

INTELBRAS Access Controllers

AP Association with the AC at Layer 2

Configuration Examples

Copyright © 2024 Intelbras S.A All rights reserved.

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

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

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

Contents

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

Introduction

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

Prerequisites

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

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

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

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

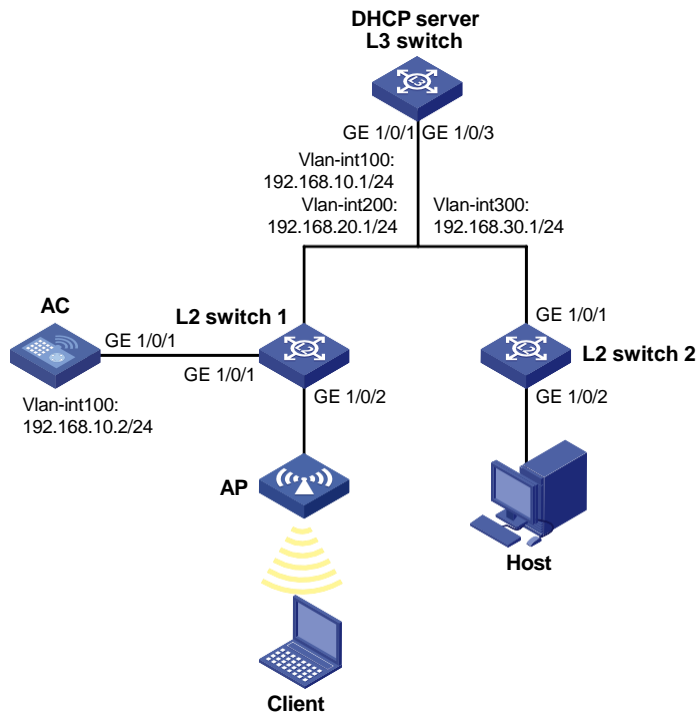
Network configuration

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

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

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

Figure 1 Network diagram



Analysis

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

Restrictions and guidelines

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

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

Procedures

Configuring the Layer 3 switch

1. Configure switch interfaces:

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

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

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

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

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

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

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

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

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

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

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

2. Configure the DHCP server:

Enable DHCP server.

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

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

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

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

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

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

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

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

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

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

Configuring the AC

1. Configure AC interfaces:

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

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

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

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

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

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

2. Configure wireless services:

Create service template 1 and enter its view.

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

Configure the SSID as **service**.

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

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

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

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

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

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

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

Enable the service template.

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

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

3. Configure the AP:

NOTE:

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

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

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

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

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

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

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

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

Bind service template 1 and VLAN 200 to radio 1.

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

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

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

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

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

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

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

Configuring Layer 2 switch 1

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Configuring Layer 2 switch 2

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

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

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

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

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

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

Verifying the configuration

Verify that the AP is in R/M state.

```
<AC> display wlan ap all
Total number of APs: 1
Total number of connected APs: 1
Total number of connected manual APs: 1
Total number of connected auto APs: 0
Total number of connected common APs: 1
Total number of connected WTUs: 0
Total number of inside APs: 0
Maximum supported APs: 3072
Remaining APs: 3071
Total AP licenses: 512
Local AP licenses: 512
Server AP licenses: 0
Remaining local AP licenses: 511
Sync AP licenses: 0
```



```

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

AP name           AP ID   State   Model           Serial ID
officeap          1       R/M     AP 3620         219801A28N819CE0002T

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

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

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

```

Configuration files

- Layer 3 switch:


```

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

```

```

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

```

```

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

```

```

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

```

```

interface Vlan-interface100
 ip address 192.168.10.1 255.255.255.0
#

```

```

interface Vlan-interface200
 ip address 192.168.20.1 255.255.255.0
#

```

```

interface Vlan-interface300
 ip address 192.168.30.1 255.255.255.0
#

```

```

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

```

```

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

```

- **AC:**

```

#
wlan service-template 1
 ssid service
 client forwarding-location ac
 akm mode psk
 preshared-key pass-phrase cipher $c$3$9tIUH$SkAUVqCH9/EPRL26ldkcEQnngexUEFj
 cipher-suite ccmp
 security-ie rsn
 service-template enable
#
interface Vlan-interface1
#

```

```

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

```

- **Layer 2 switch 1:**

```

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

```

- **Layer 2 switch 2:**

```

#
vlan 300
#

```

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

Related documentation

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

INTELBRAS Access Controllers

AP Association with the AC at Layer 2 (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
Restrictions and guidelines	1
Example: Configuring an AP to associate with the AC at Layer 2 (IPv6).....	1
Network configuration.....	1
Procedures	2
Configuring the AC.....	2
Configuring the Layer 2 switch.....	4
Verifying the configuration	5
Configuration files.....	6
Related documentation	8

Introduction

The following information provides an example for configuring APs to associate with the AC at Layer 2 on an IPv6 network.

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 IPv6 basics and WLAN access.

Restrictions and guidelines

When you configure AP's association with the AC at Layer 2 on an IPv6 network, follow these restrictions and guidelines:

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

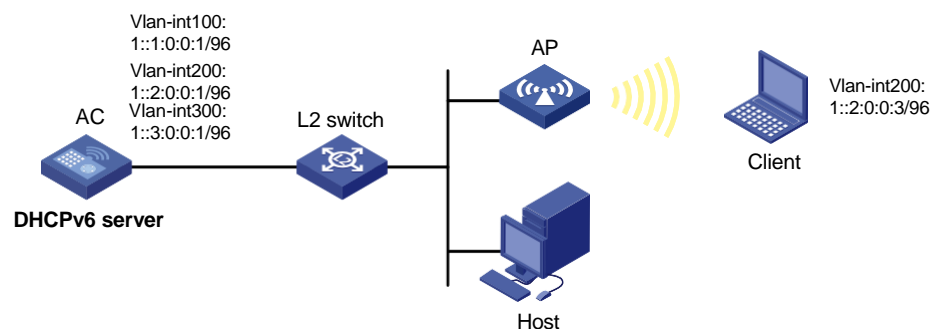
Example: Configuring an AP to associate with the AC at Layer 2 (IPv6)

Network configuration

As shown in [Figure 1](#), the AC acts as a DHCPv6 server to assign IPv6 addresses to the AP, client, and host, and the Layer 2 switch supplies power to the AP through PoE. Assume centralized forwarding is used in this example.

Configure wireless services to enable the client to access the wireless services and communicate with the host.

Figure 1 Network diagram



Procedures

Configuring the AC

1. Configure AC interfaces:

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 a CAPWAP tunnel with the AP.

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

Create VLAN 200 and VLAN-interface 200, and assign an IPv6 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] ipv6 address 1::2:0:0:1/96
[AC-Vlan-interface200] quit
```

Create VLAN 300 and VLAN-interface 300, and assign an IPv6 address to the VLAN interface. The AC will use this IPv6 address to associate with the host.

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

Configure GigabitEthernet 1/0/1 that connects the AC to the switch as a trunk port, remove the port from VLAN 1, and assign the port to VLANs 100, 200, and 300.

```
[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 100 200 300
[AC-GigabitEthernet1/0/1] quit
```

2. Configure DHCPv6:

Enable the DHCPv6 server on VLAN-interface 100, VLAN-interface 200, and VLAN-interface 300, and apply address pools 1, 2, and 3 to these interfaces, respectively.

```
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ipv6 dhcp select server
[AC-Vlan-interface100] ipv6 dhcp server apply pool 1
[AC-Vlan-interface100] quit
[AC] interface vlan-interface 200
[AC-Vlan-interface200] ipv6 dhcp server apply pool 2
[AC-Vlan-interface200] ipv6 dhcp select server
[AC-Vlan-interface200] quit
[AC] interface vlan-interface 300
[AC-Vlan-interface300] ipv6 dhcp server apply pool 3
[AC-Vlan-interface300] ipv6 dhcp select server
[AC-Vlan-interface300] quit
```


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

```
[AC] interface vlan-interface 100
[AC-Vlan-interface100] undo ipv6 nd ra halt
[AC-Vlan-interface100] ipv6 nd autoconfig managed-address-flag
[AC-Vlan-interface100] ipv6 nd autoconfig other-flag
[AC-Vlan-interface100] quit
[AC] interface vlan-interface 200
[AC-Vlan-interface200] undo ipv6 nd ra halt
[AC-Vlan-interface200] ipv6 nd autoconfig managed-address-flag
[AC-Vlan-interface200] ipv6 nd autoconfig other-flag
[AC-Vlan-interface200] quit
[AC] interface vlan-interface 300
[AC-Vlan-interface300] undo ipv6 nd ra halt
[AC-Vlan-interface300] ipv6 nd autoconfig managed-address-flag
[AC-Vlan-interface300] ipv6 nd autoconfig other-flag
[AC-Vlan-interface300] quit
```

Create DHCPv6 address pool 1 to assign an IPv6 address to the AP, and specify subnet 1::1:0:0/96 in the DHCP address pool.

```
[AC] ipv6 dhcp pool 1
[AC-dhcp6-pool-1] network 1::1:0:0/96
[AC-dhcp6-pool-1] quit
```

Create DHCPv6 address pool 2 to assign an IPv6 address to the client, and specify subnet 1::2:0:0/96 in the DHCP address pool.

```
[AC] ipv6 dhcp pool 2
[AC-dhcp6-pool-2] network 1::2:0:0/96
[AC-dhcp6-pool-2] quit
```

Create DHCPv6 address pool 3 to assign an IPv6 address to the host, and specify subnet 1::3:0:0/96 in the DHCP address pool.

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

3. Configure wireless services:

Create service template 1 and enter its view.

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

Configure the SSID as **service**.

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

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

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

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

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

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

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

Enable the service template.

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

Enable snooping DHCPv6 packets and ND packets.

```
[AC-wlan-st-1] client ipv6-snooping dhcpv6-learning enable
```

```
[AC-wlan-st-1] client ipv6-snooping nd-learning enable
```

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

4. Configure the AP:

NOTE:

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

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

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

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

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

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

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

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

Bind service template 1 and VLAN 200 to radio 1.

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

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

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

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

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

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

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

Configuring the Layer 2 switch

Create VLANs 100, 200, and 300. The switch will use VLAN 100 to forward packets between AC and AP. VLAN 200 will be used for client access. VLAN 300 will be used for host access.

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

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

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

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

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

```
[L2 switch] vlan 300
```

```
[L2 switch-vlan300] quit
```

Configure GigabitEthernet 1/0/1 that connects the switch to the AC as a trunk port, and assign the port to VLANs 100, 200, and 300.

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

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

```
[L2 switch-GigabitEthernet1/0/1] port trunk permit vlan 100 200 300
```

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

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

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

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

```
[L2 switch-GigabitEthernet1/0/2] undo port trunk permit vlan 1
```

```
[L2 switch-GigabitEthernet1/0/2] port trunk permit vlan 100
[L2 switch-GigabitEthernet1/0/2] port trunk pvid vlan 100
```

Enable PoE on GigabitEthernet 1/0/2.

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

Configure GigabitEthernet 1/0/3 that connects the switch to the host as an access port, and assign the port to VLAN 300.

```
[L2 switch] interface gigabitEthernet 1/0/3
[L2 switch-GigabitEthernet1/0/3] port access vlan 300
[L2 switch-GigabitEthernet1/0/3] quit
```

Verifying the configuration

Verify that the AP is in R/M state.

```
<AC> display wlan ap all
Total number of APs: 1
Total number of connected APs: 1
Total number of connected manual APs: 1
Total number of connected auto APs: 0
Total number of connected common APs: 1
Total number of connected WTUs: 0
Total number of inside APs: 0
Maximum supported APs: 3072
Remaining APs: 3071
Total AP licenses: 512
Local AP licenses: 512
Server AP licenses: 0
Remaining Local AP licenses: 511
Sync AP licenses: 0
```

AP information

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

AP name	APID	State	Model	Serial ID
officeap	1	R/M	AP 3620	219801A28N819CE0002T

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

```
<AC> display wlan client ipv6
Total number of clients: 1
```

MAC address	AP name	IPv6 address	VLAN
784f-43b6-077c	officeap	1::2:0:0:3	200

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

```
C:\Users\system32>ping 1::2:0:0:3 -t
```

```
Pinging 1::2:0:0:3 with 32 bytes of data:
Reply from 1::2:0:0:3: bytes=32 time=8ms TTL=255
```

```

Reply from 1::2:0:0:3: bytes=32 time<1ms TTL=255
Reply from 1::2:0:0:3: bytes=32 time<1ms TTL=255
Reply from 1::2:0:0:3: bytes=32 time<1ms TTL=255
Reply from 1::2:0:0:3: bytes=32 time<1ms TTL=255
Reply from 1::2:0:0:3: bytes=32 time<1ms TTL=255
Reply from 1::2:0:0:3: bytes=32 time<1ms TTL=255
Reply from 1::2:0:0:3: bytes=32 time<1ms TTL=255
Reply from 1::2:0:0:3: bytes=32 time<1ms TTL=255
Reply from 1::2:0:0:3: bytes=32 time<1ms TTL=255
Reply from 1::2:0:0:3: bytes=32 time<1ms TTL=255

Ping statistics for 1::2:0:0:3:
    Packets: Sent = 11, Received = 11, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 8ms, Average = 0ms
Control-C
^C
C:\Users\system32>

```

Configuration files

- AC:


```

#
dhcp enable
#
vlan 1
#
vlan 100
#
vlan 200
#
vlan 300
#
ipv6 dhcp pool 1
network 1::1:0:0:0/96
#
ipv6 dhcp pool 2
network 1::2:0:0:0/96
#
ipv6 dhcp pool 3
network 1::3:0:0:0/96
#
wlan service-template 1
ssid service
client forwarding-location ac
akm mode psk
preshared-key pass-phrase cipher $c$3$9tIUHsKAUVqCH9/EPrL26ldkcEQnngexUEFj
cipher-suite ccmp

```

```

security-ie rsn
client ipv6-snooping nd-learning enable
client ipv6-snooping dhcpv6-learning enable
service-template enable
#
interface Vlan-interface1
#
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 dhcp select server
  ipv6 dhcp server apply pool 3
  ipv6 address 1::3:0:0:1/96
  ipv6 nd autoconfig managed-address-flag
  ipv6 nd autoconfig other-flag
  undo ipv6 nd ra halt
#
interface GigabitEthernet1/0/1
  port link-type trunk
  undo port trunk permit vlan 1
  port trunk permit vlan 100 200 300
  port trunk pvid vlan 100
#
wlan ap-group group1
  ap officeap
  ap-model AP 3620
  radio 1
    radio enable
    service-template 1 vlan 200
  radio 2
#
wlan ap officeap model AP 3620
  serial-id 219801A28N819CE0002T
#

```

- **Layer 2 switch:**

```
#
vlan 100
#
vlan 200
#
vlan 300
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 1 100 200 300
 port trunk pvid vlan 100
#
interface GigabitEthernet1/0/2
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100
 port trunk pvid vlan 100
 poe enable
#
interface GigabitEthernet1/0/3
 port access vlan 300
#
```

Related documentation

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

INTELBRAS Access Controllers

Auto 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 auto AP.....	1
Network configuration.....	1
Procedures	1
Configuring the AC.....	1
Configuring the switch	2
Verifying the configuration	2
Configuration files.....	3
Related documentation	4

Introduction

The following information provides an example for configuring auto AP.

Prerequisites

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

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

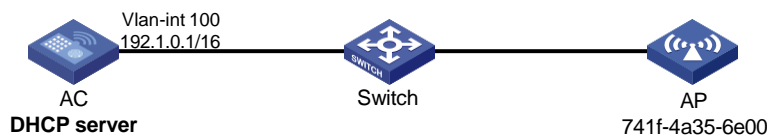
This document assumes that you have basic knowledge of auto AP.

Example: Configuring auto AP

Network configuration

As shown in [Figure 1](#), the AC acts as the DHCP server to assign an IP address to the AP. Enable the auto AP feature so that the AP can connect to the AC without manual configuration and can be automatically converted to a manual AP after coming online.

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
```

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 VLAN 100.

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

2. Configure DHCP:

Enable DHCP.

```
[AC] dhcp enable
```

Create a DHCP address pool named **1**, and specify subnet 192.1.0.0/16 and gateway IP address 192.1.0.1 in the DHCP address pool.

```
[AC] dhcp server ip-pool 1
[AC-dhcp-pool-1] network 192.1.0.0 16
[AC-dhcp-pool-1] gateway-list 192.1.0.1
[AC-dhcp-pool-1] quit
```

3. Configure auto AP:

Enable auto AP.

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

Convert auto APs to manual APs automatically after auto APs come online.

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

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
```

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 VLAN 100.

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

Configure GigabitEthernet 1/0/2 that connects the switch and the AP as an access port. 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
```

Verifying the configuration

Verify that the AP has established a CAPWAP tunnel 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: 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	R/M	AP 3620	219801A28N819CE0002T

Configuration files

- **AC:**

```

#
dhcp enable
#
vlan 100
#
dhcp server ip-pool 1
gateway-list 192.1.0.1
network 192.1.0.0 mask 255.255.0.0
#
interface Vlan-interface100
ip address 192.1.0.1 255.255.0.0
#
interface GigabitEthernet1/0/1
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 100
#
wlan auto-ap enable
wlan auto-persistent enable
#

```
- **Switch:**

```

#
vlan 100
#
interface GigabitEthernet1/0/1

```

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

Related documentation

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