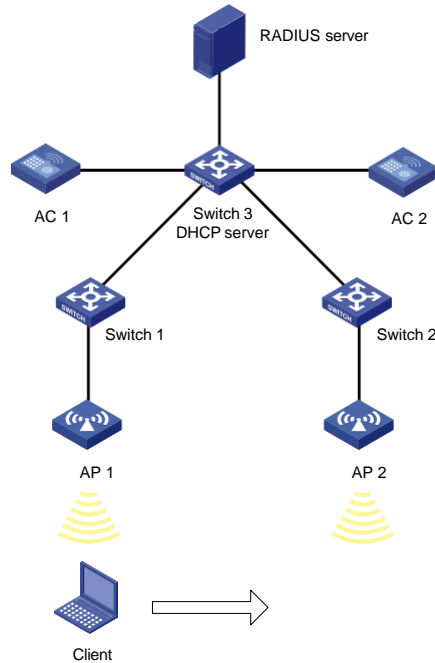
Network configuration

As shown in [Figure 1](#), AP 1 and AP 2 are managed by AC 1 and AC 2, respectively. Clients associated with AC 1 belong to VLAN 200. Clients associated with AC 2 belong to VLAN 400.

Complete the following tasks:

- Configure inter-AC roaming to enable clients to roam between AP 1 and AP 2.
- Enable local forwarding of client traffic.
- Configure VLAN-based user isolation to improve user security and reduce radio resource consumption caused by multicast and broadcast packets.

Figure 1 Network diagram



Device	Interface	IP address
AC 1	VLAN-interface 100	192.1.0.2/16
AC 2	VLAN-interface 100	192.1.0.3/16
Switch 3	VLAN-interface 100	192.1.0.1/16
	VLAN-interface 200	192.2.0.1/16
	VLAN-interface 300	192.3.0.1/16
	VLAN-interface 400	192.4.0.1/16

Analysis

- To implement inter-AC roaming, add the two ACs to the same mobility group.
- To implement fast roaming, configure RSN + 802.1X authentication for clients.
- A client will inherit the roaming VLAN when it roams between ACs, so you must assign the data forwarding links of the APs to all service VLANs.
- To assign the interfaces on the APs to the local forwarding service VLANs and configure VLAN-based isolation, execute the **map-configuration** command on the AC to deploy a configuration file to each AP.

Restrictions and guidelines

When you configure inter-AC roaming in local forwarding mode, 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.
- Make sure no Tab or space exists at the end of each command line in the configuration file to be deployed by using the **map-configuration** command.
- Use the serial ID labeled on the AP's rear panel to specify an AP.

Procedures

Configuring the configuration files

❗ IMPORTANT:

The configuration files are in .txt format and contain commands to be deployed to specific APs. To configure an AP, upload the AP configuration file to the AC and execute the **map-configuration** command after the AP establishes CAPWAP tunnels with the AC. The system then executes commands in the configuration file on the AP in sequence.

Assign the uplink interfaces on the APs to all service VLANs (VLAN 200 and VLAN 400), and specify the MAC address of the gateway as the permitted MAC address for the service VLANs.

Configure the configuration file of AP 1 as follows:

```
system-view
vlan 200
quit
vlan 400
quit
interface GigabitEthernet 1/0/1
port link-type trunk
port trunk permit vlan 200 400
quit
user-isolation vlan 200 permit-mac 000f-e212-7788
user-isolation vlan 200 enable
```

Configure the configuration file of AP 2 as follows:

```
system-view
vlan 200
quit
vlan 400
quit
interface GigabitEthernet 1/0/1
port link-type trunk
port trunk permit vlan 200 400
quit
user-isolation vlan 400 permit-mac 000f-e212-7788
user-isolation vlan 400 enable
```

Configuring AC 1

1. Configure interfaces on AC 1:

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
```

Configure interface GigabitEthernet 1/0/1 that connects AC 1 to Switch 3 as an access port, and assign the port to VLAN 100.

```
[AC1] interface gigabitethernet 1/0/1
```

```
[AC1-GigabitEthernet1/0/1] port link-type access
```

```
[AC1-GigabitEthernet1/0/1] port access vlan 100
```

```
[AC1-GigabitEthernet1/0/1] quit
```

2. Configure 802.1X authentication:

Set the 802.1X authentication method to EAP.

```
[AC1] dot1x authentication-method eap
```

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

```
[AC1] radius scheme office
```

Specify the IP address of the primary RADIUS authentication server as 192.3.0.2.

```
[AC1-radius-office] primary authentication 192.3.0.2
```

Specify the IP address of the primary RADIUS accounting server as 192.3.0.2.

```
[AC1-radius-office] primary accounting 192.3.0.2
```

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

```
[AC1-radius-office] key authentication simple 12345678
```

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

```
[AC1-radius-office] key accounting simple 12345678
```

Specify 192.1.0.2 as the NAS IPv4 address of RADIUS packets.

```
[AC1-radius-office] nas-ip 192.1.0.2
```

```
[AC1-radius-office] quit
```

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

```
[AC1] domain office
```

Perform RADIUS authentication for LAN users based on scheme **office**.

```
[AC1-isp-office] authentication lan-access radius-scheme office
```

Perform RADIUS authorization for LAN users based on scheme **office**.

```
[AC1-isp-office] authorization lan-access radius-scheme office
```

Perform RADIUS accounting for LAN users based on scheme **office**.

```
[AC1-isp-office] accounting lan-access radius-scheme office
```

```
[AC1-isp-office] quit
```

3. Configure wireless access services:

Create wireless service template 1 and enter its view.

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

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

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

Assign the service template to VLAN 200.

```
[AC1-wlan-st-1] vlan 200
```

Configure APs to forward client data traffic.

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

Set the authentication and key management mode to 802.1X.

```
[AC1-wlan-st-1] akm mode dot1x
```

Set the user access authentication mode to 802.1X authentication.

```
[AC1-wlan-st-1] client-security authentication-mode dot1x
```


Specify ISP domain **office** as the authentication domain for 802.1X clients in service template 1.

```
[AC1-wlan-st-1] dot1x domain office
```

Set the cipher suite to AES-CCMP.

```
[AC1-wlan-st-1] cipher-suite ccmp
```

Enable the RSN IE in beacon and probe responses.

```
[AC1-wlan-st-1] security-ie rsn
```

Enable the service template.

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

```
[AC1-wlan-st-1] quit
```

4. Configure APs:

! IMPORTANT:

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

Create AP **ap1**, and specify its model and serial number.

```
[AC1] wlan ap ap1 model AP 3620
```

```
[AC1-wlan-ap-ap1] serial-id 219801A28N819CE0002T
```

Create AP group **group1**, create an AP grouping rule by AP names and an AP grouping rule by AP models, bind wireless service template 1 to radio 1, and enable radio 1.

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

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

```
[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] radio enable
```

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

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

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

5. Configuring roaming:

Create mobility group 1 and enter its view.

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

Specify 192.1.0.2 as the source IP address for establishing IACTP tunnels.

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

Configure AC 1 as a member of mobility group 1, and specify 192.1.0.3 as the source IP address for establishing IACTP tunnels.

```
[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 the default route:

Configure the next hop of the default route to AC 1 as 192.1.0.1. The default route is used for the communication between AC 1 and the RADIUS server.

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

Configuring AC 2

1. Configure interfaces on AC 2:

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
```

Configure interface GigabitEthernet 1/0/1 that connects AC 2 to Switch 3 as an access port, and assign the port to VLAN 100.

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

2. Configure 802.1X authentication:

Set the 802.1X authentication method to EAP.

```
[AC2] dot1x authentication-method eap
```

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

```
[AC2] radius scheme office
```

Specify the IP address of the primary RADIUS authentication server as 192.3.0.2.

```
[AC2-radius-office] primary authentication 192.3.0.2
```

Specify the IP address of the primary RADIUS accounting server as 192.3.0.2.

```
[AC2-radius-office] primary accounting 192.3.0.2
```

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

```
[AC2-radius-office] key authentication simple 12345678
```

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

```
[AC2-radius-office] key accounting simple 12345678
```

Specify 192.1.0.3 as the NAS IPv4 address of RADIUS packets.

```
[AC2-radius-office] nas-ip 192.1.0.3
```

```
[AC2-radius-office] quit
```

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

```
[AC2] domain office
```

Perform RADIUS authentication for LAN users based on scheme **office**.

```
[AC2-isp-office] authentication lan-access radius-scheme office
```

Perform RADIUS authorization for LAN users based on scheme **office**.

```
[AC2-isp-office] authorization lan-access radius-scheme office
```

Perform RADIUS accounting for LAN users based on scheme **office**.

```
[AC2-isp-office] accounting lan-access radius-scheme office
```

```
[AC2-isp-office] quit
```

3. Configure wireless access services:

Create wireless service template 1 and enter its view.

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

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

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

Assign the service template to VLAN 400.

```
[AC2-wlan-st-1] vlan 400
# Configure APs to forward client data traffic.
[AC2-wlan-st-1] client forwarding-location ap
# Set the authentication and key management mode to 802.1X.
[AC2-wlan-st-1] akm mode dot1x
# Set the user access authentication mode to 802.1X authentication.
[AC2-wlan-st-1] client-security authentication-mode dot1x
# Specify ISP domain office as the authentication domain for 802.1X clients in service template 1.
[AC2-wlan-st-1] dot1x domain office
# Set the cipher suite to AES-CCMP.
[AC2-wlan-st-1] cipher-suite ccmp
# Enable the RSN IE in beacon and probe responses.
[AC2-wlan-st-1] security-ie rsn
# Enable the service template.
[AC2-wlan-st-1] service-template enable
[AC2-wlan-st-1] quit
```

4. Configure APs:

❗ IMPORTANT:

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

Create AP **ap2**, and specify its model and serial number.

```
[AC2] wlan ap ap2 model AP 3620
[AC2-wlan-ap-ap2] serial-id 219801A28N819CE0002U
```

Create AP group **group2**, create an AP grouping rule by AP names and an AP grouping rule by AP models, bind wireless service template 1 to radio 1, and enable radio 1.

```
[AC2] wlan ap-group group2
[AC2-wlan-ap-group-group2] ap ap2
[AC2-wlan-ap-group-group2] ap-model AP 3620
[AC2-wlan-ap-group-group2-ap-model-AP 3620] radio 1
[AC2-wlan-ap-group-group2-ap-model-AP 3620-radio-1] radio enable
[AC2-wlan-ap-group-group2-ap-model-AP 3620-radio-1] service-template
1 [AC2-wlan-ap-group-group2-ap-model-AP 3620-radio-1] quit
[AC2-wlan-ap-group-group2-ap-model-AP 3620] quit
```

5. Configuring roaming:

Create mobility group 1 and enter its view.

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

Specify 192.1.0.3 as the source IP address for establishing IACTP tunnels.

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

Configure AC 2 as a member of mobility group 1, and specify 192.1.0.2 as the source IP address for establishing IACTP tunnels.

```
[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 the default route:

Configure the next hop of the default route to AC 2 as 192.1.0.1. The default route is used for the communication between AC 2 and the RADIUS server.

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

Configuring switch 1

Create VLAN 100. The switch will use VLAN 100 to forward packets between AC 1 and AP 1.

```
<Switch1> system-view
[Switch1] vlan 100
[Switch1-vlan100] quit
```

Create VLAN 200. The switch will use VLAN 200 to communicate with wireless clients on AC 1.

```
[Switch1] vlan 200
[Switch1-vlan200] quit
```

Create VLAN 400. The switch will use VLAN 400 to forward wireless client traffic when the client roams from AC 2 to AC 1.

```
[Switch1] vlan 400
[Switch1-vlan400] quit
```

Configure GigabitEthernet1/0/1 that connects switch 1 to switch 3 as a trunk port, and assign the port to VLANs 100, 200, and 400.

```
[Switch1] interface gigabitethernet 1/0/1
[Switch1-GigabitEthernet1/0/1] port link-type trunk
[Switch1-GigabitEthernet1/0/1] port trunk permit vlan 100 200 400
[Switch1-GigabitEthernet1/0/1] quit
```

Configure GigabitEthernet1/0/2 that connects switch 1 to AP 1 as a trunk port, and assign the port to VLANs 100, 200, and 400.

```
[Switch1] interface gigabitethernet 1/0/2
[Switch1-GigabitEthernet1/0/2] port link-type trunk
[Switch1-GigabitEthernet1/0/2] port trunk permit vlan 100 200 400
[Switch1-GigabitEthernet1/0/2] port trunk pvid 100
[Switch1-GigabitEthernet1/0/2] quit
```

Configuring switch 2

Create VLAN 100. The switch will use VLAN 100 to forward packets between AC 2 and AP 2.

```
<Switch2> system-view
[Switch2] vlan 100
[Switch2-vlan100] quit
```

Create VLAN 200. The switch will use VLAN 200 to forward wireless client traffic when the client roams from AC 1 to AC 2.

```
[Switch2] vlan 200
[Switch2-vlan200] quit
```

Create VLAN 400. The switch will use VLAN 400 to communicate with wireless clients on AC 2.

```
[Switch2] vlan 400
[Switch2-vlan400] quit
```

Configure GigabitEthernet1/0/1 that connects switch 2 to switch 3 as a trunk port, and assign the port to VLANs 100, 200, and 400.

```
[Switch2] interface gigabitethernet 1/0/1
[Switch2-GigabitEthernet1/0/1] port link-type trunk
```

```
[Switch2-GigabitEthernet1/0/1] port trunk permit vlan 100 200 400
[Switch2-GigabitEthernet1/0/1] quit
```

Configure GigabitEthernet1/0/2 that connects switch 2 to AP 2 as a trunk port, assign the port to VLANs 100, 200, and 400, and set the PVID to 100.

```
[Switch2] interface gigabitethernet 1/0/2
[Switch2-GigabitEthernet1/0/2] port link-type trunk
[Switch2-GigabitEthernet1/0/2] port trunk permit vlan 100 200 400
[Switch1-GigabitEthernet1/0/2] port trunk pvid 100
[Switch2-GigabitEthernet1/0/2] quit
```

Configuring switch 3

1. Configure interfaces on switch 3:

Create VLAN 100 and VLAN-interface 100, and assign IP address 192.1.0.1/16 to the interface. Switch 3 will use this IP address to communicate with AC 1 and AC 2.

```
<Switch3> system-view
[Switch3] vlan 100
[Switch3-vlan100] quit
[Switch3] interface vlan-interface 100
[Switch3-Vlan-interface100] ip address 192.1.0.1 16
[Switch3-Vlan-interface100] quit
```

Create VLAN 200 and VLAN-interface 200, and assign IP address 192.2.0.1/16 to the interface. Switch 3 will use this IP address to communicate with wireless clients on AC 1.

```
[Switch3] vlan 200
[Switch3-vlan200] quit
[Switch3] interface vlan-interface 200
[Switch3-Vlan-interface200] ip address 192.2.0.1 16
[Switch3-Vlan-interface200] quit
```

Create VLAN 400 and VLAN-interface 400, and assign IP address 192.4.0.1/16 to the interface. Switch 3 will use this IP address to communicate with wireless clients on AC 2.

```
[Switch3] vlan 400
[Switch3-vlan400] quit
[Switch3] interface vlan-interface 400
[Switch3-Vlan-interface400] ip address 192.4.0.1 16
[Switch3-Vlan-interface400] quit
```

Create VLAN 300 and VLAN-interface 300, and assign IP address 192.3.0.1/16 to the interface. Switch 3 will use this IP address to communicate with the RADIUS server.

```
[Switch3] vlan 300
[Switch3-vlan300] quit
[Switch3] interface vlan-interface 300
[Switch3-Vlan-interface300] ip address 192.3.0.1 16
[Switch3-Vlan-interface300] quit
```

Configure interface GigabitEthernet 1/0/1 that connects Switch 3 to AC 1 as an access port, and assign the port to VLAN 100.

```
[Switch3] interface gigabitethernet 1/0/1
[Switch3-GigabitEthernet1/0/1] port link-type access
[Switch3-GigabitEthernet1/0/1] port access vlan 100
[Switch3-GigabitEthernet1/0/1] quit
```

Configure interface GigabitEthernet 1/0/2 that connects Switch 3 to AC 2 as an access port, and assign the port to VLAN 100.

```
[Switch3] interface gigabitethernet 1/0/2
[Switch3-GigabitEthernet1/0/2] port link-type access
[Switch3-GigabitEthernet1/0/2] port access vlan 100
[Switch3-GigabitEthernet1/0/2] quit
```

Configure interface GigabitEthernet 1/0/3 that connects Switch 3 to Switch 1 as a trunk port, and assign the port to VLANs 100, 200, and 400.

```
[Switch3] interface gigabitethernet 1/0/3
[Switch3-GigabitEthernet1/0/3] port link-type trunk
[Switch3-GigabitEthernet1/0/3] port trunk permit vlan 100 200 400
[Switch3-GigabitEthernet1/0/3] quit
```

Configure interface GigabitEthernet 1/0/4 that connects Switch 3 to Switch 2 as a trunk port, and assign the port to VLANs 100, 200, and 400.

```
[Switch3] interface gigabitethernet 1/0/4
[Switch3-GigabitEthernet1/0/4] port link-type trunk
[Switch3-GigabitEthernet1/0/4] port trunk permit vlan 100 200 400
[Switch3-GigabitEthernet1/0/4] quit
```

Configure interface GigabitEthernet 1/0/5 that connects Switch 3 to the RADIUS server as an access port, and assign the port to VLAN 300.

```
[Switch3] interface gigabitethernet 1/0/5
[Switch3-GigabitEthernet1/0/5] port link-type access
[Switch3-GigabitEthernet1/0/5] port access vlan 300
[Switch3-GigabitEthernet1/0/5] quit
```

2. Configure the DHCP server:

Enable DHCP.

```
[Switch3] dhcp enable
```

Create a DHCP address pool named **vlan100 for the APs. Specify the 192.1.0.0/16 subnet for the pool and exclude IP addresses 192.1.0.2 and 192.1.0.3 from dynamic allocation. Set the gateway IP address to 192.1.0.1.**

```
[Switch3] dhcp server ip-pool vlan100
[Switch3-dhcp-pool-vlan100] network 192.1.0.0 mask 255.255.0.0
[Switch3-dhcp-pool-vlan100] forbidden-ip 192.1.0.2 192.1.0.3
[Switch3-dhcp-pool-vlan100] gateway-list 192.1.0.1
[Switch3-dhcp-pool-vlan100] quit
```

Create a DHCP address pool named **vlan200 for the clients. Specify the 192.2.0.0/16 subnet for the pool. Set the gateway IP address to 192.2.0.1 and specify the DNS server address. In this example, the gateway also acts as a DNS server.**

```
[Switch3] dhcp server ip-pool vlan200
[Switch3-dhcp-pool-vlan200] network 192.2.0.0 mask 255.255.0.0
[Switch3-dhcp-pool-vlan200] gateway-list 192.2.0.1
[Switch3-dhcp-pool-vlan200] dns-list 192.2.0.1
[Switch3-dhcp-pool-vlan200] quit
```

Create a DHCP address pool named **vlan400 for the clients. Specify the 192.4.0.0/16 subnet for the pool. Set the gateway IP address to 192.4.0.1 and specify the DNS server address. In this example, the gateway also acts as a DNS server.**

```
[Switch3] dhcp server ip-pool vlan400
[Switch3-dhcp-pool-vlan400] network 192.4.0.0 mask 255.255.0.0
[Switch3-dhcp-pool-vlan400] gateway-list 192.4.0.1
```

```
[Switch3-dhcp-pool-vlan400] dns-list 192.4.0.1
[Switch3-dhcp-pool-vlan400] quit
```

Configuring the RADIUS server

In this example, the RADIUS server runs on iNC PLAT 7.2(E0403) and iNC INC - EIA 7.2(E0403). To configure the RADIUS server:

1. Add the ACs to the INC Platform as access devices:
 - a. Log in to INC.
 - b. Click the **User** tab.
 - c. From the navigation tree, select **User Access Policy > Access Device Management > Access Device**.
 - d. Click **Add** to add AC 1 and AC 2 as access devices.
 - e. Configure the following parameters:
 - Enter **192.1.0.2** for AC 1 and **192.1.0.3** for AC 2 in the **Device IP** field.
 - Enter **12345678** in the **Shared Key** field.
 - Use the default settings for other parameters.
 - f. Click **OK**.

Figure 2 Adding access devices

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

Access Configuration

Authentication Port *	<input type="text" value="1812"/>	Accounting Port *	<input type="text" value="1813"/>
Service Type	<input type="text" value="LAN Access Service"/>	Forcible Logout Type	<input type="text" value="Disconnect user"/>
Access Device Type	<input type="text" value="(General)"/>	Service Group	<input type="text" value="Ungrouped"/>
Shared Key *	<input type="text" value="12345678"/>		
Access Device Group	<input type="text" value="--"/>		

Device List

Device Name	Device IP	Device Model	Comments	Delete
	192.1.0.2			🗑
	192.1.0.3			🗑

Total Items: 2.

2. Add an access policy:
 - a. Click the **User** tab.
 - b. From the navigation tree, select **User Access Policy > Access Policy**.
 - c. Click **Add** to add an access policy that uses the following settings:
 - **Access Policy Name**—dot1x.
 - **Preferred EAP Type**—EAP-PEAP.
 - **Subtype**—MS-CHAPV2. The subtype must match the client authentication method.

Figure 3 Adding an access policy

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

Basic Information

Access Policy Name *

dot1x

Service Group *

Ungrouped

Description

Authorization Information

Access Period

None

Allocate IP *

No

Downstream Rate (Kbps)

Upstream Rate (Kbps)

Priority

Deploy User Group

Preferred EAP Type

EAP-PEAP

Subtype

EAP-MSCHAPv2

EAP Auto Negotiate

Enable

Maximum Online Duration for a Logon (Minutes)

Deploy Address Pool

Deploy VLAN

☐ Deploy User Profile

☐ Deploy ACL

3. Add an access service:
 - a. Click the **User** tab.
 - b. From the navigation tree, select **User Access Policy > Access Service**.
 - c. Click **Add** to add an access service that uses the following settings:
 - **Service Name**—dot1x.
 - **Default Access Policy**—dot1x.

Figure 4 Adding an access service

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

Basic Information

Service Name *

dot1x

Service Group *

Ungrouped

Default Security Policy *

Do not use

Default Proprietary Attribute Assignment Policy *

Do not use

Service Suffix

Default Access Policy *

dot1x

Default Internet Access Policy *

Do not use

Default Max. Devices for Single Account *

0

Default Max. Number of Online Endpoints *

0

Description

☒ Available

☐ Transparent Authentication

Access Scenario List

Add

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

OK

Cancel

4. Add an access user:
 - a. Click the **User** tab.
 - b. From the navigation tree, select **All Access Users**.
 - c. Click **Add** to add an access user that uses the following settings:
 - **User Name**—user.

- **Account Name**—dot1x.
- **Password**—dot1x.

d. Select the **dot1x** service for the user.

Figure 5 Adding an access user

User > All Access Users > Add Access User Help

Access Information

User Name * Select Add User

Account Name * ?

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

Password * Confirm Password *

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

Start Time 🕒 End Time 🕒

Max. Idle Time (Minutes) Max. Concurrent Logins

Login Message

Access Service

	Service Name	Service Suffix	Default Security Policy	Status	Allocate IP
<input checked="" type="checkbox"/>	dot1x		Do not use	Available	
<input type="checkbox"/>	manyou	emo2012b	Do not use	Available	
<input type="checkbox"/>	nodomain		Do not use	Available	
<input type="checkbox"/>	serv	system	Security PolicySecurity PolicySe	Available	

Verifying the configuration

Make the client come online from AP 1. (Details not shown.)

On AC 1, verify that the client is associated with AP 1.

```
<AC1> display wlan client verbose
Total number of clients: 1
```

```
MAC address           : 0015-00ba-0428
IPv4 address          : 192.2.0.16
IPv6 address          : N/A
Username              : N/A
AID                   : 1
AP ID                 : 1
AP name               : ap1
Radio ID              : 1
SSID                  : service
BSSID                 : 5866-ba71-3960
VLAN ID               : 200
Sleep count           : 0
Wireless mode          : 802.11ac
Channel bandwidth      : 40MHz
SM power save         : Disabled
Short GI for 20MHz     : Supported
Short GI for 40MHz     : Supported
```

```

STBC RX capability           : Supported
STBC TX capability          : Not supported
LDPC RX capability          : Not supported
Block Ack                   : N/A
Supported HT MCS set        : 0, 1, 2, 3, 4, 5, 6, 7,
                             8, 9, 10, 11, 12, 13, 14,
                             15
Supported rates              : 6, 9, 12, 18, 24, 36,
                             48, 54 Mbps
QoS mode                    : WMM
Listen interval              : 250
RSSI                         : 0
Rx/Tx rate                  : 0/0
Authentication method       : Open system
Security mode                : RSN
AKM mode                    : 802.1X
Cipher suite                 : CCMP
User authentication mode     : 802.1X
Authorization ACL ID         : N/A
Authorization user profile   : N/A
Roam status                  : N/A
Key derivation                : SHA1
PMF status                   : N/A
Forwarding policy name       : N/A
Online time                  : 0days 0hours 0minutes 17seconds
FT status                    : Inactive

```

Make the client roam to AP 2.

On AC 2, verify that the client is associated with AP 2.

```
<AC2> display wlan client verbose
```

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

```

MAC address                  : 0015-00ba-0428
IPv4 address                  : 192.2.0.16
IPv6 address                  : N/A
Username                     : N/A
AID                           : 1
AP ID                         : 1
AP name                       : ap2
Radio ID                      : 1
SSID                          : service
BSSID                         : 5860-ba71-3960
VLAN ID                       : 200
Sleep count                   : 0
Wireless mode                 : 802.11ac
Channel bandwidth              : 40MHz
SM power save                 : Disabled
Short GI for 20MHz             : Supported
Short GI for 40MHz            : Supported

```

```

STBC RX capability           : Supported
STBC TX capability          : Not supported
LDPC RX capability          : Not supported
Block Ack                   : N/A
Supported HT MCS set        : 0, 1, 2, 3, 4, 5, 6, 7,
                             8, 9, 10, 11, 12, 13, 14,
                             15
Supported rates              : 6, 9, 12, 18, 24, 36,
                             48, 54 Mbps
QoS mode                    : WMM
Listen interval              : 250
RSSI                        : 0
Rx/Tx rate                  : 0/0
Authentication method       : Open system
Security mode                : RSN
AKM mode                     : 802.1X
Cipher suite                 : CCMP
User authentication mode     : 802.1X
Authorization ACL ID         : N/A
Authorization user profile   : N/A
Roam status                  : Inter-AC roam
Key derivation                : SHA1
PMF status                   : N/A
Forwarding policy name       : N/A
Online time                  : 0days 0hours 0minutes 17seconds
FT status                    : Inactive

```

Verify that clients in VLAN 200 and VLAN 400 can access the Internet but cannot access a client in the same VLAN. (Details not shown.)

Configuration files

- Switch 1:

```

#
vlan 100
#
vlan 200
#
vlan 400
#
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
 port trunk pvid 100
#

```

- **Switch 2:**

```
#
vlan 100
#
vlan 200
#
vlan 400
#
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
    port trunk pvid 100
#
```

- **Switch 3:**

```
#
dhcp enable
#
vlan 100
#
vlan 200
#
vlan 300
#
vlan 400
#
dhcp server ip-pool vlan100
    network 192.1.0.0 mask 255.255.0.0
    gateway-list 192.1.0.1
    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
#
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
#
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-interface300
 ip address 192.3.0.1 255.255.0.0
#
interface Vlan-interface400
 ip address 192.4.0.1 255.255.0.0
#
interface GigabitEthernet1/0/1
 port link-type access
 port access vlan 100
#
interface GigabitEthernet1/0/2
 port link-type access
 port trunk access 100
#
interface GigabitEthernet1/0/3
 port link-type trunk
 port trunk permit vlan 100 200 400
#
interface GigabitEthernet1/0/4
 port link-type trunk
 port trunk permit vlan 100 200 400
#
interface GigabitEthernet1/0/5
 port link-type access
 port access vlan 300

```

- **AC 1:**

```

#
dot1x authentication-method eap
#
vlan 100
#
wlan service-template 1
 ssid service
 vlan 200
 client forwarding-location ap
 akm mode dot1x
 cipher-suite ccmp
 security-ie rsn
 client-security authentication-mode dot1x
 dot1x domain office
 service-template enable
#
interface Vlan-interface100
 ip address 192.1.0.2 255.255.0.0
#

```

```

interface GigabitEthernet1/0/1
    port link-type access
    port access vlan 100
#
ip route-static 0.0.0.0 0.0.0.0 192.1.0.1
#
radius scheme office
    primary authentication 192.3.0.2
    primary accounting 192.3.0.2
    key authentication simple 12345678
    key accounting simple 12345678
    nas-ip 192.1.0.2
#
domain office
    authentication lan-access radius-scheme office
    authorization lan-access radius-scheme office
    accounting lan-access radius-scheme office
#
wlan ap ap1 model AP 3620
    serial-id 219801A28N819CE0002T
#
wlan ap-group group1
    ap ap1
    ap-model AP 3620
    radio 1
    radio enable
    service-template 1
#
wlan mobility group 1
    source ip 192.1.0.2
    member ip 192.1.0.3
    group enable
#

```

- **AC 2:**

```

#
dot1x authentication-method eap
#
vlan 100
#
wlan service-template 1
    ssid service
    vlan 400
    client forwarding-location ap
    akm mode dot1x
    cipher-suite ccmp
    security-ie rsn
    client-security authentication-mode dot1x
    dot1x domain office

```

```

service-template enable
#
interface Vlan-interface100
 ip address 192.1.0.3 255.255.0.0
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 100 200 400
#
ip route-static 0.0.0.0 0.0.0.0 192.1.0.1
#
radius scheme office
 primary authentication 192.3.0.2
 primary accounting 192.3.0.2
 key authentication simple 12345678
 key accounting simple 12345678
 nas-ip 192.1.0.3
#
domain office
 authentication lan-access radius-scheme office
 authorization lan-access radius-scheme office
 accounting lan-access radius-scheme office
#
wlan ap ap2 model AP 3620
 serial-id 219801A28N819CE0002U
#
wlan ap-group group2
 ap ap2
 ap-model AP 3620
 radio 1
 radio enable
 service-template 1
#
wlan mobility group 1
 source ip 192.1.0.3
 member ip 192.1.0.2
 group enable

```

Related documentation

- *AP Management Command Reference in INTELBRAS Access Controllers Command References*
- *AP 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*

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

INTELBRAS Access Controllers

Cooperative Roaming for 802.11v Clients

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 cooperative roaming for 802.11v clients	1
Network configuration	1
Analysis	2
Restrictions and guidelines	2
Procedures	2
Verifying the configuration	3
Configuration files	4
Related documentation	5

Introduction

The following information provides a cooperative roaming configuration example for 802.11v clients.

Prerequisites

NOTE:

802.11v is supported on Comware 7-based ACs of 5450 and later versions and Comware 9-based ACs of 1046P01 and later versions.

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 WLAN access and WLAN roaming.

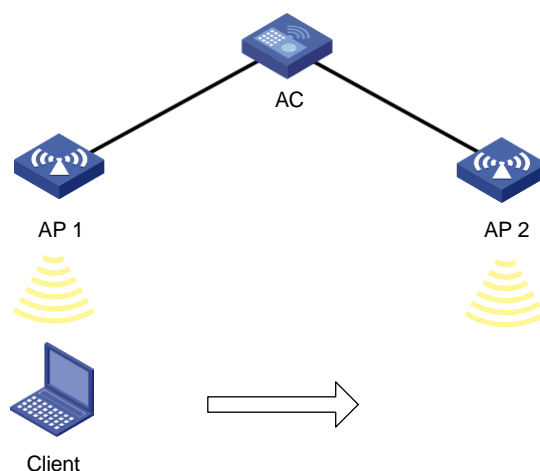
Example: Configuring cooperative roaming for 802.11v clients

Network configuration

As shown in [Figure 1](#), the AC manages AP 1 and AP 2 and an 802.11v client accesses the wireless network through AP 1.

Configure cooperative roaming on the AC to guide the client to roam to AP 2 when the RSSI is lower than 25 dBm.

Figure 1 Network diagram



Analysis

- To realize intra-AC roaming, you must apply the same wireless service template to AP 1 and AP 2.
- 802.11v cooperative roaming takes effect only on 802.11v clients. To view whether a client supports 802.11v, execute the **display wlan client verbose** command in any view on the AC after the client comes online. If the BTM field in the command output displays **active**, the client supports 802.11v.

```
[AC] display wlan client verbose | inc BTM
BTM mode                               : active
```

Restrictions and guidelines

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

Procedures

Configure the interfaces of the AC

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

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

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

```
[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 interface GigabitEthernet 1/0/1 that connects to AP 1 as an access port and assign the port to VLAN 100.

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

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

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

Configure a wireless service

Create service template 1 and enter its view.

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

```
# Set the SSID to service.
[AC-wlan-st-1] ssid service

# Set the VLAN to VLAN 200.
[AC-wlan-st-1] vlan 200

# Enable BSS transition management.
```

NOTE:

This feature can be configured only when the service template is disabled.

```
[AC-wlan-st-1] bss transition-management enable
```

```
# Enable the service template.
```

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

Configure AP settings

NOTE:

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

```
# Create manual AP officeap1 with model AP 3620 and SN 219801A28N819CE0002T.
```

```
[AC] wlan ap officeap1 model AP 3620
[AC-wlan-ap-officeap1] serial-id 219801A28N819CE0002T
[AC-wlan-ap-officeap1] quit
```

```
# Create manual AP officeap2 with model AP 3620 and SN 219801A28N819CE0002R.
```

```
[AC] wlan ap officeap2 model AP 3620
[AC-wlan-ap-officeap2] serial-id 219801A28N819CE0002R
[AC-wlan-ap-officeap2] quit
```

```
# Create AP group group1 and add AP officeap1 and AP officeap2 to the group.
```

```
[AC] wlan ap-group group1
[AC-wlan-ap-group-group1] ap officeap1 officeap2
```

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

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

```
# Enable client anti-sticky, set the RSSI threshold to 25 dBm, and set the detection interval to 6 seconds. Edit the parameters as needed. The device will detect the RSSI every 6 seconds and once the RSSI is below the threshold, the AC will guide the client for BSS transition.
```

```
[AC-wlan-ap-group-group1-ap-model-AP 3620-radio-2] sacp anti-sticky enable rssi 25
interval 6
```

```
# Enable radio 2.
```

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

Verifying the configuration

```
# Execute the display wlan sacp move-history command in any view on the AC to view the transition history of the client with MAC address 78AC-C0AF-944F. Verify that the client has roamed from AP officeap1 to AP officeap2.
```

```
<Sysname> display wlan sacp move-history mac-address 78AC-C0AF-944F
```

```
Total entries: 1
```

```
Current entries: 1
```

```
Current Clients: 1
```

Time	MAC address	AP name	Ch1	RSSI	Request/Response	Result
1/11 15:57:09	78AC-C0AF-944F	S:officeap1	6	25	1	/1 [1 ,0]
		T:officeap2	11			
1/11 15:57:10		A:officeap2	11	40		BTM-1

Configuration files

- AC

```
#
vlan 100
#
vlan 200
#
wlan service-template 1
    ssid service
    vlan 200
bss transition-management enable
service-template enable
#
interface Vlan-interface100
    ip address 192.1.1.1 255.255.255.0
#
interface Vlan-interface200
    ip address 192.2.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
    port link-type access
    port access vlan 100
#
interface GigabitEthernet1/0/2
    port link-type access
    port access vlan 100
#
wlan ap officeap1 model AP 3620
    serial-id 219801A28N819CE0002T
#
wlan ap officeap2 model AP 3620
    serial-id 219801A28N819CE0002R
#
wlan ap-group group1
    ap officeap1 officeap2
    ap-model AP 3620
radio 2
radio enable
```

```
service-template 1
sacp anti-sticky enable rssi 25 interval 6
```

Related documentation

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

INTELBRAS Access Controllers

WLAN Load Balancing 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 WLAN load balancing.....	1
Network requirements	1
Configuration restrictions and guidelines.....	2
Configuration procedures	2
Configuring the AC.....	2
Configuring the switch	4
Verifying the configuration	5
Configuration files.....	5
Related documentation	6

Introduction

The following information provides a WLAN load balancing configuration example.

Prerequisites

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

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

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

Example: Configuring WLAN load balancing

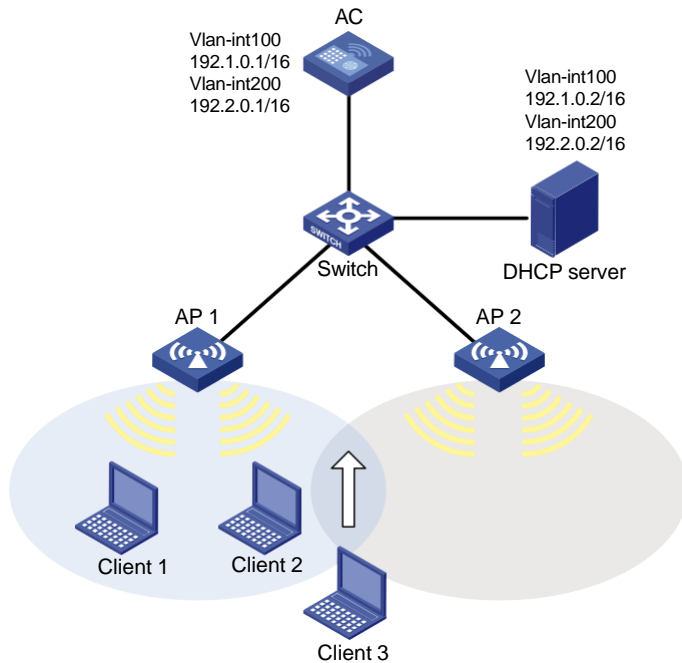
Network requirements

As shown in [Figure 1](#), the DHCP server assigns IP addresses to the APs and clients. AP 1 and AP 2 are managed by the AC and the clients can discover the APs.

Configure the AC to perform session-based load balancing on radio 2 of AP 1 and AP 2 when the following conditions are met:

- The number of sessions on one radio reaches 2.
- The session gap between the radios reaches 1.

Figure 1 Network diagram



Configuration restrictions and guidelines

When you configure WLAN load balancing, follow these restrictions and guidelines:

- Bind the same service template to the relevant APs.
- Configure the interface that the AC uses to connect to the network as a trunk port so the port can forward traffic from multiple VLANs.
- Use the actual serial ID of an AP to uniquely identify that AP.

Configuration procedures

Configuring the AC

1. Configure interfaces on the AC:

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

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

```
[AC] vlan 100
```

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

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

```
[AC-Vlan-interface100] ip address 192.1.0.1 16
```

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

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

```
[AC] vlan 200
```

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

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

```
[AC-Vlan-interface200] ip address 192.2.0.1 16
[AC-Vlan-interface200] quit
```

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

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

2. Configure the wireless service:

Create wireless service template 1 and enter its view.

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

Set the SSID to **service.**

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

Assign clients coming online through service template 1 to VLAN 200.

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

Set 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-st1] 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 the AP:

NOTE:

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

Create AP **officeap1, and specify its model and serial ID.**

```
[AC] wlan ap officeap1 model AP 3620
[AC-wlan-ap-officeap1] serial-id 219801A28N819CE0002X
```

Create AP **officeap2, and specify its model and serial ID.**

```
[AC] wlan ap officeap2 model AP 3620
[AC-wlan-ap-officeap2] serial-id 219801A28N819CE0002T
```

Create AP group **group1, add the APs to the AP group, and specify the AP model.**

```
[AC] wlan ap-group group1
[AC-wlan-ap-group-group1] ap officeap1 officeap2
[AC-wlan-ap-group-group1] ap-model AP 3620
```

Bind service template 1 to radio 2 of the AP and enable radio 2.

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

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

4. Configure load balancing:

Set the load balancing mode to session mode, and set the session threshold and session gap threshold to 2 and 1, respectively.

```
[AC] wlan load-balance mode session 2 gap 1
```

Create load balancing group 1 and enter its view.

```
[AC] wlan load-balance group 1
```

Add radio 2 of AP 1 and AP 2 to load balancing group 1.

```
[AC-wlan-lb-group-1] ap name officeap1 radio 2
```

```
[AC-wlan-lb-group-1] ap name officeap2 radio 2
```

Set the maximum number of denials to 5 for association requests.

```
[AC] wlan load-balance access-denial 5
```

Enable WLAN load balancing.

```
[AC] wlan load-balance enable
```

Configuring the switch

Create VLAN 100 and VLAN 200. The switch will use VLAN 100 to forward the traffic on CAPWAP tunnels between the AC and APs, and will use VLAN 200 to forward client traffic.

```
<Switch> system-view
```

```
[Switch] vlan 100
```

```
[Switch-vlan100] quit
```

```
[Switch] vlan 200
```

```
[Switch-vlan200] quit
```

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

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

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

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

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

Configure the interface that is connected to AP 1 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
```

Configure the interface that is connected to AP 2 as an access port, and assign the port to VLAN 100.

```
[Switch] interface gigabitethernet 1/0/3
```

```
[Switch-GigabitEthernet1/0/3] port link-type access
```

```
[Switch-GigabitEthernet1/0/3] port access vlan 100
```

Enable PoE on GigabitEthernet 1/0/3.

```
[Switch-GigabitEthernet1/0/3] poe enable
```

```
[Switch-GigabitEthernet1/0/3] quit
```

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

```
[Switch] interface gigabitethernet 1/0/4
[Switch-GigabitEthernet1/0/4] port link-type trunk
[Switch-GigabitEthernet1/0/4] port trunk permit vlan 100 200
[Switch-GigabitEthernet1/0/4] quit
```

Verifying the configuration

Verify that a third client associates with AP 2 when the number of sessions on either AP reaches 2 and the session gap between the APs reaches 1.

```
[AC] display wlan client
Total number of clients: 3
```

MAC address	Username	AP name	R	IP address	VLAN
0015-005c-8b2c	N/A	officeap1	2	192.2.0.3	200
109a-dd9f-aaa2	N/A	officeap2	2	192.2.0.5	200
2clf-2332-7f78	N/A	officeap1	2	192.2.0.4	200

Configuration files

- AC:

```
#
wlan load-balance mode session 2 gap 1
wlan load-balance enable
wlan load-balance access-denial 5
#
vlan 100
#
vlan 200
#
wlan service-template 1
  ssid service
  vlan 200
  akm mode psk
  preshared-key pass-phrase simple 12345678
  cipher-suite ccmp
  security-ie rsn
  client forwarding-location ac
  service-template enable
#
interface Vlan-interface100
  ip address 192.1.0.1 255.255.0.0
#
interface Vlan-interface200
  ip address 192.2.0.1 255.255.0.0
#
interface GigabitEthernet1/0/1
```

```

port link-type trunk
port trunk permit vlan 100 200
#
wlan ap officeap1 model AP 3620
serial-id 219801A28N819CE0002X
#
wlan ap officeap2 model AP 3620
serial-id 219801A28N819CE0002T
#
wlan ap-group group1
ap officeap1 officeap2
ap-model AP 3620
radio 2
service-template 1
radio enable
#

```

- **Switch:**

```

#
vlan 100
#
vlan 200
#
interface GigabitEthernet1/0/1
port link-mode bridge
port link-type trunk
port trunk permit vlan 100 200
#
interface GigabitEthernet1/0/2
port access vlan 100
poe enable
#
interface GigabitEthernet1/0/3
port access vlan 100
poe enable
#
interface GigabitEthernet1/0/4
port link-type trunk
port trunk permit vlan 100 200
#

```

Related documentation

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

INTELBRAS Access Controllers

Static Blacklist 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 the WLAN static blacklist.....	1
Network configuration.....	1
Restrictions and guidelines	1
Procedures	1
Configuring the AC.....	1
Configuring the switch	3
Verifying the configuration	4
Configuration files.....	4
Related documentation	6

Introduction

The following information provides an example for configuring the WLAN static blacklist.

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.

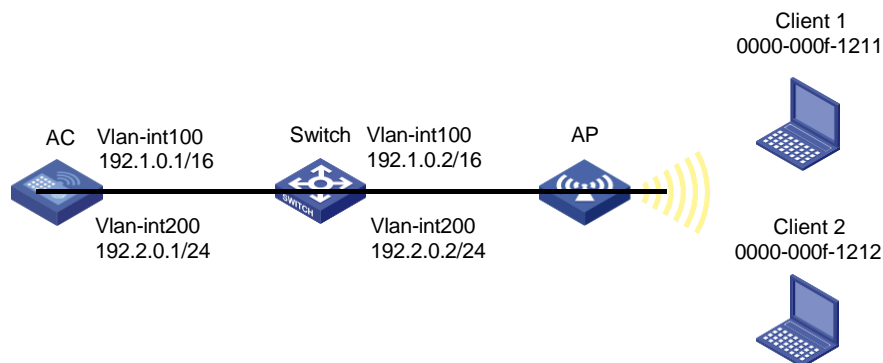
This document assumes that you have basic knowledge of WLAN static blacklists.

Example: Configuring the WLAN static blacklist

Network configuration

As shown in [Figure 1](#), the switch acts as a DHCP server to assign IP addresses to the AP and the clients, and the AC forwards client traffic. Client 1 is a rogue client. Configure the static blacklist to deny Client 1's access to the WLAN.

Figure 1 Network diagram



Restrictions and guidelines

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

Procedures

Configuring the AC

1. Configure 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 192.1.0.1 16
[AC-Vlan-interface100] quit
```

Create VLAN 200 and VLAN-interface 200, and assign an IP address to the VLAN 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 192.2.0.1 24
[AC-Vlan-interface200] quit
```

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

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

2. Configure wireless services:

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

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

Configure the SSID as **service**.

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

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

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

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

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

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

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

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

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

Enable the service template.

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

3. Configure the AP:

NOTE:

In large-scale networks, 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
```

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

```
[AC] wlan ap-group group1
[AC-wlan-ap-group-group1] ap officeap
[AC-wlan-ap-group-group1] ap-model AP 3620
# Bind service template service to radio 1.
[AC-wlan-ap-group-group1-ap-model-AP 3620] radio 1
[AC-wlan-ap-group-group1-ap-model-AP 3620-radio-1] service-template service
# Enable radio 1.
[AC-wlan-ap-group-group1-ap-model-AP 3620-radio-1] radio
enable [AC-wlan-ap-group-group1-ap-model-AP 3620-radio-1] quit
[AC-wlan-ap-group-group1-ap-model-AP 3620]
quit [AC-wlan-ap-group-group1] quit
4. Add Client 1 to the static blacklist.
[AC] wlan static-blacklist mac-address 0000-000f-1211
```

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 192.1.0.2 16
[Switch-Vlan-interface100] quit
```

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

```
[Switch] vlan 200
[Switch-vlan200] quit
[Switch] interface vlan-interface 200
[Switch-Vlan-interface200] ip address 192.2.0.2 24
[Switch-Vlan-interface200] quit
```

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

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 1 100 200
[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 100 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 100
[Switch-dhcp-pool-100] network 192.1.0.0 mask 255.255.0.0
```

Specify the gateway address as 192.1.0.1 in the DHCP address pool.

```
[Switch-dhcp-pool-100] gateway-list 192.1.0.1
[Switch-dhcp-pool-100] quit
```

Create DHCP address pool 200 to assign IP addresses to clients, and specify subnet 192.2.0.0/24 in the DHCP address pool.

```
[Switch] dhcp server ip-pool 200
[Switch-dhcp-pool-200] network 192.2.0.0 mask 255.255.255.0
```

Specify the gateway address as 192.2.0.1 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-200] gateway-list 192.2.0.1
[Switch-dhcp-pool-200] dns-list 192.2.0.1
[Switch-dhcp-pool-200] quit
```

Verifying the configuration

Verify that the MAC address of Client 1 is in the static blacklist.

```
[AC] display wlan blacklist static
Total number of clients: 1
MAC addresses:
0000-000f-1211
```

Verify that only Client 2 is associated with the AP successfully.

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

MAC address	Username	AP name	R	IP address	VLAN
0000-000f-1212	N/A	officeap	1	192.2.0.3	200

Configuration files

- AC:

```
#
vlan 1
#
vlan 100
#
vlan 200
#
wlan service-template service
  ssid service
  vlan 200
akm mode psk
preshared-key pass-phrase simple 12345678
cipher-suite ccmp
security-ie rsn
```

```

client forwarding-location ac
service-template enable
#
interface Vlan-interface100
 ip address 192.1.0.1 255.255.0.0
#
interface Vlan-interface200
 ip address 192.2.0.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 1 100 200
#
wlan ap officeap model AP 3620
 serial-id 219801A28N819CE0002T
#
wlan ap-group group1
 ap officeap
 ap-model AP 3620
 radio 1
 service-template service
 radio enable
#
wlan static-blacklist mac-address 0000-000f-1211
#

```

- **Switch:**

```

#
vlan 1
#
vlan 100
#
vlan 200
#
dhcp server ip-pool 100
 gateway-list 192.1.0.1
 network 192.1.0.0 mask 255.255.0.0
#
dhcp server ip-pool 200
 gateway-list 192.2.0.1
 network 192.2.0.0 mask 255.255.255.0
 dns-list 192.2.0.1
#
interface Vlan-interface100
 ip address 192.1.0.2 255.255.0.0
#
interface Vlan-interface200
 ip address 192.2.0.2 255.255.255.0
#

```

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

Related documentation

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

INTELBRAS Access Controllers

Client Quantity Control 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 client quantity control	1
Network configuration	1
Restrictions and guidelines	1
Procedures	2
Configuring the AC	2
Configuring the switch	3
Verifying the configuration	5
Configuration files	5
Related documentation	7

Introduction

The following information provides an example for configuring client quantity control.

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 client quantity control.

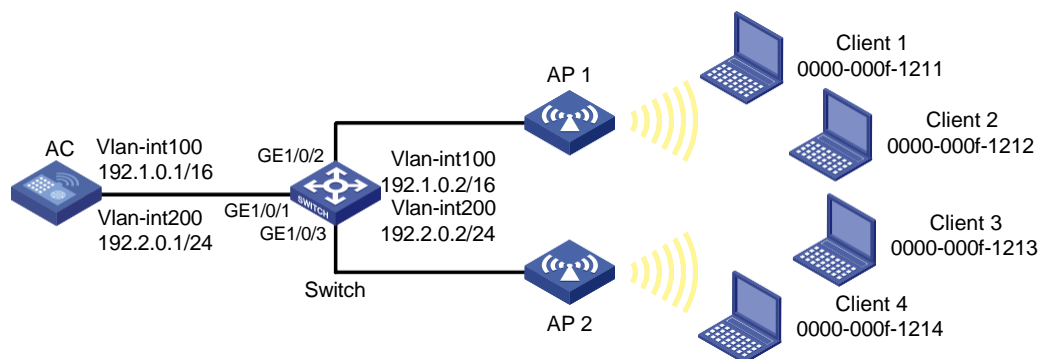
Example: Configuring client quantity control

Network configuration

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

- Set the maximum number of clients that can associate with a radio to enable AP 1 to permit only Client 1.
- Set the maximum number of clients that can associate with a service template to enable AP 2 to permit only Client 2 and Client 3.

Figure 1 Network diagram



Restrictions and guidelines

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

Procedures

Configuring the AC

1. Configure 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 192.1.0.1 16
[AC-Vlan-interface100] quit
```

Create VLAN 200 and VLAN-interface 200, and assign an IP address to the VLAN 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 192.2.0.1 24
[AC-Vlan-interface200] quit
```

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

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

2. Configure wireless services:

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

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

Configure the SSID as **service**.

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

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

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

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

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

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

Set the maximum number of clients that can associate with the service template to 2.

```
[AC-wlan-st-service] client max-count 2
```

Enable the service template.

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

3. Configure the AP:

NOTE:

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

Create manual AP **officeap1**, and specify the AP model and serial ID.

```
[AC] wlan ap officeap1 model AP 3620
[AC-wlan-ap-officeap1] serial-id 219801A28N819CE0002X
```

Create manual AP **officeap2**, and specify the AP model and serial ID.

```
[AC] wlan ap officeap2 model AP 3620
[AC-wlan-ap-officeap2] serial-id 219801A28N819CE0002T
```

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

```
[AC] wlan ap-group group1
[AC-wlan-ap-group-group1] ap officeap1
[AC-wlan-ap-group-group1] ap-model AP
3620 # Bind service template service to radio
```

1.

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

Set the maximum number of clients that can associate with radio 1 and enable radio 1.

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

Create AP group **group2**, add the AP to the AP group, and specify the AP model.

```
[AC] wlan ap-group group2
[AC-wlan-ap-group-group2] ap officeap2
[AC-wlan-ap-group-group2] ap-model AP
3620 # Bind service template service to radio
```

1.

```
[AC-wlan-ap-group-group2-ap-model-AP 3620] radio 1
[AC-wlan-ap-group-group2-ap-model-AP 3620-radio-1] service-template service
```

Enable radio 1.

```
[AC-wlan-ap-group-group2-ap-model-AP 3620-radio-1] radio
enable [AC-wlan-ap-group-group2-ap-model-AP 3620-radio-1] quit
[AC-wlan-ap-group-group2] 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 192.1.0.2 16
[Switch-Vlan-interface100] quit
```

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

```
[Switch] vlan 200
```

```
[Switch-vlan200] quit
[Switch] interface vlan-interface 200
[Switch-Vlan-interface200] ip address 192.2.0.2 24
[Switch-Vlan-interface200] quit
```

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

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

Configure GigabitEthernet 1/0/2 that connects the switch to AP 1 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
```

Configure GigabitEthernet 1/0/3 that connects the switch to AP 2 as an access port, and assign the port to VLAN 100.

```
[Switch] interface gigabitethernet 1/0/3
[Switch-GigabitEthernet1/0/3] port link-type access
[Switch-GigabitEthernet1/0/3] port access vlan 100
```

Enable PoE on GigabitEthernet 1/0/3.

```
[Switch-GigabitEthernet1/0/3] poe enable
[Switch-GigabitEthernet1/0/3] quit
```

2. Configure DHCP:

Enable DHCP.

```
[Switch] dhcp enable
```

Create DHCP address pool 100 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 100
[Switch-dhcp-pool-100] network 192.1.0.0 mask 255.255.0.0
```

Specify the gateway address as 192.1.0.1 in the DHCP address pool.

```
[Switch-dhcp-pool-100] gateway-list 192.1.0.1
[Switch-dhcp-pool-100] quit
```

Create DHCP address pool 200 to assign IP addresses to clients, and specify subnet 192.2.0.0/24 in the DHCP address pool.

```
[Switch] dhcp server ip-pool 200
[Switch-dhcp-pool-200] network 192.2.0.0 mask 255.255.255.0
```

Specify the gateway address as 192.2.0.1 and specify the DNS server address in the DHCP address pool. In this example, the gateway also acts as a DNS server.

```
[Switch-dhcp-pool-200] gateway-list 192.2.0.1
[Switch-dhcp-pool-200] dns-list 192.2.0.1
[Switch-dhcp-pool-200] quit
```

Verifying the configuration

Try to associate client 1, client 2, client 3, and client 4 with the WLAN successively. (Details not shown.)

Verify that only client 1, client 2, and client 3 have successfully associated with the WLAN.

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

Total number of clients: 3

MAC address	Username	AP name	R	IP address	VLAN
0000-000f-1211	N/A	officeap1	1	192.2.0.3	200
0000-000f-1212	N/A	officeap2	1	192.2.0.4	200
0000-000f-1213	N/A	officeap2	1	192.2.0.5	200

Configuration files

- AC:

```
#
vlan 1
#
vlan 100
#
vlan 200
#
wlan service-template service
    ssid service
    vlan 200
    akm mode psk
    preshared-key pass-phrase simple 12345678
    cipher-suite ccmp
    security-ie rsn
    client forwarding-location ac
    client max-count 2
    service-template enable
#
interface Vlan-interface100
    ip address 192.1.0.1 255.255.0.0
#
interface Vlan-interface200
    ip address 192.2.0.1 255.255.255.0
#
interface GigabitEthernet1/0/1
    port link-type trunk
    port trunk permit vlan 1 100 200
#
wlan ap officeap1 model AP 3620
    serial-id 219801A28N819CE0002X
#
```

```
wlan ap officeap2 model AP 3620
serial-id 219801A28N819CE0002T
```

```
#
wlan ap-group group1
ap officeap1
ap-model AP 3620
radio 1
service-template service
client max-count 1
radio enable
#
wlan ap-group group2
ap officeap2
ap-model AP 3620
radio 1
service-template service
radio enable
#
```

- **Switch:**

```
#
vlan 1
#
vlan 100
#
vlan 200
#
dhcp server ip-pool 100
gateway-list 192.1.0.1
network 192.1.0.0 mask 255.255.0.0
#
dhcp server ip-pool 200
gateway-list 192.2.0.1
network 192.2.0.0 mask 255.255.255.0
dns-list 192.2.0.1
#
interface Vlan-interface100
ip address 192.1.0.2 255.255.0.0
#
interface Vlan-interface200
ip address 192.2.0.2 255.255.255.0
#
interface GigabitEthernet1/0/1
port link-type trunk
port trunk permit vlan 1 100 200
#
interface GigabitEthernet1/0/2
port link-type access
port access permit vlan 100
```



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

Related documentation

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

INTELBRAS Access Controllers AP License Synchronization Configuration Examples

Copyright © 2024 Intelbras S.A All rights reserved.

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

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

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

Contents

Introduction	1
Prerequisites	1
Example: Configuring AP license synchronization	1
Network requirements	1
Configuration restrictions and guidelines	1
Configuration procedures	2
Configuring the AC 1	2
Configuring the AC 2	3
Configuring the switch	5
Verifying the configuration	6
Configuration files	7
Related documentation	9

Introduction

The following information provides an AP license synchronization configuration example.

Prerequisites

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

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

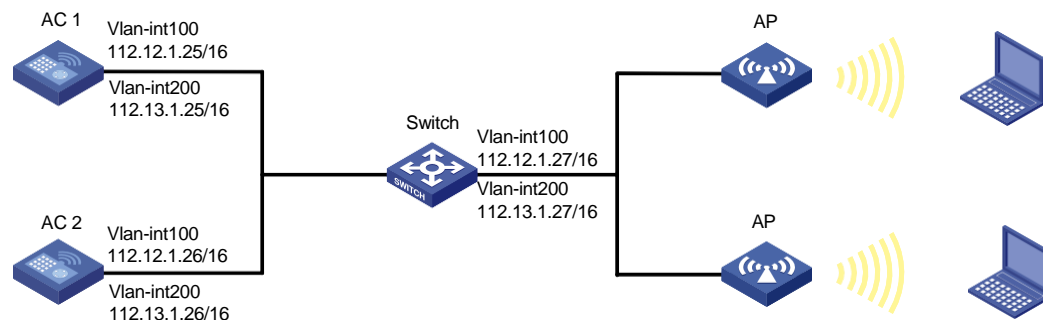
The following information is provided based on the assumption that you have basic knowledge of AP license synchronization.

Example: Configuring AP license synchronization

Network requirements

As shown in [Figure 1](#), the APs connect to AC 1 and AC 2 through the switch and the APs provide wireless service for clients. Set the SSID to **service** and enable AP license synchronization on AC 1 and AC 2. The two ACs back up licenses for each other.

Figure 1 Network diagram



Configuration restrictions and guidelines

When the master AC fails, the backup AC will take over and becomes the new master AC. The licenses synchronized to the new master AC will be valid for a 30-day grace period.

Configuration procedures

Configuring the AC 1

1. Configure interfaces on the AC 1:

Configure VLAN-interface 100 and assign it an IP address. The AC 1 will use this IP address to establish CAPWAP tunnels with APs.

```
<AC1> system-view
[AC1] vlan 100
[AC1-vlan100] quit
[AC1] interface vlan-interface 100
[AC1-Vlan-interface100] ip address 112.12.1.25 16
[AC1-Vlan-interface100] quit
```

Configure VLAN-interface 200 and assign it an IP address. The AC 1 will use VLAN 200 for client access.

```
[AC1] vlan 200
[AC1-vlan200] quit
[AC1] interface vlan-interface 200
[AC1-Vlan-interface200] ip address 112.13.1.25 16
[AC1-Vlan-interface200] quit
```

Configure GigabitEthernet 1/0/1 that connects the AC 1 to the switch as a trunk port.

```
[AC1] interface gigabitethernet1/0/1
[AC1-GigabitEthernet1/0/1] port link-type trunk
```

Remove the trunk port from VLAN 1, and assign the port to VLANs 100 and 200.

```
[AC1-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[AC1-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[AC1-GigabitEthernet1/0/1] quit
```

Enable AP license synchronization on AC 1 and configure AC 1 as the master AC.

```
[AC1] wlan ap-license-group
[AC1-wlan-ap-license-group] local ip 112.12.1.25
[AC1-wlan-ap-license-group] member ip 112.12.1.26
[AC1-wlan-ap-license-group] ap-license-synchronization enable
[AC1-wlan-ap-license-group] quit
```

2. Configure the wireless service:

Create wireless service template **service** and enter its view.

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

Set the SSID to **service**.

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

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

```
[AC1-wlan-st-service] vlan 200
```

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

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

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

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

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

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

Enable service template **service**.

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

```
[AC1-wlan-st-service] quit
```

3. Configure the AP:

NOTE:

In a large-scale network, configure AP settings in AP group view instead of AP view 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 a grouping rule by AP name to add AP **ap1** to the group.

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

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

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

```
[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
```

```
service [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
```

Configuring the AC 2

1. Configure interfaces on the AC 2:

Configure VLAN-interface 100 and assign it an IP address. The AC 2 will use this IP address to establish CAPWAP tunnels with APs.

```
<AC2> system-view
```

```
[AC2] vlan 100
```

```
[AC2-vlan100] quit
```

```
[AC2] interface vlan-interface 100
```

```
[AC2-Vlan-interface100] ip address 112.12.1.26 16
```

```
[AC2-Vlan-interface100] quit
```

Configure VLAN-interface 200 and assign it an IP address. The AC 2 will use VLAN 200 for client access.

```
[AC2] vlan 200
```

```
[AC2-vlan200] quit
```

```
[AC2] interface vlan-interface 200
```

```
[AC2-Vlan-interface200] ip address 112.13.1.26 16
```

```
[AC2-Vlan-interface200] quit
```

Configure GigabitEthernet 1/0/1 that connects the AC 2 to the switch as a trunk port.

```
[AC2] interface gigabitethernet1/0/1
```

```
[AC2-GigabitEthernet1/0/1] port link-type trunk
```

Remove the trunk port from VLAN 1, and assign the port to VLANs 100 and 200.

```
[AC2-GigabitEthernet1/0/1] undo port trunk permit vlan 1
```

```
[AC2-GigabitEthernet1/0/1] port trunk permit vlan 100 200
```

```
[AC2-GigabitEthernet1/0/1] quit
```

Enable AP license synchronization on AC 2 and configure AC 2 as the master AC.

```
[AC2] wlan ap-license-group
```

```
[AC2-wlan-ap-license-group] local ip 112.12.1.26
```

```
[AC2-wlan-ap-license-group] member ip 112.12.1.25
```

```
[AC2-wlan-ap-license-group] ap-license-synchronization enable
```

```
[AC2-wlan-ap-license-group] quit
```

2. Configure the wireless service:

Create wireless service template **service** and enter its view.

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

Set the SSID to **service**.

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

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

```
[AC2-wlan-st-service] vlan 200
```

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

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

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

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

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

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

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

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

Enable service template **service**.

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

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

3. Configure the AP:

NOTE:

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

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

```
[AC2] wlan ap ap1 model AP 3620
```

```
[AC2-wlan-ap-ap1] serial-id 219801A28N819CE0002T
```

```
[AC2-wlan-ap-ap1] quit
```

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

```
[AC2] wlan ap-group group1
```

```
[AC2-wlan-ap-group-group1] ap ap1
```

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

```
[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 service
```

```
[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
```

Configuring the switch

Create VLAN 100 and VLAN 200. The switch will use VLAN 100 to forward the traffic on CAPWAP tunnels between the AC and APs, and will use VLAN 200 to forward client traffic.

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

Configure GigabitEthernet 1/0/1 that connects the switch to the AC 1 as a trunk port.

```
[Switch] interface gigabitethernet1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
```

Remove the trunk port from VLAN 1, and assign the port to VLAN 100 and VLAN 200.

```
[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 AC 2 as a trunk port.

```
[Switch] interface gigabitethernet1/0/2
[Switch-GigabitEthernet1/0/2] port link-type trunk
```

Remove the trunk port from VLAN 1, and assign the port to VLAN 100 and VLAN 200.

```
[Switch-GigabitEthernet1/0/2] undo port trunk permit vlan 1
[Switch-GigabitEthernet1/0/2] port trunk permit vlan 100 200
[Switch-GigabitEthernet1/0/2] quit
```

Configure the interface GigabitEthernet 1/0/3 that is connected to APs as an access port, and assign the port to VLAN 100.

```
[Switch] interface gigabitethernet1/0/3
[Switch-GigabitEthernet1/0/3] port link-type access
[Switch-GigabitEthernet1/0/3] port access vlan 100
```

Enable PoE on GigabitEthernet 1/0/3.

```
[Switch-GigabitEthernet1/0/3] poe enable
[Switch-GigabitEthernet1/0/3] quit
```

Specify 112.12.1.27/16 as the IP address of the VLAN 100.

```
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ip address 112.12.1.27 16
[Switch-Vlan-interface100] quit
```

Specify 112.13.1.27/16 as the IP address of the VLAN 200.

```
[Switch] interface vlan-interface 200
[Switch-Vlan-interface200] ip address 112.13.1.27 16
[Switch-Vlan-interface200] quit
```

Enable DHCP.

```
[Switch] dhcp enable
```


Create DHCP IP pool 100 to assign IP addresses to APs, and specify the IP address range for the IP pool.

```
[Switch] dhcp server ip-pool 100
[Switch-dhcp-pool-100] network 112.12.0.0 mask 255.255.0.0
```

Specify gateway IP address 112.12.1.27 in the DHCP IP pool.

```
[Switch-dhcp-pool-100] gateway-list 112.12.1.27
[Switch-dhcp-pool-100] quit
```

Create DHCP IP pool 200 to assign IP addresses to clients, and specify the IP address range for the DHCP IP pool.

```
[Switch] dhcp server ip-pool 200
[Switch-dhcp-pool-200] network 112.13.0.0 mask 255.255.255.0
```

Specify gateway IP address 112.13.1.27 in the DHCP IP pool.

```
[Switch-dhcp-pool-200] gateway-list 112.13.1.27
```

Specify the DNS server according to the actual network plan. In this example, the gateway is specified as the DNS server.

```
[Switch-dhcp-pool-200] dns-list 112.13.1.27
[Switch-dhcp-pool-200] quit
```

Verifying the configuration

1. Display AP license synchronization group information on AC 1.

```
<AC1> display wlan ap-license-group
Group total licenses: 32
Group used licenses: 2
AP license synchronization: Enabled
Local IP: 112.12.1.25
Local role: Master
Member information:
  IP address      Total      Used      Member role    State    Online duration
  112.12.1.26     16         0         Master         UP       10hr 22min 04sec
```

2. Display AP license synchronization group information on AC 2.

```
<AC2> display wlan ap-license-group
Group total licenses: 32
Group used licenses: 2
AP license synchronization: Enabled
Local IP: 112.12.1.26
Local role: Master
Member information:
  IP address      Total      Used      Member role    State    Online duration
  112.12.1.25     16         2         Master         UP       10hr 22min 04sec
```

3. When AC 2 fails, AC 1 takes over and the sum of licenses remains 32.

```
<AC1> display wlan ap-license-group
Group total licenses: 32
Group used licenses: 2
AP license synchronization: Enabled
Local IP: 112.12.1.25
Local role: Master
```

Member information:

IP address	Total	Used	Member role	State	Online duration
112.12.1.26	16	0	Master	DOWM	00hr 00min 00sec

Configuration files

- AC 1:

```
#
vlan 100
#
vlan 200
#
wlan service-template service
    ssid service
    vlan 200
    client forwarding-location ac
    akm mode psk
    preshared-key pass-phrase cipher $c$3$QoCUXs4DmEXLHV9i25HKOnf4wdvj4i8EzJb+
    cipher-suite ccmp
    security-ie rsn
    service-template enable
#
interface Vlan-interface100
    ip address 112.12.1.25 255.255.0.0
#
interface Vlan-interface200
    ip address 112.13.1.25 255.255.0.0
#
interface GigabitEthernet1/0/1
    port link-type trunk
    undo port trunk permit vlan 1
    port trunk permit vlan 100 200
#
wlan ap-group group1
    ap ap1
    ap-model AP 3620
    radio 1
        radio enable
        service-template service
#
wlan ap ap1 model AP 3620
    serial-id 219801A28N819CE0002T
#
wlan ap-license-group
    local ip 112.12.1.25
    member ip 112.12.1.26
    ap-license-synchronization enable
#
```

- **AC 2:**

```
#
vlan 100
#
vlan 200
#
wlan service-template service
    ssid service
    vlan 200
    client forwarding-location ac
    akm mode psk
    preshared-key pass-phrase cipher $c$3$QoCUXs4DmEXLHV9i25HKOnf4wdvj4i8EzJb+
    cipher-suite ccmp
    security-ie rsn
    service-template enable
#
interface Vlan-interface100
    ip address 112.12.1.26 255.255.0.0
#
interface Vlan-interface200
    ip address 112.13.1.26 255.255.0.0
#
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 ap1
    ap-model AP 3620
    radio 1
        radio enable
        service-template service
#
wlan ap ap1 model AP 3620
    serial-id 219801A28N819CE0002T
#
wlan ap-license-group
    local ip 112.12.1.26
    member ip 112.12.1.25
    ap-license-synchronization enable
#
```

- **Switch:**

```
#
    dhcp enable
#
vlan 100
#
```

```

vlan 200
#
dhcp server ip-pool vlan100
gateway-list 112.12.1.27
network 112.12.0.0 mask 255.255.0.0
#
dhcp server ip-pool vlan200
gateway-list 112.13.1.27
network 112.13.0.0 mask 255.255.255.0
dns-list 112.13.1.27
#
interface Vlan-interface100
ip address 112.12.1.27 255.255.0.0
#
interface Vlan-interface200
ip address 112.13.1.27 255.255.255.0
#
interface GigabitEthernet1/0/1
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 100 200
#
interface GigabitEthernet1/0/2
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 100 200
#
interface GigabitEthernet1/0/3
port access vlan 100
poe enable
#

```

Related documentation

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

INTELBRAS Access Controllers BLE Module iBeacon Transmission 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: Configure iBeacon transmission for a BLE module	1
Network configuration	1
Restrictions and guidelines.....	1
Procedures	2
Verifying the configuration	3

Introduction

The following information provides an example for configuring iBeacon transmission for a BLE module.

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.

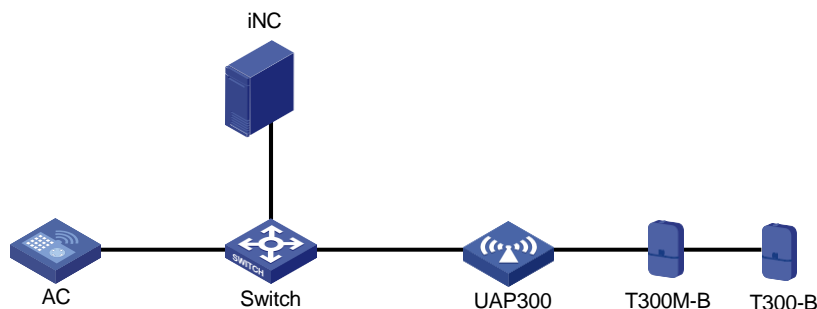
This document assumes that you have basic knowledge of IoT AP and wireless location.

Example: Configure iBeacon transmission for a BLE module

Network configuration

As shown in [Figure 1](#), the INC server acts as an IoT server, and UAP300 acts as an IoT AP to provide IoT services for the connected IoT modules T300M-B and T300-B.

Figure 1 Network diagram



Restrictions and guidelines

When you configure iBeacon transmission for a BLE module, follow these restrictions and guidelines:

- Use the actual serial ID of an AP to uniquely identify that AP.
- Enable LLDP on the PoE switch.
- The number of cascaded T300-B connected to T300M-B depends on the power supply capacity of the uplink device (UAP300).

Procedures

1. Make sure the devices can reach each other (Details not shown.).
2. Configure the AP:

NOTE:

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

Create a manual AP named `ap1`, and specify its model and serial ID.

```
<AC> system-view
[AC] wlan ap ap1 model UAP300
[AC-wlan-ap-ap1] serial-id 219801A15K816AE00029
```

Enable PoE for UAP300.

```
[AC-wlan-ap-ap1] poe port 3 enable
```

Specify the serial number for T300M-B module 1.

```
[AC-wlan-ap-ap1] module 1
[AC-wlan-ap-ap1-module-1] serial-number 219801A0YQ8164E00101
[AC-wlan-ap-ap1-module-1] quit
```

Specify the serial number for T300M-B module 2.

```
[AC-wlan-ap-ap1] module 2
[AC-wlan-ap-ap1-module-2] serial-number 219801A0YQ8164E20022
[AC-wlan-ap-ap1-module-2] quit
[AC-wlan-ap-ap1] quit
```

3. Configure modules:

NOTE:

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

Enter the view of module 1 in AP group `group1`.

```
[AC] wlan ap-group group1
[AC-wlan-ap-group-group1] ap ap1
[AC-wlan-ap-group-group1] ap-model UAP300
[AC-wlan-ap-group-group1-ap-model-UAP300] module 1
```

Enable module 1.

```
[AC-wlan-ap-group-group1-ap-model-UAP300-module-1] module enable
```

Specify BLE as the supported module type for module 1.

```
[AC-wlan-ap-group-group1-ap-model-UAP300-module-1] type ble
```

Enable the iBeacon transmission feature for module 1.

```
[AC-wlan-ap-group-group1-ap-model-UAP300-module-1] rfid-tracking ble advertisement enable
```

Configure the advertisement information for module 1.

```
[AC-wlan-ap-group-group1-ap-model-UAP300-module-1] rfid-tracking ble advertisement
uuid fda50693a4e24fb1afcfc6eb07647825
[AC-wlan-ap-group-group1-ap-model-UAP300-module-1] rfid-tracking ble advertisement
major-id 10
[AC-wlan-ap-group-group1-ap-model-UAP300-module-1] rfid-tracking ble advertisement
minor-id 7
```



```
[AC-wlan-ap-group-group1-ap-model-UAP300-module-1] quit
# Enter the view of module 2 in AP group group1.
[AC-wlan-ap-group-group1-ap-model-UAP300] module 2
# Enable module 1.
[AC-wlan-ap-group-group1-ap-model-UAP300-module-2] module enable
# Specify BLE as the supported module type for module 2.
[AC-wlan-ap-group-group1-ap-model-UAP300-module-2] type ble
# Enable the iBeacon transmission feature for module 2.
[AC-wlan-ap-group-group1-ap-model-UAP300-module-2] rfid-tracking ble advertisement
enable
# Configure the advertisement information for module 2.
[AC-wlan-ap-group-group1-ap-model-UAP300-module-2] rfid-tracking ble advertisement
uuid fda50693a4e24fblafcf6eb07647825
[AC-wlan-ap-group-group1-ap-model-UAP300-module-2] rfid-tracking ble advertisement
major-id 10
[AC-wlan-ap-group-group1-ap-model-UAP300-module-2] rfid-tracking ble advertisement
minor-id 7
[AC-wlan-ap-group-group1-ap-model-UAP300-module-2] quit
[AC-wlan-ap-group-group1-ap-model-UAP300] quit
# Set the IPv4 address and port number for the BLE location server to 3.3.3.204 and 1145,
respectively, for AP ap1.
[AC-wlan-ap-group-group1] rfid-tracking ble engine-address 3.3.3.204 engine-port
1145
# Enable BLE location for AP ap1.
[AC-wlan-ap-group-group1] rfid-tracking ble enable
# Enable neighbor list reporting for AP ap1.
[AC-wlan-ap-group-group1] rfid-tracking ble report enable
[AC-wlan-ap-group-group1] quit
```

Verifying the configuration

Display UAP information and connected module information.

```
[AC] display wlan uap name ap1
UAP name : ap1
Model : UAP300
Serial ID : 219801A15K816AE00029
MAC address : b0f9-633f-dfa0
Modules : 1
Port ID: 3
```

```
-----
Module ID Model Serial Number
-----
```

```
1 T300 219801A0YQ8164E00101
2 T300 219801A0YQ8164E20022
```

Display information about module 1.

```
[AC] display wlan module-information ap ap1 module 1
Module administrative type : BLE
Module physical type :
INTELBAS Model : T300-B
```

HW version : 1.0
SW version : 0.08
Sequence ID : 00000000000000000023
Node physical status : Normal
Module physical status : Normal
Module administrative status : Enabled

Display information about module 2.

[AC] display wlan module-information ap ap1 module 2
Module administrative type : BLE
Module physical type :
INTELBRAS Model : T300-B
HW version : 1.0
SW version : 0.08
Sequence ID : 00000000000000000023
Node physical status : Normal
Module physical status : Normal
Module administrative status : Disabled

INTELBRAS Access Controllers Medical RFID Tag Management Configuration Examples

Copyright © 2024 Intelbras S.A All rights reserved.

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

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

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

Contents

Introduction	1
Prerequisites	1
Example: Configuring medical RFID tag management	1
Network configuration	1
Restrictions and guidelines	1
Procedures	2
Configuring the AC	2
Configuring the switch	3
Verifying the configuration	3
Configuration files	4
Related documentation	5

Introduction

The following information provides an example for configuring WA4320i-X-R APs to realize medical RFID tag management.

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.

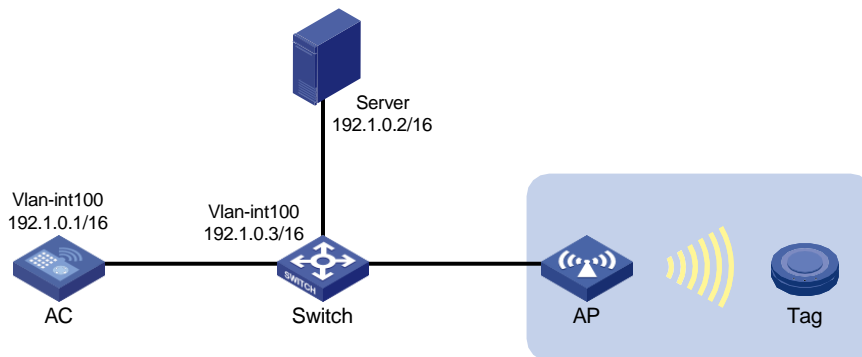
This document assumes that you have basic knowledge of IoT AP and WLAN location.

Example: Configuring medical RFID tag management

Network configuration

As shown in [Figure 1](#), configure the AP to collect medical RFID tag information and send the information to the location server for calculation. Then, users can obtain tag information in various forms such as maps, tables, or reports.

Figure 1 Network diagram



Restrictions and guidelines

When you configure medical RFID tag management, follow these restrictions and guidelines:

- Use the actual serial ID of an AP to uniquely identify that AP.
- The port number of the location server configured on the AC must be the same as the port number specified on the location server.

Procedures

Configuring the AC

1. Configure interfaces on the AC:

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

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

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

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

2. Configure the AP:

NOTE:

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

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

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

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

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

3. Configure a module:

Enter the view of module 1.

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

Specify the supported module type as RFID for module 1, and enable module 1.

```
[AC-wlan-ap-group-group1-ap-model-AP 3620-module-1] type rfid
[AC-wlan-ap-group-group1-ap-model-AP 3620-module-1] module
enable [AC-wlan-ap-group-group1-ap-model-AP 3620-module-1]quit
[AC-wlan-ap-group-group1-ap-model-AP 3620]quit
```

4. Configure IoT location:

Enable IoT location.

```
[AC-wlan-ap-group-group1] rfid-tracking iot enable
```

Specify the IP address and port number of the IoT server.

```
[AC-wlan-ap-group-group1] iot engine-address 192.1.0.2 engine-port 3000
[AC-wlan-ap-group-group1] quit
```

Configuring the switch

1. Configure interfaces on the switch:

Create VLAN 100 and VLAN-interface 100, and assign an IP address to the VLAN interface. The switch will use this VLAN to communicate with the AC.

```
<Switch> system-view
[Switch] vlan 100
[Switch-vlan100] quit
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ip address 192.1.0.3 16
[Switch-Vlan-interface100] quit
```

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

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

Configure GigabitEthernet 1/0/2 that connects the switch and the server 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
[Switch-GigabitEthernet1/0/2] quit
```

Configure GigabitEthernet 1/0/3 that connects the switch and AP as an access port, and assign the port to VLAN 100.

```
[Switch] interface gigabitethernet 1/0/3
[Switch-GigabitEthernet1/0/3] port link-type access
[Switch-GigabitEthernet1/0/3] port access vlan 100
```

Enable PoE on GigabitEthernet 1/0/3.

```
[Switch-GigabitEthernet1/0/3] poe enable
[Switch-GigabitEthernet1/0/3] quit
```

2. Configure DHCP services:

Enable DHCP.

```
[Switch] dhcp enable
```

Create a DHCP address pool named 1 to assign an IP address to the AP.

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

In DHCP address pool 1, specify subnet 192.1.0.0/16 for dynamic allocation, exclude IP addresses 192.1.0.1 and 192.1.0.2 from dynamic allocation, and specify the gateway IP address 192.1.0.3.

```
[Switch] dhcp server ip-pool 1
[Switch-dhcp-pool-1] network 192.1.0.0 mask 255.255.0.0
[Switch-dhcp-pool-1] forbidden-ip 192.1.0.1 192.1.0.2
[Switch-dhcp-pool-1] gateway-list 192.1.0.3
[Switch-dhcp-pool-1] quit
```

Verifying the configuration

Verify that the type of module 1 is RFID and the module is enabled.

```
[AC] display wlan module-information ap ap1 module 1
Module administrative type      : RFID
Module physical type           : IOT
Model                          : RFID
HW version                     : 12090031
SW version                     : 12090202
Serial ID                      : 0000051700000042
Module MAC                     : d461-fefd-0368
Module physical status         : Normal
Module administrative status   : Enabled
Description                    : Not configured
```

Verify that you can view tag information collected by the AP on the location server.

Configuration files

- **AC:**

```
#
vlan 100
#
interface Vlan-interface100
 ip address 192.1.0.1 255.255.0.0
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 100
#
wlan ap-group group1
 ap ap1
 rfid-tracking iot enable
 iot engine-address 192.1.0.2 engine-port 3000
 ap-model AP 3620
 module 1
  type rfid
  module enable
#
wlan ap ap1 model AP 3620
 serial-id 219801A28N819CE0002T
#
```

- **Switch:**

```
#
dhcp enable
#
vlan 100
#
dhcp server ip-pool 1
 gateway-list 192.1.0.3
 network 192.1.0.0 mask 255.255.0.0
 forbidden-ip 192.1.0.1
```



```
forbidden-ip 192.1.0.2
#
interface Vlan-interface100
 ip address 192.1.0.3 255.255.0.0
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 100
#
interface GigabitEthernet1/0/2
 port access vlan 100
#
interface GigabitEthernet1/0/3
 port access vlan 100
 poe enable
#
```

Related documentation

- *Internet of Things Command Reference* in *INTELBRAS Access Controllers Command References*
- *Internet of Things Configuration Guide* in *INTELBRAS Access Controllers Configuration Guides*
- *WLAN Advanced Features Command Reference* in *INTELBRAS Access Controllers Command References*
- *WLAN Advanced Features Configuration Guide* in *INTELBRAS Access Controllers Configuration Guides*

INTELBRAS Access Controllers iBeacon Management Configuration Examples

Copyright © 2024 Intelbras S.A All rights reserved.

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

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

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

Contents

Introduction	1
Prerequisites	1
Example: Configuring iBeacon management	1
Network configuration	1
Restrictions and guidelines	1
Procedures	2
Configuring the AC	2
Configuring the switch	3
Configuring the INC server	4
Verifying the configuration	7
Configuration files	7
Related documentation	9

Introduction

The following information provides an example for configuring WA4320-ACN-B APs to realize iBeacon management.

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.

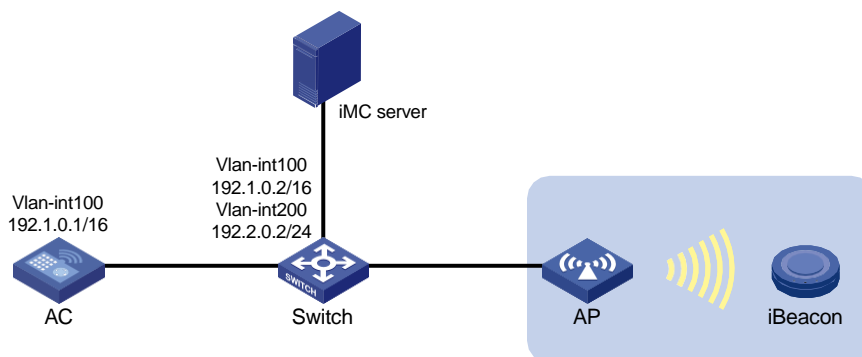
This document assumes that you have basic knowledge of IoT AP and WLAN location.

Example: Configuring iBeacon management

Network configuration

As shown in [Figure 1](#), configure the AP to manage the iBeacon device. The AP collects BLE information and sends the information to the location server on the INC server for calculation. Then, users can obtain information including electric quantity and RSSI of the iBeacon device. The AP also assigns management orders from the server to the iBeacon device.

Figure 1 Network diagram



Restrictions and guidelines

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

Procedures

Configuring the AC

1. Configure interfaces on the AC:

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

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

Create VLAN 200 and VLAN-interface 200, and configure the VLAN interface to use DHCP for IP address acquisition.

```
<AC> system-view
[AC] vlan 200
[AC-vlan200] quit
[AC] interface vlan-interface 200
[AC-Vlan-interface200] ip address dhcp-alloc
[AC-Vlan-interface200] quit
```

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

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

2. Configure the AP:

NOTE:

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

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

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

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

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

3. Configure a module:

Enter the view of module 1.

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

Specify the supported module type BLE for module 1, and enable module 1.

```
[AC-wlan-ap-group-group1-ap-model-AP 3620-module-1] type ble
[AC-wlan-ap-group-group1-ap-model-AP 3620-module-1] module enable
```

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

4. Configure BLE location:

Enable BLE location.

```
[AC-wlan-ap-group-group1] rfid-tracking ble enable
```

Set the IPv4 address and port number of the location server to 192.2.0.1 and 1145, respectively. In this example, the IP address of the BLE location server is the INC server's IP address obtained through DHCP.

```
[AC-wlan-ap-group-group1] rfid-tracking ble engine-address 192.2.0.1 engine-port
1145
```

Enable BLE neighbor list reporting for AP **ap1**.

```
[AC-wlan-ap-group-group1] rfid-tracking ble report enable
```

Configure the AP to send BLE neighbor list reports to the location server every 10 seconds.

```
[AC-wlan-ap-group-group1] rfid-tracking ble report interval 10
```

Specify the default password for deploying configuration to iBeacon devices as **AprilBrother** in plaintext form. Make sure the specified password is the same as the factory password of the iBeacon device.

```
[AC-wlan-ap-group-group1] rfid-tracking ble command-password simple AprilBrother
[AC-wlan-ap-group-group1] quit
```

Configuring the switch

1. Configure interfaces on the switch:

Create VLAN 100 and VLAN-interface 100, and assign an IP address to the VLAN interface. The switch will use this VLAN to communicate with the AC.

```
<Switch> system-view
[Switch] vlan 100
[Switch-vlan100] quit
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ip address 192.1.0.2 16
[Switch-Vlan-interface100] quit
```

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

```
[Switch] vlan 200
[Switch-vlan200] quit
[Switch] interface vlan-interface 200
[Switch-Vlan-interface200] ip address 192.2.0.2 24
[Switch-Vlan-interface200] quit
```

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

```
[Switch] interface gigabitethernet 1/0/1
[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 and the INC server as an access port, and assign the port to VLAN 200.

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

```
[Switch-GigabitEthernet1/0/2] port access vlan 200
[Switch-GigabitEthernet1/0/2] quit
```

Configure GigabitEthernet 1/0/3 that connects the switch and AP as an access port, and assign the port to VLAN 100.

```
[Switch] interface gigabitethernet 1/0/3
[Switch-GigabitEthernet1/0/3] port link-type access
[Switch-GigabitEthernet1/0/3] port access vlan 100
```

Enable PoE on GigabitEthernet 1/0/3.

```
[Switch-GigabitEthernet1/0/3] poe enable
[Switch-GigabitEthernet1/0/3] quit
```

2. Configure DHCP services:

Enable DHCP.

```
[Switch] dhcp enable
```

Create a DHCP address pool named 1 to assign an IP address to the AP.

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

In DHCP address pool 1, specify subnet 192.1.0.0/16 for dynamic allocation, exclude IP address 192.1.0.1 from dynamic allocation, and specify gateway IP address 192.1.0.2.

```
[Switch] dhcp server ip-pool 1
[Switch-dhcp-pool-1] network 192.1.0.0 mask 255.255.0.0
[Switch-dhcp-pool-1] forbidden-ip 192.1.0.1
[Switch-dhcp-pool-1] gateway-list 192.1.0.2
[Switch-dhcp-pool-1] quit
```

Create a DHCP address pool named 2, and specify subnet 192.2.0.0/24 and gateway address 192.2.0.2 for the AC's VLAN-interface 200 and the INC server.

```
[Switch] dhcp server ip-pool 2
[Switch-dhcp-pool-2] network 192.2.0.0 mask 255.255.255.0
[Switch-dhcp-pool-2] gateway-list 192.2.0.2
[Switch-dhcp-pool-2] quit
```

Configuring the INC server

In this example, the RADIUS server runs INC PLAT 7.2(E0403L02) and INC INC - WSM 7.2(E0502L03). To configure the INC server:

1. Add a location:

- a. Click the **Service** tab.
- b. From the navigation tree, select **WLAN Manager > Location View**.
- c. Click **Add**.
The **Add Location** page opens.
- d. Configure the following parameters, as shown in [Figure 2](#):
 - Enter **BLE** in the **Location Name** field.
 - Use the default settings for other parameters.
- e. Click **OK**.

Figure 2 Adding a location

The screenshot shows the 'Add Location' dialog box within the WLAN Manager interface. The breadcrumb trail at the top reads 'Service > WLAN Manager > Location View > Add Location'. The dialog has a title bar 'Add Location' and a 'Help' icon. Inside, there are four fields: 'Location Name *' with the value 'BLE', 'Location Type' with a dropdown menu showing 'Area', 'Hotspot' with an unchecked checkbox, and 'Automatically Add AP' with an unchecked checkbox. At the bottom right, there are 'OK' and 'Cancel' buttons.

2. Add a Bluetooth AP:
 - a. On the newly created location view page, click **Add**, as shown in [Figure 3](#).
The **Select Devices** page opens.
 - b. On the **Device List** area, select the target Bluetooth AP, as shown in [Figure 4](#).
 - e. Click **OK**.

Figure 3 Adding a Bluetooth AP

The screenshot shows the 'BLE' location view page in the WLAN Manager interface. The breadcrumb trail at the top reads 'Service > WLAN Manager > Location View > BLE'. There is a 'Help' icon in the top right. Below the breadcrumb, there is a row of buttons: 'Add', 'Remove', 'Refresh', 'Back', and 'More...'. Below these buttons is a table with the following columns: 'Status', 'Device Status', 'Device List', 'SN', 'Model', 'IP Address', 'IPv6 Address', 'MAC Address', 'Online Clients', and 'Operation'. The table is currently empty, with the text 'No match found.' displayed. Below the table, there is a pagination bar showing '0-0 of 0. Page 1 of 1.' and a set of navigation buttons: '<<', '<', '>', '>>', and a dropdown menu showing '50'. At the bottom left, there is a timestamp: 'Data Captured at:2016-10-18 14:48:19'.

Figure 4 Selecting a Bluetooth AP

Select Device - Windows Internet Explorer

http://2.0.0.160:8080/imc/wlan/view/deviceSelectContent.xhtml?beanName=wlanLocationDeviceBean&deviceType=2

Select Device

Device Label Device Type

Serial Number IP Address

Model Online Status

AC

Device List

<input type="checkbox"/>	Status	Device Label	SN	IP Address	IPv6 Address	Model	AC
<input checked="" type="checkbox"/>		ap1(192.1...	210236A35...	192.1.0.3		H3C WA43...	H3C(192.1..

0-0 of 0. Page 1 of 1.

Data Captured at:2016-10-18 14:52:00

3. Add a topology:
 - a. On the newly created location view page, click the icon of viewing topology, as shown in [Figure 5](#).
The topology configuration page opens.
 - b. Click the icon of adding a map, as shown in [Figure 6](#).
 - c. Click the icon of setting the measuring scale, as shown in [Figure 7](#).
 - d. Click the save icon to save the topology, as shown in [Figure 8](#).

Figure 5 Adding a topology

Service > WLAN Manager > View Management > Location View

Add Refresh Export Hotspot

Location Name

	Location Name	Total APs	Online Fit APs	Offline Fit APs	View Topology	Move Location View	Modify	Delete
	BLE	1	1	0				

1-1 of 1. Page 1 of 1.

Data Captured at:2016-10-18 18:49:57

Figure 6 Adding a map

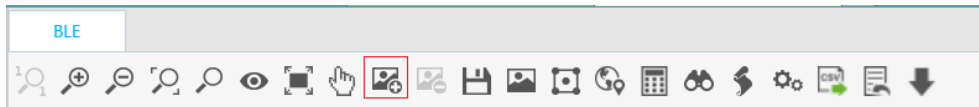


Figure 7 Adding a measuring scale

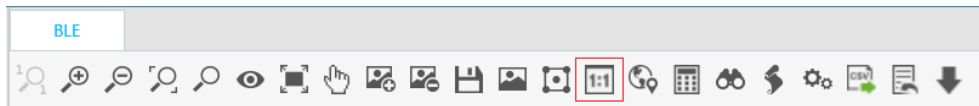
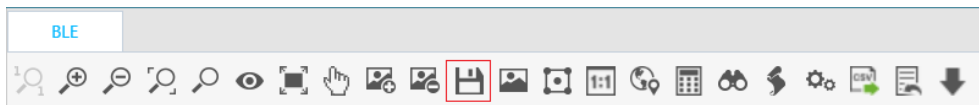


Figure 8 Saving the topology



Verifying the configuration

1. Log in to the INC management platform, and click the **Service** tab.
2. From the navigation tree, select **WLAN Manager > Location Manager> iBeacon List**.
3. On the page that opens, view the iBeacon information, including electric quantity, RSSI, UUID, Major ID, Minor ID, and transmit power.

Configuration files

- AC:

```
#
vlan 100
#
interface Vlan-interface100
 ip address 192.1.1.0.1 255.255.0.0
#
interface Vlan-interface200
 ip address dhcp-alloc
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 100 200
 undo port trunk permit vlan 1
#
wlan ap-group group1
 ap ap1
 rfid-tracking ble command-password cipher
 $c$3$AAu3rmjHUmAE0Wl2Rk1Jco6MPJ3Iqoh+pFgqhKFiHw==
 rfid-tracking ble enable
 rfid-tracking ble engine-address 192.2.0.1 engine-port 1145
 rfid-tracking ble report enable
```

```

rfid-tracking ble report interval 10
ap-model AP 3620
  radio 1
  radio 2
  module 1
    type BLE
    module enable
#
wlan ap ap1 model AP 3620
  serial-id 219801A28N819CE0002T
#

```

- **Switch:**

```

#
dhcp enable
#
vlan 100
#
vlan 200
#
dhcp server ip-pool 1
  gateway-list 192.1.0.2
  network 192.1.0.0 mask 255.255.0.0
  forbidden-ip 192.1.0.1
#
dhcp server ip-pool 2
  gateway-list 192.2.0.2
  network 192.2.0.0 mask 255.255.255.0
#
interface Vlan-interface100
  ip address 192.1.0.2 255.255.0.0
#
interface Vlan-interface200
  ip address 192.2.0.2 255.255.255.0
#
interface GigabitEthernet1/0/1
  port link-type trunk
  port trunk permit vlan 100 200
  undo port trunk permit vlan 1
#
interface GigabitEthernet1/0/2
  port access vlan 200
#
interface GigabitEthernet1/0/3
  port access vlan 100
  poe enable
#

```

Related documentation

- *Internet of Things Command Reference in INTELBRAS Access Controllers Command References*
- *Internet of Things Configuration Guide in INTELBRAS Access Controllers Configuration Guides*
- *WLAN Advanced Features Command Reference in INTELBRAS Access Controllers Command References*
- *WLAN Advanced Features Configuration Guide in INTELBRAS Access Controllers Configuration Guides*

INTELBRAS Access Controllers

Mesh Link Establishment Between Fit APs

Configuration Examples

Copyright © 2024 Intelbras S.A All rights reserved.

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

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

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

Contents

Introduction	1
Prerequisites	1
Example: Configuring a mesh link between fit APs.....	1
Network configuration.....	1
Restrictions and guidelines	1
Procedures	2
Configuring the switch	2
Configuring the AC.....	3
Verifying the configuration	6
Configuration files.....	7
Related documentation	9

Introduction

The following information provides an example of configuring a mesh link between fit APs.

Prerequisites

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

The configuration examples 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 mesh.

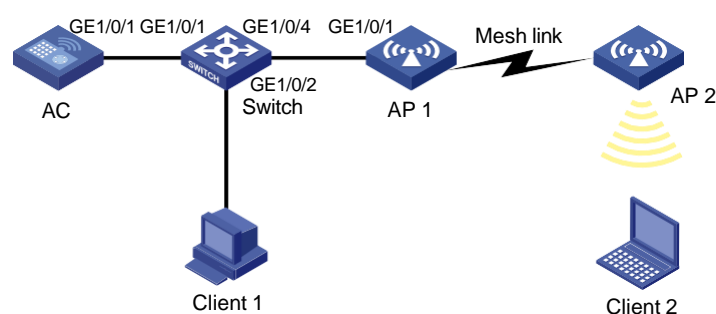
Example: Configuring a mesh link between fit APs

Network configuration

As shown in [Figure 1](#), in centralized forwarding mode, the AC is connected to the switch, and the switch assigns an IP address to APs and clients as a DHCP server. Configure devices to meet the following requirements:

- AP 1 and AP 2 obtain an IP address from the address pool on VLAN 10 configured on the switch and come online from the AC.
- The wired client and wireless client are assigned to the same VLAN and are reachable to each other at Layer 2.

Figure 1 Network diagram



Restrictions and guidelines

- Use the actual serial ID of an AP to uniquely identify that AP.
- To avoid too many packets in VLAN 1, configure GE1/0/4 that connects the switch to AP 1 as a trunk port, and remove the port from VLAN 1.

- To avoid mesh link errors, do not configure WLAN mesh and auto bandwidth adjustment of WLAN RRM at the same time.

Procedures

Configuring the switch

1. Configure interfaces on the switch:

Create VLAN 10 and VLAN-interface 10, and assign an IP address to the VLAN interface. The AC will use this IP address to establish a CAPWAP tunnel with the AP.

```
<Switch> system-view
[Switch] vlan 10
[Switch-vlan10] quit
[Switch] interface vlan-interface 10
[Switch-Vlan-interface10] ip address 172.16.1.1 255.255.255.0
[Switch-Vlan-interface10] quit
```

Create VLAN 20 and VLAN-interface 20, and assign an IP address to the VLAN interface. This VLAN will be used as the gateway for the clients.

```
[Switch] vlan 20
[Switch-vlan20] quit
[Switch] interface vlan-interface 20
[Switch-Vlan-interface20] ip address 192.168.10.1 255.255.255.0
[Switch-Vlan-interface20] quit
```

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

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

Configure GigabitEthernet 1/0/4 that connects the switch to AP 1 as a trunk port, remove the port from VLAN 1, and assign the port to all the other VLANs.

```
[Switch] interface gigabitEthernet 1/0/4
[Switch-GigabitEthernet1/0/4] port link-type trunk
[Switch-GigabitEthernet1/0/4] port trunk permit vlan all
[Switch-GigabitEthernet1/0/4] undo port trunk permit vlan 1
```

Set the PVID of GigabitEthernet 1/0/4 to VLAN 10.

```
[Switch-GigabitEthernet1/0/4] port trunk pvid vlan 10
[Switch-GigabitEthernet1/0/4] quit
```

Assign GigabitEthernet 1/0/2 that connects the switch to Client 1 to VLAN 20.

```
[Switch] interface gigabitEthernet 1/0/2
[Switch-GigabitEthernet1/0/2] port access vlan 20
[Switch-GigabitEthernet1/0/2] quit
[Switch] quit
```

2. Configure the DHCP server:

Enable DHCP.

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


Specify 172.16.1.0/24 as the address range for dynamic allocation in DHCP address pool 1, and specify 172.16.1.1 as the gateway address.

```
[Switch] dhcp server ip-pool 1
[Switch-dhcp-pool-1] network 172.16.1.0 mask 255.255.255.0
[Switch-dhcp-pool-1] gateway-list 172.16.1.1
```

Exclude 172.16.1.2 from dynamic allocation.

```
[Switch-dhcp-pool-1] forbidden-ip 172.16.1.2
[Switch-dhcp-pool-1] quit
```

Configure DHCP address pool 2. In the address pool, specify 192.168.10.1 as the gateway IP address, 192.168.10.0/24 as the subnet for dynamic allocation, and 192.168.10.1 as the DNS server address.

```
[Switch] dhcp server ip-pool 2
[Switch-dhcp-pool-2] network 192.168.10.0 mask 255.255.255.0
[Switch-dhcp-pool-2] gateway-list 192.168.10.1
[Switch-dhcp-pool-2] dns-list 192.168.10.1
[Switch-dhcp-pool-2] quit
```

Configuring the AC

1. Configure interfaces on the AC:

Create VLAN 10 and VLAN-interface 10, and assign an IP address to the VLAN interface. The AC will use this IP address to establish a CAPWAP tunnel with the AP.

```
[AC] vlan 10
[AC-vlan10] quit
[AC] interface vlan-interface 10
[AC-Vlan-interface10] ip address 172.16.1.2 255.255.255.0
[AC-Vlan-interface10] quit
```

Create VLAN 20.

```
[AC] vlan 20
[AC-vlan20] quit
```

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

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

2. Configure a wireless service:

Create service template **office**.

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

Set the SSID to **Documents**.

```
[AC-wlan-st-office] ssid Documents
```

Specify VLAN 20 for the service. Clients will join the VLAN after coming online from the service.

```
[AC-wlan-st-office] vlan 20
```

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

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

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

```
[AC-wlan-st-office] cipher-suite ccmp
[AC-wlan-st-office] security-ie wpa
```

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

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

Enable the service template.

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

3. Configure AP 1:

NOTE:

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

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

```
[AC] wlan ap ap1 model AP 5630
[AC-wlan-ap-ap1] serial-id 219801A23V8192E00021
```

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

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

Specify the radio type as dot11an, and specify the channel as 36.

```
[AC-wlan-ap-group-group1] ap-model AP 5630
[AC-wlan-ap-group-group1-ap-model-AP 5630] radio 1
[AC-wlan-ap-group-group1-ap-model-AP 5630-radio-1] type
dot11an [AC-wlan-ap-group-group1-ap-model-AP 5630-radio-1]
```

channel 36 # Enable radio 1.

```
[AC-wlan-ap-group-group1-ap-model-AP 5630-radio-1] radio enable
[AC-wlan-ap-group-group1-ap-model-AP 5630-radio-1]
quit [AC-wlan-ap-group-group1-ap-model-AP 5630] quit
[AC-wlan-ap-group-group1] quit
```

4. Configure AP 2:

NOTE:

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

Create a manual AP named **ap2, and specify the AP model and serial ID.**

```
[AC] wlan ap ap2 model AP 5630
[AC-wlan-ap-ap2] serial-id 219801A23V8192E00022
```

Create AP group **group2, and configure a grouping rule by AP name to add AP **ap2** to the group.**

```
[AC] wlan ap-group group2
[AC-wlan-ap-group-group2] ap ap2
```

Specify the radio type as dot11an, and specify the channel as 36.

```
[AC-wlan-ap-group-group2] ap-model AP 5630
[AC-wlan-ap-group-group2-ap-model-AP 5630] radio 1
[AC-wlan-ap-group-group2-ap-model-AP 5630-radio-1] type
dot11an [AC-wlan-ap-group-group2-ap-model-AP 5630-radio-1]
channel 36
```

Bind service template `office` to radio 1 and enable radio 1.

```
[AC-wlan-ap-group-group2-ap-model-AP 5630-radio-1] service-template
office [AC-wlan-ap-group-group2-ap-model-AP 5630-radio-1] radio enable
[AC-wlan-ap-group-group2-ap-model-AP 5630-radio-1]
quit [AC-wlan-ap-group-group2-ap-model-AP 5630] quit
[AC-wlan-ap-group-group2] quit
```

5. Configure a mesh profile:

Create mesh profile 1.

```
[AC] wlan mesh-profile 1
```

Set the mesh ID to 1.

```
[AC-wlan-mesh-profile-1] mesh-id 1
```

Set the authentication and key management (AKM) mode to `sae`.

```
[AC-wlan-mesh-profile-1] akm mode sae
```

Configure simple character string `meshlink` as the PSK.

```
[AC-wlan-mesh-profile-1] preshared-key pass-phrase simple meshlink
```

Enable the mesh profile.

```
[AC-wlan-mesh-profile-1] mesh-profile enable
[AC-wlan-mesh-profile-1] quit
```

Bind radio 1 in AP group `group1` to mesh profile 1. Bind radio 1 in AP group `group2` to mesh profile 1 in the same way.

```
[AC] wlan ap-group group1
[AC-wlan-ap-group-group1] ap-model AP 5630
[AC-wlan-ap-group-group1-ap-model-AP 5630] radio 1
[AC-wlan-ap-group-group1-ap-model-AP 5630-radio-1] mesh-profile 1
```

6. Add the MAC address of AP 2 to the mesh peer whitelist for APs in group `group1`. Add the MAC address of AP 1 to the mesh peer whitelist for APs in group `group2` in the same way.

```
[AC-wlan-ap-group-group1-ap-model-AP 5630-radio-1] mesh peer-mac-
address 90e7-1066-e060
[AC-wlan-ap-group-group1-ap-model-AP 5630-radio-1]
quit [AC-wlan-ap-group-group1-ap-model-AP 5630] quit
```

7. Configure a WLAN-mesh interface: The following uses AP group `group1` as an example. Configure a WLAN-mesh interface for AP group `group2` in the same way.

Create a WLAN-mesh interface.

```
[AC-wlan-ap-group-group1] interface wlan-mesh 1
```

Configure WLAN-mesh interface 1 as a trunk port, and assign the port to all VLANs.

```
[AC-wlan-ap-group-group1-wlan-mesh-1] mesh-port link-type trunk
[AC-wlan-ap-group-group1-wlan-mesh-1] mesh-port trunk permit vlan all
[AC-wlan-ap-group-group1-wlan-mesh-1] quit
```

Bind WLAN-mesh interface 1 to radio 1.

```
[AC-wlan-ap-group-group1] ap-model AP 5630
[AC-wlan-ap-group-group1-ap-model-AP 5630] radio 1
[AC-wlan-ap-group-group1-ap-model-AP 5630-radio-1] mesh-interface
1 [AC-wlan-ap-ap1-radio-1] quit
[AC-wlan-ap-ap1] quit
```

8. Editing the AP's configuration file

Edit the AP's configuration file, name it `map.txt`.

```
system-view
vlan 20
```

```
quit
interface gigabitethernet 1/0/1
port link-type trunk
port trunk permit vlan all
quit
```

9. Upload the configuration file to the AC.

```
[AC] wlan ap-group group1
[AC-wlan-ap-group-group1] ap-model AP 5630
[AC-wlan-ap-group-group1-ap-model-AP 5630] map-configuration
map.txt [AC-wlan-ap-group-group1-ap-model-AP 5630] quit
[AC-wlan-ap-group-group1] quit
```

Verifying the configuration

1. Verify that the APs have been associated with the AC. If the APs are in R/M state, the APs have been associated with the AC.

```
<AC> display wlan ap all
```

AP information

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

AP name	APID	State	Model	Serial ID
ap1	1	R/M	AP 5630	219801A23V8192E00021
ap2	2	R/M	AP 5630	219801A23V8192E00022

2. Display mesh link information on the AC.

```
<AC> display wlan mesh-link ap
```

```
AP name: ap1
```

Peer	Local	Status	RSSI	Packets (Rx/Tx)
90e7-1066-e060	542b-dea7-a8c0	Forwarding	57	6919/6452

```
AP name: ap2
```

Peer	Local	Status	RSSI	Packets (Rx/Tx)
542b-dea7-a8c0	90e7-1066-e060	Forwarding	55	7726/6801

3. Ping Client 2 from Client 1 to verify that they are reachable to each other.

```
C:\Users\system32> ping 192.168.10.3
```

```
Pinging 192.168.10.3 with 32 bytes of data:
```

```
Reply from 192.168.10.3: bytes=32 time<1ms TTL=255
Reply from 192.168.10.3: bytes=32 time<1ms TTL=255
Reply from 192.168.10.3: bytes=32 time<1ms TTL=255
Reply from 192.168.10.3: bytes=32 time<1ms TTL=255
```

```
Ping statistics for 192.168.10.3:
```

```
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

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

```
Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Configuration files

- Switch:

```
#
dhcp enable

#
vlan 10
#
vlan 20
#
dhcp server ip-pool 1
gateway-list 172.16.1.1
network 172.16.1.0 mask 255.255.255.0
forbidden-ip 172.16.1.2
#
dhcp server ip-pool 2
gateway-list 192.168.10.1
network 192.168.10.0 mask 255.255.255.0
dns-list 192.168.10.1
#
interface Vlan-interface10
ip address 172.16.1.1 255.255.255.0
#
interface Vlan-interface20
ip address 192.168.10.1 255.255.255.0
#
interface GigabitEthernet1/0/1
port link-type trunk
port trunk permit vlan all
#
interface GigabitEthernet1/0/2
port access vlan 20
#
interface GigabitEthernet1/0/4
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 2 to 4094
port trunk pvid vlan 10
#
```

- AC:

```
#
wlan mesh-profile 1
mesh-id 1
akm mode sae
preshared-key pass-phrase cipher $c$3$qVXx1KuNn4FeEi3nMUkQ7A8jcIMrN8JH2AOv
mesh-profile enable
#
vlan 10
```

```

#
vlan 20
#
wlan service-template office
    ssid Documents
    vlan 20
    client forwarding-location ac
    akm mode psk
    preshared-key pass-phrase cipher $c$3$hqxvBKKM0Go5NmRe1XGhiy/nVnzusK20fz1z
    cipher-suite ccmp
    security-ie wpa
    service-template enable
#
interface Vlan-interface10
    ip address 172.16.1.2 255.255.255.0
#
interface GigabitEthernet1/0/1
    port link-type trunk
    port trunk permit vlan all
#
wlan ap-group group1
    vlan 1
    ap ap1
    interface wlan-mesh 1
        mesh-port link-type trunk
        mesh-port trunk permit vlan all
    ap-model AP 5630
        radio 1
            type dot11an
            channel 36
            radio enable
            service-template 1
            mesh-interface 1
            mesh-profile 1
            mesh peer-mac-address 90e7-1066-e060
#
wlan ap-group group2
    map-configuration flash:/map.txt
    vlan 1
    ap ap2
    interface wlan-mesh 1
        mesh-port link-type trunk
        mesh-port trunk permit vlan all
    ap-model AP 5630
        radio 1
            type dot11an
            channel 36
            radio enable

```

```
mesh-interface 1
mesh-profile 1
mesh peer-mac-address 542b-dea7-a8c0
#
wlan ap ap1 model AP 5630
serial-id 219801A23V8192E00021
#
wlan ap ap2 model AP 5630
serial-id 219801A23V8192E00022
#
```

Related documentation

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

INTELBRAS Access Controllers

Mesh Link Establishment Between Fit AP and Fat AP

Configuration Examples

Copyright © 2024 Intelbras S.A All rights reserved.

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

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

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

Contents

Introduction	1
Prerequisites	1
Example: Configuring a mesh link between a fit AP and a fat AP.....	1
Network configuration.....	1
Restrictions and guidelines	1
Procedures	2
Configuring Switch 1	2
Configuring the AC.....	3
Configuring Switch 2	5
Configuring AP 2	6
Verifying the configuration	7
Configuration files.....	8
Related documentation	10

Introduction

The following information provides an example of configuring a mesh link between a fit AP and a fat AP.

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 mesh.

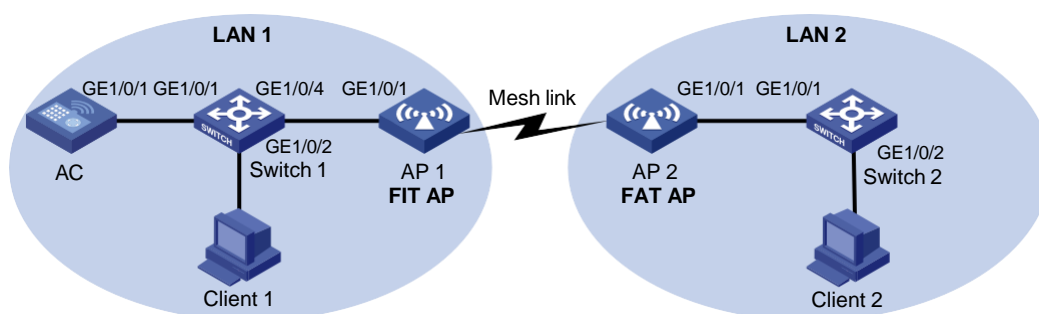
Example: Configuring a mesh link between a fit AP and a fat AP

Network configuration

As shown in [Figure 1](#), in centralized forwarding mode, the AC in LAN 1 is connected to Switch 1, and Switch 1 assigns an IP address to the AP and client in LAN 1 as a DHCP server. Switch 2 assigns an IP address to the client in LAN 2 as a DHCP server. Configure the devices to meet the following requirements:

- AP 1 obtains an IP address from the address pool on VLAN 10 configured on Switch 1 and comes online from the AC.
- The clients in LAN 1 and LAN 2 are assigned to different VLANs and are reachable to each other at Layer 3.

Figure 1 Network diagram



Restrictions and guidelines

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

- Configure GE 1/0/4 that connects Switch 1 to the AP as a trunk port, and remove the port from VLAN 1.
- To avoid mesh link errors, do not configure WLAN mesh and auto bandwidth adjustment of WLAN RRM at the same time.

Procedures

Configuring Switch 1

1. Configure interfaces on Switch 1:

Create VLAN 10 and VLAN-interface 10, and assign an IP address to the VLAN interface. The AC will use this IP address to establish a CAPWAP tunnel with the AP.

```
<Switch1> system-view
[Switch1] vlan 10
[Switch1-vlan10] quit
[Switch1] interface vlan-interface 10
[Switch1-Vlan-interface10] ip address 172.16.1.1 255.255.255.0
[Switch1-Vlan-interface10] quit
```

Create VLAN 20 and VLAN-interface 20, and assign an IP address to the VLAN interface. This VLAN will be used as the gateway for the clients.

```
[Switch1] vlan 20
[Switch1-vlan20] quit
[Switch1] interface vlan-interface 20
[Switch1-Vlan-interface20] ip address 192.168.10.1 255.255.255.0
[Switch1-Vlan-interface20] quit
```

Create VLAN 30 and VLAN-interface 30, and assign an IP address to the VLAN interface. The switch will use this VLAN to communicate with the AP.

```
[Switch1] vlan 30
[Switch1-vlan30] quit
[Switch1] interface vlan-interface 30
[Switch1-Vlan-interface30] ip address 10.12.12.1 255.255.255.0
[Switch1-Vlan-interface30] quit
```

Configure GigabitEthernet 1/0/1 that connects Switch 1 to the AC as a trunk port, and assign the port to all VLANs.

```
[Switch1] interface gigabitEthernet 1/0/1
[Switch1-GigabitEthernet1/0/1] port link-type trunk
[Switch1-GigabitEthernet1/0/1] port trunk permit vlan all
[Switch1-GigabitEthernet1/0/1] quit
```

Configure GigabitEthernet 1/0/4 that connects Switch 1 to AP 1 as a trunk port, remove the port from VLAN 1, and assign the port to all the other VLANs.

```
[Switch1] interface gigabitEthernet 1/0/4
[Switch1-GigabitEthernet1/0/4] port link-type trunk
[Switch1-GigabitEthernet1/0/4] port trunk permit vlan all
[Switch1-GigabitEthernet1/0/4] undo port trunk permit vlan 1
```

Set the PVID of GigabitEthernet 1/0/4 to VLAN 10.

```
[Switch1-GigabitEthernet1/0/4] port trunk pvid vlan 10
[Switch1-GigabitEthernet1/0/4] quit
```

Assign GigabitEthernet 1/0/2 that connects Switch 1 to Client 1 to VLAN 20.

```
[Switch1] interface gigabitEthernet 1/0/2
[Switch1-GigabitEthernet1/0/2] port access vlan 20
[Switch1-GigabitEthernet1/0/2] quit
[Switch1] quit
```

2. Configure the DHCP server:

Enable DHCP.

```
<Switch1> system-view
[Switch1] dhcp enable
```

Specify 172.16.1.0/24 as the address range for dynamic allocation in DHCP address pool 1, and specify 172.16.1.1 as the gateway address.

```
[Switch1] dhcp server ip-pool 1
[Switch1-dhcp-pool-1] network 172.16.1.0 mask 255.255.255.0
[Switch1-dhcp-pool-1] gateway-list 172.16.1.1
```

Exclude 172.16.1.2 from dynamic allocation.

```
[Switch1-dhcp-pool-1] forbidden-ip 172.16.1.2
[Switch1-dhcp-pool-1] quit
```

Configure DHCP address pool 2. In the address pool, specify 192.168.10.1 as the gateway IP address, 192.168.10.0/24 as the subnet for dynamic allocation, and 192.168.10.1 as the DNS server address.

```
[Switch1] dhcp server ip-pool 2
[Switch1-dhcp-pool-2] network 192.168.10.0 mask 255.255.255.0
[Switch1-dhcp-pool-2] gateway-list 192.168.10.1
[Switch1-dhcp-pool-2] dns-list 192.168.10.1
[Switch1-dhcp-pool-2] quit
```

3. # Configure a route to the network where Client 2 resides.

```
[Switch1] ip route-static 192.168.20.0 255.255.255.0 10.12.12.2
```

Configuring the AC

1. Configure interfaces on the AC:

Create VLAN 10 and VLAN-interface 100, and assign an IP address to the VLAN interface. The AC will use this IP address to establish a CAPWAP tunnel with the AP.

```
[AC] vlan 10
[AC-vlan10] quit
[AC] interface vlan-interface 10
[AC-Vlan-interface10] ip address 172.16.1.2 255.255.255.0
[AC-Vlan-interface10] quit
```

Configure GigabitEthernet 1/0/1 that connects the AC to Switch 1 as a trunk port, and assign the port to all VLANs.

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

2. Configure a fit AP:

NOTE:

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

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

```
[AC] wlan ap ap1 model AP 5630
[AC-wlan-ap-ap1] serial-id 219801A23V8192E00021
[AC-wlan-ap-ap1] quit
```

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

```
[AC] wlan ap-group group1
[AC-wlan-ap-group-group1] ap ap1
[AC-wlan-ap-group-group1] ap-model AP 5630
[AC-wlan-ap-group-group1-ap-model-AP 5630] radio 1
```

Enter the view of radio 1, specify the radio type as dot11an, and specify the channel as 36.

```
[AC-wlan-ap-group-group1-ap-model-AP 5630-radio-1] radio 1
[AC-wlan-ap-group-group1-ap-model-AP 5630-radio-1] type
dot11an [AC-wlan-ap-group-group1-ap-model-AP 5630-radio-1]
channel 36 # Enable radio 1.
[AC-wlan-ap-group-group1-ap-model-AP 5630-radio-1] radio enable
[AC-wlan-ap-group-group1-ap-model-AP 5630-radio-1]
quit [AC-wlan-ap-group-group1-ap-model-AP 5630-radio-1] quit [AC-wlan-ap-group-group1] quit
```

3. Configure a mesh profile:

Create mesh profile 1.

```
[AC] wlan mesh-profile 1
```

Set the mesh ID to 1.

```
[AC-wlan-mesh-profile-1] mesh-id 1
```

Set the authentication and key management (AKM) mode to **sae.**

```
[AC-wlan-mesh-profile-1] akm mode sae
```

Configure simple character string **meshlink as the PSK.**

```
[AC-wlan-mesh-profile-1] preshared-key pass-phrase simple meshlink
```

Enable the mesh profile.

```
[AC-wlan-mesh-profile-1] mesh-profile enable
[AC-wlan-mesh-profile-1] quit
```

Bind radio 1 to the mesh profile.

```
[AC] wlan ap-group group1
[AC-wlan-ap-group-group1] ap-model AP 5630
[AC-wlan-ap-group-group1-ap-model-AP 5630] radio 1
[AC-wlan-ap-group-group1-ap-model-AP 5630-radio-1] mesh-profile 1
```

4. Add the MAC address of AP 2 to the mesh peer whitelist for AP **ap1.**

```
[AC-wlan-ap-group-group1-ap-model-AP 5630-radio-1] mesh peer-mac-
address 90e7-1066-e060
[AC-wlan-ap-group-group1-ap-model-AP 5630-radio-1]
quit [AC-wlan-ap-group-group1-ap-model-AP 5630] quit
```

5. Configure a WLAN-mesh interface:

Create a WLAN-mesh interface.

```
[AC-wlan-ap-group-group1] interface wlan-mesh 1
```

Configure WLAN-mesh interface 1 as a trunk port, and assign the port to all VLANs.

```
[AC-wlan-ap-group-group1-wlan-mesh-1] mesh-port link-type trunk
[AC-wlan-ap-group-group1-wlan-mesh-1] mesh-port trunk permit vlan all
```

```
[AC-wlan-ap-group-group1-wlan-mesh-1] quit
# Bind WLAN-mesh interface 1 to radio 1.
[AC-wlan-ap-group-group1] ap-model AP 5630
[AC-wlan-ap-group-group1-ap-model-AP 5630] radio 1
[AC-wlan-ap-group-group1-ap-model-AP 5630-radio-1] mesh-interface
1 [AC-wlan-ap-group-group1-ap-model-AP 5630-radio-1] quit
[AC-wlan-ap-group-group1-ap-model-AP 5630]
quit [AC-wlan-ap-group-group1] quit
```

6. Editing the AP's configuration file

Edit the AP's configuration file, name it map.txt.

```
system-view
vlan 30
quit
interface gigabitethernet 1/0/1
port link-type trunk
port trunk permit vlan all
quit
```

7. Upload the configuration file to the AC.

```
[AC] wlan ap-group group1
[AC-wlan-ap-group-group1] ap-model AP 5630
[AC-wlan-ap-group-group1-ap-model-AP 5630] map-configuration
map.txt [AC-wlan-ap-group-group1-ap-model-AP 5630] quit
[AC-wlan-ap-group-group1] quit
```

Configuring Switch 2

1. Configure interfaces on Switch 2:

Create VLAN 40 and VLAN-interface 40, and assign an IP address to the VLAN interface. This VLAN will be used for client access.

```
<Switch2> system-view
[Switch2] vlan 40
[Switch2-vlan40] quit
[Switch2] interface vlan-interface 40
[Switch2-Vlan-interface40] ip address 192.168.20.2 255.255.255.0
[Switch2-Vlan-interface40] quit
```

Configure GigabitEthernet 1/0/1 that connects Switch 2 to the AC as a trunk port, and assign the port to all VLANs.

```
[Switch2] interface gigabitEthernet 1/0/1
[Switch2-GigabitEthernet1/0/1] port link-type trunk
[Switch2-GigabitEthernet1/0/1] port trunk permit vlan all
[Switch2-GigabitEthernet1/0/1] quit
```

Assign GigabitEthernet1/0/2 that connects Switch 2 to Client 2 to VLAN 40.

```
[Switch2] interface gigabitEthernet 1/0/2
[Switch2-GigabitEthernet1/0/2] port access vlan 40
[Switch2-GigabitEthernet1/0/2] quit
```

2. Configure the DHCP server:

Enable DHCP.

```
<Switch2> system-view
```

```
[Switch2] dhcp enable
# Specify 192.168.20.0/24 as the address range for dynamic allocation in DHCP address pool 1,
and specify 192.168.20.1 as the gateway address.
[Switch2] dhcp server ip-pool 1
[Switch2-dhcp-pool-1] network 192.168.20.0 mask 255.255.255.0
[Switch2-dhcp-pool-1] gateway-list 192.168.20.1
# Exclude 192.168.20.1 from dynamic allocation.
[Switch2-dhcp-pool-1] forbidden-ip 192.168.20.1
[Switch2-dhcp-pool-1] quit
```

Configuring AP 2

1. Configure interfaces on AP 2:

Create VLAN 30 and VLAN-interface 30, and assign an IP address to the VLAN interface. The AP will use this VLAN to communicate with Switch 1.

```
<AP2> system-view
[AP2] vlan 30
[AP2-vlan30] quit
[AP2] interface vlan-interface 30
[AP2-Vlan-interface30] ip address 10.12.12.2 255.255.255.0
[AP2-Vlan-interface30] quit
```

Create VLAN 40 and VLAN-interface 20, and assign an IP address to the VLAN interface. This VLAN will be used as the gateway for the clients.

```
[AP2] vlan 40
[AP2-vlan40] quit
[AP2] interface vlan-interface 40
[AP2-Vlan-interface40] ip address 192.168.20.1 255.255.255.0
[AP2-Vlan-interface40] quit
```

2. Configure a radio interface:

Enter the view of WLAN-Radio 1/0/1, specify the radio type as dot11an, and specify the channel as 36.

```
[AP2] interface wlan-radio 1/0/1
[AP2-WLAN-Radio1/0/1] type dot11an
[AP2-WLAN-Radio1/0/1] channel 36
[AP2-WLAN-Radio1/0/1] quit
```

3. Configure a mesh profile:

Create mesh profile 1.

```
[AP2] wlan mesh-profile 1
```

Set the mesh ID to 1.

```
[AP2-wlan-mesh-profile-1] mesh-id 1
```

Set the authentication and key management (AKM) mode to **sae**.

```
[AP2-wlan-mesh-profile-1] akm mode sae
```

Configure simple character string **meshlink** as the PSK.

```
[AP2-wlan-mesh-profile-1] preshared-key pass-phrase simple meshlink
```

Enable the mesh profile.

```
[AP2-wlan-mesh-profile-1] mesh-profile enable
```

```
[AP2-wlan-mesh-profile-1] quit
```

Bind WLAN-Radio 1/0/1 to the mesh profile.

- ```
[AP2] interface wlan-radio 1/0/1
[AP2-WLAN-Radio1/0/1] mesh-profile 1
```
- Add the MAC address of AP 1 to the mesh peer whitelist for the fat AP.**

```
[AP2-WLAN-Radio1/0/1] mesh peer-mac-address 542b-dea7-a8c0
[AP2-WLAN-Radio1/0/1] quit
```
  - Configure a WLAN-mesh interface:**

**# Create a WLAN-mesh interface.**

```
[AP2] interface wlan-mesh 1
```

**# Configure WLAN-mesh interface 1 as a trunk port, and assign the port to all VLANs.**

```
[AP2-WLAN-Mesh1] port link-type trunk
[AP2-WLAN-Mesh1] port trunk permit vlan all
[AP2-WLAN-Mesh1] quit
```

**# Bind WLAN-mesh interface 1 to WLAN-Radio 1/0/1.**

```
[AP2] interface wlan-radio 1/0/1
[AP2-WLAN-Radio1/0/1] mesh-interface 1
[AP2-WLAN-Radio1/0/1] quit
```
  - Configure a route to the network where Client 1 resides.**

```
[AP2] ip route-static 192.168.10.0 255.255.255.0 10.12.12.1
```

## Verifying the configuration

- Verify that AP 1 has been associated with the AC. If the AP is in R/M state, the AP has been associated with the AC.

```
<AC> display wlan ap name ap1
```

AP information

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

| AP name | APID | State | Model   | Serial ID            |
|---------|------|-------|---------|----------------------|
| ap1     | 1    | R/M   | AP 5630 | 219801A23V8192E00021 |

- Display mesh link information on the fat AP:

```
<AP2> display wlan mesh-link
```

| Peer MAC       | RSSI | BSSID          | Interface      | Link state | Online time |
|----------------|------|----------------|----------------|------------|-------------|
| 542b-dea7-a8c0 | 81   | d461-fe59-4d20 | WLAN-MeshLink2 | Active(an) | 20h 00m 49s |

- Ping Client 2 from Client 1 to verify that they are reachable to each other.

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

Pinging 192.168.20.3 with 32 bytes of data:

```
Reply from 192.168.20.3: bytes=32 time<1ms TTL=255
```

```
Reply from 192.168.20.3: bytes=32 time<1ms TTL=255
```

```
Reply from 192.168.20.3: bytes=32 time<1ms TTL=255
```

```
Reply from 192.168.20.3: bytes=32 time<1ms TTL=255
```

Ping statistics for 192.168.20.3:

```
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

Approximate round trip times in milli-seconds:

```
Minimum = 0ms, Maximum = 0ms, Average = 0ms
```



# Configuration files

- Switch 1:

```
#
dhcp enable

#
vlan 10
#
vlan 20
#
vlan 30
#
dhcp server ip-pool 1
 forbidden-ip 172.16.1.2
 gateway-list 172.16.1.1
 network 172.16.1.0 mask 255.255.255.0
#
dhcp server ip-pool 2
 gateway-list 192.168.10.1
 network 192.168.10.0 mask 255.255.255.0
 dns-list 192.168.10.1
#
interface Vlan-interface10
 ip address 172.16.1.1 255.255.255.0
#
interface Vlan-interface20
 ip address 192.168.10.1 255.255.255.0
#
interface Vlan-interface30
 ip address 10.12.12.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan all
#
interface GigabitEthernet1/0/2
 port access vlan 20
#
interface GigabitEthernet1/0/4
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 2 to 4094
 port trunk pvid vlan 10
#
ip route-static 192.168.20.0 255.255.255.0 10.12.12.2
#
```

- AC:

```
#
```

```

wlan mesh-profile 1
 mesh-id 1
 akm mode sae
 preshared-key pass-phrase cipher c3$qVXx1KuNn4FeEi3nMUkQ7A8jcIMrN8JH2AOv
 mesh-profile enable
#
vlan 10
#
interface Vlan-interface10
 ip address 172.16.1.2 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan all
#
wlan ap-group group1
 map-configuration flash:/map.txt
 vlan 1
 ap ap1
 interface wlan-mesh 1
 mesh-port link-type trunk
 mesh-port trunk permit vlan all
 ap-model AP 5630
 radio 1
 type dot11an
 channel 36
 radio enable
 mesh-interface 1
 mesh-profile 1
 mesh peer-mac-address 90e7-1066-e060
#
wlan ap ap1 model AP 5630
 serial-id 219801A23V8192E00021
#

```

- **Switch 2:**

```

#
 dhcp enable
#
vlan 40
#
dhcp server ip-pool 1
 forbidden-ip 192.168.20.1
 gateway-list 192.168.20.1
 network 192.168.20.0 mask 255.255.255.0
#
interface Vlan-interface40
 ip address 192.168.20.2 255.255.255.0
#

```

```

interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan all
#
interface GigabitEthernet1/0/2
 port access vlan 40
#

```

- **AP 2:**

```

#
wlan mesh-profile 1
 mesh-id 1
 akm mode sae
 preshared-key pass-phrase cipher c3$qVXx1KuNn4FeEi3nMUkQ7A8jcIMrN8JH2AOv
 mesh-profile enable
#
vlan 30
#
vlan 40
#
interface Vlan-interface30
 ip address 10.12.12.2 255.255.255.0
#
interface Vlan-interface40
 ip address 192.168.20.1 255.255.255.0
#
interface WLAN-Radiol/0/1
 mesh-profile 1
 mesh-interface 1
 mesh peer-mac-address 542b-dea7-a8c0
 type dot11an
 channel 36
#
interface WLAN-Mesh1
 port link-type trunk
 port trunk permit vlan all
#
 ip route-static 192.168.10.0 255.255.255.0 10.12.12.1
#

```

## Related documentation

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

# INTELBRAS Access Controllers

## Auto-DFS and Auto-TPC Configuration Examples

---

Copyright © 2024 Intelbras S.A All rights reserved.

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

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

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

# Contents

|                                                  |   |
|--------------------------------------------------|---|
| Introduction .....                               | 1 |
| Prerequisites .....                              | 1 |
| Restrictions and guidelines .....                | 1 |
| Example: Configuring auto-DFS and auto-TPC ..... | 1 |
| Network configuration .....                      | 1 |
| Procedures .....                                 | 2 |
| Configuring the AC .....                         | 2 |
| Configure the switch .....                       | 3 |
| Verifying the configuration .....                | 4 |
| Configuration files .....                        | 7 |
| Related documentation .....                      | 9 |

# Introduction

The following information provides an example for configuring auto dynamic frequency selection (DFS) and auto transmit power control (TPC).

## Prerequisites

The following information applies to Comware-based access controllers and access points with a software version of 5439 or later (5411 or later for the AP 7000 series access points). Procedures and information in the examples might be slightly different depending on the software or hardware version of the access controllers and access points.

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

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

## Restrictions and guidelines

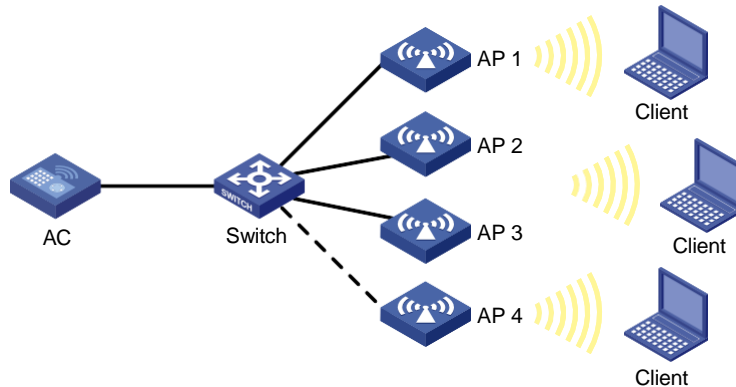
- Auto-DFS and auto-TPC are not supported in the following scenarios or devices:
  - Scenarios where the working channels and powers are not allowed to change.
  - Unified wired and wireless access controller.
  - WTU420, WTU420H, and X-share series access points.
- As a best practice, do not enable Auto-DFS or auto-TPC when CUPID location is enabled.
- Use the serial ID labeled on the AP to specify an AP.
- Do not manually specify a working channel, because it has a higher priority than the automatically selected channel.
- Make sure power lock is disabled.
- As a best practice, set the bandwidth mode for the 5 GHz radio to 40 MHz or 20 MHz.
- To enable auto-DFS or auto-TPC only for an AP or AP group, use the following commands:
  - `calibrate-channel self-decisive enable`
  - `calibrate-power self-decisive enable`

## Example: Configuring auto-DFS and auto-TPC

### Network configuration

As shown in [Figure 1](#), in centralized forwarding mode, the AC is connected to the switch, and the switch assigns an IP address to the AP and clients as a DHCP server. Configure auto-DFS and auto-TPC for the AP to change the working channel and transmit power automatically based on the wireless environment.

**Figure 1 Network diagram**



## Procedures

### Configuring the AC

**1. Configure interfaces on the AC:**

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

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

```
[AC] vlan 100
```

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

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

```
[AC-Vlan-interface100] ip address 192.1.0.1 16
```

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

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

```
[AC] vlan 200
```

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

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

```
[AC-Vlan-interface200] ip address 192.2.0.1 24
```

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

# Configure GigabitEthernet 1/0/1 that connects the switch to the AC as a trunk port, and assign the trunk port to VLAN1, VLAN 100, and VLAN 200.

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

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

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

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

**2. Configure a wireless service:**

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

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

# Configure the SSID as **service**.

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

Specify VLAN 200 in the service template.

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

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

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

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

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

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

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

# Enable the service template.

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

### 3. Configure an AP:

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

```
[AC] wlan ap ap1 model AP 5630
[AC-wlan-ap-ap1] serial-id 219801A23V8192E00021
```

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

```
[AC] wlan ap-group group1
[AC-wlan-ap-group-group1] ap ap1
[AC-wlan-ap-group-group1] ap-model AP 5630
```

# Enter the view of radio 1.

```
[AC-wlan-ap-group-group1-ap-model-AP 5630] radio 1
```

# Set the bandwidth mode to **40 MHz**.

```
[AC-wlan-ap-group-group1-ap-model-AP 5630-radio-1] channel band-width 40
```

# Bind WLAN service template **service** to radio 1 and enable the radio.

```
[AC-wlan-ap-group-group1-ap-model-AP 5630-radio-1] service-template
service [AC-wlan-ap-group-group1-ap-model-AP 5630-radio-1] radio enable
[AC-wlan-ap-group-group1-ap-model-AP 5630-radio-1]
quit [AC-wlan-ap-group-group1-ap-model-AP 5630] quit
[AC-wlan-ap-group-group1] quit
```

# Configure AP 2, AP 3, and AP 4 in the same way AP 1 is configured.

### 4. Configure auto-DFS and auto-TPC:

# Enter global configuration view.

```
[AC] wlan global-configuration
```

# Enable auto-TPC.

```
[AC-wlan-global-configuration] calibrate-power self-decisive enable all
```

# Enable auto-DFS.

```
[AC-wlan-global-configuration] calibrate-channel self-decisive enable all
[AC-wlan-global-configuration] quit
[AC] quit
```

## Configure the switch

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

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



```
[Switch-vlan100] quit
```

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

```
[Switch] vlan 200
```

```
[Switch-vlan200] quit
```

**# Configure GigabitEthernet 1/0/1 that connects the switch to the AC as a trunk port, and assign the trunk port to VLAN1, VLAN 100, and VLAN 200.**

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

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

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

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

**# Configure GigabitEthernet 1/0/2 that connects the switch to the APs as an access port, and assign the access port to VLAN 100.**

```
[Switch] interface range gigabitethernet 1/0/2 to gigabitethernet 1/0/5
```

```
[Switch-if-range] port link-type access
```

```
[Switch-if-range] port access vlan 100
```

**# Enable the PoE feature.**

```
[Switch-if-range] poe enable
```

```
[Switch-if-range] quit
```

**# Specify an IP address for VLAN-interface 100.**

```
[Switch] interface vlan-interface 100
```

```
[Switch-Vlan-interface100] ip address 192.1.0.2 16
```

```
[Switch-Vlan-interface100] quit
```

**# Specify an IP address for VLAN-interface 200.**

```
[Switch] interface vlan-interface 200
```

```
[Switch-Vlan-interface200] ip address 192.2.0.2 24
```

```
[Switch-Vlan-interface200] quit
```

**# Enable DHCP.**

```
[Switch] dhcp enable
```

**# Create DHCP address pool 100. Specify the 192.1.0.0/16 subnet and the 192.1.0.1 gateway for the pool.**

```
[Switch] dhcp server ip-pool 100
```

```
[Switch-dhcp-pool-100] network 192.1.0.0 mask 255.255.0.0
```

```
[Switch-dhcp-pool-100] gateway-list 192.1.0.1
```

```
[Switch-dhcp-pool-100] quit
```

**# Create DHCP address pool 200. Specify the 192.2.0.0/16 subnet and the 192.2.0.1 gateway for the pool.**

```
[Switch] dhcp server ip-pool 200
```

```
[Switch-dhcp-pool-200] network 192.2.0.0 mask 255.255.255.0
```

```
[Switch-dhcp-pool-200] gateway-list 192.2.0.1
```

```
[Switch-dhcp-pool-200] quit
```

## Verifying the configuration

1. View AP registration information on the AC:

**# Verify that the APs have been associated with the AC. If the APs are in R/M state, the APs have been associated with the AC.**

```
<AC> display wlan ap all
```

# AP information

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

| AP name | APID | State | Model   | Serial ID            |
|---------|------|-------|---------|----------------------|
| ap1     | 1    | R/M   | AP 5630 | 219801A23V8192E00021 |
| ap2     | 2    | R/M   | AP 5630 | 219801A23V8192E00022 |
| ap3     | 3    | R/M   | AP 5630 | 219801A23V8192E00023 |
| ap4     | 4    | R/M   | AP 5630 | 219801A23V8192E00024 |

## 2. View history and detailed RRM information on the AC.

# Display DFS and TPC information for radio 1 of AP 1 on the AC to verify that the channel and power have been changed.

<AC> display wlan rrm-history ap name ap1

### AP RRM History

Flags : I - Interference, P - Packets discarded, F - Retransmission,  
R - Radar, C - Coverage, B - Channelbusy,  
M - Manual O - Others

### AP RRM History : ap1

Radio : 1 Basic BSSID : 7848-59f3-df80

|        | Ch | Power (dBm) | Load (%) | Util (%) | Intf (%) | PER (%) | Retry (%) | Reason   | Date (yyyy-mm-dd) | Time (hh:mm:ss) |
|--------|----|-------------|----------|----------|----------|---------|-----------|----------|-------------------|-----------------|
| Before | 36 | 20          | 21       | 0        | 11       | 0       | 1         | ----C--- | 2021-02-25        | 15:12:56        |
| After  | 36 | 17          | 21       | 0        | 11       | 0       | 1         | -        | -                 | -               |
| Before | 36 | 17          | 21       | 0        | 12       | 0       | 0         | ----C--- | 2021-02-25        | 15:15:56        |
| After  | 36 | 14          | 21       | 0        | 12       | 0       | 0         | -        | -                 | -               |
| Before | 36 | 14          | 21       | 0        | 12       | 0       | 0         | ----C--- | 2021-02-25        | 15:18:56        |
| After  | 36 | 11          | 21       | 0        | 12       | 0       | 0         | -        | -                 | -               |
| Before | 36 | 11          | 18       | 0        | 11       | 0       | 10        | - ---B-- | 2021-02-25        | 15:25:21        |
| After  | 40 | 11          | 16       | 0        | 10       | 0       | 8         | -        | -                 | -               |

# Display detailed DFS and TPC information for radio 1 of AP 1 on the AC.

<AC> display wlan rrm-status ap name ap1

### AP RRM Profile : ap1

Radio : 1 Basic BSSID : 7848-59f3-df80  
Channel : 40 Tx Power (dBm) : 14

| Ch | Nbrs | Load | Util | Intf | PER | Retry | Radar | Last Detected At |
|----|------|------|------|------|-----|-------|-------|------------------|
|----|------|------|------|------|-----|-------|-------|------------------|

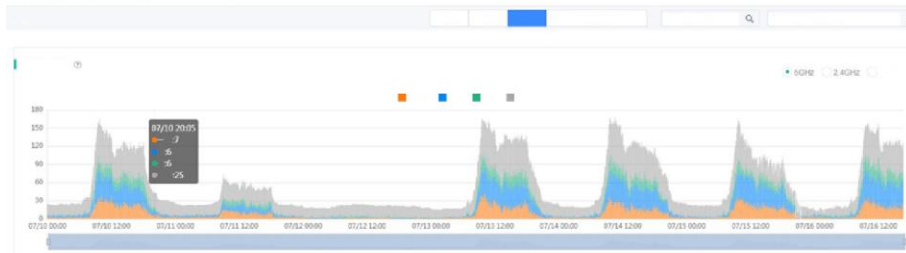
|     |    | (%) | (%) | (%) | (%) | (%) |   |                     |
|-----|----|-----|-----|-----|-----|-----|---|---------------------|
| 36  | 44 | 23  | 0   | 16  | 0   | 0   | - | 2021-02-26 15:30:32 |
| 40  | 3  | 9   | -   | 1   | 0   | -   | - | 2021-02-26 15:30:32 |
| 44  | 11 | 18  | -   | 6   | 0   | -   | - | 2021-02-26 15:30:32 |
| 48  | 8  | 30  | -   | 10  | 0   | -   | - | 2021-02-26 15:30:32 |
| 52  | 25 | 17  | -   | 12  | 0   | -   | - | 2021-02-26 15:30:32 |
| 56  | 0  | 7   | -   | 0   | 0   | -   | - | 2021-02-26 15:30:32 |
| 60  | 4  | 8   | -   | 1   | 0   | -   | - | 2021-02-26 15:30:32 |
| 64  | 7  | 7   | -   | 0   | 0   | -   | - | 2021-02-26 15:30:32 |
| 149 | 30 | 32  | -   | 24  | 0   | -   | - | 2021-02-26 15:30:32 |
| 153 | 12 | 10  | -   | 3   | 0   | -   | - | 2021-02-26 15:30:32 |
| 157 | 12 | 14  | -   | 4   | 0   | -   | - | 2021-02-26 15:30:32 |
| 161 | 5  | 8   | -   | 2   | 0   | -   | - | 2021-02-26 15:30:32 |
| 165 | 5  | 7   | -   | 1   | 0   | -   | - | 2021-02-26 15:30:32 |

| Nbr-MACAddress | Ch  | Intf<br>(%) | SignalStr<br>(dBm) | Type      | Last Detected At    |
|----------------|-----|-------------|--------------------|-----------|---------------------|
| 0023-89e2-ed80 | 36  | 0           | -29                | Unmanaged | 2021-02-26 15:30:40 |
| 0023-ee00-1168 | 52  | 0           | -88                | Unmanaged | 2021-02-26 15:30:40 |
| 04d7-a537-8540 | 149 | 0           | -68                | Unmanaged | 2021-02-26 15:30:40 |
| 1019-651b-d682 | 36  | 0           | -7                 | Unmanaged | 2021-02-26 15:30:40 |
| 1019-651b-d691 | 149 | 2           | -52                | Unmanaged | 2021-02-26 15:30:40 |
| 346b-5b6c-1e00 | 36  | 0           | -47                | Unmanaged | 2021-02-26 15:30:40 |
| 346b-5b6c-1e01 | 36  | 0           | -53                | Unmanaged | 2021-02-26 15:30:40 |
| 346b-5b76-1d20 | 36  | 0           | -35                | Managed   | 2021-02-26 15:30:40 |
| 346b-5b76-1d22 | 36  | 0           | -23                | Managed   | 2021-02-26 15:30:40 |
| 346b-5b76-1d23 | 36  | 0           | -17                | Managed   | 2021-02-26 15:30:40 |
| 346b-5b76-1d24 | 36  | 0           | -20                | Managed   | 2021-02-26 15:30:40 |
| 3891-d502-be60 | 52  | 0           | -60                | Managed   | 2021-02-26 15:30:40 |
| 3891-d502-be61 | 52  | 0           | -61                | Managed   | 2021-02-26 15:30:40 |
| 3891-d58a-8f80 | 44  | 0           | -75                | Unmanaged | 2021-02-26 15:30:40 |
| 3891-d58a-8f81 | 44  | 0           | -76                | Unmanaged | 2021-02-26 15:30:40 |
| 3891-d58a-8f82 | 44  | 0           | -75                | Unmanaged | 2021-02-26 15:30:40 |
| 3891-d58a-8f90 | 161 | 0           | -94                | Unmanaged | 2021-02-26 15:30:40 |
| 3891-d58d-6d41 | 52  | 0           | -45                | Unmanaged | 2021-02-26 15:30:40 |
| 3897-d618-90e0 | 36  | 0           | -32                | Unmanaged | 2021-02-26 15:30:40 |
| 3897-d6e0-e860 | 36  | 0           | -38                | Unmanaged | 2021-02-26 15:30:40 |

### 3. (Optional.) Connect the AC to the Cloudnet platform to view AP and client statistics.

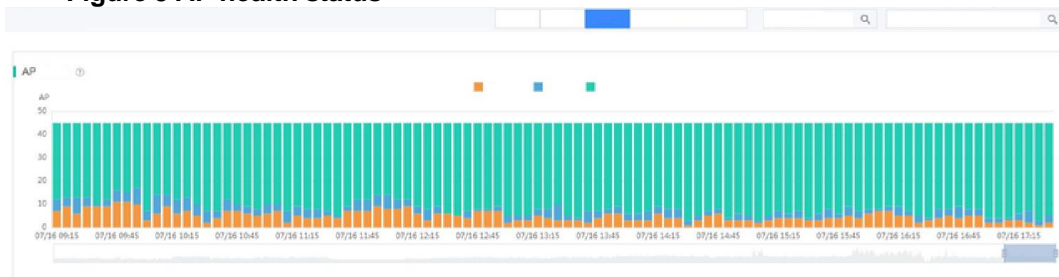
# View the health status of clients to identify whether the number of clients with a health score of excellent and good has increased.

**Figure 2 Client health status**



# View the health status of APs to identify whether the number of APs with a health score of excellent and good has increased.

**Figure 3 AP health status**



## Configuration files

- Switch:

```
#
dhcp enable
#
vlan 100
#
vlan 200
#
dhcp server ip-pool 100
gateway-list 192.1.0.1
network 192.1.0.0 mask 255.255.0.0
#
dhcp server ip-pool 200
gateway-list 192.2.0.1
network 192.2.0.0 mask 255.255.255.0
#
interface Vlan-interface100
ip address 192.1.0.2 255.255.0.0
#
interface Vlan-interface200
ip address 192.2.0.2 255.255.255.0
```

```
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 1 100 200
#
interface GigabitEthernet1/0/2
 port link-type access
 port access vlan 100
 poe enable
#
interface GigabitEthernet1/0/3
 port link-type access
 port access vlan 100
 poe enable
#
interface GigabitEthernet1/0/4
 port link-type access
 port access vlan 100
 poe enable
#
interface GigabitEthernet1/0/5
 port link-type access
 port access vlan 100
 poe enable
#
```

- **AC:**

```
#
wlan global-configuration
 calibrate-channel self-decisive enable all
 calibrate-power self-decisive enable all
#
vlan 100
#
vlan 200
#
wlan service-template service
 ssid service
 vlan 200
 client forwarding-location ap
 akm mode psk
 preshared-key pass-phrase cipher c3$HOaHaYA7Aazh6+V0xH8AvnFdV1xTZew0uBZs
 cipher-suite ccmp
 security-ie rsn
 service-template enable
#
interface Vlan-interface100
 ip address 192.1.0.1 255.255.0.0
#
```

```

interface Vlan-interface200
 ip address 192.2.0.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 1 100 200
#
wlan ap-group group1
 vlan 1
 ap ap1
 ap-model AP 5630
 radio 1
 radio enable
 channel band-width 40
 service-template service
#
wlan ap ap1 model AP 5630
 serial-id 219801A23V8192E00021
#
wlan ap ap2 model AP 5630
 serial-id 219801A23V8192E00022
#
wlan ap ap3 model AP 5630
 serial-id 219801A23V8192E00023
#
wlan ap ap4 model AP 5630
 serial-id 219801A23V8192E00024
#

```

## Related documentation

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

# INTELBRAS Access Controllers

## AP Image Downloading 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 AP image downloading ..... | 1 |
| Network configuration .....                     | 1 |
| Restrictions and guidelines .....               | 1 |
| Procedures .....                                | 2 |
| Configuring the AC .....                        | 2 |
| Verifying the configuration .....               | 3 |
| Related documentation .....                     | 4 |



# Introduction

The following information provides an example for configuring AP image downloading.

## 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.

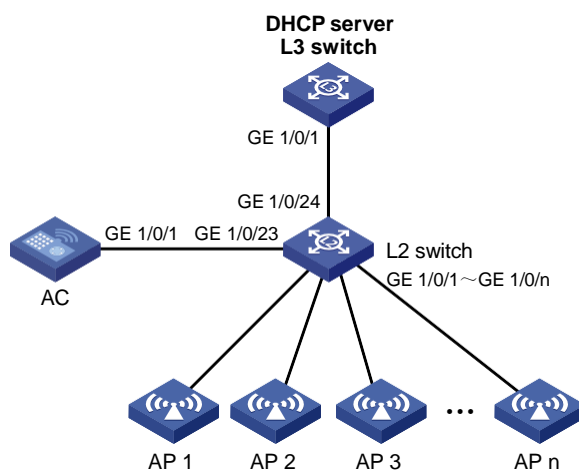
The following information is provided based on the assumption that you have basic knowledge of AP management and software upgrade.

## Example: Configuring AP image downloading

### Network configuration

As shown in [Figure 1](#), the AC is attached to the Layer 2 switch in hair-pin mode. The Layer 3 switch acts as the DHCP server to assign IP addresses to APs and the Layer 2 switch supplies power to APs through PoE. Configure AP image downloading to reduce time consumed by AC and AP upgrade.

**Figure 1 Network diagram**



### Restrictions and guidelines

- Before restarting the AC, save the running configuration.
- Make sure all APs to be upgraded are online when you configure the AC to deploy the image to APs.

- Typically, the system can deploy an image to 500 to 1000 APs per hour. Reserve sufficient time for image downloading.
- If an AP goes offline during image downloading, the downloading process for the AP is terminated. To upgrade the AP, you must configure the AC to deploy an image to the AP manually after the AP comes online.

# Procedures

## Configuring the AC

1. View the current software version of the AC.

```
<AC> display version
INTELBRAS Comware Software, Version 7.1.064, Release 5446
Copyright (c) 2004-2021 Intelbras S.A All rights reserved. INTELBRAS WC 7060
uptime is 0 weeks, 0 days, 20 hours, 51 minutes
Last reboot reason : User soft reboot
----- More -----
```

2. Configure the AC to download the image file and specify the file as the next startup configuration file:

# Configure the AC to download the image file. In this example, the TFTP server address is 192.168.0.1 and the image file name is test.ipe.

```
<AC> tftp 192.168.0.1 get test.ipe
Press CTRL+C to abort.
 % Total % Received % Xferd Average Speed Time Time Time Current
 Dload Upload Total Spent Left Speed
100 610.9M 100 610.9M 0 0 1206k 0 0:08:29 0:08:29 -: -1206k
Writing file...Done.
```

# Specify the file as the main next startup configuration file.

```
<AC> boot-loader file cfa0:/test.ipe all main
```

3. Deploy the image to all online APs.

```
<AC> system-view
[AC] wlan ap-image-deploy all
```

4. View information about image downloading:

# Display AP image downloading information, including the downloading progress, time consumed, and the numbers of APs to be upgraded, succeeded APs, ongoing APs, and failed APs.

```
[AC] display wlan ap statistics image-download
Completed : 50%
Time consumed : 03min 58s
Max. concurrent image downloads APs : 416
AP count:
 Total to download : 20
 Success : 9
 In-progress : 10
 Failed : 1
```

# Display APs that have failed to download images.

```
[AC] display wlan ap statistics image-download failed
AP name Failure reason
```

ap2 Tunnel down

# Resolve the issues that caused the failure. In this example, make AP 2 come online again.

# Re-deploy the image to the APs that have failed to download images.

```
[AC] wlan ap-image-deploy name ap2
```

**5. Save the running configuration and restart the AC and APs:**

# Verify that all APs have obtained the image. Then, save the running configuration.

```
[AC] save startup.cfg
```

The current configuration will be saved to cfa0:/startup.cfg. Continue? [Y/N]:y

cfa0:/startup.cfg exists, overwrite? [Y/N]:

Saving configuration cfa0:/startup.cfg. Please wait...

Configuration is saved to device successfully.

```
[AC] quit
```

# Restart all APs and restart the AC at the same time.

```
<AC> reset wlan ap all
```

Reset APs that have established or are to establish primary tunnels with the AC. Continue? [Y/N]:y

```
<AC> reboot
```

Start to check configuration with next startup configuration file, please wait. ....DONE!

This command will reboot the device. Continue? [Y/N]:y

Now rebooting, please wait...

## Verifying the configuration

# Verify the AC version.

```
<AC> display version
```

INTELBRAS Comware Software, Version 7.1.064, Release 5447

Copyright (c) 2004-2021 Intelbras S.A All rights reserved. INTELBRAS WC 7060

uptime is 0 weeks, 0 days, 0 hours, 10 minutes

Last reboot reason : User soft reboot

----- More -----

# Verify the version of any AP.

```
<Sysname> display wlan ap name ap1 verbose
```

AP name : ap1

AP ID : 1

AP group name : default-group

State : Run

Backup type : Master

Online time : 0 days 0 hours 12 minutes 12 seconds

System uptime : 0 days 0 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 : 192.168.0.50

UDP control port number : 18313

UDP data port number : N/A

H/W version : Ver.C  
S/W version : R5447  
----- More -----

## Related documentation

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

# INTELBRAS Access Controllers Dual-Uplink Interfaces Configuration Examples

---

Copyright © 2024 Intelbras S.A All rights reserved.

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

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

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

# Contents

|                                                   |   |
|---------------------------------------------------|---|
| Introduction .....                                | 1 |
| Prerequisites .....                               | 1 |
| Example: Configuring dual-uplink interfaces ..... | 1 |
| Network configuration .....                       | 1 |
| Analysis .....                                    | 2 |
| Restrictions and guidelines .....                 | 2 |
| Procedures .....                                  | 2 |
| Configuring the core switch .....                 | 2 |
| Configuring the AC .....                          | 3 |
| Configure the access switch .....                 | 5 |
| Verifying the configuration .....                 | 5 |
| Configuration files .....                         | 6 |
| Related documentation .....                       | 8 |

# Introduction

The following information provides an example for configuring dual-uplink interfaces to provide increased link bandwidth and load sharing.

## Prerequisites

The 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 DHCP, WLAN access, Ethernet link aggregation, and port isolation.

## Example: Configuring dual-uplink interfaces

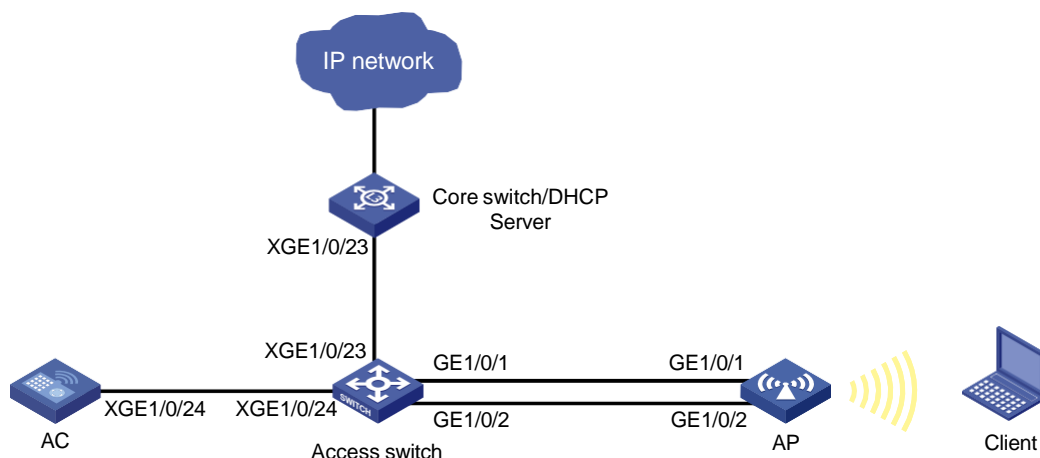
### Network configuration

As shown in [Figure 1](#), in centralized forwarding mode, the AC is connected to the access switch in hair-pin mode. The DHCP server assigns IP addresses to the AP and the client.

- Configure the client to come online in VLAN 200.
- Assign the AC to VLAN 100, and configure the AC and the AP to establish connections at Layer 2.
- Configure Layer 2 static link aggregation for the two uplink interfaces connecting the AP and the access switch. Configure load balancing based on source and destination MAC addresses for data traffic to be load balanced among different member ports of the aggregation.

You can configure the load balancing mode as needed. This example is for illustration only.

**Figure 1 Network diagram**



# Analysis

- Enable the DHCP server feature on the core switch for the core switch to act as the DHCP server.
- Enable PoE on the access switch to supply power to the AP.
- Configure wireless services on the AC for the client to access the network wirelessly.

## Restrictions and guidelines

- Use the actual serial ID of an AP to uniquely identify that AP.
- Forbids VLAN 1 traffic to be transmitted out of trunk ports to prevent packet accumulation in VLAN 1.
- As a best practice, use AP uplink interfaces that have the same port rate for link aggregation, and make sure the two peer interfaces on the switch also use the port rate. If the AP uplink interfaces use different port rates, only one interface can forward packets at a time, which increases link availability but disables load balancing.

## Procedures

### Configuring the core switch

1. Configure interfaces on the core switch:  
# Create VLAN 100 and VLAN-interface 100, and assign an IP address to the VLAN interface. The AP will obtain an IP address from the address pool matching the interface address.  

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

  
# Create VLAN 200 and VLAN-interface 200, and assign an IP address to the VLAN interface. The client will obtain an IP address from the address pool matching the interface address.  

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

  
# Configure Ten-GigabitEthernet 1/0/23 that connects the core switch to the access switch as a trunk port, remove the port from VLAN 1, and assign the port to VLANs 100 and 200.  

```
[Core switch] interface ten-gigabitethernet 1/0/23
[Core switch-Ten-GigabitEthernet1/0/23] port link-type trunk
[Core switch-Ten-GigabitEthernet1/0/23] undo port trunk permit vlan 1
[Core switch-Ten-GigabitEthernet1/0/23] port trunk permit vlan 100 200
[Core switch-Ten-GigabitEthernet1/0/23] quit
```
2. Configure the default route. (Details not shown.)
3. Configure the DHCP server:  
# Enable the DHCP server feature.



```
[Core switch] dhcp enable
Configure DHCP address pool 1, specify subnet 192.168.10.0/24, and set the gateway
address as 192.168.10.1.
[Core switch] dhcp server ip-pool 1
[Core switch-dhcp-pool-1] network 192.168.10.0 mask 255.255.255.0
[Core switch-dhcp-pool-1] gateway-list 192.168.10.1
Exclude 192.168.10.2 (IP address of VLAN-interface 100 of the AC) from IP allocation.
[Core switch-dhcp-pool-1] forbidden-ip 192.168.10.2
[Core switch-dhcp-pool-1] quit
Configure DHCP address pool 2, specify subnet 192.168.20.0/24, set the gateway address,
and specify the DNS server address. In this example, the DNS server address is also
192.168.20.1.
[Core switch] dhcp server ip-pool 2
[Core switch-dhcp-pool-2] network 192.168.20.0 mask 255.255.255.0
[Core switch-dhcp-pool-2] gateway-list 192.168.20.1
[Core switch-dhcp-pool-2] dns-list 192.168.20.1
[Core switch-dhcp-pool-2] quit
```

## Configuring the AC

### 1. Edit the AP configuration file.

# Edit the AP configuration file, name the file **map.txt**, and upload the file to the AC.

```
system-view
interface Bridge-Aggregation1
quit
interface GigabitEthernet1/0/1
undo port-isolate enable
port link-aggregation group 1
quit
interface GigabitEthernet1/0/2
undo port-isolate enable
port link-aggregation group 1
quit
link-aggregation global load-sharing mode source-mac destination-mac
```

### 2. Configure the AC interfaces:

# Create VLAN 100, and assign an IP address to VLAN-interface 100. The AP will obtain an address in the same subnet as the interface address to establish CAPWAP tunnels with the AC.

```
[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
```

# Configure Ten-GigabitEthernet 1/0/24 that connects the AC to the access switch as a trunk port, remove the port from VLAN 1, and assign the port to VLANs 100 and 200.

```
[AC] interface ten-gigabitethernet 1/0/24
```

```
[AC-Ten-GigabitEthernet1/0/24] port link-type trunk
[AC-Ten-GigabitEthernet1/0/24] undo port trunk permit vlan 1
[AC-Ten-GigabitEthernet1/0/24] port trunk permit vlan 100 200
[AC-Ten-GigabitEthernet1/0/24] quit
```

### 3. Configure wireless services:

#### # Create service template 1.

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

#### # Specify the SSID as **service**.

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

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

```
[AC-wlan-st-1] akm mode 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. If the AC acts as the client traffic forwarder by default, skip this step.

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

#### # Enable the service template.

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

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

### 4. Configure an AP:

---

#### NOTE:

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

---

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

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

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

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

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

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

#### # Bind service template 1 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] quit
```

#### # Deploy configuration file map.txt to APs in the AP group.

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

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

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

## Configure the access switch

**# Create VLANs 100 and 200. The switch will use VLAN 100 to forward the traffic on the CAPWAP tunnels between the AC and AP, and use VLAN 200 for client access.**

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

**# Configure Ten-GigabitEthernet 1/0/24 that connects the access switch to the AC as a trunk port, remove the port from VLAN 1, and assign the port to VLANs 100 and 200.**

```
[Access switch] interface ten-gigabitEthernet 1/0/24
[Access switch-Ten-GigabitEthernet1/0/24] port link-type trunk
[Access switch-Ten-GigabitEthernet1/0/24] undo port trunk permit vlan 1
[Access switch-Ten-GigabitEthernet1/0/24] port trunk permit vlan 100 200
[Access switch-Ten-GigabitEthernet1/0/24] quit
```

**# Configure Ten-GigabitEthernet 1/0/23 that connects the access switch to the core switch as a trunk port, remove the port from VLAN 1, and assign the port to VLANs 100 and 200.**

```
[Access switch] interface ten-gigabitEthernet 1/0/23
[Access switch-Ten-GigabitEthernet1/0/23] port link-type trunk
[Access switch-Ten-GigabitEthernet1/0/23] undo port trunk permit vlan 1
[Access switch-Ten-GigabitEthernet1/0/23] port trunk permit vlan 100 200
[Access switch-Ten-GigabitEthernet1/0/23] quit
```

**# Create Layer 2 aggregate interface 1, specify the interface as an access port, and assign the port to VLAN 100.**

```
[Access switch] interface bridge-aggregation 1
[Access switch-Bridge-Aggregation1] port access vlan 100
[Access switch-Bridge-Aggregation1] quit
```

**# Assign interfaces GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 to aggregation group 1, and enable PoE.**

```
[Access switch] interface gigabitEthernet 1/0/1
[Access switch-GigabitEthernet1/0/1] port link-aggregation group 1
[Access switch-GigabitEthernet1/0/1] poe enable
[Access switch-GigabitEthernet1/0/1] quit
[Access switch] interface gigabitEthernet 1/0/2
[Access switch-GigabitEthernet1/0/2] port link-aggregation group 1
[Access switch-GigabitEthernet1/0/2] poe enable
[Access switch-GigabitEthernet1/0/2] quit
```

**# Set the global load sharing mode to load share packets based on source and destination MAC addresses.**

```
[Access switch] link-aggregation global load-sharing mode source-mac destination-mac
```

## Verifying the configuration

### 1. View AP registration information on the AC:

**# Verify that the AP has been associated with the AC. If the AP is in R/M state, the AP has been 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: 20
Remaining APs: 19
Total AP licenses: 20
Local AP licenses: 20
Server AP licenses: 0
Remaining Local AP licenses: 19
Sync AP licenses: 0

```

#### AP information

```

State : I = Idle, J = Join, JA = JoinAck, IL = ImageLoad
 C = Config, DC = DataCheck, R = Run, M = Master, B = Backup
AP name AP ID State Model Serial ID
officeap 1 R/M AP 3620 219801A28N819CE0002T

```

### 2. View client information on the AC.

# Verify that the client has come online from 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 | 1 192.168.20.4 | 200  |

### 3. View detailed information about the aggregation group on the access switch.

```
[Access switch] display link-aggregation verbose
```

```
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
```

```
Port Status: S -- Selected, U -- Unselected, I -- Individual
```

```
Flags: A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
 D -- Synchronization, E -- Collecting, F -- Distributing,
 G -- Defaulted, H -- Expired
```

```
Aggregate Interface: Bridge-Aggregation1
```

```
Aggregation Mode: Static
```

```
Loadsharing Type: Shar
```

| Port | Status | Priority | Oper-Key |
|------|--------|----------|----------|
|------|--------|----------|----------|

|         |   |       |   |
|---------|---|-------|---|
| GE1/0/1 | S | 32768 | 1 |
| GE1/0/2 | S | 32768 | 1 |

## Configuration files

- Core switch:
 

```

#
dhcp enable
#
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 Ten-GigabitEthernet1/0/23
 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 service
 client forwarding-location ac
 akm mode psk
 preshared-key pass-phrase cipher c3$N//5BVbsOqdBTxi+7MJZKT6Zqh5MAMys2ZzM
 cipher-suite ccmp
 security-ie rsn
 service-template enable
#
interface Vlan-interface100
 ip address 192.168.10.2 255.255.255.0
#
interface Ten-GigabitEthernet1/0/24
 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
map-configuration map.txt
 radio 1
 service-template 1 vlan 200
 radio enable
#
wlan ap officeap model AP 3620
 serial-id 219801A28N819CE0002T
#

```

- **Access switch:**

```

#
 link-aggregation global load-sharing mode destination-mac source-mac
#
vlan 100
#
vlan 200
#
interface GigabitEthernet1/0/1
 port link-aggregation group 1
 poe enable
#
interface GigabitEthernet1/0/2
 port link-aggregation group 1
 poe enable
#
interface Ten-GigabitEthernet1/0/23
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100 200
#
interface Ten-GigabitEthernet1/0/24
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100 200
#
interface bridge-aggregation 1
 port access vlan 100

```

## Related documentation

- *AP Management Command Reference* in *INTELBRAS Access Controllers Command References*
- *AP Management Configuration Guide* in *INTELBRAS Access Controllers Configuration Guides*
- *Ethernet Link Aggregation Command Reference* in *INTELBRAS Access Controllers Command References*
- *Ethernet Link Aggregation 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*
- *Port Isolation Command Reference in INTELBRAS Access Controllers Command References*
- *Port Isolation Configuration Guide in INTELBRAS Access Controllers Configuration Guides*
- *WLAN Access Configuration Guide in INTELBRAS Access Controllers Configuration Guides*
- *WLAN Access Command Reference in INTELBRAS Access Controllers Command References*

# INTELBRAS Access Controllers

## Cloud-Managed AP Centralized Management

### Configuration Examples

---

Copyright © 2024 Intelbras S.A All rights reserved.

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

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

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



# Contents

|                                                                                                    |   |
|----------------------------------------------------------------------------------------------------|---|
| Introduction .....                                                                                 | 1 |
| Prerequisites .....                                                                                | 1 |
| Example: Configuring cloud-managed APs to come online and upgrade<br>firmware through the AC ..... | 1 |
| Network configuration .....                                                                        | 1 |
| Analysis .....                                                                                     | 2 |
| Restrictions and guidelines .....                                                                  | 2 |
| About AC discovery .....                                                                           | 2 |
| Procedures .....                                                                                   | 3 |
| Configuring Switch 1 .....                                                                         | 3 |
| Configuring Switch 2 .....                                                                         | 3 |
| Configuring Switch 3 .....                                                                         | 3 |
| Configuring the AC .....                                                                           | 4 |
| Verifying the configuration .....                                                                  | 5 |
| Configuration files .....                                                                          | 6 |
| Example: Switching cloud-managed APs to fit mode (optional) .....                                  | 7 |
| Restrictions and guidelines .....                                                                  | 7 |
| Network configuration .....                                                                        | 7 |
| Procedures .....                                                                                   | 7 |
| Verifying the configuration .....                                                                  | 7 |
| Configuration files .....                                                                          | 8 |
| Related documentation .....                                                                        | 9 |

# Introduction

The following information provides an example for managing cloud-managed APs centrally. Specifically, you can use the cloud platform to control and manage APs remotely. However, when the cloud-managed APs cannot connect to the cloud platform, you can use the AC to perform centralized management (such as image downloading) on the APs to reduce O&M difficulty and management cost.

## Prerequisites

The following information applies to Comware-based access controllers and WiFi-6 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 cloud-managed AP centralized management and auto APs.

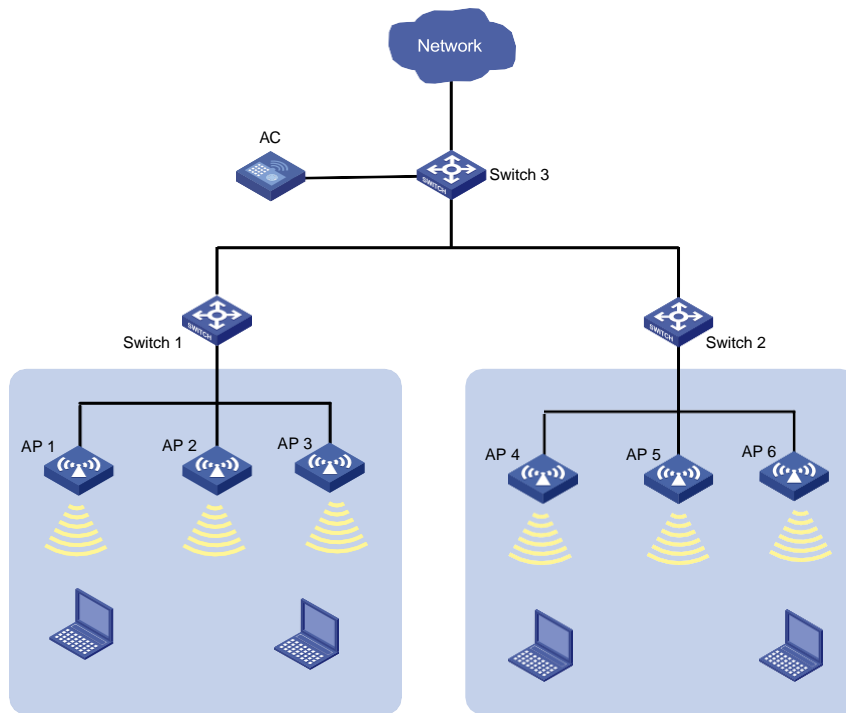
## Example: Configuring cloud-managed APs to come online and upgrade firmware through the AC

### Network configuration

As shown in [Figure 1](#), the AC is connected to Switch 3 through out-of-path deployment and Switch 3 acts as the DHCP server to assign IP addresses to APs. Switch 1 and Switch 2 supply power to APs through PoE.

Configure the feature to enable cloud-managed APs to come online and upgrade firmware through the AC. This can reduce the O&M difficulty and management cost.

**Figure 1 Network diagram**



## Analysis

- For Switch 1 and Switch 2 to supply power to APs, enable the PoE feature on the switches.
- For Switch 3 to act as a DHCP server, enable the DHCP server feature on Switch 3.
- Enable auto AP on the AC and configure auto AP persistence.
- Download the cloud-managed AP image from the official website and save the image on the AC.

## Restrictions and guidelines

- The feature is available only for Comware-based ACs of R5447P04 and later versions. Procedures and information in the examples might be slightly different depending on the software or hardware version of the access controllers and access points.
- Cloud-managed APs require licenses to come online on the AC. APs of different models use different number of license seats. To view the license seats required by APs, execute the **display wlan ap-model** command.
- Different cloud-managed APs support different AC models. To verify cloud-managed AP and AC compatibility, access the **Home > Support > Resource Center > Software Download > Wireless** page at the INTELBRAS official website and obtain the AC release notes.

## About AC discovery

An AP discovers an AC and establishes a CAPWAP tunnel with the AC through the following methods:

- **Static method:** Discovers an AC based on the AC's IP address specified by using the **wlan ac ip** command on the AP.
- **Dynamic methods:**
  - **Through DHCP:** Discovers an AC based on the AC's IP address carried in Option 43 field returned by the DHCP server.
  - **Through broadcast:** Discovers an AC by broadcasting Discovery requests to 255.255.255.255.

If the AC's IP address is not specified by using the **wlan ac ip** command, the AP uses the DHCP and broadcast methods in sequence. If the AP uses one of the methods to establish a CAPWAP with an AC successfully, AC discovery will stop.

## Procedures

### Configuring Switch 1

# Enable PoE on interface GigabitEthernet 1/0/1 that connects to the cloud-managed APs.

```
<Switch 1> system-view
[Switch 1] interface GigabitEthernet 1/0/1
[Switch 1-GigabitEthernet1/0/1] poe enable
[Switch 1-GigabitEthernet1/0/1] quit
```

### Configuring Switch 2

# Enable PoE on interface GigabitEthernet 1/0/1 that connects to the cloud-managed APs.

```
<Switch 2> system-view
[Switch 2] interface GigabitEthernet 1/0/1
[Switch 2-GigabitEthernet1/0/1] poe enable
[Switch 2-GigabitEthernet1/0/1] quit
```

### Configuring Switch 3

# Assign IP address 192.1.0.1 to VLAN-interface 1.

```
<Switch 3> system-view
[Switch 3] int Vlan-interface 1
[Switch 3-Vlan-interface1] ip address 192.1.0.1 255.255.0.0
[Switch 3-Vlan-interface1] quit
```

# Enable DHCP services. Create DHCP address pool 1 to assign IP addresses to APs.

```
[Switch 3] dhcp server enable
[Switch 3] dhcp server ip-pool 1
[Switch 3-dhcp-pool-1] network 192.1.0.0 16
[Switch 3-dhcp-pool-1] gateway-list 192.1.0.1
[Switch 3-dhcp-pool-1] forbidden-ip 192.1.0.2
[Switch 3-dhcp-pool-1] quit
```

# Apply DHCP address pool 1 to VLAN-interface 1.

```
[Switch 3] interface Vlan-interface 1
[Switch 3-Vlan-interface1] dhcp server apply ip-pool 1
[Switch 3-Vlan-interface1] quit
```

# Configuring the AC

# Assign IP address 192.1.0.2 to VLAN-interface 1 on the AC.

```
<AC> system-view
[AC] interface Vlan-interface1
[AC-Vlan-interface1] ip address 192.1.0.2 255.255.0.0
[AC-Vlan-interface1] quit
```

# Download the cloud-managed AP image to the PC. Execute the **display wlan ap-model** command to view the **Image Name** field and change the name of the image file to the same as the **Image Name** field.

---

## NOTE:

To download a cloud-managed AP image, access [https://www.intelbras.com/en/Support/Resource\\_Center/Software\\_Download/Wireless/](https://www.intelbras.com/en/Support/Resource_Center/Software_Download/Wireless/).

---

For example, change the file name from **ap6002-CMW710-R2603P01.ipe** to **ap6002.ipe**.

# Configure the PC as the FTP server. Connect the AC to the PC and then download the cloud-managed AP image through FTP.

```
<AC> ftp 192.1.0.5
ftp> get ap6002.ipe
ftp> quit
```

# Enable AP firmware upgrade. Specify the mapping relations between AP model and software version number.

---

## NOTE:

- After AP firmware upgrade is enabled, the AC compares the current AP version with the specified version in the binding. If the versions are the same, the AC will not perform the upgrade. If the versions are different, the AC will start the upgrade.
  - When specifying the mapping relations between AP model and software version number, you must save the AP image for upgrade to directory **apimg** on the AC and make sure the version number is the same as configured.
- 

```
<AC> system-view
[AC] wlan ap-group default-group
[AC-wlan-ap-gro-default-group] firmware-upgrade enable
[AC-wlan-ap-group-default-group] quit
```

# Configure the AC to obtain the AP image in the local folder with the top priority.

```
[AC] wlan image-load filepath local
```

# Specify the mapping relation between the AP model and the AP version number.

```
[AC] wlan apdb oasisap AP 5626H Ver.A E2588P01
```

# Enable auto AP.

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

# Enable auto AP association to the AC.

```
[AC] wlan auto-ap fat-and-cloud enable
```

# Convert online auto APs to manual APs.

```
[AC] wlan auto-ap persistent all
```

# Enable the system to automatically convert auto APs to manual APs. This configuration takes effect only on APs that come online afterward.

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

## Verifying the configuration

# Use the **display wlan ap all** command to view the AP information. Verify that the default AP name is the device MAC address, the AP state is **IL** during image loading and is **R/M** after the AP comes online.

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

```
Total number of APs: 1
Total number of connected APs: 1
Total number of connected manual APs: 0
Total number of connected auto APs: 1
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: 128
Local AP licenses: 128
Server AP licenses: 0
Remaining AP licenses: 127
Sync AP licenses: 0
```

### AP information

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

| AP name        | AP ID | State | Model    | Serial ID            |
|----------------|-------|-------|----------|----------------------|
| 741f-4a35-6e00 | 1     | IL    | AP 5626H | 219801A28N819CE0002T |

# Use the **display wlan ap name 741f-4a35-6e00 verbose** command to verify that the **S/W version** field is **E2588P01** after the AP firmware upgrade.

```
[AC] display wlan ap name 741f-4a35-6e00 verbose
```

```
AP name : 741f-4a35-6e00
AP ID : 1
AP group name : default-group
State : Run
Backup type : Master
Ready-for-Switchover : Ready
Online time : 1 days 22 hours 29 minutes 40 seconds
System uptime : N/A
Model : AP 5626H
Region code : CN
Region code lock : Disabled
Serial ID : 219801A28N819CE0002T
MAC address : 741f-4a35-6e00
IP address : 192.1.0.5
UDP control port number : 27392
UDP data port number : 27392
```

|             |            |
|-------------|------------|
| H/W version | : Ver.A    |
| S/W version | : E2588P01 |

## Configuration files

- **Switch 1**  
#  
interface GigabitEthernet 1/0/1  
poe enable  
#
- **Switch 2**  
#  
interface GigabitEthernet 1/0/1  
poe enable  
#
- **Switch 3**  
#  
dhcp server ip-pool 1  
gateway-list 192.1.0.1  
network 192.1.0.0 mask 255.255.0.0  
forbidden-ip 192.1.0.2  
#  
interface Vlan-interface1  
ip address 192.1.0.1 255.255.0.0  
dhcp server apply ip-pool 1  
#
- **AC**  
#  
interface Vlan-interface1  
ip address 192.1.0.2 255.255.0.0  
#  
wlan ap-group default-group  
firmware-upgrade enable  
#  
wlan image-load filepath local  
#  
wlan apdb oasisap AP 5626H Ver.A  
E2588P01 #  
wlan auto-ap enable  
wlan auto-ap fat-and-cloud enable  
wlan auto-ap persistent all  
wlan auto-persistent enable  
#

# Example: Switching cloud-managed APs to fit mode (optional)

## Restrictions and guidelines

If an AP is already in fit mode, configuring the feature has no effect on the AP.

## Network configuration

To connect cloud-managed APs to an AC to achieve centralized management, you can switch the AP mode from cloud to fit. After the switching, the APs operate as fit APs.

## Procedures

# Enter the view of default AP group **default-group**.

```
<AC> system-view
[AC] wlan ap-group default-group
```

# Configure cloud-managed APs to act in fit mode.

```
[AC-wlan-ap-group-default-group] ap-mode fit
[AC-wlan-ap-group-default-group] quit
```

## Verifying the configuration

# Use the **display wlan ap name 741f-4a35-6e00 verbose** command to verify that the **AP type** filed is **Normal AP**.

```
[AC]dis wlan ap name 741f-4a35-6e00 verbose
AP name : 741f-4a35-6e00
AP ID : 1
AP group name : default-group
State : Idle
Backup type : Idle
Ready-for-Switchover : Not ready
Online time : N/A
System uptime : N/A
Model : AP 5626H
Region code : CN
Region code lock : Disabled
Serial ID : 219801A28N819CE0002T
MAC address : Not configured
IP address : N/A
UDP control port number : N/A
UDP data port number : N/A
H/W version : N/A
S/W version : N/A
Boot version : N/A
```



|                              |                  |
|------------------------------|------------------|
| USB state                    | : N/A            |
| Power level                  | : N/A            |
| Power info                   | : N/A            |
| Description                  | : Not configured |
| 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                     | : N/A            |
| Tunnel mode                  | : N/A            |
| CAPWAP data-tunnel status    | : Down           |
| Discovery type               | : N/A            |
| Retransmission count         | : 3              |
| Retransmission interval      | : 5 seconds      |
| Firmware upgrade             | : Enabled        |
| Sent control packets         | : 0              |
| Received control packets     | : 0              |
| Echo requests                | : 0              |
| Lost echo responses          | : 0              |
| Average echo delay           | : 0              |
| Last reboot reason           | : N/A            |
| Latest IP address            | : N/A            |
| Current AC IP                | : N/A            |
| Tunnel down reason           | : N/A            |
| Connection count             | : 0              |
| 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         | : Disabled       |
| EnergySaving Level           | : N/A            |
| AP type                      | : Normal AP      |

## Configuration files

- AC
 

```
#
wlan ap-group default-group
ap-mode fit
#
```

# Related documentation

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