

INTELBRAS Access Controllers

Internal-to-External Access Through NAT

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	2
Prerequisites	2
Example: Configuring NAT to allow internal users to access the external network	2
Network configuration	2
Restrictions and guidelines	2
Procedures	3
Configuring the AC	3
Configuring the switch	5
Verifying the configuration	5
Configuration files	6
Related documentation	7

Introduction

The following information provides examples for configuring NAT to allow internal users to access the external network.

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.

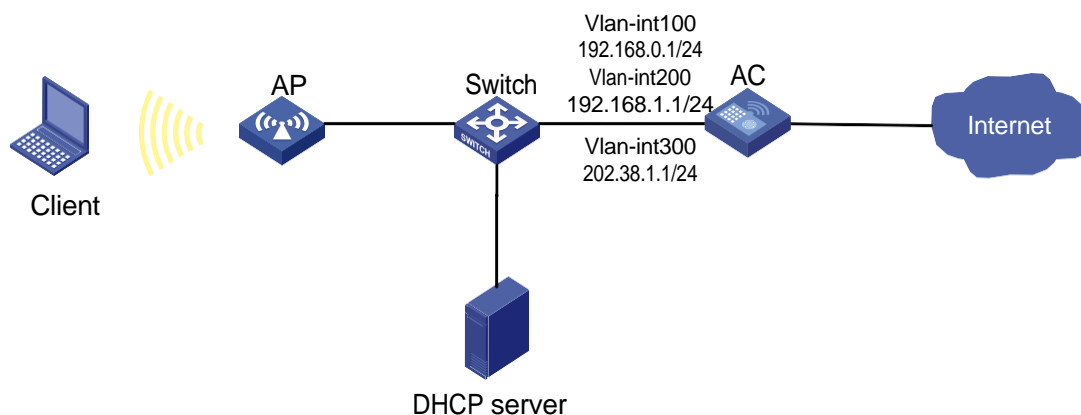
This document assumes that you have basic knowledge of NAT and WLAN.

Example: Configuring NAT to allow internal users to access the external network

Network configuration

As shown in [Figure 1](#), the AP and the clients obtain IP addresses through DHCP. Configure dynamic NAT on the AC's interface that connect to the external network to allow only the clients at the 192.168.1.0/24 to access the Internet.

Figure 1 Network diagram



Restrictions and guidelines

When you configure NAT to allow internal users to access the external network, follow these restrictions and guidelines:

- If you configure NAT on VLAN interfaces, use the address group as a best practice for dynamic NAT.
- Do not include the public IP address of the VLAN interface in the **nat address-group**.
- If the AC uses only one public IP address of the VLAN interface for dynamic NAT, use the **port-range** command to specify a proper port range. As a best practice, use the port range from 10000 to 65535 to ensure that the service ports on the AC are not used by NAT.
- Make sure the devices can reach each other. In this example, the routing configuration is not shown.

Procedures

Configuring the AC

Configuring the interfaces on the AC

Create VLAN 100 and configure VLAN-interface 100. 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 192.168.0.1 24
[AC-Vlan-interface100] quit
```

Create VLAN 200 and configure VLAN-interface 200. The clients will access the WLAN network through this VLAN.

```
[AC] vlan 200
[AC-vlan200] quit
[AC] interface vlan-interface 200
[AC-Vlan-interface200] ip address 192.168.1.1 24
[AC-Vlan-interface200] quit
```

Create VLAN 300 and configure VLAN-interface 300. The AC will use this VLAN for dynamic address translation.

```
[AC] vlan 300
[AC-vlan300] quit
[AC] interface vlan-interface 300
[AC-Vlan-interface300] ip address 202.38.1.1 24
[AC-Vlan-interface300] quit
```

Configure GigabitEthernet 1/0/1, the interface that connects to the switch, as a trunk port, and assign it 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
```

Configure GigabitEthernet 1/0/2, the interface that connects to the Internet, as an access port, and assign it to VLAN 300.

```
[AC] interface gigabitethernet 1/0/2
[AC-GigabitEthernet1/0/2] port access vlan 300
[AC-GigabitEthernet1/0/2] quit
```

Configuring WLAN services

Create service template 1 and enter its view.

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

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

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

Set the authentication and key management mode to **PSK**, and configure simple string **12345678** as the PSK.

```
[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 IE in the beacon and probe responses.

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

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

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

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

Enable the service template.

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

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

Configuring the AP

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

Create AP **officeap** with model AP 3620, and set the serial ID to 219801A28N819CE0002T.

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

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

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

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

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

Bind service template 1 to radio 2 in AP group **group1**.

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

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

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

Enable radio 2.

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

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

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

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

Configuring dynamic NAT

Configure address group 0. Add two public IP addresses 202.38.1.2 and 202.38.1.3 to the address range.

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

```
[AC-address-group-1] address 202.38.1.2 202.38.1.3
```

```
[AC-address-group-1] quit
```

Configure ACL 2000 to identify packets sourced from 192.168.1.0/24.

```
[AC] acl basic 2000
```

```
[AC-acl-ipv4-adv-2000] rule permit source 192.168.1.0 0.0.0.255
```

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

Configure outbound dynamic IP and port translation on VLAN-interface 3000 to translate the source IP address of outgoing packets permitted by ACL 2000 into addresses in the address group 0.

```
[AC] interface vlan-interface 3000
[AC-Vlan-interface3000] nat outbound 2000 address-group 0
[AC-Vlan-interface3000] quit
```

Configuring the switch

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

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

Create VLAN 200. This VLAN is used to forward packets from the client.

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

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

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

Configure GigabitEthernet 1/0/1, the interface that connects to the AP, as an access port, and assign it 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

Verify that when a user on the subnet 192.168.1.0/24 accesses the Internet, dynamic NAT is performed on the packets from the user. Execute the **display nat session verbose** command to display the NAT session information.

```
[AC] display nat session verbose
Slot 1:
Initiator:
  Source      IP/port: 192.168.1.2/1628
  Destination IP/port: 202.38.1.100/21
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: Vlan-interface200
Responder:
  Source      IP/port: 202.38.1.100/21
```

```
Destination IP/port: 202.38.1.2/1024
DS-Lite tunnel peer: -
VPN instance/VLAN ID/Inline ID: -/-/-
Protocol: TCP(6)
Inbound interface: Vlan-interface300
State: TCP_ESTABLISHED
Application: FTP
Start time: 2015-11-28 16:54:35   TTL: 2699s
Initiator->Responder:              1 packets           84 bytes
Responder->Initiator:              1 packets           84 bytes

Total sessions found: 1 s
```

Configuration files

- AC:

```
#
vlan 100
#
vlan 200
#
vlan 300
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 100 200
#
interface GigabitEthernet1/0/2
 port access vlan 300
#
wlan service-template 1
 ssid service
 client forwarding-location ac
akm mode psk
preshared-key pass-phrase cipher $c$3$N//5BVbsOqdBTxi+7MJZKT6Zqh5MAmYs2ZzM
cipher-suite ccmp
security-ie rsn
service-template enable
#
interface Vlan-interface100
 ip address 192.168.0.1 255.255.255.0
#
interface Vlan-interface200
 ip address 192.168.1.1 255.255.255.0
#
interface Vlan-interface300
 ip address 202.38.1.1 255.255.255.0
 nat outbound 2000 address-group 1
```

- ```
#
acl basic 2000
 rule 0 permit source 192.168.1.0 0.0.0.255
#
nat address-group 0
 address 202.38.1.2 202.38.1.3
#
wlan ap-group group1
 ap officeap
 ap-model AP
 3620 radio 2
 service-template 1 vlan 200
 radio enable
#
wlan ap officeap model AP 3620
 serial-id 219801A28N819CE0002T
#
```
- **Switch:**

```
#
vlan 100
#
vlan 200
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 100 200
#
interface GigabitEthernet1/0/2
 port link-type access
 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 Access Command Reference in INTELBRAS Access Controllers Command References*
- *WLAN Access Configuration Guide in INTELBRAS Access Controllers Configuration Guides*



# INTELBRAS Access Controllers Layer 2 Static Aggregation 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 Layer 2 static aggregation group ..... | 1 |
| Network configuration .....                                   | 1 |
| Procedures .....                                              | 2 |
| Configuring the AC .....                                      | 2 |
| Configuring the switch .....                                  | 2 |
| Verifying the configuration .....                             | 3 |
| Configuration files .....                                     | 4 |
| Related documentation .....                                   | 5 |

# Introduction

The following information provides Layer 2 static aggregation configuration examples.

## 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 INTELBRAS Ethernet link aggregation.

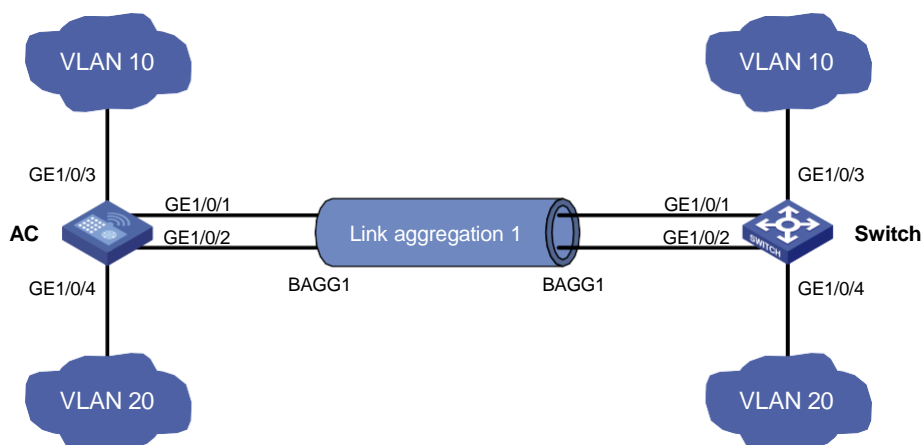
## Example: Configuring a Layer 2 static aggregation group

### Network configuration

On the network shown in [Figure 1](#), perform the following tasks:

- Configure a Layer 2 static aggregation group on the AC and the switch to increase the bandwidth and improve link reliability.
- Enable VLAN 10 at one end of the aggregate link to communicate with VLAN 10 at the other end.
- Enable VLAN 20 at one end of the aggregate link to communicate with VLAN 20 at the other end.

**Figure 1 Network diagram**



# Procedures

## Configuring the AC

### 1. Configure VLANs:

# Create VLAN 10, and assign port GigabitEthernet 1/0/3 to VLAN 10.

```
<AC> system-view
[AC] vlan 10
[AC-vlan10] port gigabitethernet 1/0/3
[AC-vlan10] quit
```

# Create VLAN 20, and assign port GigabitEthernet 1/0/4 to VLAN 20.

```
[AC] vlan 20
[AC-vlan20] port gigabitethernet 1/0/4
[AC-vlan20] quit
```

### 2. Configure a Layer 2 aggregate interface:

# Create Layer 2 aggregate interface Bridge-Aggregation 1.

```
[AC] interface bridge-aggregation 1
[AC-Bridge-Aggregation1] quit
```

# Assign port GigabitEthernet 1/0/1 to link aggregation group 1.

```
[AC] interface gigabitethernet 1/0/1
[AC-GigabitEthernet1/0/1] port link-aggregation group 1
[AC-GigabitEthernet1/0/1] quit
```

# Assign port GigabitEthernet 1/0/2 to link aggregation group 1.

```
[AC] interface gigabitethernet1/0/2
[AC-GigabitEthernet1/0/2] port link-aggregation group 1
[AC-GigabitEthernet1/0/2] quit
```

# Configure Layer 2 aggregate interface Bridge-Aggregation 1 as a trunk port and assign it to VLANs 10 and 20.

```
[AC] interface bridge-aggregation 1
[AC-Bridge-Aggregation1] port link-type trunk
[AC-Bridge-Aggregation1] port trunk permit vlan 10 20
[AC-Bridge-Aggregation1] quit
```

## Configuring the switch

### 1. Configure VLANs:

# Create VLAN 10, and assign port GigabitEthernet 1/0/3 to VLAN 10.

```
<Switch> system-view
[Switch] vlan 10
[Switch-vlan10] port gigabitethernet 1/0/3
[Switch-vlan10] quit
```

# Create VLAN 20, and assign port GigabitEthernet 1/0/4 to VLAN 20.

```
[Switch] vlan 20
[Switch-vlan20] port gigabitethernet 1/0/4
[Switch-vlan20] quit
```

### 2. Configure a Layer 2 aggregate interface:

### # Create Layer 2 aggregate interface Bridge-Aggregation 1.

```
[Switch] interface bridge-aggregation 1
[Switch-Bridge-Aggregation1] quit
```

### # Assign port GigabitEthernet 1/0/1 to link aggregation group 1.

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port link-aggregation group 1
[Switch-GigabitEthernet1/0/1] quit
```

### # Assign port GigabitEthernet 1/0/2 to link aggregation group 1.

```
[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] port link-aggregation group 1
[Switch-GigabitEthernet1/0/2] quit
```

### # Configure Layer 2 aggregate interface Bridge-Aggregation 1 as a trunk port and assign it to VLANs 10 and 20.

```
[Switch] interface bridge-aggregation 1
[Switch-Bridge-Aggregation1] port link-type trunk
[Switch-Bridge-Aggregation1] port trunk permit vlan 10 20
[Switch-Bridge-Aggregation1] quit
```

## Verifying the configuration

1. Verify that GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 on the AC are Selected ports in Layer 2 static aggregation group 1.

```
<AC> display link-aggregation verbose

Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Port Status: S -- Selected, U -- Unselected, I -- Individual
Port: A -- Auto port, M -- Management port, R -- Reference port
Flags: A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
 D -- Synchronization, E -- Collecting, F -- Distributing,
 G -- Defaulted, H -- Expired
Role: P -- Primary, S -- Secondary
Aggregate Interface: Bridge-Aggregation1
Aggregation Mode: Static
Loadsharing Type: Shar
Management VLANs: None
```

| Port    | Status | Priority | Oper-Key | Role |
|---------|--------|----------|----------|------|
| GE1/0/1 | S      | 32768    | 2        | None |
| GE1/0/2 | S      | 32768    | 2        | None |

2. Verify that the bandwidth for Layer 2 aggregate interface Bridge-Aggregation 1 is the total bandwidth of GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 on the AC.

```
<AC> display interface bridge-aggregation 1

Bridge-Aggregation1
Current state: UP
Line protocol state: UP
IP packet frame type: Ethernet II, hardware address: 741f-4a05-3db8
Description: Bridge-Aggregation1 Interface
Bandwidth: 2000000 kbps
2Gbps-speed mode, full-duplex mode
```

```

Link speed type is autonegotiation, link duplex type is autonegotiation
PVID: 1
Port link-type: Trunk
VLAN Passing: 1(default vlan), 10
VLAN permitted: 1(default vlan), 10, 20
Trunk port encapsulation: IEEE 802.1q
Last clearing of counters: Never
Last 300 seconds input: 2 packets/sec 308 bytes/sec 0%
Last 300 seconds output: 0 packets/sec 0 bytes/sec 0%
Input (total): 12659 packets, 1290752 bytes
 177 unicasts, 9919 broadcasts, 2563 multicasts, 0 pauses
Input (normal): 12659 packets, - bytes
 177 unicasts, 9919 broadcasts, 2563 multicasts, 0 pauses
Input: 0 input errors, 0 runs, 0 giants, - throttles
 0 CRC, - frame, 0 overruns, 0 aborts
 - ignored, - parity errors
Output (total): 316 packets, 295765 bytes
 307 unicasts, 9 broadcasts, 0 multicasts, 0 pauses
Output (normal): 316 packets, - bytes
 307 unicasts, 9 broadcasts, 0 multicasts, 0 pauses
Output: 0 output errors, 0 underruns, - buffer failures
 0 aborts, 0 deferred, 0 collisions, 0 late collisions
 - lost carrier, - no carrier

```

## Configuration files

- AC:
 

```

#
vlan 10
#
vlan 20
#
interface Bridge-Aggregation1
port link-type trunk
port trunk permit vlan 1 10 20
#
interface GigabitEthernet1/0/1
port link-type trunk
port trunk permit vlan 1 10 20
port link-aggregation group 1
#
interface GigabitEthernet1/0/2
port link-type trunk
port trunk permit vlan 1 10 20
port link-aggregation group 1
#

```
- Switch:
 

```

#

```

```
vlan 10
#
vlan 20
#
interface Bridge-Aggregation1
port link-type trunk
port trunk permit vlan 1 10 20
#
interface GigabitEthernet1/0/1
port link-type trunk
port trunk permit vlan 1 10 20
port link-aggregation group 1
#
interface GigabitEthernet1/0/2
port link-type trunk
port trunk permit vlan 1 10 20
port link-aggregation group 1
#
```

## Related documentation

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

# INTELBRAS Access Controllers Layer 2 Multicast 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 Layer 2 multicast..... | 1 |
| Network configuration.....                  | 1 |
| Restrictions and guidelines .....           | 1 |
| Procedures .....                            | 2 |
| Configuring the AC.....                     | 2 |
| Configuring the switch .....                | 4 |
| Verifying the configuration .....           | 5 |
| Configuration files.....                    | 6 |
| Related documentation .....                 | 7 |

# Introduction

The following information provides examples for configuring Layer 2 multicast.

## 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 Layer 2 multicast.

## Example: Configuring Layer 2 multicast

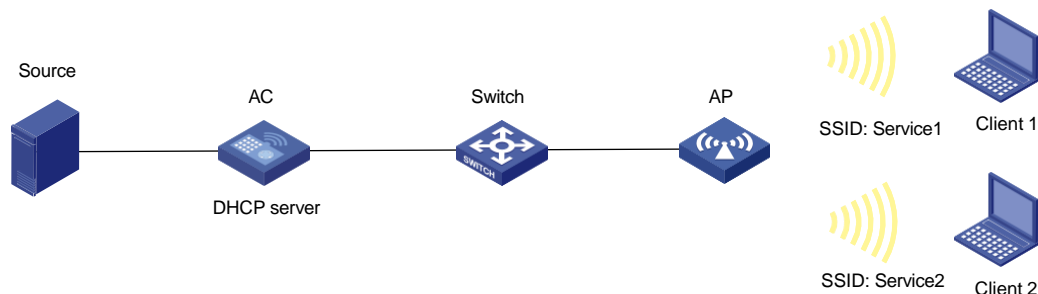
### Network configuration

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 Layer 2 multicast 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**



### 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 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, and assign the port to VLAN 100 and VLAN 200.

```
[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] 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:

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

```
[AC] wlan ap ap1 model WA4320i-ACN
[AC-wlan-ap-ap1] serial-id 210235A1GQC157001570
```

```
[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
```

# Configure the PSK AKM mode and the **12345678** plaintext key.

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

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

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

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

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

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

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

# 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
```

# Configure the PSK AKM mode and the **12345678** plaintext key.

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

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

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

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

```
[AC-wlan-st-service2] security-ie rsn
```

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

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

# Enable the service template.

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

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

5. Configure the AP:

---

**NOTE:**

In a large network, use AP groups to configure APs as a best practice.

---

# Create an AP named **ap1**, with model **AP 3620**.

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

# Set the serial ID to **219801A28N819CE0002T**.

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

# Create an AP group named **group1**, and create an AP grouping rule by AP names to add AP **ap1** to the AP group.

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

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

# Enter radio view of radio 1, and bind service template 1 to the radio.

```
[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
```

**# 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
```

**# Enter radio view of radio 2, and bind service template 1 to the radio.**

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

**# Enable radio 2.**

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

## **6. Configure IGMP snooping:**

**# 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
```

# 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, and assign the port to VLAN 100 and VLAN 200.**

```
[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] 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
 client forwarding-location ac
akm mode psk
 preshared-key pass-phrase cipher c3$N//5BVbsOqdBTxi+7MJZKT6Zqh5MAmYs2ZzM
 cipher-suite ccmp
 security-ie rsn
 service-template enable
#
wlan service-template service2
 ssid service2
 client forwarding-location ac
akm mode psk
 preshared-key pass-phrase cipher c3$N//5BVbsOqdBTxi+7MJZKT6Zqh5MAmYs2ZzM
 cipher-suite ccmp
 security-ie rsn
 service-template enable
#
interface Vlan-interface100
 ip address 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 service1 vlan 200
radio 2
radio enable
service-template service2 vlan 200
#
wlan ap ap1 model AP 3620
serial-id 219801A28N819CE0002T
#
```

- **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
#
```

## Related documentation

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



# INTELBRAS Access Controllers Static VLAN Allocation Configuration Examples

---

Copyright © 2024 Intelbras S.A All rights reserved.

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

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

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

# Contents

|                                                   |   |
|---------------------------------------------------|---|
| Introduction .....                                | 1 |
| Prerequisites .....                               | 1 |
| Example: Configuring static VLAN allocation ..... | 1 |
| Network configuration .....                       | 1 |
| Procedures .....                                  | 2 |
| Configuring the AC .....                          | 2 |
| Configure the switch .....                        | 5 |
| Verifying the configuration .....                 | 7 |
| Configuration files .....                         | 7 |
| Related documentation .....                       | 9 |

# Introduction

The following information provides an example for configuring static VLAN allocation to allow clients to evenly join VLANs in different VLAN groups.

## 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.

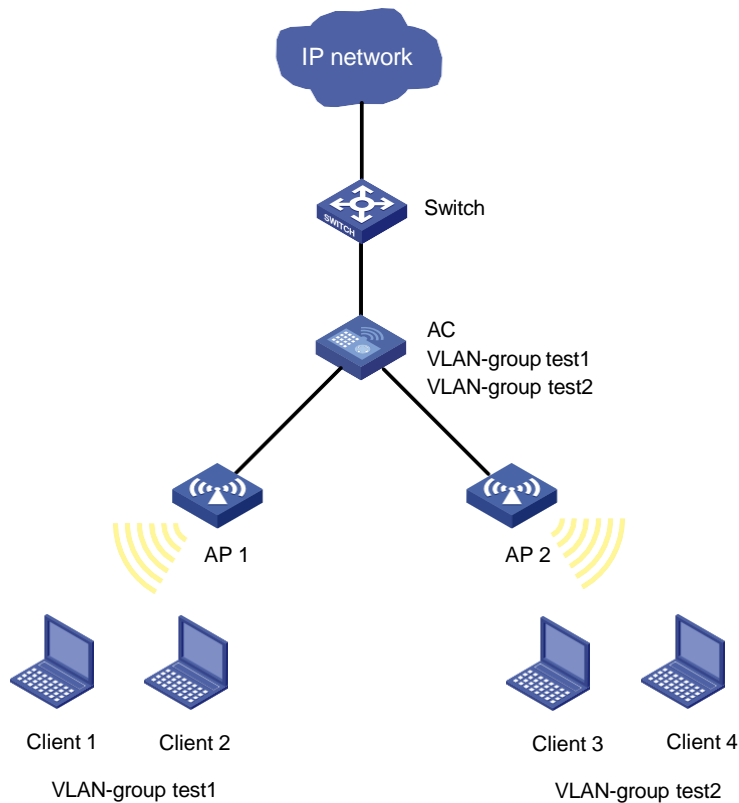
The following information is provided based on the assumption that you have basic knowledge of VLAN group.

## Example: Configuring static VLAN allocation

### Network configuration

As shown in [Figure 1](#), the switch acts as the DHCP server to assign IP addresses to the APs and clients. Configure two VLAN groups on the AC for the clients to evenly join VLANs in different VLAN groups.

**Figure 1 Network diagram**



| Device | Interface  | IP address    | Device | Interface  | IP address    |
|--------|------------|---------------|--------|------------|---------------|
| AC     | Vlan-int2  | 192.12.0.2/16 | Switch | Vlan-int2  | 192.12.0.1/16 |
|        | Vlan-int10 | 192.10.0.2/16 |        | Vlan-int10 | 192.10.0.1/16 |
|        | Vlan-int20 | 192.20.0.2/16 |        | Vlan-int20 | 192.20.0.1/16 |
|        | Vlan-int30 | 192.30.0.2/16 |        | Vlan-int30 | 192.30.0.1/16 |
|        | Vlan-int40 | 192.40.0.2/16 |        | Vlan-int40 | 192.40.0.1/16 |

## Procedures

### Configuring the AC

**1. Configure interfaces on the AC:**

# Create VLAN 2 and VLAN-interface 2, 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 2
[AC-vlan2] quit
[AC] interface vlan-interface 2
[AC-Vlan-interface2] ip address 192.12.0.2 16
[AC-Vlan-interface2] quit
```

# Create VLAN 10 and VLAN-interface 10, and assign an IP address to the VLAN interface. VLAN 10 will be used for client access.

```
[AC] vlan 10
[AC-vlan10] quit
```

```
[AC] interface vlan-interface 10
[AC-Vlan-interface10] ip address 192.10.0.2 16
[AC-Vlan-interface10] quit
```

**# Create VLAN 20 and VLAN-interface 20 and assign an IP address to the VLAN interface. VLAN 20 will be used for client access.**

```
[AC] vlan 20
[AC-vlan20] quit
[AC] interface vlan-interface 20
[AC-Vlan-interface20] ip address 192.20.0.2 16
[AC-Vlan-interface20] quit
```

**# Create VLAN 30 and VLAN-interface 30, and assign an IP address to the VLAN interface. VLAN 30 will be used for client access.**

```
[AC] vlan 30
[AC-vlan30] quit
[AC] interface vlan-interface 30
[AC-Vlan-interface30] ip address 192.30.0.2 16
[AC-Vlan-interface30] quit
```

**# Create VLAN 40 and VLAN-interface 40, and assign an IP address to the VLAN interface. VLAN 40 will be used for client access.**

```
[AC] vlan 40
[AC-vlan40] quit
[AC] interface vlan-interface 40
[AC-Vlan-interface40] ip address 192.40.0.2 16
[AC-Vlan-interface40] quit
```

**# Specify GigabitEthernet 1/0/1 that connects the AC to the switch as a trunk port, and assign it to VLANs 2, 10, 20, 30, and 40.**

```
[AC] interface gigabitethernet 1/0/1
[AC-GigabitEthernet1/0/1] port link-type trunk
[AC-GigabitEthernet1/0/1] port trunk permit vlan 2 10 20 30 40
[AC-GigabitEthernet1/0/1] quit
```

**# Specify GigabitEthernet 1/0/2 that connects the AC to the AP as a trunk port, and assign it to VLAN 2.**

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

## **2. Configure VLAN groups:**

**# Create VLAN-group test1 and add VLANs 10 and 20 to the group.**

```
[AC] vlan-group test1
[AC-vlan-group-test1] vlan-list 10 20
```

**# Create VLAN-group test2 and add VLANs 30 and 40 to the group.**

```
[AC] vlan-group test2
[AC-vlan-group-test2] vlan-list 30 40
```

## **3. Configure a wireless service:**

**# 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 authentication and key management mode to PSK, and configure simple character string of **12345678** as the PSK.

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

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

# Set the AES-CCMP cipher suite for frame encryption, and enable the RSN IE in beacon and probe responses.

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

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

# Enable the AC to forward client data traffic. (Skip this step is the AC forwards client data traffic by default.)

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

# Set the VLAN allocation method to static.

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

---

**NOTE:**

If dynamic VLAN allocation is used, clients cannot change IP addresses proactively, which might cause disconnection from the WLAN. To avoid unexpected disconnection, set the VLAN allocation method to static.

---

# Enable the service template.

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

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

#### 4. Configure AP settings:

---

**NOTE:**

On a large-scaled network, as a best practice, configuring settings in AP groups.

---

# 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
```

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

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

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

```
[AC-wlan-ap-ap2] serial-id 219801A28N819CE00033
```

```
[AC-wlan-ap-ap2] quit
```

# Create AP group **group1**, and create an AP grouping rule by AP names.

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

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

# Enter radio view of radio 1 in AP group **group1**, bind service template 1 to radio 1, and specify VLAN group **test1**.

```
[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-group test1
```

# 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
```

**# Create AP group `group2`, and create an AP grouping rule by AP names.**

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

**# Enter radio view of radio 1 in AP group `group2`, bind service template 1 to radio 1, and specify VLAN group `test2`.**

```
[AC-wlan-ap-group-group2] ap-model AP 3620
[AC-wlan-ap-group-group2-ap-model-AP 3620] radio 1
[AC-wlan-ap-group-group2-ap-model-AP 3620-radio-1] service-template 1 vlan-group
test2
```

**# 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-ap-model-AP 3620]
quit [AC-wlan-ap-group-group2] quit
```

## Configure the switch

### 1. Configure switch interfaces:

**# Create VLAN 2 and assign an IP address to VLAN-interface 2.**

```
<Switch> system-view
[Switch] vlan 2
[Switch-vlan2] quit
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] ip address 192.12.0.1 16
[Switch-Vlan-interface2] quit
```

**# Create VLAN 10 and assign an IP address to VLAN-interface 10.**

```
[Switch] vlan 10
[Switch-vlan10] quit
[Switch] interface vlan-interface 10
[Switch-Vlan-interface10] ip address 192.10.0.1 16
[Switch-Vlan-interface10] quit
```

**# Create VLAN 20 and assign an IP address to VLAN-interface 20.**

```
[Switch] vlan 20
[Switch-vlan20] quit
[Switch] interface vlan-interface 20
[Switch-Vlan-interface20] ip address 192.20.0.1 16
[Switch-Vlan-interface20] quit
```

**# Create VLAN 30 and assign an IP address to VLAN-interface 30.**

```
[Switch] vlan 30
[Switch-vlan30] quit
[Switch] interface vlan-interface 30
[Switch-Vlan-interface30] ip address 192.30.0.1 16
[Switch-Vlan-interface30] quit
```

**# Create VLAN 40 and assign an IP address to VLAN-interface 40.**

```
[Switch] vlan 40
[Switch-vlan40] quit
[Switch] interface vlan-interface 40
[Switch-Vlan-interface40] ip address 192.40.0.1 16
```

```
[Switch-Vlan-interface40] quit
```

# Configure GigabitEthernet 1/0/2 that connects the switch to the AC as a trunk port, and assign the access port to VLAN 2, 10, 20, 30, and 40.

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

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

```
[Switch-GigabitEthernet1/0/2] port trunk permit vlan 2 10 20 30 40
```

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

## 2. Configure the DHCP server:

# Enable DHCP.

```
[Switch] dhcp enable
```

# Create DHCP address pool **vlan2**, specify primary subnet 192.2.0.0/16, and specify the gateway address as 192.2.0.1. The switch will use this pool to assign addresses to the AP.

```
[Switch] dhcp server ip-pool vlan2
```

```
[Switch-dhcp-pool-vlan2] network 192.12.0.0 mask 255.255.0.0
```

```
[Switch-dhcp-pool-vlan2] gateway-list 192.12.0.1
```

```
[Switch-dhcp-pool-vlan2] quit
```

# Create DHCP address pool **vlan10**, specify primary subnet 192.10.0.0/16, specify the gateway address as 192.10.0.1, and specify a DNS server. The switch will use this pool to assign addresses to clients. In this example, the gateway acts as the DNS server.

```
[Switch] dhcp server ip-pool vlan10
```

```
[Switch-dhcp-pool-vlan10] network 192.10.0.0 mask 255.255.0.0
```

```
[Switch-dhcp-pool-vlan10] gateway-list 192.10.0.1
```

```
[Switch-dhcp-pool-vlan10] dns-list 192.10.0.1
```

```
[Switch-dhcp-pool-vlan10] quit
```

# Create DHCP address pool **vlan20**, specify primary subnet 192.20.0.0/16, specify the gateway address as 192.20.0.1, and specify a DNS server. The switch will use this pool to assign addresses to clients. In this example, the gateway acts as the DNS server.

```
[Switch] dhcp server ip-pool vlan20
```

```
[Switch-dhcp-pool-vlan20] network 192.20.0.0 mask 255.255.0.0
```

```
[Switch-dhcp-pool-vlan20] gateway-list 192.20.0.1
```

```
[Switch-dhcp-pool-vlan20] dns-list 192.20.0.1
```

```
[Switch-dhcp-pool-vlan20] quit
```

# Create DHCP address pool **vlan30**, specify primary subnet 192.30.0.0/16, specify the gateway address as 192.30.0.1, and specify a DNS server. The switch will use this pool to assign addresses to clients. In this example, the gateway acts as the DNS server.

```
[Switch] dhcp server ip-pool vlan30
```

```
[Switch-dhcp-pool-vlan30] network 192.30.0.0 mask 255.255.0.0
```

```
[Switch-dhcp-pool-vlan30] gateway-list 192.30.0.1
```

```
[Switch-dhcp-pool-vlan30] dns-list 192.30.0.1
```

```
[Switch-dhcp-pool-vlan30] quit
```

# Create DHCP address pool **vlan40**, specify primary subnet 192.40.0.0/16, specify the gateway address as 192.40.0.1, and specify a DNS server. The switch will use this pool to assign addresses to clients. In this example, the gateway acts as the DNS server.

```
[Switch] dhcp server ip-pool vlan40
```

```
[Switch-dhcp-pool-vlan40] network 192.40.0.0 mask 255.255.0.0
```

```
[Switch-dhcp-pool-vlan40] gateway-list 192.40.0.1
```

```
[Switch-dhcp-pool-vlan40] dns-list 192.40.0.1
```

```
[Switch-dhcp-pool-vlan40] quit
```



# Verifying the configuration

# Make client 1 and client 2 come online from SSID **service** provided by AP 1.

# Verify that the two clients are assigned to different VLANs in VLAN group **test1**.

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

```
Total number of clients: 2
```

| MAC address    | User name | AP name | R IP address | VLAN |
|----------------|-----------|---------|--------------|------|
| 90f0-528e-0871 | N/A       | ap1     | 1 192.10.0.3 | 10   |
| 961b-66ea-72c5 | N/A       | ap1     | 1 192.20.0.3 | 20   |

## Configuration files

- AC:

```
#
vlan 2
#
vlan 10
#
vlan 20
#
vlan 30
#
vlan 40
#
vlan-group test1
 vlan-list 10 20
#
vlan-group test2
 vlan-list 30 40
#
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
client vlan-alloc static
service-template enable
#
interface Vlan-interface2
 ip address 192.12.0.2 255.255.0.0
#
interface Vlan-interface10
 ip address 192.10.0.2 255.255.0.0
```

```

interface Vlan-interface20
 ip address 192.20.0.2 255.255.0.0
#
interface Vlan-interface30
 ip address 192.30.0.2 255.255.0.0
#
interface Vlan-interface40
 ip address 192.40.0.2 255.255.0.0
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 2 10 20 30 40
#
interface GigabitEthernet1/0/2
 port link-type trunk
 port trunk permit vlan 2
#
wlan ap-group group1
 ap ap1
 ap-model AP
 3620 radio 1
 service-template 1 vlan-group test1
 radio enable
#
wlan ap-group group2
 ap ap2
 ap-model AP
 3620 radio 1
 service-template 1 vlan-group test2
 radio enable
#
wlan ap ap1 model AP 3620
 serial-id 219801A28N819CE0002T
#
wlan ap ap2 model AP 3620
 serial-id 219801A28N819CE00033

```

- **Switch:**

```

#
dhcp enable
#
vlan 2
#
vlan 10
#
vlan 20
#
vlan 30

```

```

vlan 40
#
dhcp server ip-pool vlan2
gateway-list 192.12.0.1
 network 192.12.0.0 mask 255.255.0.0
#
dhcp server ip-pool vlan10
gateway-list 192.10.0.1
 network 192.10.0.0 mask 255.255.0.0
dns-list 192.10.0.1
#
dhcp server ip-pool vlan20
gateway-list 192.20.0.1
 network 192.20.0.0 mask 255.255.0.0
dns-list 192.20.0.1
#
dhcp server ip-pool vlan30
gateway-list 192.30.0.1
 network 192.30.0.0 mask 255.255.0.0
dns-list 192.30.0.1
#
dhcp server ip-pool vlan40
gateway-list 192.40.0.1
 network 192.40.0.0 mask 255.255.0.0
dns-list 192.40.0.1
#
interface Vlan-interface2
 ip address 192.12.0.1 255.255.0.0
#
interface Vlan-interface10
 ip address 192.10.0.1 255.255.0.0
#
interface Vlan-interface20
 ip address 192.20.0.1 255.255.0.0
#
interface Vlan-interface30
 ip address 192.30.0.1 255.255.0.0
#
interface Vlan-interface40
 ip address 192.40.0.1 255.255.0.0
#
interface GigabitEthernet1/0/2
 port link-type trunk
 port trunk permit vlan 2 10 20 30 40

```

## 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*

# INTELBRAS Access Controllers URL Redirection Configuration Examples

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

# Contents

|                                           |   |
|-------------------------------------------|---|
| Introduction .....                        | 1 |
| Prerequisites .....                       | 1 |
| Example: Configuring URL redirection..... | 1 |
| Network configuration.....                | 1 |
| Restrictions and guidelines .....         | 2 |
| Procedures .....                          | 2 |
| Configuring the AD Campus server.....     | 2 |
| Editing the AP's configuration file ..... | 2 |
| Configuring the AC.....                   | 2 |
| Configuring the switch .....              | 4 |
| Verifying the configuration .....         | 5 |
| Configuration files.....                  | 6 |
| Related documentation .....               | 8 |

# Introduction

The following information provides an example for configuring URL redirection.

## Prerequisites

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

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

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

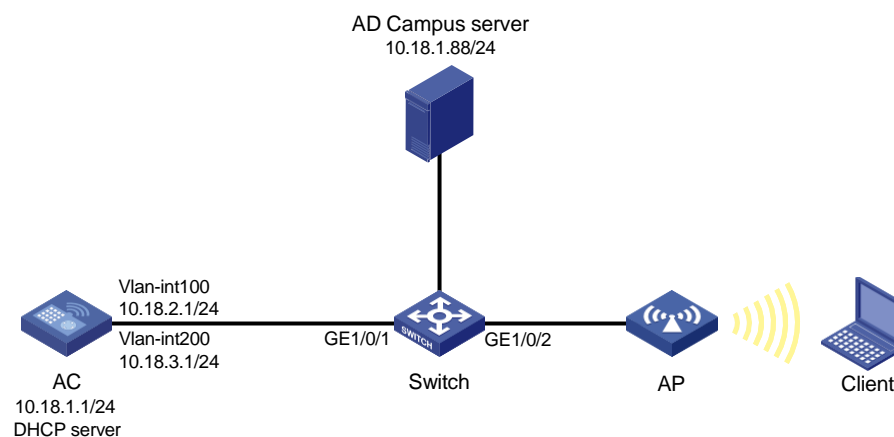
## Example: Configuring URL redirection

### Network configuration

As shown in [Figure 1](#), the AP and the client obtain an IP address from the DHCP server. To control the client's access to network resources, complete the following tasks:

- Configure VLAN 100 as the access VLAN for the AP.
- Configure VLAN 200 as the access VLAN for the client, and configure the client to be MAC authenticated on the AD Campus server.
- Configure URL redirection for a client to authenticate to the RADIUS server after it has failed a MAC authentication because the server does not have its credential information and MAC address.

**Figure 1 Network diagram**





# Restrictions and guidelines

- Use MAC-based user accounts for MAC authentication users. Make sure the username and password added on the RADIUS server are in the same format as the MAC authentication username configured on the AC.
- Use the actual serial ID of an AP to uniquely identify that AP.

## Procedures

### Configuring the AD Campus server

On the AD Campus server, add an AC, access policy, access service, access user, and ACL and URL authorization information.

### Editing the AP's configuration file

# Edit the AP's configuration file, name it map.txt and upload the configuration file to the storage media on the AC.

```
System-view
vlan 200
interface gigabitethernet1/0/1
port link-type trunk
port trunk permit vlan 200
acl advanced 3000
rule 1 permit ip destination 10.18.1.88 0
```

## 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 10.18.2.1 24
[AC-Vlan-interface100] quit
```

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

```
[AC] vlan 200
[AC-vlan200] quit
[AC] interface vlan-interface 200
[AC-Vlan-interface200] ip address 10.18.3.1 24
[AC-Vlan-interface200] quit
```

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

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

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

## 2. Configure a RADIUS scheme:

# Create a RADIUS scheme named **adcampus** and enter its view.

```
[AC] radius scheme adcampus
```

# Configure the primary authentication server, the primary accounting server, and the keys for the servers to communicate.

```
[AC-radius-rs1] primary authentication 10.18.1.88
```

```
[AC-radius-rs1] primary accounting 10.18.1.88
```

```
[AC-radius-rs1] key authentication simple 12345678
```

```
[AC-radius-rs1] key accounting simple 12345678
```

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

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

```
[AC-radius-rs1] quit
```

# Enable RADIUS session-control.

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

## 3. Configure an authentication domain:

# Create an ISP domain named **ds** and enter its view.

```
[AC] domain ds
```

# Perform RADIUS authentication for LAN users based on scheme **adcampus**.

```
[AC-isp-ds] authentication lan-access radius-scheme adcampus
```

# Perform RADIUS authorization for LAN users based on scheme **adcampus**.

```
[AC-isp-ds] authorization lan-access radius-scheme adcampus
```

# Perform RADIUS accounting for LAN users based on scheme **adcampus**.

```
[AC-isp-ds] accounting lan-access radius-scheme adcampus
```

```
[AC-isp-ds] quit
```

# Use MAC-based user accounts for MAC authentication users. The MAC addresses must be in hexadecimal notation without hyphens, and letters are in lower case.

```
[AC] mac-authentication user-name-format mac-address without-hyphen lowercase
```

## 4. Configure a wireless service:

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

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

# Configure the SSID as **url-redirect**.

```
[AC-wlan-st-redirect] ssid url-redirect
```

# Assign clients that come online from the service template to VLAN 200.

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

# Specify the AP as the client data frame forwarder.

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

# Set the authentication mode to MAC authentication.

```
[AC-wlan-st-redirect] client-security authentication-mode mac
```

# Specify ISP domain **ds** for MAC authentication clients on the service template.

```
[AC-wlan-st-redirect] mac-authentication domain ds
```

# Enable URL redirection.

```
[AC-wlan-st-redirect] client url-redirect enable
```

# Enable the service template.

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

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

5. Configure URL redirection policies:

# Create IPv4 advanced ACL 3000, and configure the following rules: permit access only to the RADIUS server and deny IP packets, and permit inbound and outbound DHCP and DNS packets.

```
[AC] acl advanced 3000
[AC-acl-ipv4-adv-3000] rule 1 permit ip destination 10.18.1.88 0
[AC-acl-ipv4-adv-3000] rule 2 permit ip source 10.18.1.88 0
[AC-acl-ipv4-adv-3000] rule 3 permit udp destination-port eq bootps
[AC-acl-ipv4-adv-3000] rule 4 permit udp destination-port eq bootpc
[AC-acl-ipv4-adv-3000] rule 5 permit udp destination-port eq dns
[AC-acl-ipv4-adv-3000] rule 6 permit udp source-port eq dns
[AC-acl-ipv4-adv-3000] rule 9 deny ip
```

6. Configure a manual AP, and bind service template **redirect** to a radio on the AP:

---

**NOTE:**

In large-scale networks, configure AP groups instead of single APs 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
```

# Add AP **ap1** to AP group **group1**.

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

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

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

# 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 the AP.

```
[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
```

## Configuring the switch

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

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

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

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

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

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

**# Configure GigabitEthernet 1/0/2 that connects the switch to the AP as a trunk port, and assign the trunk port to VLAN 100 and VLAN 200.**

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

**# Enable the PoE feature.**

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

## Verifying the configuration

1. Verify that the wireless client can associate with the AP after MAC authentication and will be redirected to the authentication page as long as the client accesses a webpage. Display MAC authentication connection information to verify that the ACL and URL have been deployed by the server.

```
[AC] dis mac-authentication connection
Total connections: 1
```

```
User MAC address : ecd0-9f92-2787
AP name : ap1
Radio ID : 1
SSID : url-redirect
BSSID : 3891-d5ba-fa60
Username : ecd09f922787
Authentication domain : ds
Initial VLAN : 200
Authorization VLAN : 200
Authorization ACL number : 3000
Authorization user profile : N/A
Authorization CAR : N/A
Authorization URL : http://
10.18.1.88:8080/byod?usermac=%m&userip=%c&userurl=%o
Termination action : N/A
Session timeout last from : N/A
Session timeout period : N/A
Online from : 2020/04/01 13:46:29
Online duration : 0h 0m 7s
```

2. Verify that the client can access the WLAN after authentication. Display MAC authentication connection information to verify that no URL is deployed by the server.

```
Total connections: 1
```

```
User MAC address : ecd0-9f92-2787
AP name : ap1
Radio ID : 1
SSID : url-redirect
```

|                            |                       |
|----------------------------|-----------------------|
| BSSID                      | : 3891-d5ba-fa60      |
| Username                   | : ecd09f922787        |
| Authentication domain      | : ds                  |
| Initial VLAN               | : 200                 |
| Authorization VLAN         | : 200                 |
| Authorization ACL number   | : N/A                 |
| Authorization user profile | : N/A                 |
| Authorization CAR          | : N/A                 |
| Authorization URL          | : N/A                 |
| Termination action         | : N/A                 |
| Session timeout last from  | : N/A                 |
| Session timeout period     | : N/A                 |
| Online from                | : 2020/04/01 13:46:40 |
| Online duration            | : 0h 0m 18s           |

## Configuration files

- AC:

```
#
mac-authentication user-name-format mac-address with-hyphen
#
vlan 100
#
vlan 200
#
wlan service-template redirect
ssid url-redirect
vlan 200
client forwarding-location ap
client url-redirect enable
client-security authentication-mode mac
mac-authentication domain ds
service-template enable
#
interface Vlan-interface100
ip address 10.18.2.1 255.255.255.0
#
interface Vlan-interface200
ip address 10.18.3.1 255.255.255.0
#
interface GigabitEthernet1/0/1
port link-type trunk
port trunk permit vlan 100 200
#
radius session-control enable
#
radius scheme adcampus
primary authentication 10.18.1.88
```

```

primary accounting 10.18.1.88
key authentication cipher c3$Sqqgz7lDs4XPnethmAgyAKVlke7qwEkYbQ==
key accounting cipher c3$4J/JBRGwqB4F213furJmKB6JWYXBFjWE6g==
user-name-format without-domain
#
domain ds
 authentication portal radius-scheme adcampus
 authorization portal radius-scheme adcampus
 accounting portal radius-scheme adcampus
#
acl advanced 3000
 rule 1 permit ip destination 10.18.1.88 0
 rule 2 permit ip source 10.18.1.88 0
 rule 3 permit udp destination-port eq bootps
 rule 4 permit udp destination-port eq bootpc
 rule 5 permit udp destination-port eq dns
 rule 6 permit udp source-port eq dns
 rule 7 permit tcp source-port eq dns
 rule 8 permit tcp destination-port eq dns
 rule 9 deny ip
#
wlan ap-group group1
 ap ap1
 ap-model AP
 3620 radio 1
 map-configuration map.txt
 service-template redirect
 radio enable
#
wlan ap ap1 model AP 3620
 serial-id 219801A28N819CE0002T
#

```

- **Switch:**

```

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

```

# Related documentation

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

# INTELBRAS Access Controllers IPv6 URL Redirection Configuration Examples

---

Copyright © 2024 Intelbras S.A All rights reserved.

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

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

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



# Contents

|                                                 |   |
|-------------------------------------------------|---|
| Introduction .....                              | 1 |
| Prerequisites .....                             | 1 |
| Example: Configuring IPv6 URL redirection ..... | 1 |
| Network configuration .....                     | 1 |
| Analysis .....                                  | 2 |
| Restrictions and guidelines .....               | 2 |
| Procedures .....                                | 2 |
| Configuring the AD Campus server .....          | 2 |
| Editing the AP's configuration file .....       | 2 |
| Configuring the AC .....                        | 3 |
| Configure the switch .....                      | 5 |
| Verifying the configuration .....               | 6 |
| Configuration files .....                       | 7 |
| Related documentation .....                     | 9 |

# Introduction

The following information provides an example for configuring IPv6 URL redirection.

## Prerequisites

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

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

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

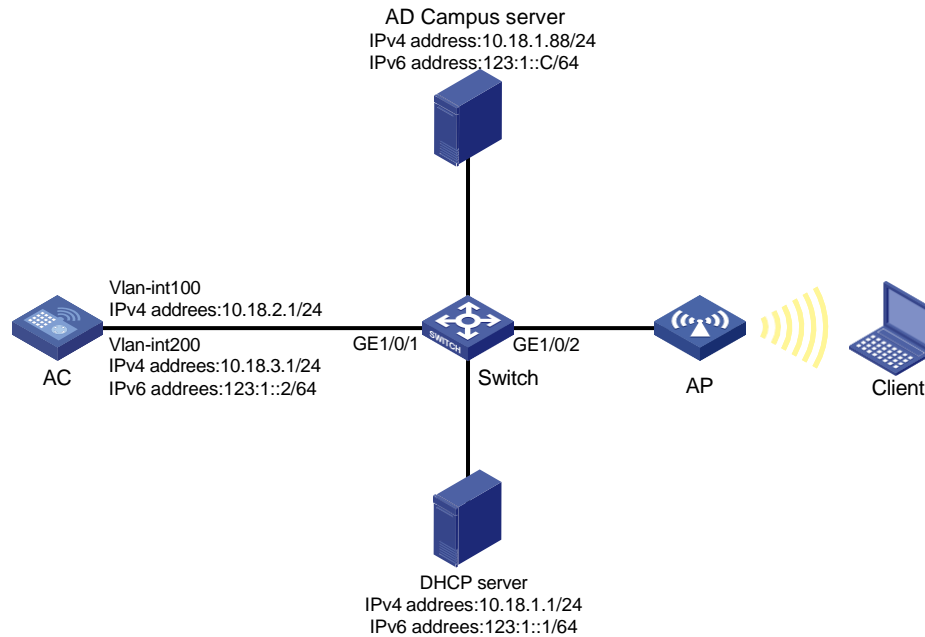
## Example: Configuring IPv6 URL redirection

### Network configuration

As shown in [Figure 1](#), the AP obtains an IP address from the DHCP server, and the client obtains an IPv6 address from the DHCP server and DHCPv6 server. To control the client's access to network resources, complete the following tasks:

- Configure VLAN 100 as the access VLAN for the AP.
- Configure VLAN 200 as the access VLAN for the client, and configure the client to be MAC authenticated on the AD Campus server.
- Configure IPv6 URL redirection for a client to authenticate to the RADIUS server after it has failed a MAC authentication because the server does not have its credential information and MAC address.

**Figure 1 Network diagram**



## Analysis

- For the client to complete MAC authentication through URL redirection and IPv6 URL redirection, configure both an IPv4 and an IPv6 address for the AC, client, and AD Campus server, and make sure they are reachable to each other.
- To display client IPv6 addresses on the AC, enable snooping DHCPv6 packets and ND packets.

## Restrictions and guidelines

- Use MAC-based user accounts for MAC authentication users. Make sure the username and password added on the RADIUS server are in the same format as the MAC authentication username configured on the AC.
- Use the actual serial ID of an AP to uniquely identify that AP.

## Procedures

### Configuring the AD Campus server

On the AD Campus server, add an AC, access policy, access service, access user, and ACL and URL authorization information.

### Editing the AP's configuration file

# Edit the AP's configuration file, name it map.txt and upload the configuration file to the storage media on the AC.

```
System-view
vlan 200
```

```

interface gigabitethernet1/0/1
port link-type trunk
port trunk permit vlan 200
acl advanced 3000
rule 1 permit ip destination 10.18.1.88 0
rule 2 permit ip source 10.18.1.88 0
acl ipv6 advanced 3000
rule 0 permit ipv6 source 123:1::C/128
rule 1 permit ipv6 destination 123:1::C/128

```

## 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 10.18.2.1 24
[AC-Vlan-interface100] quit

```

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

```

[AC] vlan 200
[AC-vlan200] quit
[AC] interface vlan-interface 200
[AC-Vlan-interface200] ip address 10.18.3.1 24
[AC-Vlan-interface200] ipv6 address 123:1::2 64
[AC-Vlan-interface200] quit

```

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

```

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

```

### 2. Configure a RADIUS scheme:

# Create a RADIUS scheme named **adcampus** and enter its view.

```

[AC] radius scheme adcampus

```

# Configure the primary authentication server, the primary accounting server, and the keys for the servers to communicate.

```

[AC-radius-rs1] primary authentication 10.18.1.88 (or [AC-radius-rs1] primary authentication ipv6 123:1::C 64)
[AC-radius-rs1] primary accounting 10.18.1.88 (or [AC-radius-rs1] primary accounting ipv6 123:1::C 64)
[AC-radius-rs1] key authentication simple 12345678
[AC-radius-rs1] key accounting simple 12345678

```

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

```

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

```

```
[AC-radius-rs1] quit
```

# Enable RADIUS session-control.

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

3. Configure an authentication domain:

# Create an ISP domain named **ds** and enter its view.

```
[AC] domain ds
```

# Perform RADIUS authentication for LAN users based on scheme **adcampus**.

```
[AC-isp-ds] authentication lan-access radius-scheme adcampus
```

# Perform RADIUS authorization for LAN users based on scheme **adcampus**.

```
[AC-isp-ds] authorization lan-access radius-scheme adcampus
```

# Perform RADIUS accounting for LAN users based on scheme **adcampus**.

```
[AC-isp-ds] accounting lan-access radius-scheme adcampus
```

```
[AC-isp-ds] quit
```

# Use MAC-based user accounts for MAC authentication users. The MAC addresses must be in hexadecimal notation without hyphens, and letters are in lower case.

```
[AC] mac-authentication user-name-format mac-address without-hyphen lowercase
```

4. Configure a wireless service:

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

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

# Configure the SSID as **url-redirect**.

```
[AC-wlan-st-redirect] ssid url-redirect
```

# Assign clients that come online from the service template to VLAN 200.

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

# Enable snooping DHCPv6 packets and ND packets.

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

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

# Specify the AP as the client data frame forwarder.

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

# Set the authentication mode to MAC authentication.

```
[AC-wlan-st-redirect] client-security authentication-mode mac
```

# Specify ISP domain **ds** for MAC authentication clients on the service template.

```
[AC-wlan-st-redirect] mac-authentication domain ds
```

# Enable URL redirection.

```
[AC-wlan-st-redirect] client url-redirect enable
```

# Enable the service template.

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

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

5. Configure URL redirection policies:

# Create IPv4 advanced ACL 3000, and configure the following rules: permit access only to the RADIUS server and deny IP packets, and permit inbound and outbound DHCP and DNS packets.

```
[AC] acl advanced 3000
```

```
[AC-acl-ipv4-adv-3000] rule 1 permit ip destination 10.18.1.88 0
```

```
[AC-acl-ipv4-adv-3000] rule 2 permit ip source 10.18.1.88 0
```

```
[AC-acl-ipv4-adv-3000] rule 3 permit udp destination-port eq bootps
```

```
[AC-acl-ipv4-adv-3000] rule 4 permit udp destination-port eq bootpc
```

```
[AC-acl-ipv4-adv-3000] rule 5 permit udp destination-port eq dns
```

```
[AC-acl-ipv4-adv-3000] rule 6 permit udp source-port eq dns
[AC-acl-ipv4-adv-3000] rule 9 deny ip
```

# Create IPv6 advanced ACL 3000, and configure the following rules: permit access only to the RADIUS server and deny IP packets, and permit inbound and outbound RS, RA, DHCPv6, and DNS packets.

```
[AC] acl ipv6 advanced 3000
[AC-acl-ipv6-adv-3000] rule 0 permit ipv6 source 123:1::C/128
[AC-acl-ipv6-adv-3000] rule 1 permit ipv6 destination 123:1::C/128
[AC-acl-ipv6-adv-3000] rule 2 permit udp destination-port eq dns
[AC-acl-ipv6-adv-3000] rule 3 permit udp source-port eq dns
[AC-acl-ipv6-adv-3000] rule 4 permit udp destination-port eq 546
[AC-acl-ipv6-adv-3000] rule 5 permit udp destination-port eq 547
[AC-acl-ipv6-adv-3000] rule 6 permit icmpv6 icmp6-type router-advertisement
[AC-acl-ipv6-adv-3000] rule 7 permit icmpv6 icmp6-type router-solicitation
[AC-acl-ipv6-adv-3000] rule 8 permit icmpv6 icmp6-type neighbor-solicitation
[AC-acl-ipv6-adv-3000] rule 9 permit icmpv6 icmp6-type neighbor-advertisement
[AC-acl-ipv6-adv-3000] rule 10 deny ipv6
[AC-acl-ipv6-adv-3000] quit
```

6. Configure a manual AP, and bind service template **redirect** to a radio on the AP:

---

**NOTE:**

In large-scale networks, configure AP groups instead of single APs 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
```

# Add AP **ap1** to AP group **group1**.

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

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

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

# 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 the AP.

```
[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 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 VLAN 100 and VLAN 200.

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

# Configure GigabitEthernet 1/0/2 that connects the switch to the AP as a trunk port, and assign the trunk port to VLAN 100 and VLAN 200.

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

# Enable the PoE feature.

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

## Verifying the configuration

1. Verify that the wireless client can associate with the AP after MAC authentication and will be redirected to the authentication page as long as the client accesses a webpage. Display MAC authentication connection information to verify that the ACL and URL have been deployed by the server.

```
[AC] dis mac-authentication connection
Total connections: 1
```

|                            |                                                               |
|----------------------------|---------------------------------------------------------------|
| User MAC address           | : ecd0-9f92-2787                                              |
| AP name                    | : ap1                                                         |
| Radio ID                   | : 1                                                           |
| SSID                       | : url-redirect                                                |
| BSSID                      | : 3891-d5ba-fa60                                              |
| Username                   | : ecd09f922787                                                |
| Authentication domain      | : ds                                                          |
| Initial VLAN               | : 200                                                         |
| Authorization VLAN         | : 200                                                         |
| Authorization ACL number   | : 3000                                                        |
| Authorization user profile | : N/A                                                         |
| Authorization CAR          | : N/A                                                         |
| Authorization URL          | : http://10.18.1.88:8080/byod?usermac=%m&userip=%c&userurl=%o |
| Authorization IPv6 URL     | : http://123:1::C:8080/portal                                 |
| Termination action         | : N/A                                                         |
| Session timeout last from  | : N/A                                                         |
| Session timeout period     | : N/A                                                         |
| Online from                | : 2020/04/01 13:46:29                                         |
| Online duration            | : 0h 0m 7s                                                    |

2. Verify that the client can access the WLAN after authentication. Display MAC authentication connection information to verify that no URL is deployed by the server.

Total connections: 1

|                            |                       |
|----------------------------|-----------------------|
| User MAC address           | : ecd0-9f92-2787      |
| AP name                    | : ap1                 |
| Radio ID                   | : 1                   |
| SSID                       | : url-redirect        |
| BSSID                      | : 3891-d5ba-fa60      |
| Username                   | : ecd09f922787        |
| Authentication domain      | : ds                  |
| Initial VLAN               | : 200                 |
| Authorization VLAN         | : 200                 |
| Authorization ACL number   | : N/A                 |
| Authorization user profile | : N/A                 |
| Authorization CAR          | : N/A                 |
| Authorization URL          | : N/A                 |
| Authorization IPv6 URL     | : N/A                 |
| Termination action         | : N/A                 |
| Session timeout last from  | : N/A                 |
| Session timeout period     | : N/A                 |
| Online from                | : 2020/04/01 13:46:40 |
| Online duration            | : 0h 0m 18s           |

## Configuration files

- AC:

```
#
 mac-authentication user-name-format mac-address with-hyphen
#
vlan 100
#
vlan 200
#
wlan service-template redirect
 ssid url-redirect
vlan 200
 client forwarding-location ap
 client url-redirect enable
 client-security authentication-mode mac
 client ipv6-snooping nd-learning enable
 client ipv6-snooping dhcpv6-learning enable
 mac-authentication domain ds
 service-template enable
#
interface Vlan-interface100
 ip address 10.18.2.1 255.255.255.0
#
interface Vlan-interface200
 ip address 10.18.3.1 255.255.255.0
```



```

 ipv6 address 123:1::2/64
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 100 200
#
 radius session-control enable
#
radius scheme adcampus
 primary authentication 10.18.1.88
 primary accounting 10.18.1.88
 key authentication cipher c3$Sggqz7lDs4XPnethmAgyAKVlke7qwEkYbQ==
 key accounting cipher c3$4J/JBRGwqB4F213furJMkB6JWYXBFjWE6g==
 user-name-format without-domain
#
domain ds
 authentication portal radius-scheme adcampus
 authorization portal radius-scheme adcampus
 accounting portal radius-scheme adcampus
#
acl advanced 3000
 rule 1 permit ip destination 10.18.1.88 0
 rule 2 permit ip source 10.18.1.88 0
 rule 3 permit udp destination-port eq bootps
 rule 4 permit udp destination-port eq bootpc
 rule 5 permit udp destination-port eq dns
 rule 6 permit udp source-port eq dns
 rule 9 deny ip
#
acl ipv6 advanced 3000
 rule 0 permit ipv6 source 123:1::C/128
 rule 1 permit ipv6 destination 123:1::C/128
 rule 2 permit udp destination-port eq dns
 rule 3 permit udp source-port eq dns
 rule 4 permit udp destination-port eq 546
 rule 5 permit udp destination-port eq 547
 rule 8 permit icmpv6 icmp6-type router-advertisement
 rule 9 permit icmpv6 icmp6-type router-solicitation
 rule 10 deny ipv6
#
wlan ap-group group1
 ap ap1
 ap-model AP
 3620 radio 1
 map-configuration map.txt
 service-template redirect
 radio enable
#

```

- ```
wlan ap ap1 model AP 3620
serial-id 219801A28N819CE0002T
#
```
- **Switch:**

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

Related documentation

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