

INTELBRAS Access Controllers

IRF Setup with Members Directly Connected

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: Setting up a two-member IRF fabric with members directly connected.....	1
Network configuration.....	1
Restrictions and guidelines.....	2
IRF setup requirements.....	2
Feature configuration and compatibility on an IRF fabric.....	3
IRF fabric tuning and maintenance	3
Procedures	3
Configuring the switch	3
Configuring AC 1	4
Configuring AC 2	4
Configuring the IRF fabric.....	5
Verifying the configuration	6
Configuration files.....	7
Related documentation	8

Introduction

The following information provides an example for setting up an IRF fabric with two member devices that are directly connected.

The Intelligent Resilient Framework (IRF) technology is proprietary to INTELBRAS. This technology is a true stacking technology that creates a large virtual stack called IRF fabric from multiple devices to provide data center class availability and scalability. IRF offers processing power, interaction, unified management, and uninterrupted maintenance of multiple devices.

Prerequisites

NOTE:

Support for this configuration example varies by device model and version.

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 IRF and Ethernet link aggregation.

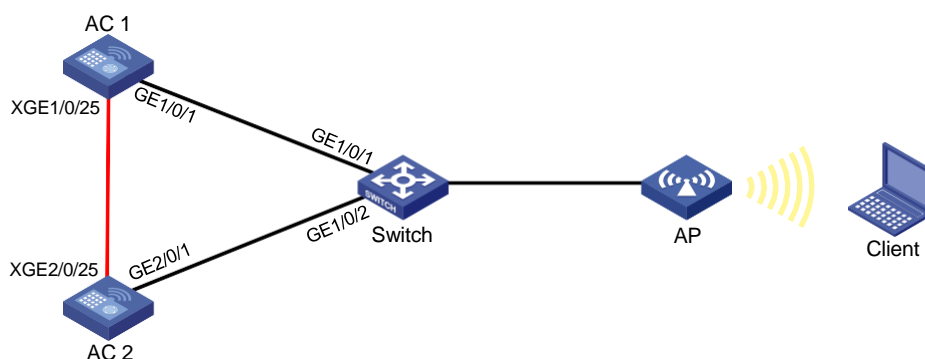
Example: Setting up a two-member IRF fabric with members directly connected

Network configuration

As shown in [Figure 1](#), use AC 1 and AC 2 to set up an IRF fabric. The IRF network interfaces on the ACs are directly connected.

Configure LACP MAD on the multi-member link aggregation to the switch, an INTELBRAS device that supports extended LACP.

Figure 1 Network diagram



Restrictions and guidelines

To ensure successful setup and maintenance of the IRF fabric, read the following information carefully.

IRF setup requirements

IRF fabric size

At the time of this writing, an IRF fabric can contain a maximum of two ACs.

Software version requirements

Make sure all IRF member devices run the same software image version.

To add a device of a different software version to the IRF fabric, make sure the software auto-update feature is enabled on the device for software synchronization.

By default, the software auto-update feature for IRF is enabled. To verify that the feature is enabled, execute the **display irf** command and then examine the **Auto upgrade** field. If the feature is disabled, use the **irf auto-update enable** command to enable it.

IRF connection requirements

To build a two-member IRF fabric, you can connect two devices directly or indirectly through a switch.

IRF physical interface restrictions

When you use 100Base-FX/1000Base-X SFP ports or 10GBase-R SFP+ ports to establish IRF links, follow these guidelines:

- Do not use 100Base-FX/1000Base-X SFP ports with 100M transceiver modules.
- Do not use 10GBase-R SFP+ ports with 1G transceiver modules.

IRF port binding requirements

You can create only one IRF port on an AC. The IRF port is named **irf-port *n***, where *n* is the IRF member ID of the AC.

When you bind physical interfaces to an IRF port, follow these restrictions and guidelines:

- The physical interfaces bound to an IRF port must be the same in speed.
- An IRF port can contain hybrid (control & data) channels, separate control and data channels, but not both. If you have bound a physical interface to the IRF port as a hybrid channel, you cannot bind additional physical interfaces to the IRF port as separate control or data channels. Conversely, if you have bound a physical interface to the IRF port as a separate data or control channel, you cannot bound additional physical interfaces as hybrid channels to the IRF port.

After you bind physical interfaces to the IRF port on an AC, you must save the configuration, and then restart the AC or activate the IRF port settings for the bindings to take effect.

Other configuration requirements

Make sure the following requirements are met:

Item	Requirements
Spanning tree feature	Do not enable the spanning tree feature on any IRF physical interfaces in the IRF fabric.
IRF member ID	Assign a unique member ID to each member device. The member ID assigned to a device takes effect after the device restarts.

Item	Requirements
Topo-domain ID	Assign the same topo-domain ID and MAD domain ID to all member devices.

Configure Layer 2 dynamic aggregate interfaces to transmit service packets only after you have established the IRF fabric.

IRF merge guidelines

If the IRF fabrics to be merged use the same bridge MAC address, you must change the bridge MAC address of one fabric.

To merge split IRF fabrics, make sure the IRF configuration on their member devices has not changed after the split.

Feature configuration and compatibility on an IRF fabric

To avoid service interference, isolate service packets from IRF packets at Layer 2.

If a multilink link aggregation is established between the IRF fabric and a switch, do not configure per-packet load sharing on the link aggregation at the switch end.

NAT is not supported on an IRF fabric.

IRF fabric tuning and maintenance

You cannot bring down an IRF link by shutting down the network interface on the IRF standby device side if that link is the only control channel in up state on the device. To bring down the IRF link, execute the **shutdown** command to shut down the network interface on the master device side for the link.

Before you can remove a network interface from an IRF port while multiple correctly operating IRF links are present, you must execute the **shutdown** command to shut that network interface down.

To change the IRF member ID of a device, execute the **irf member renumber** command on the device, and then restart the device for the change to take effect. To avoid MAD failures or service interruption, make sure the new member ID is unique among all IRF members.

All members in an IRF fabric use the same MAD domain ID. To change the MAD domain ID, execute the **irf domain** command on the master device. Make sure the new MAD domain ID is unique among all IRF fabrics present on the network for correct IRF split detection.

Procedures

Configuring the switch

Create Layer 2 aggregate interface Bridge-Aggregation 1, and configure the aggregation group of the aggregate interface to operate in dynamic mode.

```
<Switch> system-view
[Switch] interface bridge-aggregation 1
[Switch-Bridge-Aggregation1] link-aggregation mode dynamic
[Switch-Bridge-Aggregation1] quit
```

Assign GigabitEthernet 1/0/1 to aggregation group 1.

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

Assign GigabitEthernet 1/0/2 to aggregation group 1.

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

Enable link-aggregation traffic redirection.

```
[Switch] link-aggregation lacp traffic-redirect-notification enable
```

Configuring AC 1

Assign Ten-GigabitEthernet 1/0/25 to IRF-port 1.

```
<AC1> system-view
[AC1] irf-port 1
[AC1-irf-port1] port group interface ten-gigabitethernet 1/0/25
[AC1-irf-port1] quit
```

Specify the member priority as 2. AC 1 will be the master device.

```
[AC1] irf member 1 priority 2
```

Save the configuration.

```
[AC1] save
The current configuration will be written to the device. Are you sure? [Y/N]:y
Please input the file name(*.cfg)[cfa0:/startup.cfg]
(To leave the existing filename unchanged, press the enter key):
Validating file. Please wait...
Saved the current configuration to mainboard device successfully.
```

Activate the IRF port configuration.

```
[AC1] irf-port-configuration active
```

Configuring AC 2

Change the IRF member ID to 2.

```
<AC2> system-view
[AC2] irf member 1 renumber 2
Renumbering the member ID may result in configuration change or loss. Continue?[Y/N]:y
[AC2] quit
```

Reboot the AC for the new member ID to take effect.

```
<AC2> reboot
Start to check configuration with next startup configuration file, please wait..
..... DONE!
Current configuration may be lost after the reboot, save current configuration?
[Y/N]:y
Please input the file name(*.cfg)[cfa0:/startup.cfg]
(To leave the existing filename unchanged, press the enter key):
cfa0:/startup.cfg exists, overwrite? [Y/N]:y
Validating file. Please wait...
Saved the current configuration to mainboard device successfully.
This command will reboot the device. Continue? [Y/N]:y
Now rebooting, please wait...
```

Assign Ten-GigabitEthernet 2/0/25 to the IRF port.

```
<AC2> system-view
[AC2] irf-port 2
[AC2-irf-port2] port group interface ten-gigabitethernet 2/0/25
[AC2-irf-port2] quit
```

Save the configuration.

```
[AC2] save
The current configuration will be written to the device. Are you sure? [Y/N]:y
Please input the file name(*.cfg)[cfa0:/startup.cfg]
(To leave the existing filename unchanged, press the enter key):
Validating file. Please wait...
Saved the current configuration to mainboard device successfully.
```

Activate the IRF port configuration.

```
[AC2] irf-port-configuration active
System is starting...
```

AC 1 and AC 2 perform master election. AC 2 fails master election and reboots to form an IRF fabric with AC 1.

Configuring the IRF fabric

❗ IMPORTANT:

IRF split causes network conflicts, because the split IRF fabrics operate with the same IP address. To avoid this issue, configure MAD settings.

Change the name of the IRF fabric to IRF.

```
<AC1> system-view
[AC1] system-name IRF
```

Configure descriptions for AC 1 and AC 2, respectively.

```
[IRF] irf member 1 description AC 1
[IRF] irf member 2 description AC 2
```

Create a Layer 2 aggregate interface named Bridge-Aggregation 1, and configure the aggregation group of the aggregate interface to operate in dynamic mode.

```
[IRF] interface bridge-aggregation 1
[IRF-Bridge-Aggregation1] link-aggregation mode dynamic
```

Enable LACP MAD on the aggregate interface.

```
[IRF-Bridge-Aggregation1] mad enable
[IRF-Bridge-Aggregation1] quit
```

Enable link-aggregation traffic redirection.

```
[IRF] link-aggregation lacp traffic-redirect-notification enable
```

Assign GigabitEthernet 1/0/1 to aggregation group 1.

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

Assign GigabitEthernet 2/0/1 to aggregation group 1.

```
[IRF] interface gigabitethernet 2/0/1
[IRF-GigabitEthernet2/0/1] port link-aggregation group 1
```

```
[IRF-GigabitEthernet2/0/1] quit
```

Verifying the configuration

Display IRF information. Verify that AC 1 is the master device.

```
[IRF] display irf
```

Member ID	Role	Priority	CPU MAC	Description
*1	Master	2	50da-0051-2608	AC 1
+2	Standby	1	50da-0051-2670	AC 2

The asterisk (*) indicates the master.

The plus sign (+) indicates the device through which you are logged in.

The right angle bracket (>) indicates the device's stack capability is disabled.

Bridge MAC of the IRF: 50da-0051-2608

Auto upgrade : Enabled

MAC persistence : 6 min

Topo-domain ID : 0

Auto merge : Enabled

Display IRF link information. Verify that the IRF network interfaces on both member devices are up.

```
[IRF] display irf link
```

Member ID	Member Interfaces	Status
1	XGE1/0/25(ctrl&data)	Up
2	XGE2/0/25(ctrl&data)	Up

On the IRF fabric, display detailed information about aggregation groups. Verify that GigabitEthernet 1/0/1 and GigabitEthernet 2/0/1 are in aggregation group 1 and in Selected state.

```
[IRF] display link-aggregation verbose
```

Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing

Port Status: S -- Selected, U -- Unselected, I -- Individual

Flags: A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
D -- Synchronization, E -- Collecting, F -- Distributing,
G -- Defaulted, H -- Expired

Aggregate Interface: Bridge-Aggregation1

Aggregation Mode: Dynamic

Loadsharing Type: Shar

System ID: 0x8000, 50da-0051-2608

Local:

Port	Status	Priority	Oper-Key	Flag
GE1/0/1	S	32768	1	{ACDEF}
GE2/0/1	S	32768	1	{ACDEF}

Remote:

Actor	Partner	Priority	Oper-Key	SystemID	Flag
GE1/0/1	1	32768	1	0x8000, 3897-d633-f3c6	{ACDEF}
GE2/0/1	2	32768	1	0x8000, 3897-d633-f3c6	{ACDEF}

On the switch, display detailed information about aggregation groups. Verify that GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 are in aggregation group 1 and in Selected state.

```
[Switch] display link-aggregation verbose
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Port Status: S -- Selected, U -- Unselected,
               I -- Individual, * -- Management port
Flags:  A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
        D -- Synchronization, E -- Collecting, F -- Distributing,
        G -- Defaulted, H -- Expired
```

Aggregate Interface: Bridge-Aggregation1

Aggregation Mode: Dynamic

Loadsharing Type: Shar

Management VLAN : None

System ID: 0x8000, 3897-d633-f3c6

Local:

Port	Status	Priority	Oper-Key	Flag
GE1/0/1	S	32768	1	{ACDEF}
GE1/0/2	S	32768	1	{ACDEF}

Remote:

Actor	Partner	Priority	Oper-Key	SystemID	Flag
GE1/0/1	2	32768	1	0x8000, 50da-0051-2608	{ACDEF}
GE1/0/2	31	32768	1	0x8000, 50da-0051-2608	{ACDEF}

Configuration files

- IRF fabric:

```
#
sysname IRF
#
irf mac-address persistent timer
irf auto-update enable
irf auto-merge enable
irf member 1 priority 2
irf member 2 priority 1
irf member 1 description AC 1
irf member 2 description AC 2
#
link-aggregation lacp traffic-redirect-notification enable
#
irf-port 1
port group interface Ten-GigabitEthernet1/0/25
#
irf-port 2
port group interface Ten-GigabitEthernet2/0/25
#
```

```

interface Bridge-Aggregation1
  link-aggregation mode dynamic
  mad enable
#
interface GigabitEthernet1/0/1
  port link-aggregation group 1
#
interface GigabitEthernet2/0/1
  port link-aggregation group 1
#

```

- **Switch:**

```

#
  link-aggregation lacp traffic-redirect-notification enable
#
interface Bridge-Aggregation1
  link-aggregation mode dynamic
#
interface GigabitEthernet1/0/1
  port link-aggregation group 1
#
interface GigabitEthernet1/0/2
  port link-aggregation group 1
#

```

Related documentation

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

INTELBRAS Access Controllers

ARP MAD-Enabled IRF Fabric of Two Directly Connected Member Devices

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: Setting up an ARP MAD-enabled IRF fabric of two directly connected devices	1
Network configuration	1
Restrictions and guidelines	2
IRF setup requirements	2
Feature configuration and compatibility on an IRF fabric	3
IRF fabric tuning and maintenance	3
Procedures	4
Configuring the switch	4
Configuring AC 1	4
Configuring AC 2	5
Configuring the IRF fabric	6
Verifying the configuration	7
Configuration files	8
Related documentation	10

Introduction

The following information provides an example for setting up an IRF fabric that contains two directly connected access controllers (ACs) and uses ARP MAD for IRF split detection.

Prerequisites

NOTE:

Support for this configuration example varies by device model and version.

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

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

This document assumes that you have basic knowledge of IRF and Ethernet link aggregation.

Example: Setting up an ARP MAD-enabled IRF fabric of two directly connected devices

Network configuration

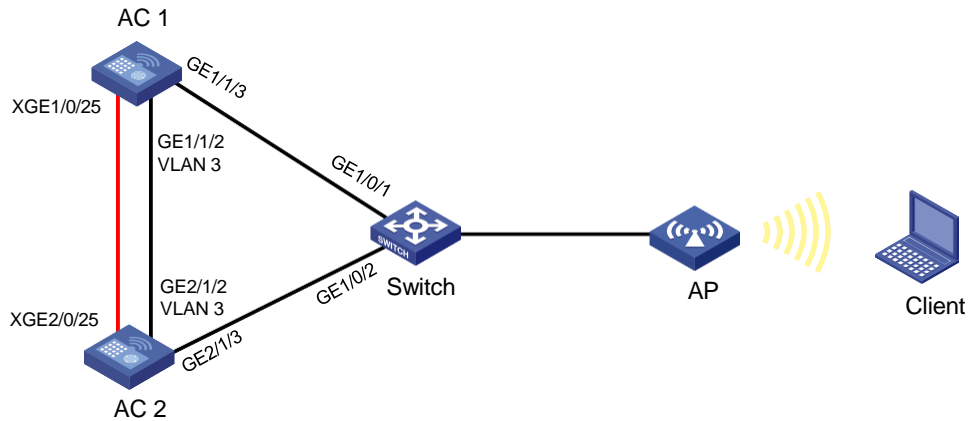
! IMPORTANT:

ARP MAD requires that the IRF member devices be directly connected, without switches between them.

As shown in [Figure 1](#), deploy two ACs (AC 1 and AC 2) for node redundancy and connect the ACs to a third-party switch on the network.

- Directly connect AC 1 and AC 2 to build an IRF fabric.
- To quickly detect a multi-active collision caused by IRF split, configure a minimum of one multi-active detection (MAD) mechanism. Because the switch does not support LACP MAD, this example uses ARP MAD instead.
- Configure the IRF fabric to establish a dynamic aggregate link with the switch to forward IRF service packets.
- Create VLAN 3 on the IRF fabric for ARP MAD.

Figure 1 Network diagram



Restrictions and guidelines

To ensure successful setup and maintenance of the IRF fabric, read the following information carefully.

IRF setup requirements

IRF fabric size

At the time of this writing, an IRF fabric can contain a maximum of two ACs.

Software version requirements

Make sure all IRF member devices run the same software image version.

To add a device of a different software version to the IRF fabric, make sure the software auto-update feature is enabled on the device for software synchronization.

By default, the software auto-update feature for IRF is enabled. To verify that the feature is enabled, execute the `display irf` command and then examine the **Auto upgrade** field. If the feature is disabled, use the `irf auto-update enable` command to enable it.

IRF connection requirements

To build a two-member IRF fabric, you can connect two devices directly or indirectly through a switch.

IRF physical interface restrictions

When you use 100Base-FX/1000Base-X SFP ports or 10GBase-R SFP+ ports to establish IRF links, follow these guidelines:

- Do not use 100Base-FX/1000Base-X SFP ports with 100M transceiver modules.
- Do not use 10GBase-R SFP+ ports with 1G transceiver modules.

IRF port binding requirements

You can create only one IRF port on an AC. The IRF port is named **irf-port *n***, where *n* is the IRF member ID of the AC.

When you bind physical interfaces to an IRF port, follow these restrictions and guidelines:

- The physical interfaces bound to an IRF port must be the same in speed.

- An IRF port can contain hybrid (control & data) channels, separate control and data channels, but not both. If you have bound a physical interface to the IRF port as a hybrid channel, you cannot bind additional physical interfaces to the IRF port as separate control or data channels. Conversely, if you have bound a physical interface to the IRF port as a separate data or control channel, you cannot bound additional physical interfaces as hybrid channels to the IRF port.

After you bind physical interfaces to the IRF port on an AC, you must save the configuration, and then restart the AC or activate the IRF port settings for the bindings to take effect.

Other configuration requirements

Make sure the following requirements are met:

Item	Requirements
Spanning tree feature	<ul style="list-style-type: none"> • On the IRF members—To avoid loops, enable the spanning tree feature on the physical ports used for ARP MAD. Disable the spanning tree feature on the other physical ports. • On the switch—To avoid service interruption, disable the spanning tree feature on the physical ports used for IRF services.
IRF member ID	Assign a unique member ID to each member device. The member ID assigned to a device takes effect after the device restarts.
Topo-domain ID	Assign the same topo-domain ID and MAD domain ID to all member devices.

Configure Layer 2 dynamic aggregate interfaces to transmit service packets only after you have established the IRF fabric.

IRF merge guidelines

If the IRF fabrics to be merged use the same bridge MAC address, you must change the bridge MAC address of one fabric.

To merge split IRF fabrics, make sure the IRF configuration on their member devices has not changed after the split.

Feature configuration and compatibility on an IRF fabric

To avoid service interference, isolate service packets from IRF packets at Layer 2.

If a multilink aggregation is established between the IRF fabric and a switch, do not configure per-packet load sharing on the link aggregation at the switch end.

NAT is not supported on an IRF fabric.

IRF fabric tuning and maintenance

You cannot bring down an IRF link by shutting down the network interface on the IRF standby device side if that link is the only control channel in up state on the device. To bring down the IRF link, execute the **shutdown** command to shut down the network interface on the master device side for the link.

Before you can remove a network interface from an IRF port while multiple correctly operating IRF links are present, you must execute the **shutdown** command to shut that network interface down.

To change the IRF member ID of a device, execute the **irf member renumber** command on the device, and then restart the device for the change to take effect. To avoid MAD failures or service interruption, make sure the new member ID is unique among all IRF members.

All members in an IRF fabric use the same MAD domain ID. To change the MAD domain ID, execute the **irf domain** command on the master device. Make sure the new MAD domain ID is unique among all IRF fabrics present on the network for correct IRF split detection.

Procedures

Configuring the switch

Create Bridge-Aggregation 1 and configure Layer 2 aggregation group 1 to operate in dynamic aggregation mode.

```
<Switch> system-view
[Switch] interface bridge-aggregation 1
[Switch-Bridge-Aggregation1] link-aggregation mode dynamic
[Switch-Bridge-Aggregation1] quit
```

Add GigabitEthernet 1/0/1 to aggregation group 1.

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

Add GigabitEthernet 1/0/2 to aggregation group 1.

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

Enable link-aggregation traffic redirection to ensure traffic continuity when a Selected port goes down.

```
[Switch] link-aggregation lacp traffic-redirect-notification enable
```

Configuring AC 1

1. Configure the IRF port:

Shut down the interfaces to be bound to the IRF port. In this example, shut down Ten-GigabitEthernet 1/0/25.

```
<AC1> system-view
[AC1] interface ten-gigabitethernet 1/0/25
[AC1-Ten-GigabitEthernet1/0/25] shutdown
[AC1-Ten-GigabitEthernet1/0/25] quit
```

Create IRF port 1 and add Ten-GigabitEthernet 1/0/25 to the IRF port.

```
[AC1] irf-port 1
[AC1-irf-port1] port group interface ten-gigabitethernet 1/0/25
[AC1-irf-port1] quit
```

Bring up Ten-GigabitEthernet 1/0/25.

```
[AC1] interface ten-gigabitethernet 1/0/25
[AC1-Ten-GigabitEthernet1/0/25] undo shutdown
[AC1-Ten-GigabitEthernet1/0/25] quit
```

2. Set the IRF member priority.

In this example, set the IRF member priority of AC 1 to 2 for AC 1 to win the master election.

```
[AC1] irf member 1 priority 2
```

3. Save the running configuration.

```
[AC1] save
The current configuration will be written to the device. Are you sure? [Y/N]:y
Please input the file name(*.cfg)[cfa0:/startup.cfg]
(To leave the existing filename unchanged, press the enter key):
```


Validating file. Please wait...

Saved the current configuration to mainboard device successfully.

4. Activate the IRF port settings.

```
[AC1] irf-port-configuration active
```

Configuring AC 2

1. Set the IRF member ID:

Set the member ID of AC 2 to 2.

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

```
[AC2] irf member 1 renumber 2
```

Renumbering the member ID may result in configuration change or loss. Continue? [

Y/N]:y

```
[AC2] quit
```

Restart AC 2 for the member ID to take effect.

```
<AC2> reboot
```

Start to check configuration with next startup configuration file, please wait..

.DONE!

Current configuration may be lost after the reboot, save current configuration?

[Y/N]:y

Please input the file name(*.cfg) [cfa0:/startup.cfg]

(To leave the existing filename unchanged, press the enter key):

cfa0:/startup.cfg exists, overwrite? [Y/N]:y

Validating file. Please wait...

Saved the current configuration to mainboard device successfully.

This command will reboot the device. Continue? [Y/N]:y

Now rebooting, please wait...

2. Configure the IRF port:

Shut down the interfaces to be bound to the IRF port. In this example, shut down Ten-GigabitEthernet 2/0/25.

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

```
[AC2] interface ten-gigabitethernet 2/0/25
```

```
[AC2-Ten-GigabitEthernet2/0/25] shutdown
```

```
[AC2-Ten-GigabitEthernet2/0/25] quit
```

Create IRF port 2 and bind Ten-GigabitEthernet 2/0/25 to the IRF port.

```
[AC2] irf-port 2
```

```
[AC2-irf-port2] port group interface ten-gigabitethernet 2/0/25
```

```
[AC2-irf-port2] quit
```

Bring up Ten-GigabitEthernet 2/0/25.

```
[AC2] interface ten-gigabitethernet 2/0/25
```

```
[AC2-Ten-GigabitEthernet2/0/25] undo shutdown
```

```
[AC2-irf-port2] quit
```

3. Save the running configuration.

```
[AC2] save
```

The current configuration will be written to the device. Are you sure? [Y/N]:y

Please input the file name(*.cfg) [cfa0:/startup.cfg]

(To leave the existing filename unchanged, press the enter key):

Validating file. Please wait...

Saved the current configuration to mainboard device successfully.

4. Activate the IRF port settings.

```
[AC2] irf-port-configuration active
System is starting...
```

AC 1 and AC 2 perform master election. AC 2 fails the master election and restarts to form an IRF fabric with AC 1.

Configuring the IRF fabric

! IMPORTANT:

If the IRF fabric splits, the two ACs might operate with the same IP address on the network. To avoid IP conflict and other network issues, configure MAD.

1. Change the system name to IRF.

```
<AC1> system-view
[AC1] system-name IRF
```

2. Specify member descriptions.

Configure the description as AC 1 for IRF member 1 and AC 2 for IRF member 2.

```
[IRF] irf member 1 description AC 1
[IRF] irf member 2 description AC 2
```

3. Configure the IRF service VLAN, assign an IP address to VLAN-interface 101, and enable periodic sending of gratuitous ARP packets on the interface to make sure correct ARP entry learning after the IRF split.

This example uses VLAN 101 as the IRF service VLAN.

```
[IRF] vlan 101
[IRF-vlan101] quit
[IRF] interface vlan-interface 101
[IRF-Vlan-interface101] ip address 10.128.52.250 255.255.255.0
[IRF-Vlan-interface101] arp send-gratuitous-arp interval 1000
```

4. Configure link aggregation:

Create Bridge-Aggregation 1 and configure Layer 2 aggregation group 1 to operate in dynamic aggregation mode.

```
[IRF] interface bridge-aggregation 1
[IRF-Bridge-Aggregation1] link-aggregation mode dynamic
[IRF-Bridge-Aggregation1] port link-type trunk
[IRF-Bridge-Aggregation1] undo port trunk permit vlan 1
[IRF-Bridge-Aggregation1] port trunk permit vlan 101
```

Add GigabitEthernet 1/1/3 to aggregation group 1.

```
[IRF] interface gigabitethernet 1/1/3
[IRF-GigabitEthernet1/1/3] port link-type trunk
[IRF-GigabitEthernet1/1/3] port trunk permit vlan 101
[IRF-GigabitEthernet1/1/3] undo port trunk permit vlan 1
[IRF-GigabitEthernet1/1/3] port link-aggregation group 1
[IRF-GigabitEthernet1/1/3] quit
```

Add GigabitEthernet 2/1/3 to aggregation group 1.

```
[IRF] interface gigabitethernet 2/1/3
[IRF-GigabitEthernet2/1/3] port link-type trunk
[IRF-GigabitEthernet2/1/3] port trunk permit vlan 101
```

```
[IRF-GigabitEthernet2/1/3] undo port trunk permit vlan 1
[IRF-GigabitEthernet2/1/3] port link-aggregation group 1
[IRF-GigabitEthernet2/1/3] quit
```

5. Configure ARP MAD:

! IMPORTANT:

If VLAN 1 is not used for services, enable the spanning tree feature also on VLAN 1 to prevent miscabling of idle physical ports in VLAN 1 from causing loops.

Enable the spanning tree feature globally, set its operating mode to PVST, and disable the feature on the all VLANs except for VLAN 3 (the VLAN for ARP MAD).

```
[IRF] stp global enable
[IRF] stp mode pvst
[IRF] undo stp vlan 2 4 to 4094 enable
```

Configure the IRF bridge MAC address to change as soon as the address owner leaves.

```
[IRF] undo irf mac-address persistent
```

Set the IRF domain ID to 1.

```
[IRF] irf domain 1
```

Create VLAN 3 for MAD, and assign GigabitEthernet 1/1/2 on AC 1 and GigabitEthernet 2/1/2 on AC 2 to VLAN 3.

```
[IRF] vlan 3
[IRF-vlan3] quit
[IRF] interface GigabitEthernet1/1/2
[IRF-GigabitEthernet1/1/2] port access vlan 3
[IRF-GigabitEthernet1/1/2] quit
[IRF] interface GigabitEthernet2/1/2
[IRF-GigabitEthernet2/1/2] port access vlan 3
[IRF-GigabitEthernet2/1/2] quit
```

Create VLAN-interface 3, assign an IP address to the interface, and enable ARP MAD.

```
[IRF] interface vlan-interface 3
[IRF-Vlan-interface3] ip address 192.168.2.1 24
[IRF-Vlan-interface3] mad arp enable
You need to assign a domain ID (range: 0-4294967295)
[Current domain is: 0]: 1
The assigned domain ID is: 1
```

6. Configure gratuitous ARP packet retransmission.

Set the maximum number of gratuitous ARP packet transmissions and the transmission interval for a device MAC address change.

```
[IRF] gratuitous-arp mac-change retransmit 3 interval 2
```

Verifying the configuration

1. Verify that AC 1 is the master device, with a higher priority than AC 2.

```
[IRF] display irf
```

Member ID	Role	Priority	CPU MAC	Description
*1	Master	2	50da-0051-2608	AC 1
+2	Standby	1	50da-0051-2670	AC 2

The asterisk (*) indicates the master.

The plus sign (+) indicates the device through which you are logged in.

The right angle bracket (>) indicates the device's stack capability is disabled.

Bridge MAC of the IRF: 50da-0051-2608

Auto upgrade : Enabled

MAC persistence : Disabled

Topo-domain ID : 0

Auto merge : Enabled

2. Verify that both IRF ports are in Up state.

```
[IRF] display irf link
```

Member ID	Member Interfaces	Status
1	XGE1/0/25(ctrl&data)	Up
2	XGE2/0/25(ctrl&data)	Up

3. Verify that ARP MAD is configured correctly.

```
[IRF] display mad verbose
```

Multi-active recovery state: No

Excluded ports (user-configured):

Excluded ports (system-configured):

Ten-GigabitEthernet1/0/25

Ten-GigabitEthernet2/0/25

MAD ARP enabled interface:

Vlan-interface3

MAD ND disabled.

MAD LACP disabled.

MAD BFD disabled.

Configuration files

- IRF

```
#
sysname IRF
#
undo irf mac-address persistent
irf auto-update enable
irf auto-merge enable
irf member 1 priority 2
irf member 2 priority 1
irf member 1 description AC 1
irf member 2 description AC 2
#
link-aggregation lacp traffic-redirect-notification enable
#
irf-port 1
port group interface Ten-GigabitEthernet1/0/25
#
irf-port 2
port group interface Ten-GigabitEthernet2/0/25
```

```

#
vlan 3
#
interface Bridge-Aggregation1
    port link-type trunk
    undo port trunk permit vlan 1
    port trunk permit vlan 101
    link-aggregation mode dynamic
#
vlan 101
#
interface Vlan-interface3
ip address 192.168.10.10 255.255.255.0
    mad arp enable
#
interface Vlan-interface101
    ip address 10.128.52.250 255.255.255.0
    arp send-gratuitous-arp interval 1000
#
interface GigabitEthernet1/1/2
    port access vlan 3
#
interface GigabitEthernet1/1/3
    port link-type trunk
    undo port trunk permit vlan 1
    port trunk permit vlan 101
    port link-aggregation group 1
#
interface GigabitEthernet2/1/2
    port access vlan 3
#
interface GigabitEthernet2/1/3
    port link-type trunk
    undo port trunk permit vlan 1
    port trunk permit vlan 101
    port link-aggregation group 1
#
undo stp vlan 2 4 to 4094 enable
stp mode pvst
stp global enable
#
    gratuitous-arp mac-change retransmit 3 interval 2
#

```

- **Switch**

```

#
    link-aggregation lacp traffic-redirect-notification enable
#
interface Bridge-Aggregation1

```

```
link-aggregation mode dynamic
#
interface GigabitEthernet1/0/1
port link-aggregation group 1
#
interface GigabitEthernet1/0/2
port link-aggregation group 1
#
```

Related documentation

- *High Availability Command Reference in INTELBRAS Access Controllers Command References*
- *High Availability 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

IRF Setup with Members Not Directly Connected

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: Setting up a two-member IRF fabric with members not directly connected.....	1
Network configuration.....	1
Restrictions and guidelines.....	2
IRF setup requirements.....	2
Feature configuration and compatibility on an IRF fabric.....	3
IRF fabric tuning and maintenance	3
Procedures	3
Configuring AC 1	3
Configuring AC 2.....	4
Configuring the IRF fabric.....	5
Configuring Switch	5
Verifying the configuration	6
Configuration files.....	7
Related documentation	9

Introduction

The following information provides an example for setting up a two-member IRF fabric with members not directly connected.

The Intelligent Resilient Framework (IRF) technology is proprietary to INTELBRAS. This technology is a true stacking technology that creates a large virtual stack called IRF fabric from multiple devices to provide data center class availability and scalability. IRF offers processing power, interaction, unified management, and uninterrupted maintenance of multiple devices.

Prerequisites

NOTE:

Support for this configuration example varies by device model and version.

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.

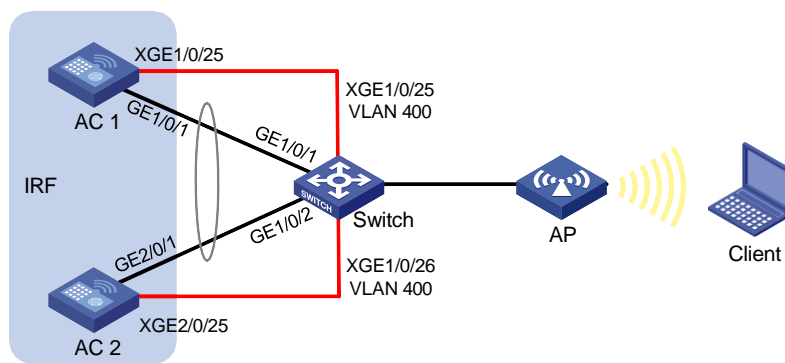
The following information is provided based on the assumption that you have basic knowledge of IRF and Ethernet link aggregation.

Example: Setting up a two-member IRF fabric with members not directly connected

Network configuration

As shown in [Figure 1](#), use AC 1 and AC 2 to set up an IRF fabric. The IRF network interfaces of the ACs are connected through a Layer 2 switch.

Figure 1 Network diagram



Restrictions and guidelines

To ensure successful setup and maintenance of the IRF fabric, read the following information carefully.

IRF setup requirements

IRF fabric size

At the time of this writing, an IRF fabric can contain a maximum of two ACs.

Software version requirements

Make sure all IRF member devices run the same software image version.

To add a device of a different software version to the IRF fabric, make sure the software auto-update feature is enabled on the device for software synchronization.

By default, the software auto-update feature for IRF is enabled. To verify that the feature is enabled, execute the **display irf** command and then examine the **Auto upgrade** field. If the feature is disabled, use the **irf auto-update enable** command to enable it.

IRF connection requirements

To build a two-member IRF fabric, you can connect two devices directly or indirectly through a switch.

IRF physical interface restrictions

When you use 100Base-FX/1000Base-X SFP ports or 10GBase-R SFP+ ports to establish IRF links, follow these guidelines:

- Do not use 100Base-FX/1000Base-X SFP ports with 100M transceiver modules.
- Do not use 10GBase-R SFP+ ports with 1G transceiver modules.

IRF port binding requirements

You can create only one IRF port on an AC. The IRF port is named **irf-port *n***, where *n* is the IRF member ID of the AC.

When you bind physical interfaces to an IRF port, follow these restrictions and guidelines:

- The physical interfaces bound to an IRF port must be the same in speed.
- An IRF port can contain hybrid (control & data) channels, separate control and data channels, but not both. If you have bound a physical interface to the IRF port as a hybrid channel, you cannot bind additional physical interfaces to the IRF port as separate control or data channels. Conversely, if you have bound a physical interface to the IRF port as a separate data or control channel, you cannot bound additional physical interfaces as hybrid channels to the IRF port.

After you bind physical interfaces to the IRF port on an AC, you must save the configuration, and then restart the AC or activate the IRF port settings for the bindings to take effect.

Other configuration requirements

Make sure the following requirements are met:

Item	Requirements
Ethernet link aggregation	<ul style="list-style-type: none">• On the switch, you must configure the aggregate interfaces connected to IRF network interfaces to operate in static mode. If you configure the aggregate interfaces to operate in dynamic mode, the switch might get stuck and the IRF fabric might even split.• On the switch, you must configure the aggregate interfaces used for LACP MAD to operate in dynamic mode.

Item	Requirements
Spanning tree feature	<ul style="list-style-type: none"> • On the IRF members—To avoid service interruption, disable the spanning tree feature on the IRF members when LACP MAD is used. • On the switch—To avoid service interruption, disable the spanning tree feature on the physical ports used for IRF services.
IRF member ID	Assign a unique member ID to each member device. The member ID assigned to a device takes effect after the device restarts.
Topo-domain ID	Assign the same topo-domain ID and MAD domain ID to all member devices.

Configure Layer 2 dynamic aggregate interfaces to transmit service packets only after you have established the IRF fabric.

IRF merge guidelines

If the IRF fabrics to be merged use the same bridge MAC address, you must change the bridge MAC address of one fabric.

To merge split IRF fabrics, make sure the IRF configuration on their member devices has not changed after the split.

Feature configuration and compatibility on an IRF fabric

To avoid service interference, isolate service packets from IRF packets at Layer 2.

If a multilink bundle is established between the IRF fabric and a switch, do not configure per-packet load sharing on the link aggregation at the switch end.

NAT is not supported on an IRF fabric.

IRF fabric tuning and maintenance

You cannot bring down an IRF link by shutting down the network interface on the IRF standby device side if that link is the only control channel in up state on the device. To bring down the IRF link, execute the **shutdown** command to shut down the network interface on the master device side for the link.

Before you can remove a network interface from an IRF port while multiple correctly operating IRF links are present, you must execute the **shutdown** command to shut that network interface down.

To change the IRF member ID of a device, execute the **irf member renumber** command on the device, and then restart the device for the change to take effect. To avoid MAD failures or service interruption, make sure the new member ID is unique among all IRF members.

All members in an IRF fabric use the same MAD domain ID. To change the MAD domain ID, execute the **irf domain** command on the master device. Make sure the new MAD domain ID is unique among all IRF fabrics present on the network for correct IRF split detection.

Procedures

Configuring AC 1

Assign Ten-GigabitEthernet 1/0/25 to the IRF port.

```
<AC1> system-view
```

```
[AC1] irf-port 1
```

```
[AC1-irf-port1] port group interface ten-gigabitethernet 1/0/25
```

```
[AC1-irf-port1] quit
```

Specify the member priority as 2. AC 1 will be the master device.

```
[AC1] irf member 1 priority 2
```

Save the configuration.

```
[AC1] save
```

The current configuration will be written to the device. Are you sure? [Y/N]:y

Please input the file name(*.cfg)[cfa0:/startup.cfg]

(To leave the existing filename unchanged, press the enter key):

Validating file. Please wait...

Saved the current configuration to mainboard device successfully.

Activate the IRF port configuration.

```
[AC1] irf-port-configuration active
```

Configuring AC 2

Change the IRF member ID to 2.

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

```
[AC2] irf member 1 renumber 2
```

Renumbering the member ID may result in configuration change or loss. Continue?[Y/N]:y

```
[AC2] quit
```

Reboot the AC for the new member ID to take effect.

```
<AC2> reboot
```

Start to check configuration with next startup configuration file, please wait..

..... DONE!

Current configuration may be lost after the reboot, save current configuration?

[Y/N]:y

Please input the file name(*.cfg)[cfa0:/startup.cfg]

(To leave the existing filename unchanged, press the enter key):

cfa0:/startup.cfg exists, overwrite? [Y/N]:y

Validating file. Please wait...

Saved the current configuration to mainboard device successfully.

This command will reboot the device. Continue? [Y/N]:y

Now rebooting, please wait...

Assign Ten-GigabitEthernet 2/0/25 to the IRF port.

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

```
[AC2] irf-port 2
```

```
[AC2-irf-port2] port group interface ten-gigabitethernet 2/0/25
```

```
[AC2-irf-port2] quit
```

Save the configuration.

```
[AC2] save
```

The current configuration will be written to the device. Are you sure? [Y/N]:y

Please input the file name(*.cfg)[cfa0:/startup.cfg]

(To leave the existing filename unchanged, press the enter key):

Validating file. Please wait...

Saved the current configuration to mainboard device successfully.

Activate the IRF port configuration.

```
[AC2] irf-port-configuration active
```

AC 1 and AC 2 perform master election. AC 2 fails the master election and reboots to form an IRF fabric with AC 1.

Configuring the IRF fabric

Change the name of the IRF fabric to IRF.

```
<AC1> system-view
[AC1] system-name IRF
```

Configure descriptions for AC 1 and AC 2, respectively.

```
[IRF] irf member 1 description AC 1
[IRF] irf member 2 description AC 2
```

Create Layer 2 aggregate interface Bridge-Aggregation 1, and configure the aggregation group of the aggregate interface to operate in dynamic mode.

```
[IRF] interface bridge-aggregation 1
[IRF-Bridge-Aggregation1] link-aggregation mode dynamic
```

Enable LACP MAD on Bridge-Aggregation 1.

```
[IRF-Bridge-Aggregation1] mad enable
[IRF-Bridge-Aggregation1] quit
```

Enable link-aggregation traffic redirection.

```
[IRF] link-aggregation lacp traffic-redirect-notification enable
```

Assign GigabitEthernet 1/0/1 to aggregation group 1.

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

Assign GigabitEthernet 2/0/1 to aggregation group 1.

```
[IRF] interface gigabitethernet 2/0/1
[IRF-GigabitEthernet2/0/1] port link-aggregation group 1
[IRF-GigabitEthernet2/0/1] quit
```

Configuring Switch

1. Configure links for interfaces connected to the IRF network interfaces:

Create VLAN 400 and assign the network interfaces on IRF links to the VLAN.

```
<Switch> system-view
[Switch] vlan 400
[Switch-vlan400] port ten-gigabitethernet 1/0/25
[Switch-vlan400] port ten-gigabitethernet 1/0/26
[Switch-vlan400] quit
```

Disable the spanning tree feature on Ten-GigabitEthernet 1/0/25 and Ten-GigabitEthernet 1/0/26.

```
[Switch] interface ten-gigabitethernet 1/0/25
[Switch-Ten-GigabitEthernet1/0/25] undo stp enable
[Switch-Ten-GigabitEthernet1/0/25] quit
[Switch] interface ten-gigabitethernet 1/0/26
[Switch-Ten-GigabitEthernet1/0/26] undo stp enable
[Switch-Ten-GigabitEthernet1/0/26] quit
```

2. Configure links used for transmitting service packets and LACP MAD packets between the switch and IRF fabric:

Create Layer 2 aggregate interface Bridge-Aggregation 1, and configure the aggregation group of the aggregate interface to operate in dynamic mode.

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

Assign GigabitEthernet 1/0/1 to aggregation group 1.

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

Assign GigabitEthernet 1/0/2 to aggregation group 1.

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

3. Enable link-aggregation traffic redirection.

```
[Switch] link-aggregation lacp traffic-redirect-notification enable
```

Verifying the configuration

Display IRF information. Verify that AC 1 is the master device.

```
[IRF] display irf
```

Member ID	Role	Priority	CPU MAC	Description
*1	Master	2	50da-0051-2608	AC 1
+2	Standby	1	50da-0051-2670	AC 2

The asterisk (*) indicates the master.

The plus sign (+) indicates the device through which you are logged in.

The right angle bracket (>) indicates the device's stack capability is disabled.

Bridge MAC of the IRF: 50da-0051-2608

Auto upgrade : Enabled

MAC persistence : 6 min

Topo-domain ID : 0

Auto merge : Enabled

Display IRF link information. Verify that the IRF network interfaces on both member devices are up.

```
[IRF] display irf link
```

Member ID	Member Interfaces	Status
1	XGE1/0/25(ctrl&data)	Up
2	XGE2/0/25(ctrl&data)	Up

On the IRF fabric, display detailed information about aggregation groups. Verify that GigabitEthernet 1/0/1 and GigabitEthernet 2/0/1 are in aggregation group 1 and are in Selected state.

```
[IRF] display link-aggregation verbose
```

Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing

Port Status: S -- Selected, U -- Unselected, I -- Individual

Flags: A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,

D -- Synchronization, E -- Collecting, F -- Distributing,

G -- Defaulted, H -- Expired

Aggregate Interface: Bridge-Aggregation1

Aggregation Mode: Dynamic

Loadsharing Type: Shar

System ID: 0x8000, 50da-0051-2608

Local:

Port	Status	Priority	Oper-Key	Flag
GE1/0/1	S	32768	1	{ACDEF}
GE2/0/1	S	32768	1	{ACDEF}

Remote:

Actor	Partner	Priority	Oper-Key	SystemID	Flag
GE1/0/1	1	32768	1	0x8000, 3897-d633-f3c6	{ACDEF}
GE2/0/1	2	32768	1	0x8000, 3897-d633-f3c6	{ACDEF}

On the switch, display detailed information about aggregation groups. Verify that GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 are in aggregation group 1 and are in Selected state.

[Switch] display link-aggregation verbose

Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing

Port Status: S -- Selected, U -- Unselected,

I -- Individual, * -- Management port

Flags: A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,

D -- Synchronization, E -- Collecting, F -- Distributing,

G -- Defaulted, H -- Expired

Aggregate Interface: Bridge-Aggregation1

Aggregation Mode: Dynamic

Loadsharing Type: Shar

Management VLAN : None

System ID: 0x8000, 3897-d633-f3c6

Local:

Port	Status	Priority	Oper-Key	Flag
GE1/0/1	S	32768	1	{ACDEF}
GE1/0/2	S	32768	1	{ACDEF}

Remote:

Actor	Partner	Priority	Oper-Key	SystemID	Flag
GE1/0/1	2	32768	1	0x8000, 50da-0051-2608	{ACDEF}
GE1/0/2	31	32768	1	0x8000, 50da-0051-2608	{ACDEF}

Configuration files

- IRF fabric:

sysname IRF
#

```

irf mac-address persistent timer
irf auto-update enable
irf auto-merge enable
irf member 1 priority 2
irf member 2 priority 1
irf member 1 description AC 1
irf member 2 description AC 2
#
link-aggregation lacp traffic-redirect-notification enable
#
irf-port 1
port group interface Ten-GigabitEthernet1/0/25
#
irf-port 2
port group interface Ten-GigabitEthernet2/0/25
#
interface Bridge-Aggregation1
link-aggregation mode dynamic
mad enable
#
interface GigabitEthernet1/0/1
port link-aggregation group 1
#
interface GigabitEthernet2/0/1
port link-aggregation group 1
#

```

- **Switch:**

```

#
link-aggregation lacp traffic-redirect-notification enable
#
vlan 400
#
interface Bridge-Aggregation1
link-aggregation mode dynamic
#
interface GigabitEthernet1/0/1
port link-aggregation group 1
#
interface GigabitEthernet1/0/2
port link-aggregation group 1
#
interface Ten-GigabitEthernet1/0/25
port access vlan 400
undo stp enable
#
interface Ten-GigabitEthernet1/0/26
port access vlan 400
undo stp enable

```


#

Related documentation

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

INTELBRAS Access Controller Modules IRF Setup with Members in One Chassis 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: Setting up an IRF fabric with access controller modules in the same chassis.....	1
Network configuration.....	1
Restrictions and guidelines.....	2
IRF setup requirements.....	2
Feature configuration and compatibility on an IRF fabric.....	3
IRF fabric tuning and maintenance	4
Procedures	4
Configuring the switch	4
Configuring AC 1	5
Configuring AC 2	6
Configuring the IRF fabric.....	7
Verifying the configuration	8
Configuration files.....	10
Related documentation	12

Introduction

The following information provides an example for setting up an IRF fabric with two access controller modules in the same chassis.

The Intelligent Resilient Framework (IRF) technology is proprietary to INTELBRAS. This technology is a true stacking technology that creates a large virtual stack called IRF fabric from multiple devices to provide data center class availability and scalability. IRF offers processing power, interaction, unified management, and uninterrupted maintenance of multiple devices.

Prerequisites

NOTE:

Support for this configuration example varies by device model and version.

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 IRF and Ethernet link aggregation.

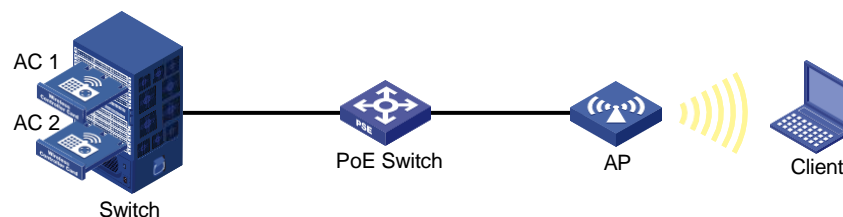
Example: Setting up an IRF fabric with access controller modules in the same chassis

Network configuration

As shown in [Figure 1](#), AC 1 and AC 2 are access controller modules. The ACs are inserted into slot 2 and slot 5 of the switch, respectively.

Use the access controller modules to set up an IRF fabric. Configure LACP MAD on the multi-member link aggregation to the switch.

Figure 1 Network diagram



Restrictions and guidelines

To ensure successful setup and maintenance of the IRF fabric, read the following information carefully.

IRF setup requirements

IRF fabric size

At the time of this writing, an IRF fabric can contain a maximum of two ACs.

Software version requirements

Make sure all IRF member devices run the same software image version.

To add a device of a different software version to the IRF fabric, make sure the software auto-update feature is enabled on the device for software synchronization.

By default, the software auto-update feature for IRF is enabled. To verify that the feature is enabled, execute the **display irf** command and then examine the **Auto upgrade** field. If the feature is disabled, use the **irf auto-update enable** command to enable it.

IRF connection requirements

To build a two-member IRF fabric, you can connect two devices directly or indirectly through a switch.

IRF port binding requirements

You can create only one IRF port on an AC. The IRF port is named **irf-port *n***, where *n* is the IRF member ID of the AC.

When you bind physical interfaces to an IRF port, follow these restrictions and guidelines:

- The physical interfaces bound to an IRF port must be the same in speed.
- An IRF port can contain hybrid (control & data) channels, separate control and data channels, but not both. If you have bound a physical interface to the IRF port as a hybrid channel, you cannot bind additional physical interfaces to the IRF port as separate control or data channels. Conversely, if you have bound a physical interface to the IRF port as a separate data or control channel, you cannot bound additional physical interfaces as hybrid channels to the IRF port.

To use WLAN hardware fast forwarding on an IRF fabric that contains access controller modules, follow these restrictions and guidelines:

Modules	Configuration restrictions and guidelines
LSQM1WCMX20 LSUM1WCMX20RT EWPXM2WCMD0F	You must configure each module as follows: <ul style="list-style-type: none">• Use one Ten-GigabitEthernet interface as a non-IRF network interface.• Use the other Ten-GigabitEthernet interface as an IRF network interface.

Modules	Configuration restrictions and guidelines
LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX40 LSUM1WCMX40RT EWPXM1MAC0	<p>On these modules, the network interfaces are grouped, as follows:</p> <ul style="list-style-type: none"> Ten-GigabitEthernet n/0/1 and Ten-GigabitEthernet n/0/3 belong to one group. Ten-GigabitEthernet n/0/2 and Ten-GigabitEthernet n/0/4 belong to another group. <p>NOTE:</p> <p>The integer n represents the IRF member ID.</p> <p>You must configure each module as follows:</p> <ul style="list-style-type: none"> Use the interfaces in one group as non-IRF network interfaces. Configure the interfaces in the other group as IRF network interfaces.

After you bind physical interfaces to the IRF port on an AC, you must save the configuration, and then restart the AC or activate the IRF port settings for the bindings to take effect.

Other configuration requirements

Make sure the following requirements are met:

Item	Requirements
Spanning tree feature	To avoid service interruption, do not enable the spanning tree feature on the access controller modules.
Ethernet link aggregation	<ul style="list-style-type: none"> On the switch—Aggregate the physical links that connect to the IRF network interfaces of the IRF fabric. On the IRF members—If Bridge-Aggregation 1 exists by default, delete the aggregate interface to remove all the member ports from the aggregate interface.
IRF member ID	Assign a unique member ID to each member device. The member ID assigned to a device takes effect after the device restarts.
Topo-domain ID	Assign the same topo-domain ID and MAD domain ID to all member devices.

Configure Layer 2 dynamic aggregate interfaces to transmit service packets only after you have established the IRF fabric.

IRF merge guidelines

If the IRF fabrics to be merged use the same bridge MAC address, you must change the bridge MAC address of one fabric.

To merge split IRF fabrics, make sure the IRF configuration on their member devices has not changed after the split.

Feature configuration and compatibility on an IRF fabric

To avoid service interference, isolate service packets from IRF packets at Layer 2.

If a multcard link aggregation is established between the IRF fabric and a switch, do not configure per-packet load sharing on the link aggregation at the switch end.

NAT is not supported on an IRF fabric.

IRF fabric tuning and maintenance

You cannot bring down an IRF link by shutting down the network interface on the IRF standby device side if that link is the only control channel in up state on the device. To bring down the IRF link, execute the **shutdown** command to shut down the network interface on the master device side for the link.

Before you can remove a network interface from an IRF port while multiple correctly operating IRF links are present, you must execute the **shutdown** command to shut that network interface down.

To change the IRF member ID of a device, execute the **irf member renumber** command on the device, and then restart the device for the change to take effect. To avoid MAD failures or service interruption, make sure the new member ID is unique among all IRF members.

All members in an IRF fabric use the same MAD domain ID. To change the MAD domain ID, execute the **irf domain** command on the master device. Make sure the new MAD domain ID is unique among all IRF fabrics present on the network for correct IRF split detection.

Procedures

Configuring the switch

1. Configure links for interfaces connected to the IRF network interfaces:

Create Layer 2 aggregate interface Bridge-Aggregation 1 for AC 1 IRF connection.

```
<Switch> system-view
[Switch] interface bridge-aggregation 1
[Switch-Bridge-Aggregation1] quit
```

Assign internal port Ten-GigabitEthernet 2/2/0/1 to aggregation group 1.

```
[Switch] interface ten-gigabitethernet 2/2/0/1
[Switch-Ten-GigabitEthernet2/2/0/1] port link-aggregation group 1
[Switch-Ten-GigabitEthernet2/2/0/1] quit
```

Assign internal port Ten-GigabitEthernet 2/2/0/3 to aggregation group 1.

```
[Switch] interface ten-gigabitethernet 2/2/0/3
[Switch-Ten-GigabitEthernet2/2/0/3] port link-aggregation group 1
[Switch-Ten-GigabitEthernet2/2/0/3] quit
```

Create Layer 2 aggregate interface Bridge-Aggregation 2 for AC 2 IRF connection.

```
[Switch] interface bridge-aggregation 2
[Switch-Bridge-Aggregation2] quit
```

Assign internal port Ten-GigabitEthernet 2/5/0/1 to aggregation group 2.

```
[Switch] interface ten-gigabitethernet 2/5/0/1
[Switch-Ten-GigabitEthernet2/5/0/1] port link-aggregation group 2
[Switch-Ten-GigabitEthernet2/5/0/1] quit
```

Assign internal port Ten-GigabitEthernet 2/5/0/3 to aggregation group 2.

```
[Switch] interface ten-gigabitethernet 2/5/0/3
[Switch-Ten-GigabitEthernet2/5/0/3] port link-aggregation group 2
[Switch-Ten-GigabitEthernet2/5/0/3] quit
```

Create VLAN 400 and assign the aggregate interfaces to the VLAN. The VLAN will transmit traffic for IRF links.

```
[Switch] vlan 400
[Switch-vlan400] port bridge-aggregation 1
```

```
[Switch-vlan400] port bridge-aggregation 2
[Switch-vlan400] quit
```

Disable the spanning tree feature on Bridge-Aggregation 1 and Bridge-Aggregation 2.

```
[Switch] interface bridge-aggregation 1
[Switch-Bridge-Aggregation1] undo stp enable
[Switch-Bridge-Aggregation1] quit
[Switch] interface bridge-aggregation 2
[Switch-Bridge-Aggregation2] undo stp enable
[Switch-Bridge-Aggregation2] quit
```

2. Configure links used for transmitting LACP MAD packets:

Create Layer 2 aggregate interface Bridge-Aggregation 3, and configure the aggregation group of the aggregate interface to operate in dynamic mode.

```
[Switch] interface bridge-aggregation 3
[Switch-Bridge-Aggregation3] link-aggregation mode dynamic
[Switch-Bridge-Aggregation3] quit
```

Assign internal port Ten-GigabitEthernet 2/2/0/2 to aggregation group 3.

```
[Switch] interface ten-gigabitethernet 2/2/0/2
[Switch-Ten-GigabitEthernet2/2/0/2] port link-aggregation group 3
[Switch-Ten-GigabitEthernet2/2/0/2] quit
```

Assign internal port Ten-GigabitEthernet 2/2/0/4 to aggregation group 3.

```
[Switch] interface ten-gigabitethernet 2/2/0/4
[Switch-Ten-GigabitEthernet2/2/0/4] port link-aggregation group 3
[Switch-Ten-GigabitEthernet2/2/0/4] quit
```

Assign internal port Ten-GigabitEthernet 2/5/0/2 to aggregation group 3.

```
[Switch] interface ten-gigabitethernet 2/5/0/2
[Switch-Ten-GigabitEthernet2/5/0/2] port link-aggregation group 3
[Switch-Ten-GigabitEthernet2/5/0/2] quit
```

Assign internal port Ten-GigabitEthernet 2/5/0/4 to aggregation group 3.

```
[Switch] interface ten-gigabitethernet 2/5/0/4
[Switch-Ten-GigabitEthernet2/5/0/4] port link-aggregation group 3
[Switch-Ten-GigabitEthernet2/5/0/4] quit
```

3. Enable link-aggregation traffic redirection.

```
[Switch] link-aggregation lacp traffic-redirect-notification enable
```

Configuring AC 1

Assign internal ports Ten-GigabitEthernet 1/0/1 and Ten-GigabitEthernet 1/0/3 to the IRF port.

```
<AC1> system-view
```

```
[AC1] irf-port 1
```

```
[AC1-irf-port1] port group interface ten-gigabitethernet 1/0/1
```

You must perform the following tasks for a successful IRF setup:

Save the configuration after completing IRF configuration.

Execute the `"irf-port-configuration active"` command to activate the IRF ports.

```
[AC1-irf-port1] port group interface ten-gigabitethernet 1/0/3
```

You must perform the following tasks for a successful IRF setup:

Save the configuration after completing IRF configuration.

Execute the `"irf-port-configuration active"` command to activate the IRF ports.

```
[AC1-irf-port1] quit
```


Specify the member priority as 2. AC 1 will be the master device.

```
[AC1] irf member 1 priority 2
```

Save the configuration.

```
[AC1] save
```

The current configuration will be written to the device. Are you sure? [Y/N]:y

Please input the file name(*.cfg)[cfa0:/startup.cfg]

(To leave the existing filename unchanged, press the enter key):irf.cfg

Validating file. Please wait...

Saved the current configuration to mainboard device successfully.

Activate the IRF port configuration.

```
[AC1] irf-port-configuration active
```

Configuring AC 2

Change the IRF member ID to 2.

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

```
[AC2] irf member 1 renumber 2
```

Renumbering the member ID may result in configuration change or loss. Continue? [

Y/N]:y

```
[AC2] quit
```

Reboot AC 2 for the new member ID to take effect.

```
<AC2> reboot
```

Start to check configuration with next startup configuration file, please wait..

..... DONE!

Current configuration may be lost after the reboot, save current configuration?

[Y/N]:y

Please input the file name(*.cfg)[cfa0:/startup.cfg]

(To leave the existing filename unchanged, press the enter key):irf.cfg

cfa0:/startup.cfg exists, overwrite? [Y/N]:y

Validating file. Please wait...

Saved the current configuration to mainboard device successfully.

This command will reboot the device. Continue? [Y/N]:y

Now rebooting, please wait...

Assign internal ports Ten-GigabitEthernet 2/0/1 and Ten-GigabitEthernet 2/0/3 to the IRF port.

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

```
[AC2] irf-port 2
```

```
[AC2-irf-port2] port group interface ten-gigabitethernet 2/0/1
```

You must perform the following tasks for a successful IRF setup:

Save the configuration after completing IRF configuration.

Execute the \"irf-port-configuration active\" command to activate the IRF ports.

```
[AC2-irf-port2] port group interface ten-gigabitethernet 2/0/3
```

You must perform the following tasks for a successful IRF setup:

Save the configuration after completing IRF configuration.

Execute the \"irf-port-configuration active\" command to activate the IRF ports.

```
[AC2-irf-port2] quit
```

Save the configuration.

```
[AC2] save
```

```
The current configuration will be written to the device. Are you sure? [Y/N]:y
Please input the file name(*.cfg)[cfa0:/ irf.cfg]
(To leave the existing filename unchanged, press the enter key):
Validating file. Please wait...
Saved the current configuration to mainboard device successfully.
```

Activate the IRF port configuration.

```
[AC2] irf-port-configuration active
```

AC 1 and AC 2 perform master election. AC 2 fails the master election and reboots to form an IRF fabric with AC 1.

Configuring the IRF fabric

❗ IMPORTANT:

IRF split causes network conflicts, because the split IRF fabrics operate with the same IP address. To avoid this issue, configure MAD settings.

Change the name of the IRF fabric to IRF.

```
<AC1> system-view
[AC1] system-name IRF
```

Configure descriptions for AC 1 and AC 2, respectively.

```
[IRF] irf member 1 description AC 1
[IRF] irf member 2 description AC 2
```

Delete the system-defined aggregate interface named Bridge-Aggregation 1. The member ports will automatically leave the aggregation group of Bridge-Aggregation 1.

```
[IRF] undo interface bridge-aggregation 1
```

Create Layer 2 aggregate interface Bridge-Aggregation 3, and configure the aggregation group of the aggregate interface to operate in dynamic mode.

```
[IRF] interface bridge-aggregation 3
[IRF-Bridge-Aggregation3] link-aggregation mode dynamic
```

Enable LACP MAD on Bridge-Aggregation 3.

```
[IRF-Bridge-Aggregation3] mad enable
[IRF-Bridge-Aggregation3] quit
```

Enable link-aggregation traffic redirection.

```
[IRF] link-aggregation lacp traffic-redirect-notification enable
```

Assign internal port Ten-GigabitEthernet 1/0/2 to aggregation group 3.

```
[IRF] interface ten-gigabitethernet 1/0/2
[IRF-Ten-GigabitEthernet1/0/2] port link-aggregation group 3
[IRF-Ten-GigabitEthernet1/0/2] quit
```

Assign internal port Ten-GigabitEthernet 1/0/4 to aggregation group 3.

```
[IRF] interface ten-gigabitethernet 1/0/4
[IRF-Ten-GigabitEthernet1/0/4] port link-aggregation group 3
[IRF-Ten-GigabitEthernet1/0/4] quit
```

Assign internal port Ten-GigabitEthernet 2/0/2 to aggregation group 3.

```
[IRF] interface ten-gigabitethernet 2/0/2
[IRF-Ten-GigabitEthernet2/0/2] port link-aggregation group 3
[IRF-Ten-GigabitEthernet2/0/2] quit
```

Assign internal port Ten-GigabitEthernet 2/0/4 to aggregation group 3.

```
[IRF] interface ten-gigabitethernet 2/0/4
[IRF-Ten-GigabitEthernet2/0/4] port link-aggregation group 3
[IRF-Ten-GigabitEthernet2/0/4] quit
```

Verifying the configuration

Display IRF information. Verify that AC 1 is the master device.

```
[IRF] display irf
```

Member ID	Role	Priority	CPU MAC	Description
*+1	Master	2	50da-005b-8b98	AC 1
2	Standby	1	70f9-6d17-2e37	AC 2

The asterisk (*) indicates the master.

The plus sign (+) indicates the device through which you are logged in.

The right angle bracket (>) indicates the device's stack capability is disabled.

Bridge MAC of the IRF: 50da-005b-8b98

Auto upgrade : Enabled

MAC persistence : 6 min

Topo-domain ID : 0

Auto merge : Enabled

Display IRF link information. Verify that the IRF network interfaces on both member devices are up.

```
[IRF] display irf link
```

Member ID	Member Interfaces	Status
1	XGE1/0/1(ctrl&data)	Up
	XGE1/0/3(ctrl&data)	Up
2	XGE2/0/1(ctrl&data)	Up
	XGE2/0/3(ctrl&data)	Up

On the IRF fabric, display detailed information about aggregation groups. Verify that Ten-GigabitEthernet 1/0/2, Ten-GigabitEthernet 1/0/4, Ten-GigabitEthernet 2/0/2, and Ten-GigabitEthernet 2/0/4 are in aggregation group 3 and in Selected state.

```
[IRF] display link-aggregation verbose
```

Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Port Status: S -- Selected, U -- Unselected, I -- Individual
Flags: A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
D -- Synchronization, E -- Collecting, F -- Distributing,
G -- Defaulted, H -- Expired

Aggregate Interface: Bridge-Aggregation3

Aggregation Mode: Dynamic

Loadsharing Type: NonS

System ID: 0x8000, 50da-005b-8b98

Local:

Port	Status	Priority	Oper-Key	Flag
XGE1/0/2	S	32768	1	{ACDEF}
XGE1/0/4	S	32768	1	{ACDEF}

XGE2/0/2	S	32768	1	{ACDEF}
XGE2/0/4	S	32768	1	{ACDEF}

Remote:

Actor	Partner	Priority	Oper-Key	SystemID	Flag
XGE1/0/2	1943	32768	3	0x8000, 741f-4a56-9890	{ACDEF}
XGE1/0/4	1944	32768	3	0x8000, 741f-4a56-9890	{ACDEF}
XGE2/0/2	2234	32768	3	0x8000, 741f-4a56-9890	{ACDEF}
XGE2/0/4	2235	32768	3	0x8000, 741f-4a56-9890	{ACDEF}

On the switch, display detailed information about aggregation groups. Verify the link aggregation settings and verify that all member ports in the aggregation groups are in Selected state.

```
[Switch]display link-aggregation verbose
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Port Status: S -- Selected, U -- Unselected, I -- Individual
Flags: A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
       D -- Synchronization, E -- Collecting, F -- Distributing,
       G -- Defaulted, H -- Expired
```

Aggregate Interface: Bridge-Aggregation1

Aggregation Mode: Static

Loadsharing Type: Shar

Port	Status	Priority	Oper-Key
XGE2/2/0/1	S	32768	1
XGE2/2/0/3	S	32768	1

Aggregate Interface: Bridge-Aggregation2

Aggregation Mode: Static

Loadsharing Type: Shar

Port	Status	Priority	Oper-Key
XGE2/5/0/1	S	32768	2
XGE2/5/0/3	S	32768	2

Aggregate Interface: Bridge-Aggregation3

Aggregation Mode: Dynamic

Loadsharing Type: Shar

System ID: 0x8000, 741f-4a56-9890

Local:

Port	Status	Priority	Oper-Key	Flag
XGE2/2/0/2	S	32768	3	{ACDEF}
XGE2/2/0/4	S	32768	3	{ACDEF}
XGE2/5/0/2	S	32768	3	{ACDEF}
XGE2/5/0/4	S	32768	3	{ACDEF}

Remote:

Actor	Partner	Priority	Oper-Key	SystemID	Flag
-------	---------	----------	----------	----------	------

XGE2/2/0/2	5	32768	1	0x8000, 50da-005b-8b98 {ACDEF}
XGE2/2/0/4	6	32768	1	0x8000, 50da-005b-8b98 {ACDEF}
XGE2/5/0/2	11	32768	1	0x8000, 50da-005b-8b98 {ACDEF}
XGE2/5/0/4	12	32768	1	0x8000, 50da-005b-8b98 {ACDEF}

Configuration files

- IRF fabric:

```
#
sysname IRF
#
irf mac-address persistent timer
irf auto-update enable
irf auto-merge enable
irf member 1 priority 2
irf member 2 priority 1
irf member 1 description AC 1
irf member 2 description AC 2
#
link-aggregation lacp traffic-redirect-notification enable
#
irf-port 1
port group interface Ten-GigabitEthernet1/0/1
port group interface Ten-GigabitEthernet1/0/3
#
irf-port 2
port group interface Ten-GigabitEthernet2/0/1
port group interface Ten-GigabitEthernet2/0/3
#
interface Bridge-Aggregation3
link-aggregation mode dynamic
mad enable
#
interface Ten-GigabitEthernet1/0/2
port link-aggregation group 3
#
interface Ten-GigabitEthernet1/0/4
port link-aggregation group 3
#
interface Ten-GigabitEthernet2/0/2
port link-aggregation group 3
#
interface Ten-GigabitEthernet2/0/4
port link-aggregation group 3
#
```

- Switch:

```
#
link-aggregation lacp traffic-redirect-notification enable
```

```

#
vlan 400
#
interface Bridge-Aggregation1
    port access vlan 400
    undo stp enable
#
interface Bridge-Aggregation2
    port access vlan 400
    undo stp enable
#
interface Bridge-Aggregation3
    link-aggregation mode dynamic
#
interface Ten-GigabitEthernet2/2/0/1
    port link-mode bridge
    port access vlan 400
    port link-aggregation group 1
#
interface Ten-GigabitEthernet2/2/0/2
    port link-mode bridge
    port link-aggregation group 3
#
interface Ten-GigabitEthernet2/2/0/3
    port link-mode bridge
    port access vlan 400
    port link-aggregation group 1
#
interface Ten-GigabitEthernet2/2/0/4
    port link-mode bridge
    port link-aggregation group 3
#
interface Ten-GigabitEthernet2/5/0/1
    port link-mode bridge
    port access vlan 400
    port link-aggregation group 2
#
interface Ten-GigabitEthernet2/5/0/2
    port link-mode bridge
    port link-aggregation group 3
#
interface Ten-GigabitEthernet2/5/0/3
    port link-mode bridge
    port access vlan 400
    port link-aggregation group 2
#
interface Ten-GigabitEthernet2/5/0/4
    port link-mode bridge

```

```
port link-aggregation group 3
#
```

Related documentation

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

INTELBRAS Access Controller Modules

IRF Setup with Members in Different Chassis

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: Setting up an IRF fabric with access controller modules in different chassis.....	1
Network configuration.....	1
Restrictions and guidelines.....	2
IRF setup requirements.....	2
Feature configuration and compatibility on an IRF fabric.....	4
IRF fabric tuning and maintenance	4
Procedures	4
Configuring IRF 1	4
Configuring AC 1	5
Configuring AC 2.....	6
Configuring IRF 2	7
Verifying the configuration	8
Configuration files.....	10
Related documentation	12

Introduction

The following information provides an example for setting up an IRF fabric with access controller modules in different chassis.

The Intelligent Resilient Framework (IRF) technology is proprietary to INTELBRAS. This technology is a true stacking technology that creates a large virtual stack called IRF fabric from multiple devices to provide data center class availability and scalability. IRF offers processing power, interaction, unified management, and uninterrupted maintenance of multiple devices.

Prerequisites

NOTE:

Support for this configuration example varies by device model and version.

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 IRF and Ethernet link aggregation.

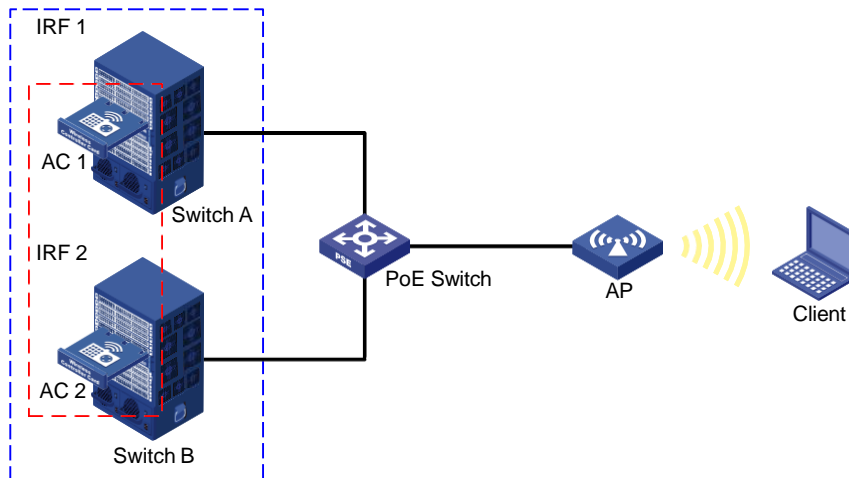
Example: Setting up an IRF fabric with access controller modules in different chassis

Network configuration

As shown in [Figure 1](#), AC 1 is inserted into slot 1 on Switch A and AC 2 is inserted into slot 4 on Switch B. Switch A and Switch B are in an IRF fabric named IRF 1.

Use AC 1 and AC 2 to set up an IRF fabric named IRF 2. Configure LACP MAD on the multi-member link aggregation to IRF 1.

Figure 1 Network diagram



Restrictions and guidelines

To ensure successful setup and maintenance of the IRF fabric, read the following information carefully.

IRF setup requirements

IRF fabric size

At the time of this writing, an IRF fabric can contain a maximum of two ACs.

Software version requirements

Make sure all IRF member devices run the same software image version.

To add a device of a different software version to the IRF fabric, make sure the software auto-update feature is enabled on the device for software synchronization.

By default, the software auto-update feature for IRF is enabled. To verify that the feature is enabled, execute the `display irf` command and then examine the **Auto upgrade** field. If the feature is disabled, use the `irf auto-update enable` command to enable it.

IRF connection requirements

To build a two-member IRF fabric, you can connect two devices directly or indirectly through a switch.

IRF port binding requirements

You can create only one IRF port on an AC. The IRF port is named **irf-port *n***, where *n* is the IRF member ID of the AC.

When you bind physical interfaces to an IRF port, follow these restrictions and guidelines:

- The physical interfaces bound to an IRF port must be the same in speed.
- An IRF port can contain hybrid (control & data) channels, separate control and data channels, but not both. If you have bound a physical interface to the IRF port as a hybrid channel, you cannot bind additional physical interfaces to the IRF port as separate control or data channels. Conversely, if you have bound a physical interface to the IRF port as a separate data or control channel, you cannot bound additional physical interfaces as hybrid channels to the IRF port.

To use WLAN hardware fast forwarding on an IRF fabric that contains access controller modules, follow these restrictions and guidelines:

Modules	Configuration restrictions and guidelines
LSQM1WCMX20 LSUM1WCMX20RT EWPXM2WCMD0F	<p>You must configure each module as follows:</p> <ul style="list-style-type: none"> Use one Ten-GigabitEthernet interface as a non-IRF network interface. Use the other Ten-GigabitEthernet interface as an IRF network interface.
LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX40 LSUM1WCMX40RT EWPXM1MAC0	<p>On these modules, the network interfaces are grouped, as follows:</p> <ul style="list-style-type: none"> Ten-GigabitEthernet n/0/1 and Ten-GigabitEthernet n/0/3 belong to one group. Ten-GigabitEthernet n/0/2 and Ten-GigabitEthernet n/0/4 belong to another group. <p>NOTE:</p> <p>The integer n represents the IRF member ID.</p> <p>You must configure each module as follows:</p> <ul style="list-style-type: none"> Use the interfaces in one group as non-IRF network interfaces. Configure the interfaces in the other group as IRF network interfaces.

After you bind physical interfaces to the IRF port on an AC, you must save the configuration, and then restart the AC or activate the IRF port settings for the bindings to take effect.

Other configuration requirements

Make sure the following requirements are met:

Item	Requirements
Ethernet link aggregation	<ul style="list-style-type: none"> On the switch—You must configure the aggregate interfaces connected to IRF network interfaces to operate in static mode. If you configure the aggregate interfaces to operate in dynamic mode, the switch might get stuck and the IRF fabric might even split. On the switch—You must configure the aggregate interfaces used for LACP MAD to operate in dynamic mode. On the switch—Aggregate the physical links that connect to the IRF network interfaces of the IRF fabric. On the IRF members—If Bridge-Aggregation 1 exists by default, delete the aggregate interface to remove all the member ports from the aggregate interface.
Spanning tree feature	To avoid service interruption, disable the spanning tree feature on the IRF members or on the ports used for IRF services on the switch.
IRF member ID	<p>Assign a unique member ID to each member device.</p> <p>The member ID assigned to a device takes effect after the device restarts.</p>
Topo-domain ID	Assign the same topo-domain ID and MAD domain ID to all member devices.

Configure Layer 2 dynamic aggregate interfaces to transmit service packets only after you have established the IRF fabric.

IRF merge guidelines

If the IRF fabrics to be merged use the same bridge MAC address, you must change the bridge MAC address of one fabric.

To merge split IRF fabrics, make sure the IRF configuration on their member devices has not changed after the split.

Feature configuration and compatibility on an IRF fabric

To avoid service interference, isolate service packets from IRF packets at Layer 2.

If a multcard link aggregation is established between the IRF fabric and a switch, do not configure per-packet load sharing on the link aggregation at the switch end.

NAT is not supported on an IRF fabric.

IRF fabric tuning and maintenance

You cannot bring down an IRF link by shutting down the network interface on the IRF standby device side if that link is the only control channel in up state on the device. To bring down the IRF link, execute the **shutdown** command to shut down the network interface on the master device side for the link.

Before you can remove a network interface from an IRF port while multiple correctly operating IRF links are present, you must execute the **shutdown** command to shut that network interface down.

To change the IRF member ID of a device, execute the **irf member renumber** command on the device, and then restart the device for the change to take effect. To avoid MAD failures or service interruption, make sure the new member ID is unique among all IRF members.

All members in an IRF fabric use the same MAD domain ID. To change the MAD domain ID, execute the **irf domain** command on the master device. Make sure the new MAD domain ID is unique among all IRF fabrics present on the network for correct IRF split detection.

Procedures

Configuring IRF 1

In this example, IRF 1 has been set up.

1. Configure links used for transmitting LACP MAD packets between IRF 1 and IRF 2:

Create Layer 2 aggregate interface Bridge-Aggregation 1, and configure the aggregation group of the aggregate interface to operate in dynamic mode.

```
<IRF1> system-view
[IRF1] interface bridge-aggregation 1
[IRF1-Bridge-Aggregation1] link-aggregation mode dynamic
[IRF1-Bridge-Aggregation1] quit
```

Assign internal port Ten-GigabitEthernet 1/2/0/2 to aggregation group 1.

```
[IRF1] interface ten-gigabitethernet 1/2/0/2
[IRF1-Ten-GigabitEthernet1/2/0/2] port link-aggregation group 1
[IRF1-Ten-GigabitEthernet1/2/0/2] quit
```

Assign internal port Ten-GigabitEthernet 1/2/0/4 to aggregation group 1.

```
[IRF1] interface ten-gigabitethernet 1/2/0/4
[IRF1-Ten-GigabitEthernet1/2/0/4] port link-aggregation group 1
[IRF1-Ten-GigabitEthernet1/2/0/4] quit
```

Assign internal port Ten-GigabitEthernet 2/4/0/2 to aggregation group 1.

```
[IRF1] interface ten-gigabitethernet 2/4/0/2
[IRF1-Ten-GigabitEthernet2/4/0/2] port link-aggregation group 1
[IRF1-Ten-GigabitEthernet2/4/0/2] quit
```

Assign internal port Ten-GigabitEthernet 2/4/0/4 to aggregation group 1.

```
[IRF1] interface ten-gigabitethernet 2/4/0/4
[IRF1-Ten-GigabitEthernet2/4/0/4] port link-aggregation group 1
[IRF1-Ten-GigabitEthernet2/4/0/4] quit
```

2. Configure links used for network interfaces that connect to IRF 2:

Create Layer 2 aggregate interface Bridge-Aggregation 2 for aggregating links to the IRF network interfaces of AC 1.

```
[IRF1] interface bridge-aggregation 2
[IRF1-Bridge-Aggregation2] quit
```

Assign internal port Ten-GigabitEthernet 1/2/0/1 to aggregation group 2.

```
[IRF1] interface ten-gigabitethernet 1/2/0/1
[IRF1-Ten-GigabitEthernet1/2/0/1] port link-aggregation group 2
[IRF1-Ten-GigabitEthernet1/2/0/1] quit
```

Assign internal port Ten-GigabitEthernet 1/2/0/3 to aggregation group 2.

```
[IRF1] interface ten-gigabitethernet 1/2/0/3
[IRF1-Ten-GigabitEthernet1/2/0/3] port link-aggregation group 2
[IRF1-Ten-GigabitEthernet1/2/0/3] quit
```

Create Layer 2 aggregate interface Bridge-Aggregation 3 for aggregating links to the IRF network interfaces of AC 2.

```
[IRF1] interface bridge-aggregation 3
[IRF1-Bridge-Aggregation3] quit
```

Assign internal port Ten-GigabitEthernet 2/4/0/1 to aggregation group 3.

```
[IRF1] interface ten-gigabitethernet 2/4/0/1
[IRF1-Ten-GigabitEthernet2/4/0/1] port link-aggregation group 3
[IRF1-Ten-GigabitEthernet2/4/0/1] quit
```

Assign internal port Ten-GigabitEthernet 2/4/0/3 to aggregation group 3.

```
[IRF1] interface ten-gigabitethernet 2/4/0/3
[IRF1-Ten-GigabitEthernet2/4/0/3] port link-aggregation group 3
[IRF1-Ten-GigabitEthernet2/4/0/3] quit
```

Create VLAN 400 and assign Bridge-Aggregation 2 and Bridge-Aggregation 3 to the VLAN. The VLAN will transmit traffic for IRF links.

```
[IRF1] vlan 400
[IRF1-vlan400] port bridge-aggregation 2
[IRF1-vlan400] port bridge-aggregation 3
[IRF1-vlan400] quit
```

Disable the spanning tree feature on Bridge-Aggregation 2 and Bridge-Aggregation 3.

```
[IRF1] interface bridge-aggregation 2
[IRF1-Bridge-Aggregation2] undo stp enable
[IRF1-Bridge-Aggregation2] quit
[IRF1] interface bridge-aggregation 3
[IRF1-Bridge-Aggregation3] undo stp enable
[IRF1-Bridge-Aggregation3] quit
```

3. Enable link-aggregation traffic redirection.

```
[IRF1] link-aggregation lacp traffic-redirect-notification enable
```

Configuring AC 1

Assign internal ports Ten-GigabitEthernet 1/0/1 and Ten-GigabitEthernet 1/0/3 to the IRF port.

```
<AC1> system-view
```

```
[AC1] irf-port 1
[AC1-irf-port1] port group interface ten-gigabitethernet 1/0/1
You must perform the following tasks for a successful IRF setup:
Save the configuration after completing IRF configuration.
Execute the \"irf-port-configuration active\" command to activate the IRF ports.
[AC1-irf-port1] port group interface ten-gigabitethernet 1/0/3
You must perform the following tasks for a successful IRF setup:
Save the configuration after completing IRF configuration.
Execute the \"irf-port-configuration active\" command to activate the IRF ports.
[AC1-irf-port1] quit
```

Specify the member priority as 2. AC 1 will be the master device.

```
[AC1] irf member 1 priority 2
```

Save the configuration.

```
[AC1] save
The current configuration will be written to the device. Are you sure? [Y/N]:y
Please input the file name(*.cfg)[cfa0:/startup.cfg]
(To leave the existing filename unchanged, press the enter key):irf.cfg
Validating file. Please wait...
Saved the current configuration to mainboard device successfully.
```

Activate the IRF port configuration.

```
[AC1] irf-port-configuration active
```

Configuring AC 2

Change the IRF member ID to 2.

```
<AC2> system-view
[AC2] irf member 1 renumber 2
Renumbering the member ID may result in configuration change or loss. Continue?[Y/N]:y
[AC2] quit
```

Reboot AC 2 for the new member ID to take effect.

```
<AC2> reboot
Start to check configuration with next startup configuration file, please wait..
..... DONE!
Current configuration may be lost after the reboot, save current configuration?
[Y/N]:y
Please input the file name(*.cfg)[cfa0:/startup.cfg]
(To leave the existing filename unchanged, press the enter key):irf.cfg
cfa0:/startup.cfg exists, overwrite? [Y/N]:y
Validating file. Please wait...
Saved the current configuration to mainboard device successfully.
This command will reboot the device. Continue? [Y/N]:y
Now rebooting, please wait...
```

Assign internal ports Ten-GigabitEthernet 2/0/1 and Ten-GigabitEthernet 2/0/3 to the IRF port.

```
<AC2> system-view
[AC2] irf-port 2
[AC2-irf-port2] port group interface ten-gigabitethernet 2/0/1
```

You must perform the following tasks for a successful IRF setup:
Save the configuration after completing IRF configuration.
Execute the `"irf-port-configuration active"` command to activate the IRF ports.
[AC2-irf-port2] port group interface ten-gigabitethernet 2/0/3
You must perform the following tasks for a successful IRF setup:
Save the configuration after completing IRF configuration.
Execute the `"irf-port-configuration active"` command to activate the IRF ports.
[AC2-irf-port2] quit

Save the configuration.

```
[AC2] save
The current configuration will be written to the device. Are you sure? [Y/N]:y
Please input the file name(*.cfg)[cfa0:/ irf.cfg]
(To leave the existing filename unchanged, press the enter key):
Validating file. Please wait...
Saved the current configuration to mainboard device successfully.
```

Activate IRF port configuration.

```
[AC2] irf-port-configuration active
```

AC 1 and AC 2 perform master election. AC 2 fails the master election and reboots to form an IRF fabric with AC 1.

Configuring IRF 2

❗ IMPORTANT:

IRF split causes network conflicts, because the split IRF fabrics operate with the same IP address. To avoid this issue, configure MAD settings.

Change the name of the IRF fabric to **IRF2**.

```
<AC1> system-view
[AC1] system-name IRF2
```

Configure descriptions for AC 1 and AC 2, respectively.

```
[IRF2] irf member 1 description AC 1
[IRF2] irf member 2 description AC 2
```

Delete the system-defined aggregate interface named Bridge-Aggregation 1. The member ports will automatically leave the aggregation group of Bridge-Aggregation 1.

```
[IRF2] undo interface bridge-aggregation 1
```

Create Layer 2 aggregate interface Bridge-Aggregation 1, and configure the aggregation group of the aggregate interface to operate in dynamic mode.

```
[IRF2] interface bridge-aggregation 1
[IRF2-Bridge-Aggregation1] link-aggregation mode dynamic
```

Enable LACP MAD on Bridge-Aggregation 1.

```
[IRF2-Bridge-Aggregation1] mad enable
[IRF2-Bridge-Aggregation1] quit
```

Enable link-aggregation traffic redirection.

```
[IRF2] link-aggregation lacp traffic-redirect-notification enable
```

Assign internal port Ten-GigabitEthernet 1/0/2 to aggregation group 1.

```
[IRF2] interface ten-gigabitethernet 1/0/2
[IRF2-Ten-GigabitEthernet1/0/2] port link-aggregation group 1
```



```
[IRF2-Ten-GigabitEthernet1/0/2] quit

# Assign internal port Ten-GigabitEthernet 1/0/4 to aggregation group 1.
[IRF2] interface ten-gigabitethernet 1/0/4
[IRF2-Ten-GigabitEthernet1/0/4] port link-aggregation group 1
[IRF2-Ten-GigabitEthernet1/0/4] quit

# Assign internal port Ten-GigabitEthernet 2/0/2 to aggregation group 1.
[IRF2] interface ten-gigabitethernet 2/0/2
[IRF2-Ten-GigabitEthernet2/0/2] port link-aggregation group 1
[IRF2-Ten-GigabitEthernet2/0/2] quit

# Assign internal port Ten-GigabitEthernet 2/0/4 to aggregation group 1.
[IRF2] interface ten-gigabitethernet 2/0/4
[IRF2-Ten-GigabitEthernet2/0/4] port link-aggregation group 1
[IRF2-Ten-GigabitEthernet2/0/4] quit
```

Verifying the configuration

Display IRF information on IRF 2. Verify that AC 1 is the master device.

```
[IRF2] display irf
```

Member ID	Role	Priority	CPU MAC	Description
*+1	Master	2	70f9-6d6d-5a10	AC 1
2	Standby	1	70f9-6d6d-5a80	AC 2

The asterisk (*) indicates the master.

The plus sign (+) indicates the device through which you are logged in.

The right angle bracket (>) indicates the device's stack capability is disabled.

Bridge MAC of the IRF: 70f9-6d6d-5a10

Auto upgrade : Enabled

MAC persistence : 6 min

Topo-domain ID : 0

Auto merge : Enabled

Display IRF link information. Verify that the IRF network interfaces on both member devices are up.

```
[IRF2] display irf link
```

Member ID	Member Interfaces	Status
1	XGE1/0/1(ctrl&data)	Up
	XGE1/0/3(ctrl&data)	Up
2	XGE2/0/1(ctrl&data)	Up
	XGE2/0/3(ctrl&data)	Up

On IRF 2, display detailed information about aggregation groups. Verify that Ten-GigabitEthernet 1/0/2, Ten-GigabitEthernet 1/0/4, Ten-GigabitEthernet 2/0/2, and Ten-GigabitEthernet 2/0/4 are in aggregation group 1 and in Selected state.

```
[IRF2] display link-aggregation verbose
```

Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing

Port Status: S -- Selected, U -- Unselected, I -- Individual

Flags: A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
D -- Synchronization, E -- Collecting, F -- Distributing,
G -- Defaulted, H -- Expired

Aggregate Interface: Bridge-Aggregation1

Aggregation Mode: Dynamic

Loadsharing Type: NonS

System ID: 0x8000, 50da-005b-8b98

Local:

Port	Status	Priority	Oper-Key	Flag
XGE1/0/2	S	32768	1	{ACDEF}
XGE1/0/4	S	32768	1	{ACDEF}
XGE2/0/2	S	32768	1	{ACDEF}
XGE2/0/4	S	32768	1	{ACDEF}

Remote:

Actor	Partner	Priority	Oper-Key	SystemID	Flag
XGE1/0/2	1943	32768	3	0x8000, 741f-4a56-9890	{ACDEF}
XGE1/0/4	1944	32768	3	0x8000, 741f-4a56-9890	{ACDEF}
XGE2/0/2	2234	32768	3	0x8000, 741f-4a56-9890	{ACDEF}
XGE2/0/4	2235	32768	3	0x8000, 741f-4a56-9890	{ACDEF}

On IRF 1, display detailed information about aggregation groups. Verify the link aggregation settings and verify that all member ports in the aggregation groups are in Selected state.

[IRF1] display link-aggregation verbose

Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing

Port Status: S -- Selected, U -- Unselected, I -- Individual

Flags: A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
D -- Synchronization, E -- Collecting, F -- Distributing,
G -- Defaulted, H -- Expired

Aggregate Interface: Bridge-Aggregation1

Aggregation Mode: Dynamic

Loadsharing Type: Shar

System ID: 0x8000, 0cda-41c5-a6a0

Local:

Port	Status	Priority	Oper-Key	Flag
XGE1/2/0/2	S	32768	1	{ACDEF}
XGE1/2/0/4	S	32768	1	{ACDEF}
XGE2/4/0/2	S	32768	1	{ACDEF}
XGE2/4/0/4	S	32768	1	{ACDEF}

Remote:

Actor	Partner	Priority	Oper-Key	SystemID	Flag
XGE1/2/0/2	5	32768	2	0x8000, 70f9-6d6d-5a80	{ACDEF}
XGE1/2/0/4	6	32768	2	0x8000, 70f9-6d6d-5a80	{ACDEF}
XGE2/4/0/2	11	32768	2	0x8000, 70f9-6d6d-5a80	{ACDEF}
XGE2/4/0/4	12	32768	2	0x8000, 70f9-6d6d-5a80	{ACDEF}

Aggregate Interface: Bridge-Aggregation2

Aggregation Mode: Static

Loadsharing Type: Shar

Port	Status	Priority	Oper-Key
XGE1/2/0/1	S	32768	3
XGE1/2/0/3	S	32768	3

Aggregate Interface: Bridge-Aggregation3

Aggregation Mode: Static

Loadsharing Type: Shar

Port	Status	Priority	Oper-Key
XGE2/4/0/1	S	32768	2
XGE2/4/0/3	S	32768	2

Configuration files

- IRF 2:

```
#
sysname IRF2
#
irf mac-address persistent timer
irf auto-update enable
irf auto-merge enable
irf member 1 priority 2
irf member 2 priority 1
irf member 1 description AC 1
irf member 2 description AC 2
#
link-aggregation lacp traffic-redirect-notification enable
#
irf-port 1
port group interface Ten-GigabitEthernet1/0/1
port group interface Ten-GigabitEthernet1/0/3
#
irf-port 2
port group interface Ten-GigabitEthernet2/0/1
port group interface Ten-GigabitEthernet2/0/3
#
interface Bridge-Aggregation1
link-aggregation mode dynamic
mad enable
#
interface Ten-GigabitEthernet1/0/2
port link-aggregation group 1
#
interface Ten-GigabitEthernet1/0/4
port link-aggregation group 1
```

```

#
interface Ten-GigabitEthernet2/0/2
  port link-aggregation group 1
#
interface Ten-GigabitEthernet2/0/4
  port link-aggregation group 1
#
• IRF 1:
#
  link-aggregation lacp traffic-redirect-notification enable
#
vlan 400
#
interface Bridge-Aggregation1
  link-aggregation mode dynamic
#
interface Bridge-Aggregation2
  port access vlan 400
  undo stp enable
#
interface Bridge-Aggregation3
  port access vlan 400
  undo stp enable
#
interface Ten-GigabitEthernet1/2/0/1
  port link-mode bridge
  port access vlan 400
  port link-aggregation group 2
#
interface Ten-GigabitEthernet1/2/0/2
  port link-mode bridge
  port link-aggregation group 1
#
interface Ten-GigabitEthernet1/2/0/3
  port link-mode bridge
  port access vlan 400
  port link-aggregation group 2
#
interface Ten-GigabitEthernet1/2/0/4
  port link-mode bridge
  port link-aggregation group 1
#
interface Ten-GigabitEthernet2/4/0/1
  port link-mode bridge
  port access vlan 400
  port link-aggregation group 3
#
interface Ten-GigabitEthernet2/4/0/2

```

```
port link-mode bridge
port link-aggregation group 1
#
interface Ten-GigabitEthernet2/4/0/3
port link-mode bridge
port access vlan 400
port link-aggregation group 3
#
interface Ten-GigabitEthernet2/4/0/4
port link-aggregation group 1
#
```

Related documentation

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

INTELBRAS Access Controllers

Dual-Link Backup and AP License Synchronization

Configuration Examples

Copyright © 2024 Intelbras S.A All rights reserved.

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

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

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

Contents

Introduction	1
Prerequisites	1
Example: Configuring dual-link backup and AP license synchronization	1
Network requirements	1
Restrictions and guidelines	2
Procedures	2
Configuring AC 1	2
Configuring AC 2	3
Configuring the switch	4
Verifying the configuration	5
Configuration files	6
Related documentation	8

Introduction

The following information provides a dual-link backup and AP license synchronization configuration example.

Prerequisites

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

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

This document assumes that you have basic knowledge of AP management, WLAN high availability, and AP license synchronization features.

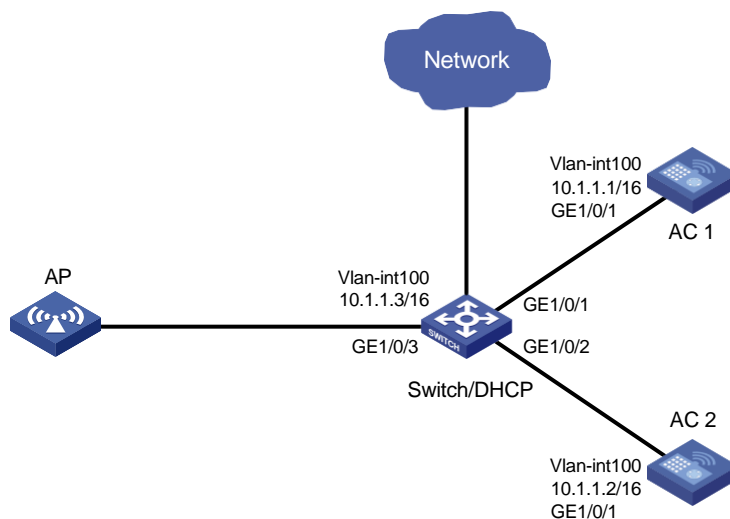
Example: Configuring dual-link backup and AP license synchronization

Network requirements

As shown in [Figure 1](#), configure AC 1 as the master AC and AC 2 as the backup AC. When AC 1 fails and AC 2 takes over, the AP can communicate through AC 2. Configure the master CAPWAP tunnel preemption feature on the two ACs so that the AP reconnects to AC 1 when AC 1 recovers.

Enable AP license synchronization on AC 1 and AC 2 for the two ACs to back up licenses for each other.

Figure 1 Network diagram



Restrictions and guidelines

When you configure dual-link backup and AP license synchronization, follow these restrictions and guidelines:

- Make sure the device model is compatible with the software version.
- Use the actual serial ID of an AP to uniquely identify that AP.
- If you use a manual AP to establish CAPWAP tunnels with the ACs, make sure the name of the AP is the same on the two ACs and either a serial ID or MAC address is configured for the AP on the two ACs.
- As a best practice, install a license on the master AC before enabling AP license synchronization.
- Before enabling AP license synchronization, you must specify IP addresses and roles for the AC and its member ACs in the AP license synchronization group.
- Configure both AC 1 and AC 2 as the master in the AP license synchronization group.
- When the master AC fails, the backup AC takes over and becomes the new master AC. The licenses synchronized to the new master AC will be valid for a 30-day grace period.
- Dual-link backup is applicable to both centralized forwarding and local forwarding. This example uses centralized forwarding.

Procedures

Configuring AC 1

Installing a license

Install a license on AC 1. (Details not shown.)

Configuring interfaces on AC 1

Configure VLAN 100 and VLAN-interface 100, and assign an IP address to the VLAN interface. AC 1 will use this IP address to establish CAPWAP tunnels with APs.

```
<AC1> system-view
[AC1] vlan 100
[AC1-vlan100] quit
[AC1] interface vlan-interface 100
[AC1-Vlan-interface100] ip address 10.1.1.1 16
[AC1-Vlan-interface100] quit
```

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

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

Configuring dual-link backup

Create AP group **group1**, and set the connection priority to 7.

```
[AC1] wlan ap-group group1
[AC1-wlan-ap-group-group1] priority 7
```

Specify a backup AC.

```
[AC1-wlan-ap-group-group1] backup-ac ip 10.1.1.2
```

```
# Enable master CAPWAP tunnel preemption.
[AC1-wlan-ap-group-group1] wlan tunnel-preempt enable

# Create an AP grouping rule by AP names.
[AC1-wlan-ap-group-group1] ap ap1
[AC1-wlan-ap-group-group1] quit
```

Configuring AP license synchronization

```
# Enable AP license synchronization on AC 1 and configure AC 1 as the master AC.
[AC1] wlan ap-license-group
[AC1-wlan-als-group] local ip 10.1.1.1
[AC1-wlan-als-group] member ip 10.1.1.2
[AC1-wlan-als-group] ap-license-synchronization enable
[AC1-wlan-als-group] quit
```

Configuring a manual AP

```
# Create an AP named ap1, and specify the AP model and serial ID.
[AC1] wlan ap ap1 model AP 3620
[AC1-wlan-ap-ap1] serial-id 219801A28N819CE0002T
```

Configuring AC 2

(Optional.) Installing a license

```
# Install a license on AC 2. (Details not shown.)
```

Configuring interfaces on AC 2

```
# Configure VLAN 100 and VLAN-interface 100, and assign an IP address to the VLAN interface. AC 2 will use this IP address to establish CAPWAP tunnels with APs.
```

```
<AC2> system-view
[AC2] vlan 100
[AC2-vlan100] quit
[AC2] interface Vlan-interface 100
[AC2-Vlan-interface100] ip address 10.1.1.2 16
[AC2-Vlan-interface100] quit
```

```
# Configure GigabitEthernet 1/0/1 that connects AC 2 to the switch as a trunk port, and assign it to all VLANs.
```

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

Configuring dual-link backup

```
# Create AP group group1, and specify a backup AC. Use the default setting for the connection priority.
```

```
[AC2] wlan ap-group group1
[AC2-wlan-ap-group-group1] backup-ac ip 10.1.1.1
```

```
# Create an AP grouping rule by AP names.
```

```
[AC2-wlan-ap-group-group1] ap ap1
[AC2-wlan-ap-group-group1] quit
```

Configuring AP license synchronization

Enable AP license synchronization on AC 1 and configure AC 1 as the master AC.

```
[AC2] wlan ap-license-group
[AC2-wlan-als-group] local ip 10.1.1.2
[AC2-wlan-als-group] member ip 10.1.1.1
[AC2-wlan-als-group] ap-license-synchronization enable
[AC2-wlan-als-group] quit
```

Configuring a manual AP

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

```
[AC2] wlan ap ap1 model AP 3620
[AC2-wlan-ap-ap1] serial-id 219801A28N819CE0002T
```

Configuring the switch

Configuring interfaces on the switch

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

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

Create VLAN interface 100, and assign it an IP address.

```
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ip address 10.1.1.3 16
[Switch-Vlan-interface100] quit
```

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

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

Configure GigabitEthernet 1/0/2 that connects the switch to AC 2 as a trunk port, and assign the port to all VLANs.

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

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

```
[Switch] interface gigabitethernet 1/0/3
[Switch-GigabitEthernet1/0/3] port link-type access
[Switch-GigabitEthernet1/0/3] port access vlan 100
```

Enable the PoE feature.

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

Configuring DHCP

Create DHCP address pool 100. Specify the 10.1.0.0/16 subnet for the pool.

```
[Switch] dhcp server ip-pool 100
[Switch-dhcp-pool-100] network 10.1.0.0 mask 255.255.0.0
[Switch-dhcp-pool-100] quit

# Enable DHCP.
[Switch] dhcp enable
```

Verifying the configuration

Display AP license synchronization group information on AC 1 to verify that the number of licenses in the group is the sum of licenses installed on AC 1 and AC 2.

```
<AC1> display wlan ap-license-group
Group total licenses: 256
Group used licenses: 1
AP license synchronization: Enabled
Local IP: 10.1.1.1
Local role: Master
Member information: 1
```

IP address	Total	Used	Member role	State	Online duration
10.1.1.2	0	0	Master	UP	00hr 1min 51sec

Verify that the AP state is R/M on AC 1.

```
<AC1> display wlan ap all
Total number of APs: 1
Total number of connected APs: 1
Total number of connected manual APs: 1
Total number of connected auto APs: 0
Total number of connected common APs: 1
Total number of connected WTUs: 0
Total number of inside APs: 0
Maximum supported APs: 384
Remaining APs: 383
Total AP licenses: 256
Local AP licenses: 256
Server AP licenses: 0
Remaining local AP licenses: 255
Sync AP licenses: 0
```

AP information

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

AP name	APID	State	Model	Serial ID
ap1	1	R/M	AP 3620	219801A28N819CE0002T

Verify that the AP state is R/M on AC 1 and R/B on AC 2, and the number of licenses is 256.

```
<AC2> display wlan ap all
Total number of APs: 1
Total number of connected APs: 1
Total number of connected manual APs: 1
Total number of connected auto APs: 0
```

```

Total number of connected common APs: 1
Total number of connected WTUs: 0
Total number of inside APs: 0
Maximum supported APs: 384
Remaining APs: 383
Total AP licenses: 256
Local AP licenses: 256
Server AP licenses: 0
Remaining local AP licenses: 256
Sync AP licenses: 256

```

AP information

```

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

```

AP name	APID	State	Model	Serial ID
ap1	1	R/B	AP 3620	219801A28N819CE0002T

Shut down VLAN-interface 1 on AC 2 and wait for no longer than 30 seconds, during which service interruption occurs. Verify that the AP is in R/M state.

```
<AC2> display wlan ap all
```

```

Total number of APs: 1
Total number of connected APs: 1
Total number of connected manual APs: 1
Total number of connected auto APs: 0
Total number of connected common APs: 1
Total number of connected WTUs: 0
Total number of inside APs: 0
Maximum supported APs: 384
Remaining APs: 383
Total AP licenses: 256
Local AP licenses: 256
Server AP licenses: 0
Remaining local AP licenses: 255
Sync AP licenses: 256

```

AP information

```

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

```

AP name	APID	State	Model	Serial ID
ap1	1	R/M	AP 3620	219801A28N819CE0002T

Bring up VLAN-interface 1 on AC 1. Verify that the AP state is R/M on AC 1 and R/B on AC 2. (Details not shown.)

Configuration files

- AC 1:
#

```

vlan 100
#
interface Vlan-interface100
 ip address 10.1.1.1 255.255.0.0
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan all
#
wlan ap-group group1
 priority 7
 wlan tunnel-preempt enable
 backup-ac ip 10.1.1.2
 ap ap1
#
wlan ap ap1 model AP 3620
 serial-id 219801A28N819CE0002T
#
wlan ap-license-group
 local ip 10.1.1.1
 member ip 10.1.1.2
 ap-license-synchronization enable
#

```

- **AC 2:**

```

#
vlan 100
#
interface Vlan-interface100
 ip address 10.1.1.2 255.255.0.0
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan all
#
wlan ap-group group1
 backup-ac ip 10.1.1.1
 ap ap1
#
wlan ap ap1 model AP 3620
 serial-id 219801A28N819CE0002T
#
wlan ap-license-group
 local ip 10.1.1.2
 member ip 10.1.1.1
 ap-license-synchronization enable
#

```

- **Switch**

```

#

```

```

    dhcp enable
#
vlan 100
#
dhcp server ip-pool 100
    network 10.1.0.0 mask 255.255.0.0
#
interface Vlan-interface100
    ip address 10.1.1.3 255.255.0.0
#
#
interface GigabitEthernet1/0/1
    port link-type trunk
    port trunk permit vlan all
#
interface GigabitEthernet1/0/2
    port link-type trunk
    port trunk permit vlan all
#
interface GigabitEthernet1/0/3
    port link-type access
    port access vlan 100
    poe enable
#

```

Related documentation

- *AP License Synchronization Command Reference* in *INTELBRAS Access Controllers Command References*
- *AP License Synchronization Configuration Guide* in *INTELBRAS Access Controllers Configuration Guides*
- *AP Management Command Reference* in *INTELBRAS Access Controllers Command References*
- *AP Management Configuration Guide* in *INTELBRAS Access Controllers Configuration Guides*
- *WLAN High Availability Command Reference* in *INTELBRAS Access Controllers Command References*
- *WLAN High Availability Configuration Guide* in *INTELBRAS Access Controllers Configuration Guides*

INTELBRAS Access Controllers

Remote 802.1X Authentication on an AC Hierarchy Network with Dual-link Central AC Backup 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
General restrictions and guidelines	1
Example: Configuring remote 802.1X authentication on an AC hierarchy network with dual-link central AC backup	1
Network configuration	1
Analysis	2
Restrictions and guidelines	2
Procedures	3
Editing the AP configuration file	3
Configuring Central AC 1	3
Configuring Central AC 2	5
Configuring the local AC	8
Configuring the Layer 3 switch	9
Configuring the Layer 2 switch	10
Configuring the DHCP server	11
Configuring the RADIUS server	12
Verifying the configuration	15
Configuration files	15
Related documentation	20

Introduction

The following information provides an example of configuring remote 802.1X authentication for clients on a network that deploys an AC hierarchy in which two central ACs are used for redundancy.

Prerequisites

NOTE:

Support for this configuration example varies by device model and version.

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, WLAN access authentication, WLAN access, and WLAN high availability features.

General restrictions and guidelines

Central ACs on an AC hierarchy network do not support IRF.

Example: Configuring remote 802.1X authentication on an AC hierarchy network with dual-link central AC backup

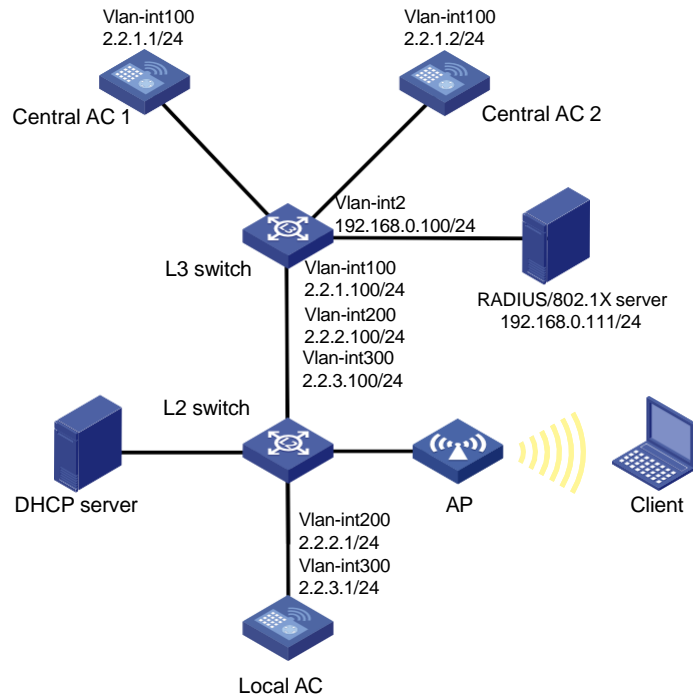
Network configuration

As shown in [Figure 1](#), in the AC hierarchy network, Central AC 1 acts as the master central AC and Central AC 2 acts as the backup central AC. The AP and the client obtain IP addresses from the DHCP server, and an INC server acts as the RADIUS server.

Configure the devices to meet the following requirements:

- The central ACs operate in active/standby mode and back up each other.
- The AP, the central ACs, and the local AC have network connectivity to one another.
 - The AP obtains the IP addresses of the master and backup central ACs through DHCP Option 43.
 - The AC rediscovery feature is configured on the central ACs for the AP to associate with the local AC.
 - The AP can associate with the master central AC when the local AC fails.
- The central ACs act as the authenticator and use the RADIUS server to perform authentication, authorization, and accounting for the client. 802.1X authentication is enabled for the service template through which the client accesses the network.

Figure 1 Network diagram



Analysis

For dual-link central AC backup to operate correctly, configure the local AC and manual AP settings on both central ACs. Make sure the priority settings on the local AC, the master central AC, and the backup central AC are correctly configured so that the local AC can re-associate with the master central AC when the master central AC recovers from a failure.

For the RADIUS server to dynamically change client authorization information or forcibly disconnect a wireless client, enable the RADIUS session-control feature on the central ACs.

For GigabitEthernet 1/0/1 to forward client data traffic in VLAN 300, edit a .txt AP configuration file and upload the file to the central ACs. In the file, the port is added to VLAN 300.

To avoid dynamic authorization failures, configure the RADIUS Dynamic Authorization Extensions Server (DAS) feature on the central ACs.

Restrictions and guidelines

When you configure remote 802.1X authentication on an AC hierarchy network with dual central ACs, follow these restrictions and guidelines:

- Make sure the master and backup central ACs run the same version of software and have the same settings.
- Use the actual serial ID of an AP to uniquely identify that AP.
- On the local AC, do not enable the auto AP feature. In addition, create a manual AP for the AP in local AC view on the central ACs for the central ACs to manage the AP.

Procedures

Editing the AP configuration file

Use a text editor to edit the APs' configuration file, and then upload the file to each central AC. In this example, the configuration file name is **apmap.txt**.

The following is the AP configuration for this example:

```
system-view
vlan 300
interface gigabitethernet1/0/1
port link-type trunk
port trunk permit vlan 300
```

Configuring Central AC 1

Configuring interfaces on Central AC 1

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

```
<Central-AC1> system-view
[Central-AC1] vlan 100
[Central-AC1-vlan100] quit
[Central-AC1] interface vlan-interface 100
[Central-AC1-Vlan-interface100] ip address 2.2.1.1 24
[Central-AC1-Vlan-interface100] quit
```

Specify GigabitEthernet 1/0/1 that connects Central AC 1 to the Layer 3 switch as a trunk port, and assign the port to VLAN 100.

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

Configuring a local AC for Central AC 1

Create local AC **3510** with model **WX3510H** and enter local AC view.

```
[Central-AC1] wlan local-ac name 3510 model WX3510H
```

Specify the serial ID of the local AC.

```
[Central-AC1-wlan-local-ac-3510] serial-id 210235A1JNB165000120
```

Set the priority to 7 for tunnel establishment to the local AC.

```
[Central-AC1-wlan-local-ac-3510] priority 7
```

Enable master CAPWAP tunnel preemption.

```
[Central-AC1-wlan-local-ac-3510] wlan tunnel-preempt enable
[Central-AC1-wlan-local-ac-3510] quit
```

Configuring RADIUS-based 802.1X authentication

1. Configure a RADIUS scheme:

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

```
[Central-AC1] radius scheme iNC
```

Specify the IP address of the primary RADIUS authentication server.

- ```
[Central-AC1-radius-iNC] primary authentication 192.168.0.111
```
- # Specify the IP address of the primary RADIUS accounting server.
- ```
[Central-AC1-radius-iNC] primary accounting 192.168.0.111
```
- # Set the shared key to **123456** in plaintext form for secure communication with the RADIUS authentication server.
- ```
[Central-AC1-radius-iNC] key authentication simple 123456
```
- # Set the shared key to **123456** in plaintext form for secure communication with the RADIUS accounting server.
- ```
[Central-AC1-radius-iNC] key accounting simple 123456
```
- # Exclude the domain name from usernames sent to the RADIUS servers.
- ```
[Central-AC1-radius-iNC] user-name-format without-domain
```
- # Specify IP address 2.2.1.1 as the source IP address for outgoing RADIUS packets.
- ```
[Central-AC1-radius-iNC] nas-ip 2.2.1.1
```
- ```
[Central-AC1-radius-iNC] quit
```
- # Enable RADIUS session-control.
- ```
[Central-AC1] radius session-control enable
```
2. Configure an authentication domain:

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

```
[Central-AC1] domain iNC
```

Configure the ISP domain to use RADIUS scheme **iNC** for 802.1X user authentication, authorization, and accounting.

```
[Central-AC1-isp-iNC] authentication lan-access radius-scheme iNC
```

```
[Central-AC1-isp-iNC] authorization lan-access radius-scheme iNC
```

```
[Central-AC1-isp-iNC] accounting lan-access radius-scheme iNC
```

```
[Central-AC1-isp-iNC] quit
```
 3. Configure EAP relay as the method for the AC to exchange packets with the RADIUS server.
- ```
[Central-AC1] dot1x authentication-method eap
```

## Configuring a service template

- # Create service template **dot1x** and set the SSID of the service template.
- ```
[Central-AC1] wlan service-template dot1x
```
- ```
[Central-AC1-wlan-st-dot1x] ssid 118341-fc-3510-bd-dot1x
```
- # Configure APs to forward client data traffic from all VLANs. If APs act as the client data traffic forwarder by default, skip this step.
- ```
[Central-AC1-wlan-st-dot1x] client forwarding-location ap
```
- # Specify central ACs as the authenticator.
- ```
[Central-AC1-wlan-st-dot1x] client-security authentication-location central-ac
```
- # Set the AKM mode to 802.1X, specify the CCMP cipher suite, enable the RSN IE in beacon and probe responses, set the access authentication mode to 802.1X authentication, and specify ISP domain **iNC** for authenticating the 802.1X client.
- ```
[Central-AC1-wlan-st-dot1x] akm mode dot1x
```
- ```
[Central-AC1-wlan-st-dot1x] cipher-suite ccmp
```
- ```
[Central-AC1-wlan-st-dot1x] security-ie rsn
```
- ```
[Central-AC1-wlan-st-dot1x] client-security authentication-mode dot1x
```
- ```
[Central-AC1-wlan-st-dot1x] dot1x domain iNC
```
- # Enable the service template.
- ```
[Central-AC1-wlan-st-dot1x] service-template enable
```
- ```
[Central-AC1-wlan-st-dot1x] quit
```

Creating a manual AP

NOTE:

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

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

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

Create AP group **group1**.

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

Enable the AC rediscovery feature.

```
[Central-AC1-wlan-ap-group-group1] control-address enable
```

Specify 2.2.2.1 as the IP address to be carried in the CAPWAP Control IP Address message element.

```
[Central-AC1-wlan-ap-group-group1] control-address ip 2.2.2.1
```

Specify Central AC 2 as a backup AC.

```
[Central-AC1-wlan-ap-group-group1] backup-ac ip 2.2.1.2
```

Enable vertical backup.

```
[Central-AC1-wlan-ap-group-group1] switch-back enable
```

Configure an AP grouping rule by AP name to add AP named **ap1** to the group.

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

Deploy configuration file **apmap.txt** to the AP group.

```
[Central-AC1-wlan-ap-group-group1] ap-model AP 3620
[Central-AC1-wlan-ap-group-group1-ap-model-AP 3620] map-configuration cfa0:/apmap.txt
```

Bind service template **dot1x** to radio 1 and specify VLAN 300 for the radio.

```
[Central-AC1-wlan-ap-group-group1-ap-model-AP 3620] radio 1
[Central-AC1-wlan-ap-group-group1-ap-model-AP 3620-radio-1] service-template dot1x vlan 300
```

Enable radio 1.

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

Configuring IP routing

Configure a default route with next hop 2.2.1.100 (an IP address on the Layer 3 switch).

```
[Central-AC1] ip route-static 0.0.0.0 0 24 2.2.1.100
```

Configuring Central AC 2

Configuring interfaces on Central AC 2

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

```
<Central-AC2> system-view
[Central-AC2] vlan 100
```

```
[Central-AC2-vlan100] quit
[Central-AC2] interface vlan-interface 100
[Central-AC2-Vlan-interface100] ip address 2.2.1.2 24
[Central-AC2-Vlan-interface100] quit
```

Specify GigabitEthernet1/0/1 that connects Central AC 2 to the Layer 3 switch as a trunk port, and assign the port to VLAN 100.

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

Configuring a local AC for Central AC 2

Create local AC 3510 with model WX3510H.

```
[Central-AC2] wlan local-ac name 3510 model WX3510H
```

Specify the serial ID of the local AC.

```
[Central-AC2-wlan-local-ac-3510] serial-id 210235A1JNB165000120
```

Set the priority to 6 for tunnel establishment to the local AC.

```
[Central-AC2-wlan-local-ac-3510] priority 6
```

Enable master CAPWAP tunnel preemption.

```
[Central-AC2-wlan-local-ac-3510] wlan tunnel-preempt enable
[Central-AC2-wlan-local-ac-3510] quit
```

Configuring RADIUS-based 802.1X authentication

1. Configure a RADIUS scheme:

Create RADIUS scheme iNC and enter its view.

```
[Central-AC2] radius scheme iNC
```

Specify the primary RADIUS authentication server.

```
[Central-AC2-radius-iNC] primary authentication 192.168.0.111
```

Specify the primary RADIUS accounting server.

```
[Central-AC2-radius-iNC] primary accounting 192.168.0.111
```

Set the shared key to 123456 in plaintext form for secure communication with the RADIUS authentication server.

```
[Central-AC2-radius-iNC] key authentication simple 123456
```

Set the shared key to 123456 in plaintext form for secure communication with the RADIUS accounting server.

```
[Central-AC2-radius-iNC] key accounting simple 123456
```

Exclude the domain name from usernames sent to the RADIUS servers.

```
[Central-AC2-radius-iNC] user-name-format without-domain
```

Specify IP address 2.2.1.2 as the source IP address for outgoing RADIUS packets.

```
[Central-AC2-radius-iNC] nas-ip 2.2.1.2
```

```
[Central-AC2-radius-iNC] quit
```

Enable RADIUS session-control.

```
[Central-AC2] radius session-control enable
```

Enable RADIUS DAS and enter its view.

```
[Central-AC2] radius dynamic-author server
```

Specify the RADIUS server at 192.168.0.111 as a DAC and set the shared key to 12345 in plain text for authenticating DAE packets from the RADIUS server.

```
[Central-AC2-radius-da-server] client ip 192.168.0.111 key simple 12345
```

- ```
[Central-AC2-radius-da-server] quit
```
2. Configure an authentication domain:  
 # Create ISP domain **iNC** and enter its view.  

```
[Central-AC2] domain iNC
```

 # Configure the ISP domain to use RADIUS scheme **iNC** for 802.1X user authentication, authorization, and accounting.  

```
[Central-AC2-isp-iNC] authentication lan-access radius-scheme iNC
[Central-AC2-isp-iNC] authorization lan-access radius-scheme iNC
[Central-AC2-isp-iNC] accounting lan-access radius-scheme iNC
[Central-AC2-isp-iNC] quit
```
  3. Configure EAP relay as the method for the AC to exchange packets with the RADIUS server.  

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

## Configuring a service template

- ```
[Central-AC2] wlan service-template dot1x
[Central-AC2-wlan-st-dot1x] ssid 118341-fc-3510-bd-dot1x
```
- # Configure APs to forward client data traffic from all VLANs. If APs act as client traffic forwarder by default, skip this step.
- ```
[Central-AC2-wlan-st-dot1x] client forwarding-location ap
```
- # Specify central ACs as the authenticator.
- ```
[Central-AC2-wlan-st-dot1x] client-security authentication-location central-ac
```
- # Set the AKM mode to 802.1X, specify the CCMP cipher suite, enable the RSN IE in beacon and probe responses, set the access authentication mode to 802.1X authentication, and specify ISP domain **iNC** for authenticating the 802.1X client.
- ```
[Central-AC2-wlan-st-dot1x] akm mode dot1x
[Central-AC2-wlan-st-dot1x] cipher-suite ccmp
[Central-AC2-wlan-st-dot1x] security-ie rsn
[Central-AC2-wlan-st-dot1x] client-security authentication-mode dot1x
[Central-AC2-wlan-st-dot1x] dot1x domain iNC
```
- # Enable the service template.
- ```
[Central-AC2-wlan-st-dot1x] service-template enable
[Central-AC2-wlan-st-dot1x] quit
```

Creating a manual AP

NOTE:

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

- ```
[Central-AC2] wlan ap ap1 model AP 3620
[Central-AC2-wlan-ap-ap1] serial-id 219801A28N819CE0002T
[Central-AC2-wlan-ap-ap1] quit
```
- # Create AP group **group1**.
- ```
[Central-AC2] wlan ap-group group1
```
- # Enable the AC rediscovery feature.
- ```
[Central-AC2-wlan-ap-group-group1] control-address enable
```



# Specify 2.2.2.1 as the IP address to be carried in the CAPWAP Control IP Address message element.

```
[Central-AC2-wlan-ap-group-group1] control-address ip 2.2.2.1
```

# Specify Central AC 1 as a backup AC for the AP.

```
[Central-AC2-wlan-ap-group-group1] backup-ac ip 2.2.1.1
```

# Enable vertical backup.

```
[Central-AC2-wlan-ap-group-group1] switch-back enable
```

# Configure a grouping rule by AP name to add the AP named **ap1** to the group.

```
[Central-AC2-wlan-ap-group-group1] ap ap1
```

# Deploy configuration file **apmap.txt** to the AP group.

```
[Central-AC2-wlan-ap-group-group1] ap-model AP 3620
```

```
[Central-AC2-wlan-ap-group-group1-ap-model-AP 3620] map-configuration cfa0:/apmap.txt
```

# Bind service template **dot1x** to radio 1 and specify VLAN 300 for radio 1.

```
[Central-AC2-wlan-ap-group-group1-ap-model-AP 3620] radio 1
```

```
[Central-AC2-wlan-ap-group-group1-ap-model-AP 3620-radio-1] service-template dot1x vlan 300
```

# Enable radio 1.

```
[Central-AC2-wlan-ap-group-group1-ap-model-AP 3620-radio-1] radio
```

```
enable [Central-AC2-wlan-ap-group-group1-ap-model-AP 3620-radio-1] quit
```

```
[Central-AC2-wlan-ap-group-group1-ap-model-AP 3620] quit
```

```
[Central-AC2-wlan-ap-group-group1] quit
```

## Configuring IP routing

# Configure a default route with next hop 2.2.1.100 (an IP address on the Layer 3 switch).

```
[Central-AC2] ip route-static 0.0.0.0 0 24 2.2.1.100
```

## Configuring the local AC

### 1. Configure the local AC feature:

# Enable the local AC feature.

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

```
[Local AC] wlan local-ac enable
```

# Specify Central AC 1 and Central AC 2 for the local AC.

```
[Local AC] wlan central-ac ip 2.2.1.1
```

```
[Local AC] wlan central-ac ip 2.2.1.2
```

# Configure the local AC to use VLAN 100 to establish CAPWAP tunnels with the central ACs.

```
[Local AC] wlan local-ac capwap source-vlan 100
```

### 2. Configure interfaces:

# Create VLAN 100, create VLAN-interface 100, and assign an IP address to the VLAN interface. The local AC will use this IP address to establish CAPWAP tunnels with the central ACs.

```
[Local AC] vlan 100
```

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

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

```
[Local AC-Vlan-interface100] ip address 2.2.1.10 255.255.255.0
```

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

**# Create VLAN 200, create VLAN-interface 200, and assign an IP address to the VLAN interface. The local AC assigns VLAN 200 to an AP when the AP comes online.**

```
[Local AC] vlan 200
[Local AC-vlan200] quit
[Local AC] interface vlan-interface 200
[Local AC-Vlan-interface200] ip address 2.2.2.1 255.255.255.0
[Local AC-Vlan-interface200] quit
```

**# Create VLAN 300, create VLAN-interface 300, and assign an IP address to the VLAN interface. The local AC assigns this VLAN to a wireless client when the client comes online.**

```
[Local AC] vlan 300
[Local AC-vlan300] quit
[Local AC] interface vlan-interface 300
[Local AC-Vlan-interface300] ip address 2.2.3.1 255.255.255.0
[Local AC-Vlan-interface300] quit
```

**# Specify GigabitEthernet 1/0/1 that connects the local AC to the Layer 2 switch as a trunk port, and assign the port to VLANs 100 and 200.**

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

## Configuring the Layer 3 switch

**# Create VLAN 100, create VLAN-interface 100, and assign an IP address to the VLAN interface. The switch will use this VLAN to forward data and control packets between the central ACs and the local AC.**

```
<L3 switch> system-view
[L3 switch] vlan 100
[L3 switch-vlan100] quit
[L3 switch] interface vlan-interface 100
[L3 switch-Vlan-interface100] ip address 2.2.1.100 255.255.255.0
[L3 switch-Vlan-interface100] quit
```

**# Create VLAN 200, create VLAN-interface 200, and assign an IP address to the VLAN interface. The switch will use this VLAN to forward CAPWAP tunnel packets between the local AC and the AP.**

```
[L3 switch] vlan 200
[L3 switch-vlan200] quit
[L3 switch] interface vlan-interface 200
[L3 switch-Vlan-interface200] ip address 2.2.2.100 255.255.255.0
[L3 switch-Vlan-interface200] quit
```

**# Create VLAN 300 for wireless clients, create VLAN-interface 300, and assign an IP address to the VLAN interface.**

```
[L3 switch] vlan 300
[L3 switch-vlan300] quit
[L3 switch] interface vlan-interface 300
[L3 switch-Vlan-interface300] ip address 2.2.3.100 255.255.255.0
[L3 switch-Vlan-interface300] quit
```

**# Create VLAN 2 for wireless clients, create VLAN-interface 2, and assign an IP address to the VLAN interface. The VLAN interface will be used to connect to the INC server.**

```
[L3 switch] vlan 2
```

```
[L3 switch-vlan2] quit
[L3 switch] interface vlan-interface 2
[L3 switch-Vlan-interface2] ip address 192.168.0.100 255.255.255.0
[L3 switch-Vlan-interface2] quit
```

**# Add the interface that connects the Layer 3 switch to the INC server to VLAN 2. (Details not shown.)**

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

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

**# Configure GigabitEthernet 1/0/3 (the port connected to Central AC 2) as a trunk port, and assign the port to VLAN 100.**

```
[L3 switch] interface gigabitethernet 1/0/3
[L3 switch-GigabitEthernet1/0/3] port link-type trunk
[L3 switch-GigabitEthernet1/0/3] port trunk permit vlan 100
[L3 switch-GigabitEthernet1/0/3] quit
```

**# Configure GigabitEthernet 1/0/2 (the port connected to Central AC 2) as a trunk port, and assign the port to VLAN 200 and VLAN 300.**

```
[L3 switch] interface gigabitethernet 1/0/2
[L3 switch-GigabitEthernet1/0/2] port link-type trunk
[L3 switch-GigabitEthernet1/0/2] port trunk permit vlan 200 300
[L3 switch-GigabitEthernet1/0/2] quit
```

## Configuring the Layer 2 switch

**# Create VLAN 100, VLAN 200, and VLAN 300.**

```
<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 (the port connected to the Layer 3 switch) as a trunk port, and assign the port to VLAN 100, VLAN 200, and VLAN 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 1/0/3 (the port connected to the local AC) as a trunk port, and assign the port to VLAN 100 and VLAN 200.**

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

**# Configure GigabitEthernet 1/0/4 (the port connected to the DHCP server) as a trunk port, and assign the port to VLAN 200 and VLAN 300.**

```
[L2 switch] interface gigabitEthernet 1/0/4
[L2 switch-GigabitEthernet1/0/4] port link-type trunk
[L2 switch-GigabitEthernet1/0/4] port trunk permit vlan 200 300
[L2 switch-GigabitEthernet1/0/4] quit
```

**# Configure GigabitEthernet 1/0/2 (the port connected to the AP) as a trunk port, remove the port from VLAN 1, assign the port to VLAN 200 and VLAN 300, and enable PoE on the port.**

```
[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 pvid vlan 200
[L2 switch-GigabitEthernet1/0/2] port trunk permit vlan 200 300
[L2 switch-GigabitEthernet1/0/2] poe enable
[L2 switch-GigabitEthernet1/0/2] quit
```

## Configuring the DHCP server

**# Configure GigabitEthernet 1/0/1 (the port connected to the Layer 2 switch) as a trunk port, and assign the port to VLAN 200 and VLAN 300.**

```
<DHCP Server> system-view
[DHCP Server] interface gigabitEthernet 1/0/1
[DHCP Server-GigabitEthernet1/0/1] port link-type trunk
[DHCP Server-GigabitEthernet1/0/1] port trunk permit vlan 200 300
[DHCP Server-GigabitEthernet1/0/1] quit
```

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

```
[DHCP Server] vlan 200
[DHCP Server-vlan200] quit
[DHCP Server] interface vlan-interface 200
[DHCP Server-Vlan-interface200] ip address 2.2.2.200 255.255.255.0
[DHCP Server-Vlan-interface100] quit
```

**# Create VLAN 300, create VLAN-interface 300, and assign an IP address to the VLAN interface.**

```
[DHCP Server] vlan 300
[DHCP Server-vlan300] quit
[DHCP Server] interface vlan-interface 300
[DHCP Server-Vlan-interface300] ip address 2.2.3.200 255.255.255.0
[DHCP Server-Vlan-interface300] quit
```

**# Enable the DHCP service.**

```
[DHCP Server] dhcp enable
```

**# Configure DHCP address pool **vlan200**. In the address pool, specify the Layer 3 switch as the gateway and 2.2.2.0/24 as the subnet for dynamic allocation, and then exclude the IP addresses of the Layer 3 switch and the IP address of the local AC in VLAN 200 from dynamic allocation.**

```
[DHCP Server] dhcp server ip-pool vlan200
[DHCP Server-dhcp-pool-vlan200] gateway-list 2.2.2.100
[DHCP Server-dhcp-pool-vlan200] network 2.2.2.0 mask 255.255.255.0
[DHCP Server-dhcp-pool-vlan200] forbidden-ip 2.2.2.100 2.2.2.1
```

**# Configure Option 43 to deploy the IP address of central AC 1 (2.2.1.1) and the IP address of central AC 2 (2.2.1.2) to the AP.**

```
[DHCP Server-dhcp-pool-vlan200] option 43 hex 800b0000010202010102020102
[DHCP Server-dhcp-pool-vlan200] quit
```

# Configure DHCP address pool **vlan300**. In the address pool, specify the Layer 3 switch as the gateway, 2.2.3.0/24 as the subnet for dynamic allocation, and 8.8.8.8 as the DNS server address, and then exclude the IP address of the Layer 3 switch and the IP address of the local AC in VLAN 300 from dynamic allocation.

```
[DHCP Server] dhcp server ip-pool vlan300
[DHCP Server-dhcp-pool-vlan300] gateway-list 2.2.3.100
[DHCP Server-dhcp-pool-vlan300] network 2.2.3.0 mask 255.255.255.0
[DHCP Server-dhcp-pool-vlan300] dns-list 8.8.8.8
[DHCP Server-dhcp-pool-vlan300] forbidden-ip 2.2.3.100 2.2.3.1
```

## Configuring the RADIUS server

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

### Adding the central ACs as access devices to INC

This example only illustrates the process to add Central AC 1 to INC as an access device. You can add Central AC 2 at 2.2.1.2 to INC in the same way Central AC 1 is added.

To add Central AC 1 to INC as an access device:

1. Log in to INC and click the **User** tab.
2. From the navigation tree, select **User Access Policy > Access Device Management > Access Device**.
3. Click **Add**.  
The **Add Access Device** page opens.
4. In the **Access Configuration** area, configure the following parameters, as shown in [Figure 2](#):
  - Enter **123456** in the **Shared Key** and **Confirm Shared Key** fields. The shared key must be the same as the authentication and accounting shared keys configured on the AC.
  - Use the default values for other parameters.
5. In the **Device List** area, click **Select** or **Add Manually** to add Central AC 1 at 2.2.1.1 as an access device.  
The IP address must be the source IP address specified for outgoing RADIUS packets on the AC.
6. Click **OK**.

**Figure 2 Adding an access device**

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

Access Configuration

|                       |               |                      |                 |
|-----------------------|---------------|----------------------|-----------------|
| Authentication Port * | 1812          | Accounting Port *    | 1813            |
| Service Type          | Unlimited     | Forcible Logout Type | Disconnect user |
| Access Device Type    | H3C (General) | Service Group        | Ungrouped       |
| Shared Key *          | *****         | Confirm Shared Key * | *****           |
| Access Location Group | --            |                      |                 |

Device List

Select Add Manually Clear All

| Device Name | Device IP | Device Model | Comments | Delete |
|-------------|-----------|--------------|----------|--------|
|             | 2.2.1.1   |              |          |        |

Total Items: 1.

OK Cancel

## Adding an access policy

1. From the navigation tree, select **User Access Policy > Access Policy**.
2. Click **Add**.
3. On the **Add Access Policy** page, configure the following parameters, as shown in [Figure 3](#):
  - o Enter **802.1X-CAC1** in the **Access Policy Name** field.
  - o Select **Ungrouped** from the **Service Group** list.
  - o Select **EAP-PEAP** from the **Preferred EAP Type** list, and select **EAP-MSCHAPv2** from the **Subtype** list.

The certificate subtype on the INC server must be the same as the identity authentication method configured on the wireless client.

  - o Use the default values for other parameters.
4. Click **OK**.

**Figure 3 Adding an access policy**

Basic Information

|                      |             |
|----------------------|-------------|
| Access Policy Name * | 802.1X-CAC1 |
| Service Group *      | Ungrouped   |
| Description          |             |

Authorization Information

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

## Adding an access service

1. From the navigation tree, select **User Access Policy > Access Service**.

2. Click **Add**.
3. On the **Add Access Service** page, configure the following parameters, as shown in [Figure 4](#):
  - o Enter **802.1X-CAC1** in the **Service Name** field.
  - o Select **802.1X-CAC1** from the **Default Access Policy** list.
  - o Use the default values for other parameters.
4. Click **OK**.

**Figure 4 Adding an access service**

**Basic Information**

Service Name \* 802.1X-CAC1 Service Suffix

Service Group \* Ungrouped Default Access Policy \* 802.1X-CAC1 Add

Default Proprietary Attribute Assignment Policy \* Do not use ⓘ

Default Max. Devices for Single Account \* 0 ⓘ

Daily Max. Online Duration \* 0 ⓘ

Description

☒ Available ⓘ ☒ Transparent Authentication ⓘ

**Access Scenario List**

Add

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

OK Cancel

## Adding an access user

1. From the navigation tree, select **Access User > Access User**.  
The access user list opens.
2. Click **Add**.  
The **Add Access User** page opens.
3. In the **Access Information** area, configure the following parameters, as shown in [Figure 5](#):
  - a. Click **Select** or **Add User** to associate the user with INC Platform user **802.1X-CAC**.
  - b. Enter **client** in the **Account Name** field.
  - c. Enter **123456** in the **Password** and **Confirm Password** fields.
4. In the **Access Service** area, select **802.1X-CAC1** from the list.
5. Click **OK**.

**Figure 5 Adding an access user account**

**Access Information**

User Name \* 802.1X-CAC Select Add User

Account Name \* client ⓘ

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

Password \* 123456 Confirm Password \* 123456

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

Start Time 0 End Time 0

Max. Idle Time (Minutes)

Max. Concurrent Logins 1

Login Message

**Access Service**

| Service Name                                    | Service Suffix | Status    | Allocate IP |
|-------------------------------------------------|----------------|-----------|-------------|
| <input checked="" type="checkbox"/> 802.1X-CAC1 |                | Available |             |

OK OK & Print Cancel

# Verifying the configuration

# On the wireless client, verify that the client can pass 802.1X authentication, associate with the AP, and access the wireless network. (Details not shown.)

# Display detailed WLAN client information.

```
<System> display wlan client
```

Total number of clients: 1

| MAC address    | User name | AP name | R IP address | VLAN |
|----------------|-----------|---------|--------------|------|
| 90f0-5266-7601 | client    | ap1     | 1 2.2.3.58   | 300  |

# Display online 802.1X user information.

```
<System> display dot1x connection
```

Total connections: 1

|                            |                           |
|----------------------------|---------------------------|
| User MAC address           | : 90f0-5266-7601          |
| AP name                    | : ap1                     |
| Radio ID                   | : 1                       |
| SSID                       | : 118341-fc-3510-bd-dot1x |
| BSSID                      | : 60da-838a-97f0          |
| Username                   | : client                  |
| Authentication domain      | : iNC                     |
| IPv4 address               | : 2.2.3.58                |
| Authentication method      | : EAP                     |
| Initial VLAN               | : 300                     |
| Authorization VLAN         | : 100                     |
| Authorization ACL number   | : N/A                     |
| Authorization user profile | : N/A                     |
| Termination action         | : Default                 |
| Session timeout period     | : 36000001 s              |
| Online from                | : 2020/12/21 11:27:11     |
| Online duration            | : 0h 1m 1s                |

## Configuration files

- Layer 3 switch:

```
#
Vlan 2
#
vlan 100
#
vlan 200
#
vlan 300
#
interface Vlan-interface2
 ip address 192.168.0.100 255.255.255.0
#
interface Vlan-interface100
```



```

ip address 2.2.1.100 255.255.255.0
#
interface Vlan-interface200
ip address 2.2.2.100 255.255.255.0
#
interface Vlan-interface300
ip address 2.2.3.100 255.255.255.0
#
interface GigabitEthernet1/0/1
port link-type trunk
port trunk permit vlan 1 100
#
interface GigabitEthernet1/0/2
port link-type trunk
port trunk permit vlan 1 200 300
#
interface GigabitEthernet1/0/3
port link-type trunk
port trunk permit vlan 1 100
#

```

- **Central AC 1:**

```

#
dot1x authentication-method eap
#
vlan 100
#
wlan service-template dot1x
ssid 118341-fc-3510-bd-dot1x
client forwarding-location ap
client-security authentication-location central-ac
akm mode dot1x
cipher-suite ccmp
security-ie rsn
client-security authentication-mode dot1x
dot1x domain iNC
service-template enable
#
interface Vlan-interface100
ip address 2.2.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
port link-type trunk
port trunk permit vlan 1 100
#
ip route-static 0.0.0.0 0 2.2.1.100
#
radius session-control enable
#

```

```

radius scheme iNC
primary authentication 192.168.0.111
primary accounting 192.168.0.111
key authentication cipher c3$YVdYhyr5oUtYPySJKGJqNbEzSPAITDchdA==
key accounting cipher c3$/Vmhl1A5ctoybnGIjEUo9M7Fb5UWh0hd1g==
nas-ip 2.2.1.1
#
domain iNC
authentication lan-access radius-scheme iNC
authorization lan-access radius-scheme iNC
accounting lan-access radius-scheme iNC
#
wlan ap-group group1
backup-ac ip 2.2.1.2
control-address enable
control-address ip 2.2.2.1
switch-back enable
ap ap1
ap-model AP 3620
map-configuration cfa0:/map.txt
radio 1
radio enable
service-template dot1x vlan 300
radio 2
#
wlan ap ap1 model AP 3620
serial-id 219801A28N819CE0002T
#
wlan local-ac name 3510 model WX3510H
serial-id 210235A1JNB165000120
priority 7
wlan tunnel-preempt enable
#

```

- **Central AC 2:**

```

#
dot1x authentication-method eap
#
vlan 100
#
wlan service-template dot1x
ssid 118341-fc-3510-bd-dot1x
client forwarding-location ap
client-security authentication-location central-ac
akm mode dot1x
cipher-suite ccmp
security-ie rsn
client-security authentication-mode dot1x

```

```

dot1x domain iNC
service-template enable
#
interface Vlan-interface100
ip address 2.2.1.2 255.255.255.0
#
interface GigabitEthernet1/0/1
port link-type trunk
port trunk permit vlan 1 100
#
ip route-static 0.0.0.0 0 2.2.1.100
#
radius session-control enable
#
radius scheme iNC
primary authentication 192.168.0.111
primary accounting 192.168.0.111
key authentication cipher c3$YVdYhyr5oUtYPySJKGJqNbEzSPAITDchdA==
key accounting cipher c3$/Vmhl1A5ctoybnGIjEUo9M7Fb5UWh0hd1g==
nas-ip 2.2.1.2
#
domain iNC
authentication lan-access radius-scheme iNC
authorization lan-access radius-scheme iNC
accounting lan-access radius-scheme iNC
#
wlan ap-group group1
backup-ac ip 2.2.1.1
control-address enable
control-address ip 2.2.2.1
switch-back enable
ap ap1
ap-model AP 3620
map-configuration cfa0:/map.txt
radio 1
radio enable
service-template dot1x vlan 300
radio 2
#
wlan ap ap1 model AP 3620
serial-id 219801A28N819CE0002T
#
wlan local-ac name 3510 model WX3510H
serial-id 210235A1JNB165000120
priority 6
wlan tunnel-preempt enable
#

```

- 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
#
interface GigabitEthernet1/0/2
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 200 300
 port trunk pvid vlan 200
 poe enable
#
interface GigabitEthernet1/0/3
 port link-type trunk
 port trunk permit vlan 1 100 200
#
interface GigabitEthernet1/0/4
 port link-type trunk
 port trunk permit vlan 1 200 300
#

```

- **DHCP server:**

```

#
dhcp enable
#
vlan 200
#
vlan 300
#
dhcp server ip-pool vlan200
 gateway-list 2.2.2.100
 network 2.2.2.0 mask 255.255.255.0
 forbidden-ip 2.2.2.1
 forbidden-ip 2.2.2.100
 option 43 hex 800b0000010202010102020102
#
dhcp server ip-pool vlan300
 gateway-list 2.2.3.100
 network 2.2.3.0 mask 255.255.255.0
 dns-list 8.8.8.8
 forbidden-ip 2.2.3.1
 forbidden-ip 2.2.3.100
#

```

```

interface Vlan-interface200
 ip address 2.2.2.200 255.255.255.0
#
interface Vlan-interface300
 ip address 2.2.3.200 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 1 200 300
#

```

- **Local AC:**

```

#
vlan 100
#
vlan 200
#
vlan 300
#
interface Vlan-interface100
 ip address 2.2.1.10 255.255.255.0
#
interface Vlan-interface200
 ip address 2.2.2.1 255.255.255.0
#
interface Vlan-interface300
 ip address 2.2.3.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 1 100 200
#
 wlan local-ac enable
#
 wlan local-ac capwap source-vlan 100
#
 wlan central-ac ip 2.2.1.1
 wlan central-ac ip 2.2.1.2
#

```

## Related documentation

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

- *WLAN Access Command Reference in INTELBRAS Access Controllers Command References*

# INTELBRAS Access Controllers

## Remote Portal Authentication on an AC Hierarchy Network with Dual-Link Central AC Backup Configuration Examples

---

Copyright © 2024 Intelbras S.A All rights reserved.

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

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

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

# Contents

|                                                                                                                     |    |
|---------------------------------------------------------------------------------------------------------------------|----|
| Introduction .....                                                                                                  | 1  |
| Prerequisites .....                                                                                                 | 1  |
| Example: Configuring remote portal authentication on an AC hierarchy network with dual-link central AC backup ..... | 1  |
| Network configuration .....                                                                                         | 1  |
| Analysis .....                                                                                                      | 2  |
| Restrictions and guidelines .....                                                                                   | 2  |
| Procedures .....                                                                                                    | 3  |
| Editing the AP's configuration file .....                                                                           | 3  |
| Configuring central AC 1 .....                                                                                      | 3  |
| Configure central AC 2 .....                                                                                        | 6  |
| Configuring the local AC .....                                                                                      | 10 |
| Configuring the Layer 3 switch .....                                                                                | 11 |
| Configuring the Layer 2 switch .....                                                                                | 12 |
| Configuring the DHCP server .....                                                                                   | 12 |
| Configuring the RADIUS server .....                                                                                 | 13 |
| Configuring the portal server .....                                                                                 | 16 |
| Verifying the configuration .....                                                                                   | 18 |
| Configuration files .....                                                                                           | 19 |
| Related documentation .....                                                                                         | 25 |



# Introduction

The following information provides an example of configuring remote portal authentication for clients on an AC hierarchy network where two central ACs are deployed for redundancy.

## Prerequisites

---

**NOTE:**

Support for this configuration example varies by device model and version.

---

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, WLAN user authentication, WLAN access, and WLAN high availability.

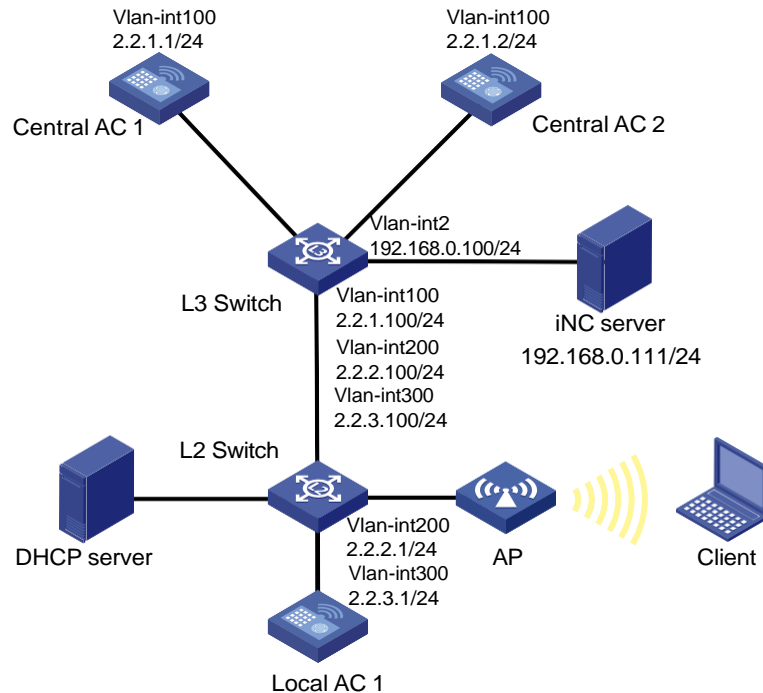
## Example: Configuring remote portal authentication on an AC hierarchy network with dual-link central AC backup

### Network configuration

As shown in [Figure 1](#), the AC hierarchy network contains two central ACs. The AP and client obtain an IP address from the DHCP server, and the INC server acts as both the portal authentication server and RADIUS server. Configure the devices to meet the following requirements:

- The central ACs operate in master/backup mode and back up each other. Central AC 1 acts as the master central AC, and central AC 2 acts as the backup central AC
- The AP obtains the IP addresses of the central ACs from the DHCP server through DHCP Option 43. The AC rediscovery feature is configured on the central ACs. For the AP to associate with the local AC, enable the AC rediscovery feature in the view of the manual AP. In addition, configure the central ACs to add the IP address of the local AC to the CAPWAP Control IP Address message element in the discovery responses sent to the AP. The AP, central ACs, and the local AC are reachable to each other so that the AP can associate with a central AC when the local AC fails.
- Use direct portal authentication for wireless clients.
- Use the central ACs as the authenticator.
- Configure the AP to forward client data traffic.

**Figure 1 Network diagram**



## Analysis

- Make sure the master and backup central ACs run the same version of software and have the same settings.
- For GigabitEthernet 1/0/1 to forward client data traffic in VLAN 300, edit the configuration file of the AP and upload the file to the central ACs.
- For portal users that have been authenticated on an AC to roam to another AC to access the network resources without re-authentication, enable roaming for portal users.
- To avoid portal authentication failure caused by frequent portal client onboarding and offboarding, disable the Rule ARP entry feature for portal clients.
- For the RADIUS server to dynamically change client authorization information or forcibly disconnect a wireless client, enable the RADIUS session-control feature on the central ACs.

## Restrictions and guidelines

- Central ACs on an AC hierarchy network do not support IRF.
- Use the actual serial ID of an AP to uniquely identify that AP.
- On the local AC, do not enable the auto AP feature. In addition, create a manual AP for the AP in local AC view on the central ACs for the central ACs to manage the AP.
- For dual-link central AC backup to operate correctly, configure the local AC and manual AP settings on both central ACs. Make sure the priority settings on the local AC, the master central AC, and the backup central AC are correctly configured so that the local AC can re-associate with the master central AC when the master central AC recovers.

# Procedures

## Editing the AP's configuration file

# Edit the AP's configuration file, name it apmap.txt and upload the configuration file to the AC.

```
System-view
vlan 300
interface gigabitethernet1/0/1
port link-type trunk
port trunk permit vlan 300
```

## Configuring central AC 1

### 1. Configure interfaces on central AC 1:

# Create VLAN 100 and VLAN-interface 100, and assign an IP address to the VLAN interface. The central AC will use this IP address to establish a management tunnel with the local AC.

```
<Central-AC1> system-view
[Central-AC1] vlan 100
[Central-AC1-vlan100] quit
[Central-AC1] interface vlan-interface 100
[Central-AC1-Vlan-interface100] ip address 2.2.1.1 24
[Central-AC1-Vlan-interface100] quit
```

# Configure GigabitEthernet 1/0/1 (the port connected to the Layer 3 switch) as a trunk port, and assign the port to VLAN 100.

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

### 2. Configure a local AC for central AC 1:

# Create local AC 3510 with model WX3510H and enter local AC view.

```
[Central-AC1] wlan local-ac name 3510 model WX3510H
```

# Specify the serial ID of the local AC.

```
[Central-AC1-wlan-local-ac-3510] serial-id 210235A1JNB165000120
```

# Set the priority to 7 for tunnel establishment to the local AC.

```
[Central-AC1-wlan-local-ac-3510] priority 7
```

# Enable master CAPWAP tunnel preemption.

```
[Central-AC1-wlan-local-ac-3510] wlan tunnel-preempt enable
[Central-AC1-wlan-local-ac-3510] quit
```

### 3. Configure portal authentication for clients:

#### o Configure a RADIUS scheme:

# Create a RADIUS scheme named **iNC** and enter RADIUS scheme view.

```
[Central-AC1] radius scheme iNC
```

# Specify the IP address of the primary RADIUS authentication server.

```
[Central-AC1-radius-iNC] primary authentication 192.168.0.111
```

# Specify the IP address of the primary RADIUS accounting server.

```
[Central-AC1-radius-iNC] primary accounting 192.168.0.111
```

# Set the shared key to **123456** in plaintext form for secure communication with the RADIUS authentication server.

```
[Central-AC1-radius-iNC] key authentication simple 123456
```

# Set the shared key to **123456** in plaintext form for secure communication with the RADIUS accounting server.

```
[Central-AC1-radius-iNC] key accounting simple 123456
```

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

```
[Central-AC1-radius-iNC] user-name-format without-domain
```

# Specify IP address 2.2.1.1 as the source IP address for outgoing RADIUS packets.

```
[Central-AC1-radius-iNC] nas-ip 2.2.1.1
```

```
[Central-AC1-radius-iNC] quit
```

# Enable RADIUS session-control.

```
[Central-AC1] radius session-control enable
```

- o Configure an authentication domain:

# Create ISP domain **iNC** and enter its view.

```
[Central-AC1] domain iNC
```

# Configure the ISP domain to use RADIUS scheme **iNC** for portal user authentication, authorization, and accounting.

```
[Central-AC1-isp-iNC] authentication lan-access radius-scheme iNC
```

```
[Central-AC1-isp-iNC] authorization lan-access radius-scheme iNC
```

```
[Central-AC1-isp-iNC] accounting lan-access radius-scheme iNC
```

# Set the idle timeout period to 15 minutes for the users in the **iNC** ISP domain.

```
[Central-AC1-isp-iNC] authorization-attribute idle-cut 15 1024
```

```
[Central-AC1-isp-iNC] quit
```

#### 4. Configure a wireless service:

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

```
[Central-AC1] wlan service-template st1
```

- # Configure the SSID as **service**.

```
[Central-AC1-wlan-st-st1] ssid service
```

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

```
[Central-AC1-wlan-st-st1] akm mode psk
```

```
[Central-AC1-wlan-st-st1] preshared-key pass-phrase simple 12345678
```

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

```
[Central-AC1-wlan-st-st1] cipher-suite ccmp
```

```
[Central-AC1-wlan-st-st1] security-ie rsn
```

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

```
[Central-AC1-wlan-st-st1] client forwarding-location ap
```

- # Specify the central AC as the authenticator.

```
[Central-AC1-wlan-st-st1] client-security authentication-location central-ac
```

- # Specify the authentication domain as **iNC** for portal users.

```
[Central-AC1-wlan-st-st1] portal domain iNC
```

- # Enable the service template.

```
[Central-AC1-wlan-st-st1] service-template enable
```

```
[Central-AC1-wlan-st-st1] quit
```

#### 5. Configure portal authentication:

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

```
[Central-AC1] portal server newpt
[Central-AC1-portal-server-newpt] ip 192.168.0.111 key simple radius
[Central-AC1-portal-server-newpt] port 50100
```

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

```
[Central-AC1-portal-server-newpt] server-type cmcc
[Central-AC1-portal-server-newpt] quit
```

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

```
[Central-AC1] portal web-server newpt
[Central-AC1-portal-websvr-newpt] url http://192.168.0.111:8080/portal
```

# Add parameters **ssid**, **wlanuserip**, **wlanacname**, and **nasip** to the URL of portal Web server **newpt**. Specify the AP's SSID, the IP address of the client, the AC's name, and NAS IP 2.2.1.1 as the values for the parameters, respectively. (The parameters are required to be carried in the URL of a portal Web server of the CMCC type.)

```
[Central-AC1-portal-websvr-newpt] url-parameter ssid ssid
[Central-AC1-portal-websvr-newpt] url-parameter wlanuserip source-address
[Central-AC1-portal-websvr-newpt] url-parameter wlanacname value Central-AC1
[Central-AC1-portal-websvr-newpt] url-parameter nasip value 2.2.1.1
```

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

```
[Central-AC1-portal-websvr-newpt] server-type cmcc
[Central-AC1-portal-websvr-newpt] quit
```

# Configure a destination-based portal-free rule numbered 0 to permit traffic destined for IP address 192.168.0.111 (the portal Web server).

```
[Central-AC1] portal free-rule 0 destination ip 192.168.0.111 24
```

# Configure two portal-free rules, allowing access to the DNS server without portal authentication.

```
[Central-AC1] portal free-rule 1 destination ip any udp 53
[Central-AC1] portal free-rule 2 destination ip any tcp 53
```

# Enable portal roaming.

```
[Central-AC1] portal roaming enable
```

# Disable the Rule ARP entry feature for portal clients.

```
[Central-AC1] undo portal refresh arp enable
```

# Enable direct IPv4 portal authentication on service template **st1**.

```
[Central-AC1] wlan service-template st1
[Central-AC1-wlan-st-st1] portal enable method direct
```

# Specify IPv4 portal Web server **newpt** on service template **st1** for portal authentication.

```
[Central-AC1-wlan-st-st1] portal apply web-server newpt
```

# On service template **st1**, configure the BAS-IP attribute as 2.2.1.1 for portal packets sent to the portal authentication server.

```
[Central-AC1-wlan-st-st1] portal bas-ip 2.2.1.1
[Central-AC1-wlan-st-st1] quit
```

## 6. Configure 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.

```

[Central-AC1] wlan ap ap1 model AP 3620
[Central-AC1-wlan-ap-ap1] serial-id 219801A28N819CE0002T
[Central-AC1-wlan-ap-ap1] quit
Create AP group group1.
[Central-AC1] wlan ap-group group1
Enable AC rediscovery.
[Central-AC1-wlan-ap-group-group1] control-address enable
Specify a local AC.
[Central-AC1-wlan-ap-group-group1] control-address ip 2.2.2.1
Specify a backup AC for the central AC.
[Central-AC1-wlan-ap-group-group1] backup-ac ip 2.2.1.2
Enable automatic switch-back after a local-central AC switchover.
[Central-AC1-wlan-ap-group-group1] switch-back enable
Add AP ap1 to AP group group1.
[Central-AC1-wlan-ap-group-group1] ap ap1
Deploy a configuration file to the AP.
[Central-AC1-wlan-ap-group-group1] ap-model AP 3620
[Central-AC1-wlan-ap-group-group1-ap-model-AP 3620] map-configuration
cfa0:/apmap.txt
Bind service template st1 to radio 1 in AP group group1.
[Central-AC1-wlan-ap-group-group1-ap-model-AP 3620] radio 1
[Central-AC1-wlan-ap-group-group1-ap-model-AP 3620-radio-1] service-template st1
vlan 300
Enable radio 1.
[Central-AC1-wlan-ap-group-group1-ap-model-AP 3620-radio-1] radio
enable [Central-AC1-wlan-ap-group-group1-ap-model-AP 3620-radio-1] quit
[Central-AC1-wlan-ap-group-group1-ap-model-AP 3620] quit
[Central-AC1-wlan-ap-group-group1] quit

```

7. Configure a static route:

**# Configure a static route, whose next hop address is 2.2.1.100, IP address of the Layer 3 switch.**

```

[Central-AC1] ip route-static 0.0.0.0 24 2.2.1.100

```

## Configure central AC 2

### 1. Configure interfaces on central AC 2:

**# Create VLAN 100 and VLAN-interface 100, and assign an IP address to the VLAN interface. The central AC will use this IP address to establish a management tunnel with the local AC.**

```

<Central-AC2> system-view
[Central-AC2] vlan 100
[Central-AC2-vlan100] quit
[Central-AC2] interface vlan-interface 100
[Central-AC2-Vlan-interface100] ip address 2.2.1.2 24
[Central-AC2-Vlan-interface100] quit

```

**# Configure GigabitEthernet 1/0/1 (the port connected to the Layer 3 switch) as a trunk port, and assign the port to VLAN 100.**

```

[Central-AC2] interface gigabitethernet 1/0/1
[Central-AC2-GigabitEthernet1/0/1] port link-type trunk

```

```
[Central-AC2-GigabitEthernet1/0/1] port trunk permit vlan 100
[Central-AC2-GigabitEthernet1/0/1] quit
```

## 2. Configure a local AC for central AC 2:

# Create local AC 3510 with model WX3510H and enter local AC view.

```
[Central-AC2] wlan local-ac name 3510 model WX3510H
```

# Specify the serial ID of the local AC.

```
[Central-AC2-wlan-local-ac-3510] serial-id 210235A1JNB165000120
```

# Set the priority to 6 for tunnel establishment to the local AC.

```
[Central-AC2-wlan-local-ac-3510] priority 6
```

# Enable master CAPWAP tunnel preemption.

```
[Central-AC2-wlan-local-ac-3510] wlan tunnel-preempt enable
```

```
[Central-AC2-wlan-local-ac-3510] quit
```

## 3. Configure portal authentication for clients:

### o Configure a RADIUS scheme:

# Create a RADIUS scheme named **iNC** and enter RADIUS scheme view.

```
[Central-AC2] radius scheme iNC
```

# Specify the IP address of the primary RADIUS authentication server.

```
[Central-AC2-radius-iNC] primary authentication 192.168.0.111
```

# Specify the IP address of the primary RADIUS accounting server.

```
[Central-AC2-radius-iNC] primary accounting 192.168.0.111
```

# Set the shared key to **123456** in plaintext form for secure communication with the RADIUS authentication server.

```
[Central-AC2-radius-iNC] key authentication simple 123456
```

# Set the shared key to **123456** in plaintext form for secure communication with the RADIUS accounting server.

```
[Central-AC2-radius-iNC] key accounting simple 123456
```

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

```
[Central-AC2-radius-iNC] user-name-format without-domain
```

# Specify IP address 2.2.1.2 as the source IP address for outgoing RADIUS packets.

```
[Central-AC2-radius-iNC] nas-ip 2.2.1.2
```

```
[Central-AC2-radius-iNC] quit
```

# Enable RADIUS session-control.

```
[Central-AC2] radius session-control enable
```

### o Configure an authentication domain:

# Create ISP domain **iNC** and enter its view.

```
[Central-AC2] domain iNC
```

# Configure the ISP domain to use RADIUS scheme **iNC** for portal user authentication, authorization, and accounting.

```
[Central-AC2-isp-iNC] authentication lan-access radius-scheme iNC
```

```
[Central-AC2-isp-iNC] authorization lan-access radius-scheme iNC
```

```
[Central-AC2-isp-iNC] accounting lan-access radius-scheme iNC
```

# Set the idle timeout period to 15 minutes and the minimum traffic that must be generated in the idle timeout period to 1024 bytes for the users in the **iNC** ISP domain.

```
[Central-AC2-isp-iNC] authorization-attribute idle-cut 15 1024
```

```
[Central-AC2-isp-iNC] quit
```

## 4. Configure a wireless service:

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

```
[Central-AC2] wlan service-template st1
```

# Configure the SSID as **service**.

```
[Central-AC2-wlan-st-st1] ssid service
```

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

```
[Central-AC2-wlan-st-st1] akm mode psk
```

```
[Central-AC2-wlan-st-st1] preshared-key pass-phrase simple 12345678
```

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

```
[Central-AC2-wlan-st-st1] cipher-suite ccmp
```

```
[Central-AC2-wlan-st-st1] security-ie rsn
```

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

```
[Central-AC2-wlan-st-st1] client forwarding-location ap
```

# Specify the central AC as the authenticator.

```
[Central-AC2-wlan-st-st1] client-security authentication-location central-ac
```

# Specify the authentication domain as **inc** for portal users.

```
[Central-AC2-wlan-st-st1] portal domain inc
```

# Enable the service template.

```
[Central-AC2-wlan-st-st1] service-template enable
```

```
[Central-AC2-wlan-st-st1] quit
```

## 5. Configure portal authentication:

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

```
[Central-AC2] portal server newpt
```

```
[Central-AC2-portal-server-newpt] ip 192.168.0.111 key simple radius
```

```
[Central-AC2-portal-server-newpt] port 50100
```

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

```
[Central-AC2-portal-server-newpt] server-type cmcc
```

```
[Central-AC2-portal-server-newpt] quit
```

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

```
[Central-AC2] portal web-server newpt
```

```
[Central-AC2-portal-websvr-newpt] url http://192.168.0.111:8080/portal
```

# Add parameters **ssid**, **wlanuserip**, **wlanacname**, and **nasip** to the URL of portal Web server **newpt**. Specify the AP's SSID, the IP address of the client, the AC's name, and NAS IP 2.2.1.2 as the values for the parameters, respectively. (The parameters are required to be carried in the URL of a portal Web server of the CMCC type.)

```
[Central-AC2-portal-websvr-newpt] url-parameter ssid ssid
```

```
[Central-AC2-portal-websvr-newpt] url-parameter wlanuserip source-address
```

```
[Central-AC2-portal-websvr-newpt] url-parameter wlanacname value Central-AC2
```

```
[Central-AC2-portal-websvr-newpt] url-parameter nasip value 2.2.1.2
```

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

```
[Central-AC2-portal-websvr-newpt] server-type cmcc
```

```
[Central-AC2-portal-websvr-newpt] quit
```

# Configure a destination-based portal-free rule numbered 0 to permit traffic destined for IP address 192.168.0.111 (the portal Web server).

```
[Central-AC2] portal free-rule 0 destination ip 192.168.0.111 24
```



**# Configure two portal-free rules, allowing access to the DNS server without portal authentication.**

```
[Central-AC2] portal free-rule 1 destination ip any udp 53
[Central-AC2] portal free-rule 2 destination ip any tcp 53
```

**# Enable portal roaming.**

```
[Central-AC2] portal roaming enable
```

**# Disable the Rule ARP entry feature for portal clients.**

```
[Central-AC2] undo portal refresh arp enable
```

**# Enable direct IPv4 portal authentication on service template **st1**.**

```
[Central-AC2] wlan service-template st1
[Central-AC2-wlan-st-st1] portal enable method direct
```

**# Specify IPv4 portal Web server **newpt** on service template **st1** for portal authentication.**

```
[Central-AC2-wlan-st-st1] portal apply web-server newpt
```

**# On service template **st1**, configure the BAS-IP attribute as 2.2.1.2 for portal packets sent to the portal authentication server.**

```
[Central-AC2-wlan-st-st1] portal bas-ip 2.2.1.2
[Central-AC2-wlan-st-st1] quit
```

## 6. Configure 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.**

```
[Central-AC2] wlan ap ap1 model AP 3620
[Central-AC2-wlan-ap-ap1] serial-id 219801A28N819CE0002T
[Central-AC2-wlan-ap-ap1] quit
```

**# Create AP group **group1**.**

```
[Central-AC2] wlan ap-group group1
```

**# Enable AC rediscovery.**

```
[Central-AC2-wlan-ap-group-group1] control-address enable
```

**# Specify the local AC.**

```
[Central-AC2-wlan-ap-group-group1] control-address ip 2.2.2.1
```

**# Specify central AC 1 as the backup AC for central AC 2.**

```
[Central-AC2-wlan-ap-group-group1] backup-ac ip 2.2.1.1
```

**# Enable automatic switch-back after a local-central AC switchover.**

```
[Central-AC2-wlan-ap-group-group1] switch-back enable
```

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

```
[Central-AC2-wlan-ap-group-group1] ap ap1
```

**# Deploy a configuration file to the AP.**

```
[Central-AC2-wlan-ap-group-group1] ap-model AP 3620
[Central-AC2-wlan-ap-group-group1-ap-model-AP 3620] map-configuration
cfa0:/apmap.txt
```

**# Bind service template **st1** to radio 1 in AP group **group1**.**

```
[Central-AC2-wlan-ap-group-group1-ap-model-AP 3620] radio 1
[Central-AC2-wlan-ap-group-group1-ap-model-AP 3620-radio-1] service-template st1
vlan 300
```

**# Enable radio 1.**

```
[Central-AC2-wlan-ap-group-group1-ap-model-AP 3620-radio-1] radio enable
```

```
[Central-AC2-wlan-ap-group-group1-ap-model-AP 3620-radio-1]
quit [Central-AC2-wlan-ap-group-group1-ap-model-AP 3620] quit
[Central-AC2-wlan-ap-group-group1] quit
```

**7. Configure a static route:**

**# Configure a static route, whose next hop address is 2.2.1.100, IP address of the Layer 3 switch.**

```
[Central-AC2] ip route-static 0.0.0.0 0 24 2.2.1.100
```

## Configuring the local AC

**1. Configure the local AC feature:**

**# Enable the local AC feature.**

```
<Local AC> system-view
[Local AC] wlan local-ac enable
```

**# Specify central ACs for the local AC.**

```
[Local AC] wlan central-ac ip 2.2.1.1
[Local AC] wlan central-ac ip 2.2.1.2
```

**# Configure the local AC to use VLAN 100 to establish a tunnel with the central ACs.**

```
[Local AC] wlan local-ac capwap source-vlan 100
```

**2. Configure interfaces:**

**# Create VLAN 100, create VLAN-interface 100, and assign an IP address to the VLAN interface. The local AC will use this IP address to establish CAPWAP tunnels with the central ACs.**

```
[Local AC] vlan 100
[Local AC-vlan100] quit
[Local AC] interface Vlan-interface100
[Local AC-Vlan-interface100] ip address 2.2.1.10 255.255.255.0
[Local AC-Vlan-interface100] quit
```

**# Create VLAN 200, create VLAN-interface 200, and assign an IP address to the VLAN interface. The local AC assigns VLAN 200 to an AP when the AP comes online.**

```
[Local AC] vlan 200
[Local AC-vlan200] quit
[Local AC] interface Vlan-interface200
[Local AC-Vlan-interface200] ip address 2.2.2.1 255.255.255.0
[Local AC-Vlan-interface200] quit
```

**# Create VLAN 300, create VLAN-interface 300, and assign an IP address to the VLAN interface. The local AC assigns this VLAN to a wireless client when the client comes online.**

```
[Local AC] vlan 300
[Local AC-vlan300] quit
[Local AC] interface Vlan-interface300
[Local AC-Vlan-interface300] ip address 2.2.3.1 255.255.255.0
[Local AC-Vlan-interface300] quit
```

**# Configure GigabitEthernet 1/0/1 (the port connected to the Layer 2 switch) as a trunk port, and assign the port to VLAN 100 and VLAN 200.**

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

## Configuring the Layer 3 switch

**# Create VLAN 100, create VLAN-interface 100, and assign an IP address to the VLAN interface. The switch will use this VLAN to forward data and control packets between the central ACs and the local AC.**

```
<L3 switch> system-view
[L3 switch] vlan 100
[L3 switch-vlan100] quit
[L3 switch] interface vlan-interface 100
[L3 switch-Vlan-interface100] ip address 2.2.1.100 255.255.255.0
[L3 switch-Vlan-interface100] quit
```

**# Create VLAN 200, create VLAN-interface 200, and assign an IP address to the VLAN interface. The switch will use this VLAN to forward CAPWAP tunnel packets between the local AC and the AP.**

```
[L3 switch] vlan 200
[L3 switch-vlan200] quit
[L3 switch] interface vlan-interface 200
[L3 switch-Vlan-interface200] ip address 2.2.2.100 255.255.255.0
[L3 switch-Vlan-interface200] quit
```

**# Create VLAN 300 for wireless clients, create VLAN-interface 300, and assign an IP address to the VLAN interface.**

```
[L3 switch] vlan 300
[L3 switch-vlan300] quit
[L3 switch] interface vlan-interface 300
[L3 switch-Vlan-interface300] ip address 2.2.3.100 255.255.255.0
[L3 switch-Vlan-interface300] quit
```

**# Create VLAN 2, create VLAN-interface 2, and assign an IP address to the VLAN interface. The switch will use this VLAN to connect to the INC server.**

```
[L3 switch] vlan 2
[L3 switch-vlan2] quit
[L3 switch] interface vlan-interface 2
[L3 switch-Vlan-interface2] ip address 192.168.0.100 255.255.255.0
[L3 switch-Vlan-interface2] quit
```

**Assign the port that connects the Layer 3 switch to the INC server to VLAN 2. (Details not shown.)**

**# Configure GigabitEthernet 1/0/1 that connects the Layer 3 switch to central AC 1 as a trunk port, and assign the port to VLAN 100.**

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

**# Configure GigabitEthernet 1/0/3 that connects the Layer 3 switch to central AC 2 as a trunk port, and assign the port to VLAN 100.**

```
[L3 switch] interface gigabitEthernet 1/0/3
[L3 switch-GigabitEthernet1/0/3] port link-type trunk
[L3 switch-GigabitEthernet1/0/3] port trunk permit vlan 100
[L3 switch-GigabitEthernet1/0/3] quit
```

**# Configure GigabitEthernet 1/0/2 that connects the Layer 3 switch to the Layer 2 switch as a trunk port, and assign the port to VLAN 200 and VLAN 300.**

```
[L3 switch] interface gigabitEthernet 1/0/2
```

```
[L3 switch-GigabitEthernet1/0/2] port link-type trunk
[L3 switch-GigabitEthernet1/0/2] port trunk permit vlan 200 300
[L3 switch-GigabitEthernet1/0/2] quit
```

## Configuring the Layer 2 switch

**# Create VLAN 100, VLAN 200, and VLAN 300.**

```
<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 Layer 2 switch to the Layer 3 switch as a trunk port, and assign the port to VLAN 100, VLAN 200, and VLAN 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 1/0/3 that connects the Layer 2 switch to the local AC as a trunk port, and assign the port to VLAN 100 and VLAN 200.**

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

**# Configure GigabitEthernet 1/0/4 that connects the Layer 2 switch to the DHCP server as a trunk port, and assign the port to VLAN 200 and VLAN 300.**

```
[L2 switch] interface gigabitEthernet 1/0/4
[L2 switch-GigabitEthernet1/0/4] port link-type trunk
[L2 switch-GigabitEthernet1/0/4] port trunk permit vlan 200 300
[L2 switch-GigabitEthernet1/0/4] quit
```

**# Configure GigabitEthernet 1/0/2 that connects the Layer 2 switch to the AP as a trunk port, remove the port from VLAN 1, assign the port to VLAN 200 and VLAN 300, and enable PoE on the port.**

```
[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 pvid vlan 200
[L2 switch-GigabitEthernet1/0/2] port trunk permit vlan 200 300
[L2 switch-GigabitEthernet1/0/2] poe enable
[L2 switch-GigabitEthernet1/0/2] quit
```

## Configuring the DHCP server

**# Configure GigabitEthernet 1/0/1 that connects the DHCP server to the Layer 2 switch as a trunk port, and assign the port to VLAN 200 and VLAN 300.**

```
<DHCP Server> system-view
[DHCP Server] interface gigabitEthernet 1/0/1
```

```
[DHCP Server-GigabitEthernet1/0/1] port link-type trunk
[DHCP Server-GigabitEthernet1/0/1] port trunk permit vlan 200 300
[DHCP Server-GigabitEthernet1/0/1] quit
```

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

```
[DHCP Server] vlan 200
[DHCP Server-vlan200] quit
[DHCP Server] interface vlan-interface 200
[DHCP Server-Vlan-interface200] ip address 2.2.2.200 255.255.255.0
[DHCP Server-Vlan-interface100] quit
```

**# Create VLAN 300, create VLAN-interface 300, and assign an IP address to the VLAN interface.**

```
[DHCP Server] vlan 300
[DHCP Server-vlan300] quit
[DHCP Server] interface vlan-interface 300
[DHCP Server-Vlan-interface300] ip address 2.2.3.200 255.255.255.0
[DHCP Server-Vlan-interface300] quit
```

**# Enable the DHCP service.**

```
[DHCP Server] dhcp enable
```

**# Configure DHCP address pool vlan200. In the address pool, specify 2.2.2.100 (the IP address of VLAN-interface 200 on the Layer 3 switch) as the gateway IP address and 2.2.2.0/24 as the subnet for dynamic allocation, and then exclude 2.2.2.100 and 2.2.2.1 from dynamic allocation.**

```
[DHCP Server] dhcp server ip-pool vlan200
[DHCP Server-dhcp-pool-vlan200] gateway-list 2.2.2.100
[DHCP Server-dhcp-pool-vlan200] network 2.2.2.0 mask 255.255.255.0
[DHCP Server-dhcp-pool-vlan200] forbidden-ip 2.2.2.100 2.2.2.1
```

**# Configure Option 43 to specify the IP addresses of the central ACs in address pool vlan200. The right-most bytes 0202010102020102 (2.2.1.1 and 2.2.1.2) represent the IP addresses of central AC 1 and central AC 2.**

```
[DHCP Server-dhcp-pool-vlan200] option 43 hex 800b0000010202010102020102
[DHCP Server-dhcp-pool-vlan200] quit
[DHCP Server-dhcp-pool-vlan200] quit
```

**# Configure DHCP address pool vlan300. In the address pool, specify 2.2.3.100 (the IP address of VLAN-interface 300 on the Layer 3 switch) as the gateway IP address, 2.2.3.0/24 as the subnet for dynamic allocation, and 8.8.8.8 as the DNS server address, and then exclude 2.2.3.100 and 2.2.3.1 from dynamic allocation.**

```
[DHCP Server] dhcp server ip-pool vlan300
[DHCP Server-dhcp-pool-vlan300] gateway-list 2.2.3.100
[DHCP Server-dhcp-pool-vlan300] network 2.2.3.0 mask 255.255.255.0
[DHCP Server-dhcp-pool-vlan300] dns-list 8.8.8.8
[DHCP Server-dhcp-pool-vlan300] forbidden-ip 2.2.3.100 2.2.3.1
```

## Configuring the RADIUS server

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

The INC server configuration is the same for central AC 1 and central AC 2, except for the AC IP address. This section configures central AC 1 as an example. Refer to central AC 1 configuration when you configure central AC 2 and remember to change the IP address setting for central AC 2.

1. Add central AC 1 as an access device.

- a. Log in to INC and click the **User** tab.
- b. From the navigation pane, select **User Access Policy > Access Device Management > Access Device**.
- c. Click **Add**.
- d. In the **Device List** area, click **Add Manually** to open the **Add Access Device Manually** page. Enter **2.2.1.1** in the **Start IP** field and then click **OK**.
- e. In the **Access Configuration** area, set the shared key to **123456**, which must be the same as that configured on the AC.
- f. Use the default settings for other parameters.
- g. Click **OK**.

**Figure 2 Adding central AC 1 as an access device**

**Access Configuration**

|                            |                                                                 |                      |           |
|----------------------------|-----------------------------------------------------------------|----------------------|-----------|
| Authentication Port *      | 1812                                                            | Accounting Port *    | 1813      |
| Service Type               | LAN Access Service                                              | Service Group        | Ungrouped |
| Access Device Type         | H3C(General)                                                    | Confirm Shared Key * |           |
| Shared Key *               | *****                                                           |                      |           |
| Access Device Group        | --                                                              |                      |           |
| Certificate Authentication | <input checked="" type="radio"/> None <input type="radio"/> EAP |                      |           |
| Certificate Type           | EAP-TLS Auth                                                    |                      |           |

**Device List**

Select Add Manually Clear All

| Device Name | Device IP | Device Model | Comments | Delete |
|-------------|-----------|--------------|----------|--------|
|             | 2.2.1.1   |              |          |        |

Total Items: 1.

OK Cancel

2. Add an access policy.
  - a. From the navigation pane, select **User Access Policy > Access Policy**.
  - b. Click **Add**.
  - c. Enter the access policy name.
  - d. Select the **Ungrouped** service group.
  - e. Use the default settings for other parameters.

**Figure 3 Adding an access policy**

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

---

**Basic Information**

Access Policy Name \*

Service Group \*

Description

---

**Authorization Information**

Access Period

Downstream Rate(Kbps)

Priority

Certificate Authentication ☒ None ☐ EAP

Certificate Type

Deploy VLAN

☐ Deploy User Profile

☐ Deploy ACL

Allocate IP \*

Upstream Rate(Kbps)

☐ RSA Authentication

Deploy User Group  ?

3. Add an access service.
  - a. From the navigation pane, select **User Access Policy > Access Service**.
  - b. Click **Add**.
  - c. Enter the service name.
  - d. Select **AccessPolicy**.
  - e. Use the default settings for other parameters.
  - f. Click **OK**.

**Figure 4 Adding an access service**

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

---

**Basic Information**

Service Name \*

Service Group \*

Default Proprietary Attribute Assignment Policy \*  ?

Default Max. Number of Bound Endpoints \*

Description

☒ Available ?

Service Suffix

Default Access Policy \*  ?

Default Max. Number of Online Endpoints \*

☐ Transparent Authentication on Portal Endpoints ?

---

**Access Scenario List**

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

4. Add an access user.
  - a. From the navigation pane, select **Access User > All Access Users**.
  - b. Click **Add**.
  - c. Select an existing access user or click **Add User** to add a new access user.

- d. In the Access Service area, select **RadiusServer** from the list.
- e. Set the password.
- f. Use the default settings for other parameters.
- g. Click **OK**.

**Figure 5 Adding an access user**

The screenshot shows two windows from a network management interface. The top window, titled 'Access Information', contains fields for 'User Name' (client1), 'Account Name' (client), 'Password', and 'Confirm Password'. It also has checkboxes for 'Tidal Account', 'Default BYOD User', 'MAC Authentication User', 'Computer User', 'Fast Access User', 'Allow User to Change Password', 'Enable Password Strategy', and 'Modify Password at Next Login'. The bottom window, titled 'Access Service', displays a table with columns 'Service Name', 'Service Suffix', 'Status', and 'Allocate IP'. The 'RadiusServer' service is listed with a status of 'Available' and is selected with a checkbox.

## Configuring the portal server

1. Configure the portal authentication service:
  - a. From the navigation pane, select **User Access Policy > Portal Service > Server**.
  - b. Configure the portal server parameters as needed.  
This example uses the default settings.
  - c. Click **OK**.

**Figure 6 Configuring the portal server**

The screenshot shows the 'Portal Server' configuration page. The breadcrumb navigation at the top reads 'User > User Access Policy > Portal Service > Server'. The page is divided into three main sections: 'Basic Information' with a 'Log Level' dropdown set to 'Info'; 'Portal Server' with fields for 'Request Timeout(Seconds)' (4), 'User Heartbeat Interval(Minutes)' (5), 'Server Heartbeat Interval(Seconds)' (20), and 'LB Device Address'; and 'Portal Web' with fields for 'Request Timeout(Seconds)' (15), 'Verify Endpoint Requests' (Yes), 'HTTP Heartbeat Display' (New Page), 'Packet Code', 'Use Cache' (Yes), 'HTTPS Heartbeat Display' (Original Page), and a 'Portal Page' text area containing the URL 'http://192.168.0.111:8080/portal/'. A small IP address '192.168.0.111' is visible in the bottom right corner.

2. Configure an IP address group:
  - a. From the navigation pane, select **User Access Policy > Portal Service > IP Group**.
  - b. Click **Add**.
  - c. Enter the IP group name.



- d. Enter the start IP address and end IP address of the IP group.  
Make sure the client IP address is in the IP group.
- e. Select a service group.  
This example uses the default group **Ungrouped**.
- f. Select **Normal** from the **Action** list.
- g. Click **OK**.

**Figure 7 Adding an IP address group**

The screenshot shows the 'Add IP Group' form within the 'User > User Access Policy > Portal Service > IP Group' navigation path. The form contains the following fields:

- IP Group Name \***: Portal.user
- Start IP \***: 2.2.3.1
- End IP \***: 2.2.3.255
- Service Group**: Ungrouped (dropdown menu)
- Action \***: Normal (dropdown menu)

At the bottom right, there are **OK** and **Cancel** buttons.

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

**Figure 8 Adding a portal device**

The screenshot shows the 'Add Device' form within the 'User Access Policy > Portal Service' navigation path. The form is titled 'Device Information' and contains the following fields:

- Device Name \***: NAS
- Version \***: CMCC 1.0 (dropdown menu)
- Listening Port \***: 2000
- Authentication Retries \***: 0
- Support Server Heartbeat \***: No (dropdown menu)
- Key \***: \*\*\*\*\*
- Access Method \***: Directly Connected (dropdown menu)
- Device Description**: (empty text area)
- Service Group \***: Ungrouped (dropdown menu)
- IP Address \***: 2.2.1.1
- Local Challenge \***: No (dropdown menu)
- Logout Retries \***: 1
- Support User Heartbeat \***: No (dropdown menu)
- Confirm Key \***: \*\*\*\*\*

At the bottom right, there are **OK** and **Cancel** buttons.

4. Associate the portal device with the IP address group:

- a. Click the **Port Group** icon in the **Operation** field of device **NAS**.

**Figure 9 Device list**

The screenshot shows the 'Query Devices' interface. At the top, there are search filters for Device Name, Version, Deploy Result, and Service Group. Below the filters is a table with the following data:

| Device Name | Version  | Service Group | IP Address | Last Deployed at | Deploy Result | Operation         |
|-------------|----------|---------------|------------|------------------|---------------|-------------------|
| NAS         | CMCC 1.0 | Ungrouped     | 2.2.1.1    |                  | Not Deployed  | [Port Group Icon] |

At the bottom, there is a pagination bar showing '1-1 of 1, Page 1 of 1' and a table size selector set to '50'.

- b. Click **Add**.
- c. Enter the port group name.
- d. Select the configured IP address group.  
The IP address used by the user to access the network must be within this IP address group.
- e. Use the default settings for other parameters.
- f. Click **OK**.

**Figure 10 Adding a port group**

The screenshot shows the 'Add Port Group' configuration window. It contains the following fields and settings:

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

At the bottom right, there are 'OK' and 'Cancel' buttons.

## Verifying the configuration

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

# Display information about all portal users.

```
[Central-AC1] display portal user all
Total portal users: 1
Username: client
 AP name: ap1
 Radio ID: 1
 SSID: service
```

```

Portal server: newpt
State: Online
VPN instance: N/A
MAC IP VLAN Interface
0021-6330-0933 2.2.3.143 300 WLAN-BSS1/0/4
Authorization information:
 DHCP IP pool: vlan300
 User profile: N/A
 Session group profile: N/A
 ACL number: N/A
 Inbound CAR: N/A
 Outbound CAR: N/A

```

## Configuration files

- Layer 3 switch:

```

#
Vlan 2
#
vlan 100
#
vlan 200
#
vlan 300
#
interface Vlan-interface2
 ip address 192.168.0.100 255.255.255.0
#
interface Vlan-interface100
 ip address 2.2.1.100 255.255.255.0
#
interface Vlan-interface200
 ip address 2.2.2.100 255.255.255.0
#
interface Vlan-interface300
 ip address 2.2.3.100 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 1 100
#
interface GigabitEthernet1/0/2
 port link-type trunk
 port trunk permit vlan 1 200 300
#
interface GigabitEthernet1/0/3
 port link-type trunk
 port trunk permit vlan 1 100

```

```

#
• Central AC 1:
#
vlan 100
#
wlan service-template st1
 ssid service
client forwarding-location ap
client-security authentication-location central-ac
akm mode psk
preshared-key pass-phrase cipher c3$oLf6pOZ6bxrf25nodjOJKYEfnZ6g6ErccHyQ
cipher-suite ccmp
security-ie rsn
portal enable method direct
portal domain iNC
portal bas-ip 2.2.1.1
portal apply web-server newpt
service-template enable
#
interface Vlan-interface100
 ip address 2.2.1.1 255.255.255.0
#
interface gigabitethernet 1/0/1
 port link-type trunk
 port trunk permit vlan 1 100
#
ip route-static 0.0.0.0 24 2.2.1.100
#
radius session-control enable
#
radius scheme iNC
 primary authentication 192.168.0.111
 primary accounting 192.168.0.111
 key authentication cipher c3$inPh3pDjv+jZhbhAmYd7sPQMF8bJX0VmvA==
 key accounting cipher c3$lZDbA3Qutvq0fWYBaI4ESvGfDW2uBOfF1A==
 user-name-format without-domain
 nas-ip 2.2.1.1
#
domain iNC
 authorization-attribute idle-cut 15 1024
 authentication lan-access radius-scheme iNC
 authorization lan-access radius-scheme iNC
 accounting lan-access radius-scheme iNC
#
portal free-rule 0 destination ip 192.168.0.0 255.255.255.0
portal free-rule 1 destination ip any udp 53
portal free-rule 2 destination ip any tcp 53
#

```

```

portal web-server newpt
url http://192.168.0.111:8080/portal
server-type cmcc
url-parameter nasip value 2.2.1.1
url-parameter ssid ssid
url-parameter wlanacname value Central-AC1
url-parameter wlanuserip source-address
#
portal server newpt
ip 192.168.0.111 key cipher c3$8MR9sJDNDI9wpjox6qMBHOLQcTV1Y7f9
server-type cmcc
#
wlan ap-group group1
backup-ac ip 2.2.1.2
control-address enable
control-address ip 2.2.2.1
switch-back enable
ap ap1
ap-model AP 3620
map-configuration cfa0:/map.txt
radio 1
radio enable
service-template st1 vlan 300
radio 2
#
wlan ap ap1 model AP 3620
serial-id 219801A28N819CE0002T
#
wlan local-ac name 3510 model WX3510H
serial-id 210235A1JNB165000120
priority 7
wlan tunnel-preempt enable
#
• Central AC 2:
#
vlan 100
#
wlan service-template st1
ssid service
client forwarding-location ap
client-security authentication-location central-ac
akm mode psk
preshared-key pass-phrase cipher c3$oLf6pOZ6bxrf25nodjOJKYEfnZ6g6ErccHyQ
cipher-suite ccmp
security-ie rsn
portal enable method direct
portal domain iNC
portal bas-ip 2.2.1.2

```

```

portal apply web-server newpt
service-template enable
#
interface Vlan-interface100
ip address 2.2.1.2 255.255.255.0
#
interface gigabitethernet 1/0/1
port link-type trunk
port trunk permit vlan 1 100
#
ip route-static 0.0.0.0 24 2.2.1.100
#
radius session-control enable
#
radius scheme iNC
primary authentication 192.168.0.111
primary accounting 192.168.0.111
key authentication cipher c3$inPh3pDjv+jZhbhAmYd7sPQMF8bJX0VmvA==
key accounting cipher c3$lZDbA3Qutvq0fWYBaI4ESvGfDW2uBOfF1A==
user-name-format without-domain
nas-ip 2.2.1.2
#
domain iNC
authorization-attribute idle-cut 15 1024
authentication lan-access radius-scheme iNC
authorization lan-access radius-scheme iNC
accounting lan-access radius-scheme iNC
#
portal free-rule 0 destination ip 192.168.0.0 255.255.255.0
portal free-rule 1 destination ip any udp 53
portal free-rule 2 destination ip any tcp 53
#
portal web-server newpt
url http://192.168.0.111:8080/portal
server-type cmcc
url-parameter nasip value 2.2.1.2
url-parameter ssid ssid
url-parameter wlanacname value Central-AC2
url-parameter wlanuserip source-address
#
portal server newpt
ip 192.168.0.111 key cipher c3$8MR9sJDNDI9wpjox6qMBHOLQcTVlY7f9
server-type cmcc
#
wlan ap-group group1
backup-ac ip 2.2.1.1
control-address enable
control-address ip 2.2.2.1

```

```

switch-back enable
ap ap1
ap-model AP 3620
map-configuration cfa0:/map.txt
radio 1
 radio enable
 service-template st1 vlan 300
radio 2
#
wlan ap ap1 model AP 3620
 serial-id 219801A28N819CE0002T
#
wlan local-ac name 3510 model WX3510H
 serial-id 210235A1JNB165000120
 priority 6
 wlan tunnel-preempt enable
#

```

- **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
#
interface GigabitEthernet1/0/2
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 200 300
 port trunk pvid vlan 200
 poe enable
#
interface GigabitEthernet1/0/3
 port link-type trunk
 port trunk permit vlan 1 100 200
#
interface GigabitEthernet1/0/4
 port link-type trunk
 port trunk permit vlan 1 200 300
#

```

- **DHCP server:**

```

#
dhcp enable
#

```

```

vlan 200
#
vlan 300
#
dhcp server ip-pool vlan200
 gateway-list 2.2.2.100
 network 2.2.2.0 mask 255.255.255.0
 forbidden-ip 2.2.2.1
 forbidden-ip 2.2.2.100
option 43 hex 800b0000010202010102020102
#
dhcp server ip-pool vlan300
 gateway-list 2.2.3.100
network 2.2.3.0 mask 255.255.255.0
 dns-list 8.8.8.8
 forbidden-ip 2.2.3.1
 forbidden-ip 2.2.3.100
#
interface Vlan-interface200
 ip address 2.2.2.200 255.255.255.0
#
interface Vlan-interface300
 ip address 2.2.3.200 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 1 200 300
#

```

- **Local AC:**

```

#
vlan 100
#
vlan 200
#
vlan 300
#
interface Vlan-interface100
 ip address 2.2.1.10 255.255.255.0
#
interface Vlan-interface200
 ip address 2.2.2.1 255.255.255.0
#
interface Vlan-interface300
 ip address 2.2.3.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 1 100 200

```



```
#
wlan local-ac enable
#
wlan local-ac capwap source-vlan 100
#
wlan central-ac ip 2.2.1.1
wlan central-ac ip 2.2.1.2
#
```

## Related documentation

- *High Availability Command Reference in INTELBRAS Access Controllers Command References*
- *High Availability 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

## OAuth-Based Portal MAC-trigger Authentication on a Local-Forwarding Dual-Link Backup Network 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 OAuth-based portal MAC-trigger authentication on a local-forwarding dual-link backup network ..... | 1  |
| Network configuration .....                                                                                             | 1  |
| Analysis .....                                                                                                          | 2  |
| Restrictions and guidelines .....                                                                                       | 2  |
| Procedures .....                                                                                                        | 3  |
| Editing the AP configuration file .....                                                                                 | 3  |
| Configuring AC 1 .....                                                                                                  | 3  |
| Configuring AC 2 .....                                                                                                  | 6  |
| Configuring the switch .....                                                                                            | 10 |
| Configuring the DHCP server .....                                                                                       | 11 |
| Configuring the INC server .....                                                                                        | 12 |
| Verifying the configuration .....                                                                                       | 16 |
| Configuration files .....                                                                                               | 20 |
| Related documentation .....                                                                                             | 24 |

# Introduction

The following information provides an example of configuring OAuth-based portal MAC-trigger authentication on a local-forwarding dual-link backup 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 WLAN high availability, AAA, portal MAC-trigger authentication, and WLAN access.

## Example: Configuring OAuth-based portal MAC-trigger authentication on a local-forwarding dual-link backup network

### Network configuration

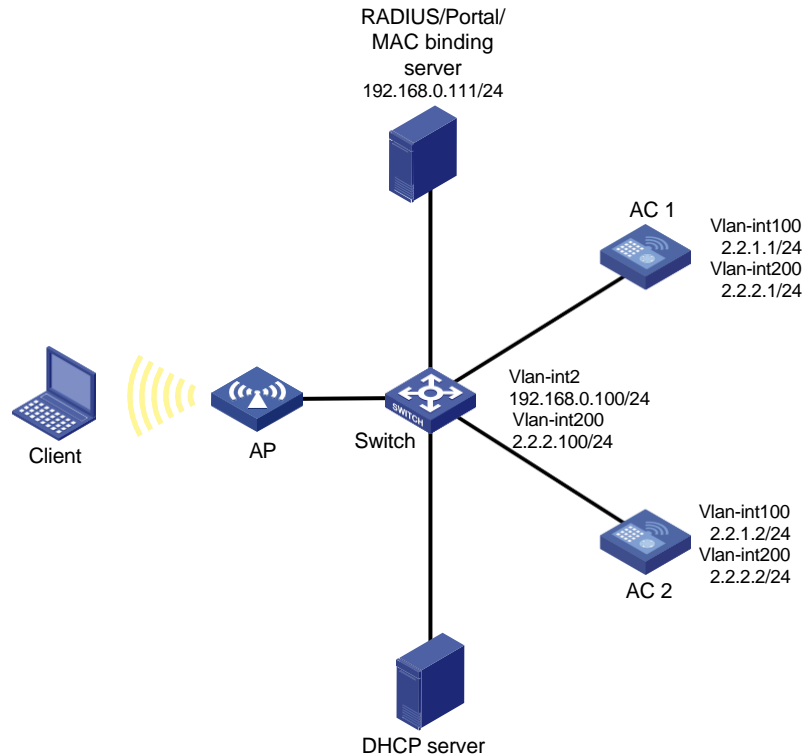
As shown in [Figure 1](#):

- The AP and the client obtain IP addresses from the DHCP server.
- The network deploys an INC server as the portal authentication server, portal Web server, MAC binding server, and RADIUS server.

Configure the devices to meet the following requirements:

- The ACs operate in active/standby mode. When AC 1 (the master AC) fails, the AP associates with AC 2 (the backup AC). When AC 1 recovers, the AP re-associates with AC 1.
- The ACs use a service template to provide OAuth-based portal MAC-trigger authentication for the client. Before passing the authentication, the client can access only the portal Web server. After passing the authentication, the client can access other network resources. If the client goes offline and then attempts to come online again, the client does not need to enter the username and password.
- The AP forwards the client traffic locally.
- The client can access network resources through any Layer 2 ports in its access VLAN without re-authentication.
- The RADIUS server can dynamically change user authorization information or forcibly disconnect users.

**Figure 1 Network diagram**



## Analysis

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

In local forwarding mode, to ensure that valid clients can perform portal authentication, enable validity check on wireless clients.

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

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

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

For dual-link backup to operate correctly, configure a manual AP or auto AP on the ACs. Make sure that the AP can establish CAPWAP tunnels with each of the ACs.

To implement MAC-trigger authentication by using the OAuth protocol, enable cloud MAC-trigger authentication by using the **cloud-binding enable** command.

## Restrictions and guidelines

Make sure the master and backup ACs have the same portal authentication configuration. The following items in the portal authentication can be different on the master and backup ACs:

- The portal Web server configuration.
- The BAS-IP attribute for portal packets sent to the portal authentication server.

- The specified interface of the AC for portal client access during portal authentication.

If you configure a manual AP on the ACs, make sure the AP name, serial ID, and MAC address of the manual AP are the same on the ACs.

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

Some endpoints by default use random MAC addresses. For transparent MAC authentication to take effect on such an endpoint, disable the endpoint from using a random MAC address.

You must upload the configuration file of the AP to both the master and backup ACs.

## Procedures

### Editing the AP configuration file

# Use a text editor to edit the AP's configuration file. Name the configuration file **map.txt**, and then upload the file to the storage medium of the ACs.

The content of the configuration file is as follows:

```
system-view
vlan 200
interface gigabitethernet1/0/1
port link-type trunk
port trunk permit vlan 200
```

### Configuring AC 1

#### 1. Configure interfaces:

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

```
<AC1> system-view
[AC1] vlan 100
[AC1-vlan100] quit
[AC1] interface vlan-interface 100
[AC1-Vlan-interface100] ip address 2.2.1.1 24
[AC1-Vlan-interface100] quit
```

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

```
[AC1] vlan 200
[AC1-vlan200] quit
[AC1] interface vlan-interface 200
[AC1-Vlan-interface200] ip address 2.2.2.1 24
[AC1-Vlan-interface200] quit
```

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

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

#### 2. Configure a static route:

- # Configure a static route to the INC server.
- ```
[AC1] ip route-static 192.168.0.0 255.255.0.0 2.2.2.100
```
3. Configure the DNS server. (Details not shown.)
 4. Configure the wireless service:
 - # Create a service template named **st1**.

```
[AC1] wlan service-template st1
```

 - # Set the SSID of the service template.

```
[AC1-wlan-st-st1] ssid service
```

 - # Specify VLAN 200 for the service template.

```
[AC1-wlan-st-st1] vlan 200
```

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

```
[AC1-wlan-st-st1] akm mode psk
```

```
[AC1-wlan-st-st1] preshared-key pass-phrase simple 12345678
```

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

```
[AC1-wlan-st-st1] cipher-suite ccmp
```

```
[AC1-wlan-st-st1] security-ie rsn
```

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

```
[AC1-wlan-st-st1] client forwarding-location ap
```

```
[AC1-wlan-st-st1] quit
```
 5. Configure the AP:

NOTE:

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

Create an AP named **office** with model **AP 3620**, and then specify the serial ID of the AP.

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

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

```
[AC1-wlan-ap-office] quit
```

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

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

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

Set the AP connection priority to 7.

```
[AC1-wlan-ap-group-group1] priority 7
```

Specify AC 2 as the backup AC for AC 1. Set the backup AC address as the IP address of VLAN-interface 100 on AC 2.

```
[AC1-wlan-ap-group-group1] backup-ac ip 2.2.1.2
```

Enable master CAPWAP tunnel preemption.

```
[AC1-wlan-ap-group-group1] wlan tunnel-preempt enable
```

Deploy configuration file **map.txt** to the AP.

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

```
[AC1-wlan-ap-group-group1-ap-model-AP 3620] map-configuration map.txt
```

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

```
[AC1-wlan-ap-group-group1-ap-model-AP 3620] radio 2
```

```
[AC1-wlan-ap-group-group1-ap-model-AP 3620-radio-2] service-template st1
```

Enable radio 2.

```
[AC1-wlan-ap-group-group1-ap-model-AP 3620-radio-2] radio
```

```
enable [AC1-wlan-ap-group-group1-ap-model-AP 3620-radio-2] quit
```

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

6. Configure portal authentication:

Create an ISP domain named dm1.

```
[AC1] domain dm1
```

Configure the AC not to perform AAA on portal users.

```
[AC1-isp-dm1] authentication portal none
[AC1-isp-dm1] authorization portal none
[AC1-isp-dm1] accounting portal none
[AC1-isp-dm1] quit
```

Create a portal Web server named newpt, specify http://192.168.0.111:8080/INC - WSMAuth/protocol as the server's URL, and then configure the server type as OAuth. (Make sure the server's URL is the same as the URL of the actual portal Web server.)

```
[AC1] portal web-server newpt
[AC1-portal-websvr-newpt] url http://192.168.0.111:8080/INC -
WSMAuth/protocol [AC1-portal-websvr-newpt] server-type oauth
```

Enable the optimized captive-bypass feature for iOS users.

```
[AC1-portal-websvr-newpt] captive-bypass ios optimize enable
[AC1-portal-websvr-newpt] quit
```

Create an HTTP-based local portal Web service.

```
[AC1] portal local-web-server http
[AC1-portal-local-websvr-http] quit
```

Configure destination-based portal-free rules 2 and 3 to allow portal users to access the DNS server without authentication.

```
[AC1] portal free-rule 2 destination ip any udp 53
[AC1] portal free-rule 3 destination ip any tcp 53
```

Configure the safe-redirect feature to reduce the redirect workload on the portal server.

```
[AC1] portal safe-redirect enable
[AC1] portal safe-redirect method get post
[AC1] portal safe-redirect user-agent CaptiveNetworkSupport
[AC1] portal safe-redirect user-agent MicroMessenger
[AC1] portal safe-redirect user-agent Mozilla
[AC1] portal safe-redirect user-agent WeChat
[AC1] portal safe-redirect user-agent iPhone
[AC1] portal safe-redirect user-agent micromessenger
```

Specify VLAN-interface 200 as the interface for portal clients to access the AC during portal authentication.

```
[AC1] portal client-gateway interface vlan-interface 200
```

Set the NAS ID. (Make sure the NAS ID is the same as that in the configuration file INC\client\conf\wportal\conf.properties.)

```
[AC1] wlan global-configuration
[AC1-wlan-global-configuration] nas-id wportal
[AC1-wlan-global-configuration] quit
```

Set the user synchronization interval to 60 seconds for portal authentication using OAuth.

```
[AC1] portal oauth user-sync interval 60
```

Configure destination-based portal-free rules to allow users to access the portal Web server, AC 1, and AC 2 without authentication.


```

[AC1] portal free-rule 0 destination ip 192.168.0.111 32
[AC1] portal free-rule 1 destination ip 2.2.2.1 32
[AC1] portal free-rule 4 destination ip 2.2.2.2 32
# Enable roaming for portal users.
[AC1] portal roaming enable
# Disable the Rule ARP entry feature.
[AC1] undo portal refresh arp enable
# Enable the RADIUS session-control feature.
[AC1] radius session-control enable
# Enable validity check on wireless portal clients.
[AC1] portal host-check enable
# Enable direct portal authentication on service template st1.
[AC1] wlan service-template st1
[AC1-wlan-st-st1] portal enable method direct
# Specify ISP domain dm1 as the portal authentication domain.
[AC1-wlan-st-st1] portal domain dm1
# Specify portal Web server newpt on service template st1.
[AC1-wlan-st-st1] portal apply web-server newpt
# Enable portal temporary pass and set the temporary pass period to 300 seconds on service
template st1.
[AC1-wlan-st-st1] portal temp-pass period 300 enable
# Configure the BAS-IP as 2.2.2.1 for portal packets sent from service template st1 to the portal
authentication server.
[AC1-wlan-st-st1] portal bas-ip 2.2.2.1
[AC1-wlan-st-st1] quit
7. Configure MAC-trigger authentication:
# Create a MAC binding server named mts.
[AC1] portal mac-trigger-server mts
# Specify 192.168.0.111 as the IP address of the MAC binding server.
[AC1-portal-mac-trigger-server-mts] ip 192.168.0.111
# Enable cloud MAC-trigger authentication (using OAuth for authentication).
[AC1-portal-mac-trigger-server-mts] cloud-binding enable
[AC1-portal-mac-trigger-server-mts] quit
# Specify MAC binding server mts on service template st1.
[AC1] wlan service-template st1
[AC1-wlan-st-st1] portal apply mac-trigger-server mts
# Enable service template st1.
[AC1-wlan-st-st1] service-template enable
[AC1-wlan-st-st1] quit

```

Configuring AC 2

1. Configure interfaces:

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

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

```
[AC2] vlan 100
[AC2-vlan100] quit
[AC2] interface vlan-interface 100
[AC2-Vlan-interface100] ip address 2.2.1.2 24
[AC2-Vlan-interface100] quit
```

Create VLAN 200, create VLAN-interface 200, and then assign the VLAN interface an IP address. This VLAN will be used for wireless client access.

```
[AC2] vlan 200
[AC2-vlan200] quit
[AC2] interface vlan-interface 200
[AC2-Vlan-interface200] ip address 2.2.2.2 24
[AC2-Vlan-interface200] quit
```

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

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

2. Configure a static route:

Configure a static route to the INC server.

```
[AC2] ip route-static 192.168.0.0 255.255.0.0 2.2.2.100
```

3. Configure the DNS server. (Details not shown.)

4. Configure the wireless service:

Create a service template named **st1**.

```
[AC2] wlan service-template st1
```

Set the SSID of the service template.

```
[AC2-wlan-st-st1] ssid service
```

Specify VLAN 200 for the service template.

```
[AC2-wlan-st-st1] vlan 200
```

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

```
[AC2-wlan-st-st1] akm mode psk
```

```
[AC2-wlan-st-st1] preshared-key pass-phrase simple 12345678
```

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

```
[AC2-wlan-st-st1] cipher-suite ccmp
```

```
[AC2-wlan-st-st1] security-ie rsn
```

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

```
[AC2-wlan-st-st1] client forwarding-location ap
```

```
[AC2-wlan-st-st1] quit
```

5. Configure the AP:

NOTE:

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

Create an AP named **office** with model **AP 3620**, and then specify the serial ID of the AP.

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

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

```
[AC2-wlan-ap-office] quit
```

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

```
[AC2] wlan ap-group group1
[AC2-wlan-ap-group-group1] ap office
```

Set the AP connection priority to 6.

```
[AC2-wlan-ap-group-group1] priority 6
```

Specify AC 1 as the backup AC for AC 2. Set the backup AC address as the IP address of VLAN-interface 100 on AC 1.

```
[AC2-wlan-ap-group-group1] backup-ac ip 2.2.1.1
```

Enable master CAPWAP tunnel preemption.

```
[AC2-wlan-ap-group-group1] wlan tunnel-preempt enable
```

Deploy configuration file **map.txt** to the AP.

```
[AC2-wlan-ap-group-group1] ap-model AP 3620
[AC2-wlan-ap-group-group1-ap-model-AP 3620] map-configuration map.txt
```

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

```
[AC2-wlan-ap-group-group1-ap-model-AP 3620] radio 2
[AC2-wlan-ap-group-group1-ap-model-AP 3620-radio-2] service-template st1
```

Enable radio 2.

```
[AC2-wlan-ap-group-group1-ap-model-AP 3620-radio-2] radio
enable [AC2-wlan-ap-group-group1-ap-model-AP 3620-radio-2] quit
[AC2-wlan-ap-group-group1-ap-model-AP 3620]
quit [AC2-wlan-ap-group-group1] quit
```

6. Configure portal authentication:

Create an ISP domain named **dm1**.

```
[AC2] domain dm1
```

Configure the AC not to perform AAA on portal users.

```
[AC2-isp-dm1] authentication portal none
[AC2-isp-dm1] authorization portal none
[AC2-isp-dm1] accounting portal none
[AC2-isp-dm1] quit
```

Create a portal Web server named **newpt**, specify **http://192.168.0.111:8080/INC - WSMAuth/protocol** as the server's URL, and configure the server type as OAuth. (Make sure the server's URL is the same as the URL of the actual portal Web server.)

```
[AC2] portal web-server newpt
[AC2-portal-websvr-newpt] url http://192.168.0.111:8080/INC -
WSMAuth/protocol [AC2-portal-websvr-newpt] server-type oauth
```

Enable the optimized captive-bypass feature for iOS users.

```
[AC2-portal-websvr-newpt] captive-bypass ios optimize enable
[AC2-portal-websvr-newpt] quit
```

Create an HTTP-based local portal Web service and enter its view.

```
[AC2] portal local-web-server http
[AC2-portal-local-websvr-http] quit
```

Configure destination-based portal-free rules 2 and 3 to allow portal users to access the DNS server without authentication.

```
[AC2] portal free-rule 2 destination ip any udp 53
[AC2] portal free-rule 3 destination ip any tcp 53
```

Configure the safe-redirect feature to reduce the redirect workload on the portal server.

```
[AC2] portal safe-redirect enable
```

```
[AC2] portal safe-redirect method get post
[AC2] portal safe-redirect user-agent CaptiveNetworkSupport
[AC2] portal safe-redirect user-agent MicroMessenger
[AC2] portal safe-redirect user-agent Mozilla
[AC2] portal safe-redirect user-agent WeChat
[AC2] portal safe-redirect user-agent iPhone
[AC2] portal safe-redirect user-agent micromessenger
```

Specify VLAN-interface 200 as the interface for portal clients to access the AC during portal authentication.

```
[AC2] portal client-gateway interface vlan-interface 200
```

Set the NAS ID. (Make sure the NAS ID is the same as that in the configuration file `INC\client\conf\wportal\conf.properties`.)

```
[AC2] wlan global-configuration
[AC2-wlan-global-configuration] nas-id wportal
[AC2-wlan-global-configuration] quit
```

Set the user synchronization interval to 60 seconds for portal authentication using OAuth.

```
[AC2] portal oauth user-sync interval 60
```

Configure destination-based portal-free rules to allow users to access the portal Web server, AC 1, and AC 2 without authentication.

```
[AC2] portal free-rule 0 destination ip 192.168.0.111 32
[AC2] portal free-rule 1 destination ip 2.2.2.1 32
[AC2] portal free-rule 4 destination ip 2.2.2.2 32
```

Enable roaming for portal users.

```
[AC2] portal roaming enable
```

Disable the Rule ARP entry feature.

```
[AC2] undo portal refresh arp enable
```

Enable validity check on wireless portal clients.

```
[AC2] portal host-check enable
```

Enable the RADIUS session-control feature.

```
[AC2] radius session-control enable
```

Enable direct portal authentication on service template `st1`.

```
[AC2] wlan service-template st1
[AC2-wlan-st-st1] portal enable method direct
```

Specify ISP domain `dm1` as the portal authentication domain.

```
[AC2-wlan-st-st1] portal domain dm1
```

Specify portal Web server `newpt` on service template `st1`.

```
[AC2-wlan-st-st1] portal apply web-server newpt
```

Enable portal temporary pass and set the temporary pass period to 300 seconds on service template `st1`.

```
[AC2-wlan-st-st1] portal temp-pass period 300 enable
```

Configure the BAS-IP as 2.2.2.2 for portal packets sent from service template `st1` to the portal authentication server.

```
[AC2-wlan-st-st1] portal bas-ip 2.2.2.2
[AC2-wlan-st-st1] quit
```

7. Configure MAC-trigger authentication:

Create a MAC binding server named `mts`.

```
[AC2] portal mac-trigger-server mts
```

Specify 192.168.0.111 as the IP address of the MAC binding server.

```
[AC2-portal-mac-trigger-server-mts] ip 192.168.0.111
# Enable cloud MAC-trigger authentication (using OAuth for authentication).
[AC2-portal-mac-trigger-server-mts] cloud-binding enable
[AC2-portal-mac-trigger-server-mts] quit
# Specify MAC binding server mts on service template st1.
[AC2] wlan service-template st1
[AC2-wlan-st-st1] portal apply mac-trigger-server mts
# Enable service template st1.
[AC2-wlan-st-st1] service-template enable
[AC2-wlan-st-st1] quit
```

Configuring the switch

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

Create VLAN 2. The switch will use this VLAN to communicate with the INC server.

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

Assign the port that connects the switch to the INC server to VLAN 2. (Details not shown.)

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

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

Configure GigabitEthernet 1/0/4 (the port connected to AC 2) as a trunk port, and assign the port to VLAN 100 and VLAN 200.

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

Configure GigabitEthernet 1/0/2 (the port connected to the AP) as a trunk port, set the PVID to 100, and assign the port to VLAN 100 and VLAN 200.

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

Enable PoE on GigabitEthernet 1/0/2.

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

Configure GigabitEthernet 1/0/3 (the port connected to the DHCP server) as a trunk port, set the PVID to 100, and assign the port to VLAN 100 and VLAN 200.

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

Assign an IP address to VLAN-interface 200.

```
[Switch] interface vlan-interface 200
[Switch-Vlan-interface200] ip address 2.2.2.100 255.255.255.0
[Switch-Vlan-interface200] quit
```

Assign an IP address to the VLAN-interface 2.

```
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] ip address 192.168.0.100 255.255.255.0
[Switch-Vlan-interface2] quit
```

Configuring the DHCP server

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

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

Assign an IP address to VLAN-interface 100.

```
[DHCP] interface vlan-interface 100
[DHCP-Vlan-interface100] ip address 2.2.1.200 255.255.255.0
[DHCP-Vlan-interface100] quit
```

Assign an IP address to VLAN-interface 200.

```
[DHCP] interface vlan-interface 200
[DHCP-Vlan-interface200] ip address 2.2.2.200 255.255.255.0
[DHCP-Vlan-interface200] quit
```

Enable the DHCP service.

```
[DHCP] dhcp enable
```

Configure DHCP address pool **VLAN100**. In the address pool, specify 2.2.1.200 as the gateway IP address and 2.2.1.0/24 as the subnet for dynamic allocation, and then exclude IP addresses 2.2.1.1 and 2.2.1.2 from dynamic allocation.

```
[DHCP] dhcp server ip-pool VLAN100
[DHCP-dhcp-pool-vlan100] gateway-list 2.2.1.200
[DHCP-dhcp-pool-vlan100] network 2.2.1.0 mask 255.255.255.0
[DHCP-dhcp-pool-vlan100] forbidden-ip 2.2.1.1 2.2.1.2
[DHCP-dhcp-pool-vlan100] quit
```

Configure DHCP address pool **VLAN200**. In the address pool, specify 2.2.2.100 as the gateway IP address and 2.2.2.0/24 as the subnet for dynamic allocation, and 8.8.8.8 as the DNS server address, and then exclude IP addresses 2.2.2.100, 2.2.2.1, and 2.2.2.2 from dynamic allocation.

```
[DHCP] dhcp server ip-pool VLAN200
[DHCP-dhcp-pool-vlan200] gateway-list 2.2.2.100
[DHCP-dhcp-pool-vlan200] network 2.2.2.0 mask 255.255.255.0
[DHCP-dhcp-pool-vlan200] dns-list 8.8.8.8
[DHCP-dhcp-pool-vlan200] forbidden-ip 2.2.2.100 2.2.2.1 2.2.2.2
```

[DHCP-dhcp-pool-vlan200] quit

Configuring the INC server

In this example, the INC server runs INC PLAT 7.3 (E0605) and INC IPM 7.3 (E0516).

The INC server configuration is the same for AC 1 and AC 2, except for the AC IP address. This section configures AC 1 as an example. Refer to AC 1 configuration when you configure AC 2 and remember to change the IP address setting for AC 2.

1. Add an access user:
 - a. Log in to INC and click the **Service** tab.
 - b. From the navigation tree, select **Intelligent Portal Management > User Management > Users**.
 - c. Click **Add** to open the **Add User** page.
 - d. Enter username **client** and password **admin@123**.
 - e. Use the default settings for other parameters.
 - f. Click **OK**.

Figure 2 Adding an access user

The screenshot shows the 'Add User' configuration page. The form includes the following fields and values:

- Username: client
- User Group: Ungrouped
- User Password: [masked]
- Confirm Password: [masked]
- Identity Number: [empty]
- Telephone Number: [empty]
- Set Online User Count: By User Group
- Start Time: [empty]
- End Time: [empty]
- Remark: [empty]

Buttons: OK, Cancel

2. Add an authentication page template:
 - a. From the navigation tree, select **Intelligent Portal Management > Page Template List**.
 - b. Click **Add** to open the **Add Theme** page.
 - c. Enter template name **theme** in the **Theme Name** field.
 - d. Use the default settings for other parameters.
 - e. Click **OK** to open the page for editing the template.

Figure 3 Adding an authentication page template


- f. On the **theme** page, click the **Authentication** icon  in the **Basic Controls** area.
- g. Click **Edit** in authentication edit area, select **Other** and **Account** in the **Authentication Method** area, click **OK**, and then click **Save Page**.
- h. Use the default settings for other configuration.
- i. Click **Confirm Release**.

Figure 4 Editing the template

3. Add an authentication policy:
 - a. From the navigation tree, select **Intelligent Portal Management > Authentication Policies**.
 - b. Click **Add** to open the **Add Authentication Policy** page.
 - c. Enter authentication policy name **policy1**, and select **theme** from the **Page Template** list.
 - d. Select a transparent authentication period to enable portal transparent authentication (MAC-trigger authentication).

- e. Use the default settings for other parameters.
- f. Click **OK**.

Figure 5 Adding an authentication policy

Intelligent Portal Management > Add Authentication Policy

Add Authentication Policy

Name *	policy1
Description	
Page Template *	theme ▼
Authentication Free	<input type="checkbox"/> ?
Only Mobile Endpoints	<input type="checkbox"/> ?
Transparent Authentication Period *	Today ▼
Match SSID for Transparent Authentication	<input type="checkbox"/>
Idle Time Before Network Cut (Minutes) *	30 ?
Idle Traffic Before Network Cut (Bytes) *	10240 ?
Max. Online Duration Per Access (Seconds) *	0 ?
Maximum Online Duration Per Day (Seconds) *	0 ?
Maximum Traffic Per Day (MB) *	0 ?

OK Cancel

4. Add a site:
 - a. From the navigation tree, select **Intelligent Portal Management > Site Management**.
 - b. Click **Add** to open the **Add Site** page.
 - c. Enter the site name, the site address, the expected number of clients to be supported, and the telephone number.
 - d. Click **OK**.

Figure 6 Adding a site

Intelligent Portal Management > Site Management > Add Site

Site Basic Information

Site Name * userspot

Site Address * useraddress ?

Expected Supported Number * 2

Telephone * 81819999

Site Introduction

Site Group * Ungrouped ▼

User Group * Ungrouped ▼

- e. In the **Associated APs** area, click **Add** to associate an AP.
- f. Enter the serial number and MAC address of the AP.
- g. Click **OK**.

Figure 7 Adding an AP

The 'Add' dialog box has a title bar with the word 'Add' in blue. Below the title bar are three input fields: 'AP Serial Number *' with the value '219801A0CNC138011454', 'AP IP Address' which is empty, and 'AP MAC Address *' with the value '70F9-6DD7-D900'. At the bottom right are two buttons: 'OK' and 'Cancel'.

- i. In the **Bind Authentication Policy** area, click **Add** to bind the AP to an authentication policy.
- j. Select authentication policy **policy1**.
- k. Use the default settings for other parameters.
- l. Click **OK**.

Figure 8 Binding the AP to an authentication policy

The 'Bind to Authentication Policies' dialog box has a title bar with the text 'Bind to Authentication Policies' in blue. Below the title bar are four input fields: 'Authentication Policy' is a dropdown menu showing 'policy1'; 'SSID' is an empty text field; 'Start Time' and 'End Time' are empty text fields, each with a blue clock icon to its right. At the bottom right are two buttons: 'OK' and 'Cancel'.

Verifying the configuration

1. Verify that the AP can come online from AC 1 and AC 2.

Display AP information on AC 1.

```
<AC1> display wlan ap all
Total number of APs: 1
Total number of connected APs: 1
Total number of connected manual APs: 1
Total number of connected auto APs: 0
Total number of connected common APs: 1
Total number of connected WTUs: 0
Total number of inside APs: 0
Maximum supported APs: 6144
Remaining APs: 6143
```

```

Total AP licenses: 2048
Local AP licenses: 2048
Server AP licenses: 0
Remaining Local AP licenses: 2047
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
office	1	R/M	AP 3620	219801A28N819CE0002T

The output shows that the AP has come online from AC 1 and the AP is in the R/M state.

Display AP information on AC 2.

```

<AC2> display wlan ap all
Total number of APs: 1
Total number of connected APs: 1
Total number of connected manual APs: 1
Total number of connected auto APs: 0
Total number of connected common APs: 1
Total number of connected WTUs: 0
Total number of inside APs: 0
Maximum supported APs: 6144
Remaining APs: 6143
Total AP licenses: 2048
Local AP licenses: 2048
Server AP licenses: 0
Remaining Local AP licenses: 2048
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
office	1	R/B	AP 3620	219801A28N819CE0002T

The output shows that the AP has come online from AC 2 and the AP is in R/B state.

2. Verify that user **Client** can perform portal authentication through a Web browser on the wireless client. Before passing authentication, all Web accesses are redirected to the portal authentication page (<http://192.168.0.111:8080/portal>). After passing authentication, the user can access other network resources.

Display online portal user information on the ACs. This example uses AC 1.

```

[AC1] display portal user all
Total portal users: 1
Username: client
  AP name: office
  Radio ID: 2
  SSID: service

```

```

Portal server: newpt
State: Online
VPN instance: N/A
MAC                IP                VLAN    Interface
0021-6330-0933    2.2.2.3            200     WLAN-BSS1/0/16
Authorization information:
  DHCP IP pool: N/A
  User profile: N/A
  Session group profile: N/A
  ACL number: N/A
  Inbound CAR: N/A
  Outbound CAR: N/A

```

The output shows that the user has come online.

Verify that the user can come online without entering the username and password when attempting to come online again. (Details not shown.)

3. Verify that the local forwarding mode can take effect.

Display portal filtering rules on the ACs. This example uses AC 1.

```

[AC1] display portal rule all ap office
Slot 1:

```

The output shows that AC 1 does not have portal filtering rules, indicating that AC 1 does not forward client data traffic.

Display portal filtering rules on the AP.

```

[AP] display portal rule all

```

IPv4 portal rules on WLAN-BSS1/0/16:

```

Rule 1:
Type                : Static
Action              : Permit
Protocol            : Any
Status              : Active
Source:
  IP                 : 0.0.0.0
  Mask               : 0.0.0.0
  Port               : Any
  MAC                : 0000-0000-0000
  Interface          : WLAN-BSS1/0/16
  VLAN               : Any
Destination:
  IP                 : 192.168.0.111
  Mask               : 255.255.255.255
  Port               : Any

```

```

Rule 2:
Type                : Dynamic
Action              : Permit
Status              : Active
Source:
  IP                 : 2.2.2.3

```

MAC : 0021-6330-0933
Interface : WLAN-BSS1/0/16
VLAN : Any

Rule 3:

Type : Static
Action : Redirect
Status : Active
Source:
IP : 0.0.0.0
Mask : 0.0.0.0
Interface : WLAN-BSS1/0/16
VLAN : Any
Protocol : TCP
Destination:
IP : 0.0.0.0
Mask : 0.0.0.0
Port : 443

Rule 4:

Type : Static
Action : Redirect
Status : Active
Source:
IP : 0.0.0.0
Mask : 0.0.0.0
Interface : WLAN-BSS1/0/16
VLAN : Any
Protocol : TCP
Destination:
IP : 0.0.0.0
Mask : 0.0.0.0
Port : 80

Rule 5:

Type : Static
Action : Deny
Status : Active
Source:
IP : 0.0.0.0
Mask : 0.0.0.0
Interface : WLAN-BSS1/0/16
VLAN : Any
Destination:
IP : 0.0.0.0
Mask : 0.0.0.0

The output shows that the AP has portal filtering rules, indicating that the AP forwards client data traffic.

Configuration files

- AC 1:

```
#
wlan global-configuration
    nas-id wiportal
#
vlan 100
#
vlan 200
#
wlan service-template st1
    ssid service
    vlan 200
    client forwarding-location ap
akm mode psk
    preshared-key pass-phrase cipher $c$3$0Lf6pOZ6bxrf25nodjOJKYEfnZ6g6ErccHyQ
    cipher-suite ccmp
    security-ie rsn
    portal enable method direct
    portal domain dm1
    portal bas-ip 2.2.2.1
    portal apply web-server newpt
    portal apply mac-trigger-server mts
    portal temp-pass period 300 enable
    service-template enable
#
interface Vlan-interface100
    ip address 2.2.1.1 255.255.255.0
#
interface Vlan-interface200
    ip address 2.2.2.1 255.255.255.0
#
interface GigabitEthernet1/0/1
    port link-type trunk
    port trunk permit vlan 1 100 200
#
ip route-static 192.168.0.0 16 2.2.2.100
#
radius session-control enable
#
domain dm1
    authentication portal none
    authorization portal none
    accounting portal none
#
portal host-check enable
portal client-gateway interface Vlan-interface200
```

```

portal free-rule 0 destination ip 192.168.0.111 255.255.255.255
portal free-rule 1 destination ip 2.2.2.1 255.255.255.255
portal free-rule 2 destination ip any udp 53
portal free-rule 3 destination ip any tcp 53
portal free-rule 4 destination ip 2.2.2.2 255.255.255.255
portal safe-redirect enable
portal safe-redirect method get post
portal safe-redirect user-agent CaptiveNetworkSupport
portal safe-redirect user-agent MicroMessenger
portal safe-redirect user-agent Mozilla
portal safe-redirect user-agent WeChat
portal safe-redirect user-agent iPhone
portal safe-redirect user-agent micromessenger
#
portal web-server newpt
  url http://192.168.0.111:8080/INC -
  WSMAuth/protocol captive-bypass ios optimize
  enable
  server-type oauth
#
portal local-web-server http
#
portal mac-trigger-server mts
  ip 192.168.0.111
  cloud-binding enable
#
wlan ap-group group1
  priority 7
  wlan tunnel-preempt enable
  backup-ac ip 2.2.1.2
  ap office
  ap-model AP 3620
map-configuration flash:/map.txt
radio 1
  radio 2
  radio enable
  service-template st1
#
wlan ap office model AP 3620
serial-id 219801A28N819CE0002T
#
• AC 2:
#
wlan global-configuration
  nas-id wiportal
#
vlan 100
#
vlan 200

```



```

#
wlan service-template st1
    ssid service
    vlan 200
    client forwarding-location ap
akm mode psk
    preshared-key pass-phrase cipher $c$3$oLf6pOZ6bxrf25nodjOJKYEfnZ6g6ErccHyQ
    cipher-suite ccmp
    security-ie rsn
    portal enable method direct
    portal domain dml
    portal bas-ip 2.2.2.2
    portal apply web-server newpt
    portal mac-trigger-server mts
    portal temp-pass period 300 enable
    service-template enable
#
interface Vlan-interface100
    ip address 2.2.1.2 255.255.255.0
#
interface Vlan-interface200
    ip address 2.2.2.2 255.255.255.0
#
interface GigabitEthernet1/0/1
    port link-type trunk
    port trunk permit vlan 1 100 200
#
ip route-static 192.168.0.0 16 2.2.2.100
#
radius session-control enable
#
domain dml
    authentication portal none
    authorization portal none
    accounting portal none
#
portal host-check enable
portal client-gateway interface Vlan-interface200
portal free-rule 0 destination ip 192.168.0.111 255.255.255.255
portal free-rule 1 destination ip 2.2.2.1 255.255.255.255
portal free-rule 2 destination ip any udp 53
portal free-rule 3 destination ip any tcp 53
portal free-rule 4 destination ip 2.2.2.2 255.255.255.255
portal safe-redirect enable
portal safe-redirect method get post
portal safe-redirect user-agent CaptiveNetworkSupport
portal safe-redirect user-agent MicroMessenger
portal safe-redirect user-agent Mozilla

```

```

portal safe-redirect user-agent WeChat
portal safe-redirect user-agent iPhone
portal safe-redirect user-agent micromessenger
#
portal web-server newpt
  url http://192.168.0.111:8080/INC -
  WSMAuth/protocol captive-bypass ios optimize
  enable
  server-type oauth
#
portal local-web-server http
#
portal mac-trigger-server mts
  ip 192.168.0.111
  cloud-binding enable
#
wlan ap-group group1
  priority 6
  wlan tunnel-preempt enable
  backup-ac ip 2.2.1.1
  ap office
  ap-model AP 3620
map-configuration flash:/map.txt
radio 1
  radio 2
  radio enable
  service-template st1
#
wlan ap office model AP 3620
serial-id 219801A28N819CE0002T
#

```

- **Switch:**

```

#
vlan 2
#
vlan 100
#
vlan 200
#
interface Vlan-interface2
  ip address 192.168.0.100 255.255.255.0
#
interface Vlan-interface200
  ip address 2.2.2.100 255.255.255.0
#
interface GigabitEthernet1/0/1
  port link-type trunk
  port trunk permit vlan 1 100 200
#

```

```

interface GigabitEthernet1/0/2
  port link-type trunk
  port trunk pvid vlan 100
  port trunk permit vlan 100 200
  poe enable
#
interface GigabitEthernet1/0/3
  port link-type trunk
  port trunk permit vlan 100 200
#
interface GigabitEthernet1/0/4
  port link-type trunk
  port trunk permit vlan 1 100 200
#

```

- **DHCP server:**

```

#
interface GigabitEthernet1/0/1
  port link-type trunk
  port trunk permit vlan 100 200
#
interface vlan-interface 100
  ip address 2.2.2.200 255.255.255.0
#
interface vlan-interface 200
  ip address 2.2.2.200 255.255.255.0
#
dhcp enable
#
dhcp server ip-pool vlan100
  gateway-list 2.2.1.200
  network 2.2.1.0 mask 255.255.255.0
  forbidden-ip 2.2.1.1
  forbidden-ip 2.2.1.2
#
dhcp server ip-pool vlan200
  gateway-list 2.2.2.100
  network 2.2.2.0 mask 255.255.255.0
  dns-list 8.8.8.8
  forbidden-ip 2.2.2.1
  forbidden-ip 2.2.2.2
  forbidden-ip 2.2.2.100
#

```

Related documentation

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

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

INTELBRAS Access Controllers

Dual-Link Backup OAuth-Based Portal Authentication in Local Forwarding Configuration Examples

Copyright © 2024 Intelbras S.A All rights reserved.

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

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

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

Contents

Introduction	1
Prerequisites	1
Example: Configuring OAuth-based portal authentication for dual-link AC backup and local forwarding	1
Network configuration	1
Analysis	2
Restrictions and guidelines	2
Procedures	3
Editing the AP configuration file	3
Configuring AC 1	3
Configuring AC 2	6
Configuring the switch	9
Configuring the DHCP server	10
Configuring the INC server	11
Verifying the configuration	15
Configuration files	18
Related documentation	23

Introduction

The following information provides an example for configuring OAuth-based portal authentication in a dual-link backup network enabled with local forwarding.

Prerequisites

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

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

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

Example: Configuring OAuth-based portal authentication for dual-link AC backup and local forwarding

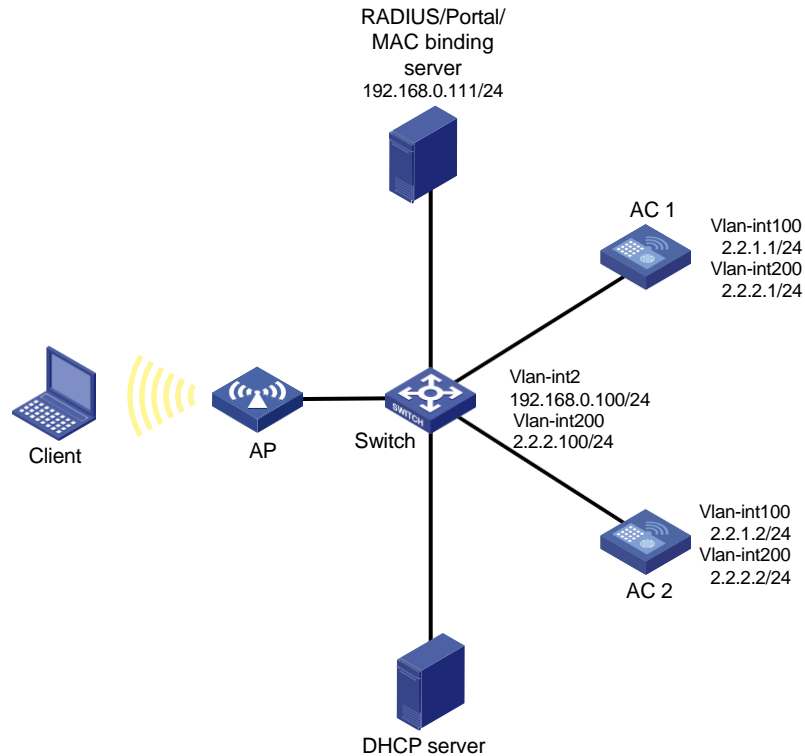
Network configuration

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

Configure the devices to meet the following requirements:

- The AP associates with both ACs and the two ACs to back up each other. When the master AC fails, the backup AC takes over, and the AP can provide services correctly through the backup AC.
- Before passing portal authentication, the client can access only the portal Web server. After passing the authentication, the client can access other network resources.
- The AP forwards all the client traffic.
- The client can access network resources through any Layer 2 ports in its access VLAN without re-authentication.
- The INC server can dynamically modify user authorization information and log off clients.

Figure 1 Network diagram



Analysis

- To allow an authenticated user to access network resources on any Layer 2 ports in its access VLAN without re-authentication, you must enable the portal roaming feature.
- In a local-forwarding WLAN, the AC does not keep ARP entries for portal clients. To ensure that valid users can perform portal authentication, you must enable wireless client validity check on the AC.
- To avoid possible authentication failure caused by frequent logins and logouts of portal clients in a short time, disable the Rule ARP entry feature.
- To allow the RADIUS server to modify user authorization information and log off users, enable the RADIUS session-control feature.
- To assign interface GigabitEthernet 1/0/1 on the AP to VLAN 200 for local forwarding, you must edit the configuration file of the AP and then upload the file to the storage medium of the AC.
- For dual-link backup to operate correctly, you must configure manual AP or auto AP settings on both ACs. This ensures that the AP can establish CAPWAP tunnels with both ACs.

Restrictions and guidelines

When you configure OAuth-based portal authentication for dual-link AC backup and local forwarding, follow these restrictions and guidelines:

- Use the actual serial ID of an AP to uniquely identify that AP.
- If you configure manual APs, make sure the manual APs configured on the two ACs have the same AP name and identifier (serial ID or MAC address).

- Make sure the two ACs have the same portal authentication settings, except for the portal Web server, portal BAS-IP, and authentication-specific AC interface settings.
- You must upload the AP configuration file to both the master and backup ACs.

Procedures

Editing the AP configuration file

Use a text editor to edit the AP configuration file, name the file **map.txt**, and then upload the file to the storage medium of the ACs. The file content and format are as follows:

```
system-view
vlan 200
interface gigabitethernet1/0/1
port link-type trunk
port trunk permit vlan 200
```

Configuring AC 1

1. Configure VLANs and interfaces:

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

```
<AC1> system-view
[AC1] vlan 100
[AC1-vlan100] quit
[AC1] interface vlan-interface 100
[AC1-Vlan-interface100] ip address 2.2.1.1 24
[AC1-Vlan-interface100] quit
```

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

```
[AC1] vlan 200
[AC1-vlan200] quit
[AC1] interface vlan-interface 200
[AC1-Vlan-interface200] ip address 2.2.2.1 24
[AC1-Vlan-interface200] quit
```

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

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

2. Configure a static route to the INC server.

```
[AC1] ip route-static 192.168.0.0 255.255.0.0 2.2.2.100
```

3. Configure DNS server settings. (Details not shown.)

4. Configure wireless services:

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

```
[AC1] wlan service-template st1
```

Specify the SSID as **service**.

```
[AC1-wlan-st-st1] ssid service
```

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

```
[AC1-wlan-st-st1] vlan 200
```

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

```
[AC1-wlan-st-st1] akm mode psk
```

```
[AC1-wlan-st-st1] preshared-key pass-phrase simple 12345678
```

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

```
[AC1-wlan-st-st1] cipher-suite ccmp
```

```
[AC1-wlan-st-st1] security-ie rsn
```

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

```
[AC1-wlan-st-st1] client forwarding-location ap
```

```
[AC1-wlan-st-st1] quit
```

5. Configure the AP:

NOTE:

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

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

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

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

```
[AC1-wlan-ap-office] quit
```

Create AP group **group1**.

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

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

Set the AP connection priority for the AC to 7.

```
[AC1-wlan-ap-group-group1] priority 7
```

Specify AC 2 as the backup AC for AC 1.

```
[AC1-wlan-ap-group-group1] backup-ac ip 2.2.1.2
```

Enable master CAPWAP tunnel preemption.

```
[AC1-wlan-ap-group-group1] wlan tunnel-preempt enable
```

Deploy configuration file **map.txt** to the AP.

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

```
[AC1-wlan-ap-group-group1-ap-model-AP 3620] map-configuration map.txt
```

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

```
[AC1-wlan-ap-group-group1-ap-model-AP 3620] radio 2
```

```
[AC1-wlan-ap-group-group1-ap-model-AP 3620-radio-2] service-template st1
```

Enable radio 2.

```
[AC1-wlan-ap-group-group1-ap-model-AP 3620-radio-2] radio
```

```
enable [AC1-wlan-ap-group-group1-ap-model-AP 3620-radio-2] quit
```

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

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

6. Configure portal authentication:

Create domain **dm1** and enter its view.

```
[AC1] domain dm1
```

Configure the authentication, authorization, and accounting methods as none for portal users.

```
[AC1-isp-dm1] authentication portal none
```

```
[AC1-isp-dm1] authorization portal none
```

```
[AC1-isp-dm1] accounting portal none
```

```

[AC1-isp-dm1] quit
# Create a portal Web server named newpt, specify the server's URL as
http://192.168.0.111/INC - WSMAuth/protocol, and specify the server type as OAuth.
[AC1] portal web-server newpt
[AC1-portal-websvr-newpt] url http://192.168.0.111:8080/INC -
WSMAuth/protocol [AC1-portal-websvr-newpt] server-type oauth
# Enable the optimized captive-bypass feature for iOS users.
[AC1-portal-websvr-newpt] captive-bypass ios optimize enable
[AC1-portal-websvr-newpt] quit
# Create an HTTP-based local portal Web service and enter its view.
[AC1] portal local-web-server http
[AC1-portal-local-websvr-http] quit
# Configure destination-based portal-free rule to permit traffic to the DNS server.
[AC1] portal free-rule 2 destination ip any udp 53
[AC1] portal free-rule 3 destination ip any tcp 53
# Configure portal safe-redirect to reduce the workload of the authentication server.
[AC1] portal safe-redirect enable
[AC1] portal safe-redirect method get post
[AC1] portal safe-redirect user-agent CaptiveNetworkSupport
[AC1] portal safe-redirect user-agent MicroMessenger
[AC1] portal safe-redirect user-agent Mozilla
[AC1] portal safe-redirect user-agent WeChat
[AC1] portal safe-redirect user-agent iPhone
[AC1] portal safe-redirect user-agent micromessenger
# Specify VLAN-interface 200 on the AC for clients to access during portal authentication.
[AC1] portal client-gateway interface vlan-interface 200
# Specify the NAS-ID. Make sure the NAS-ID is the same as the ID in file
iNC\client\conf\wiportal\conf.properties.
[AC1] wlan global-configuration
[AC1-wlan-global-configuration] nas-id wiportal
[AC1-wlan-global-configuration] quit
# Set the user synchronization interval to 60 seconds for portal authentication using OAuth.
[AC1] portal oauth user-sync interval 60
# Configure a destination-based portal-free rule: specify the rule number as 0 and IP address as
192.168.0.111. This rule allows users to reach the portal Web server.
[AC1] portal free-rule 0 destination ip 192.168.0.111 32
# Configure a destination-based portal-free rule: specify the rule number as 1 and IP address as
2.2.2.1. This rule allows users to reach AC 1.
[AC1] portal free-rule 1 destination ip 2.2.2.1 32
# Configure a destination-based portal-free rule: specify the rule number as 4 and IP address as
2.2.2.2. This rule allows users to reach AC 2.
[AC1] portal free-rule 4 destination ip 2.2.2.2 32
# Enable intra-VLAN roaming for portal users.
[AC1] portal roaming enable
# Disable the Rule ARP entry feature for portal clients.
[AC1] undo portal refresh arp enable
# Enable RADIUS session control.
[AC1] radius session-control enable

```

```

# Enable validity check on wireless portal clients.
[AC1] portal host-check enable

# Enable direct IPv4 portal authentication for service template st1.
[AC1] wlan service-template st1
[AC1-wlan-st-st1] portal enable method direct

# Configure the authentication domain for IPv4 portal users as dm1 on service template st1.
[AC1-wlan-st-st1] portal domain dm1

# Apply portal Web server newpt to service template st1.
[AC1-wlan-st-st1] portal apply web-server newpt

# Enable portal temporary pass and set the temporary pass period to 300 seconds.
[AC1-wlan-st-st1] portal temp-pass period 300 enable

# On the service template, configure the BAS-IP attribute as 2.2.2.1 for portal packets sent to
the portal authentication server.
[AC1-wlan-st-st1] portal bas-ip 2.2.2.1

# Enable the service template.
[AC1-wlan-st-st1] service-template enable
[AC1-wlan-st-st1] quit

```

Configuring AC 2

1. Configure VLANs and interfaces:

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

```

<AC2> system-view
[AC2] vlan 100
[AC2-vlan100] quit
[AC2] interface vlan-interface 100
[AC2-Vlan-interface100] ip address 2.2.1.2 24
[AC2-Vlan-interface100] quit

```

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

```

[AC2] vlan 200
[AC2-vlan200] quit
[AC2] interface vlan-interface 200
[AC2-Vlan-interface200] ip address 2.2.2.2 24
[AC2-Vlan-interface200] quit

```

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

```

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

```

2. Configure a static route to the INC server.

```

[AC2] ip route-static 192.168.0.0 255.255.0.0 2.2.2.100

```

3. Configure DNS server settings. (Details not shown.)

4. Configure wireless services:

Create service template st1 and enter its view.

```

[AC2] wlan service-template st1

```

Specify the SSID as **service**.

```
[AC2-wlan-st-st1] ssid service
```

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

```
[AC2-wlan-st-st1] vlan 200
```

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

```
[AC2-wlan-st-st1] akm mode psk
```

```
[AC2-wlan-st-st1] preshared-key pass-phrase simple 12345678
```

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

```
[AC2-wlan-st-st1] cipher-suite ccmp
```

```
[AC2-wlan-st-st1] security-ie rsn
```

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

```
[AC2-wlan-st-st1] client forwarding-location ap
```

```
[AC2-wlan-st-st1] quit
```

5. Configure the AP:

NOTE:

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

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

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

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

```
[AC2-wlan-ap-office] quit
```

Create AP group **group1**.

```
[AC2] wlan ap-group group1
```

```
[AC2-wlan-ap-group-group1] ap office
```

Set the AP connection priority for the AC to 6.

```
[AC2-wlan-ap-group-group1] priority 6
```

Specify AC 1 as the backup AC for AC 2.

```
[AC2-wlan-ap-group-group1] backup-ac ip 2.2.1.1
```

Enable master CAPWAP tunnel preemption

```
[AC2-wlan-ap-group-group1] wlan tunnel-preempt enable
```

Deploy configuration file **map.txt** to the AP.

```
[AC2-wlan-ap-group-group1] ap-model AP 3620
```

```
[AC2-wlan-ap-group-group1-ap-model-AP 3620] map-configuration map.txt
```

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

```
[AC2-wlan-ap-group-group1-ap-model-AP 3620] radio 2
```

```
[AC2-wlan-ap-group-group1-ap-model-AP 3620-radio-2] service-template st1
```

Enable radio 2.

```
[AC2-wlan-ap-group-group1-ap-model-AP 3620-radio-2] radio
```

```
enable [AC2-wlan-ap-group-group1-ap-model-AP 3620-radio-2] quit
```

```
[AC2-wlan-ap-group-group1-ap-model-AP 3620]
```

```
quit [AC2-wlan-ap-group-group1] quit
```

6. Configure portal authentication:

Create domain **dm1** and enter its view.

```
[AC2] domain dm1
```

Configure the authentication, authorization, and accounting methods as none for portal users.

```
[AC2-isp-dm1] authentication portal none
[AC2-isp-dm1] authorization portal none
[AC2-isp-dm1] accounting portal none
[AC2-isp-dm1] quit
```

Create a portal Web server named **newpt**, specify the server's URL as **http://192.168.0.111/INC - WSMAuth/protocol**, and specify the server type as OAuth. (The URL is for illustration only.)

```
[AC2] portal web-server newpt
[AC2-portal-websvr-newpt] url http://192.168.0.111:8080/INC -
WSMAuth/protocol [AC2-portal-websvr-newpt] server-type oauth
```

Enable the optimized captive-bypass feature for iOS users.

```
[AC2-portal-websvr-newpt] captive-bypass ios optimize enable
[AC2-portal-websvr-newpt] quit
```

Create an HTTP-based local portal Web service and enter its view.

```
[AC2] portal local-web-server http
[AC2-portal-local-websvr-http] quit
```

Configure destination-based portal-free rule to permit traffic to the DNS server.

```
[AC2] portal free-rule 2 destination ip any udp 53
[AC2] portal free-rule 3 destination ip any tcp 53
```

Configure portal safe-redirect to reduce the workload of the authentication server.

```
[AC2] portal safe-redirect enable
[AC2] portal safe-redirect method get post
[AC2] portal safe-redirect user-agent CaptiveNetworkSupport
[AC2] portal safe-redirect user-agent MicroMessenger
[AC2] portal safe-redirect user-agent Mozilla
[AC2] portal safe-redirect user-agent WeChat
[AC2] portal safe-redirect user-agent iPhone
[AC2] portal safe-redirect user-agent micromessenger
```

Specify VLAN-interface 200 on the AC for clients to access during portal authentication.

```
[AC2] portal client-gateway interface vlan-interface 200
```

Specify the NAS-ID. Make sure the NAS-ID is the same as the ID in file **iNC\client\conf\wportal\conf.properties**.

```
[AC2] wlan global-configuration
[AC2-wlan-global-configuration] nas-id wportal
[AC2-wlan-global-configuration] quit
```

Set the user synchronization interval to 60 seconds for portal authentication using OAuth.

```
[AC2] portal oauth user-sync interval 60
```

Configure a destination-based portal-free rule: specify the rule number as **0** and IP address as **192.168.0.111**. This rule allows users to reach the portal Web server.

```
[AC2] portal free-rule 0 destination ip 192.168.0.111 32
```

Configure a destination-based portal-free rule: specify the rule number as **1** and IP address as **2.2.2.1**. This rule allows users to reach AC 1.

```
[AC2] portal free-rule 1 destination ip 2.2.2.1 32
```

Configure a destination-based portal-free rule: specify the rule number as **4** and IP address as **2.2.2.2**. This rule allows users to reach AC 2.

```
[AC2] portal free-rule 4 destination ip 2.2.2.2 32
```

Enable intra-VLAN roaming for portal users.

```
[AC2] portal roaming enable
```

```

# Disable the Rule ARP entry feature for portal clients.
[AC2] undo portal refresh arp enable

# Enable RADIUS session control.
[AC2] portal host-check enable

# Enable validity check on wireless portal clients.
[AC2] radius session-control enable

# Enable direct IPv4 portal authentication for service template st1.
[AC2] wlan service-template st1
[AC2-wlan-st-st1] portal enable method direct

# Configure the authentication domain for IPv4 portal users as dm1 on service template st1.
[AC2-wlan-st-st1] portal domain dm1

# Apply portal Web server newpt to service template st1.
[AC2-wlan-st-st1] portal apply web-server newpt

# Enable portal temporary pass and set the temporary pass period to 300 seconds.
[AC2-wlan-st-st1] portal temp-pass period 300 enable

# On the service template, configure the BAS-IP attribute as 2.2.2.2 for portal packets sent to
the portal authentication server.
[AC2-wlan-st-st1] portal bas-ip 2.2.2.2

# Enable the service template.
[AC2-wlan-st-st1] service-template enable
[AC2-wlan-st-st1] quit

```

Configuring the switch

```

# Create VLAN 100 for forwarding CAPWAP tunnel traffic between AC and AP.
<Switch> system-view
[Switch] vlan 100
[Switch-vlan100] quit

# Create VLAN 200 for forwarding client traffic.
[Switch] vlan 200
[Switch-vlan200] quit

# Create VLAN 2 for forwarding client traffic.
[Switch] vlan 2
[Switch-vlan2] quit

# Add the interface that connects the switch to the INC server to VLAN 2. (Details not shown.)

# Configure GigabitEthernet 1/0/1 that connects the switch to AC 1 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 1/0/4 that connects the switch to AC 2 as a trunk port, and assign it to
VLAN 100 and VLAN 200.
[Switch] interface gigabitethernet 1/0/4
[Switch-GigabitEthernet1/0/4] port link-type trunk
[Switch-GigabitEthernet1/0/4] port trunk permit vlan 100 200
[Switch-GigabitEthernet1/0/4] quit

```

Configure GigabitEthernet 1/0/2 that connects the switch to the AP as a trunk port, set the PVID to 100, and assign the interface 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 pvid vlan 100
[Switch-GigabitEthernet1/0/2] port trunk permit vlan 100 200
```

Enable PoE on GigabitEthernet 1/0/2.

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

Configure GigabitEthernet 1/0/3 that connects the switch to the DHCP server as a trunk port, and assign the interface to VLAN 100 and VLAN 200.

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

Assign an IP address to VLAN-interface 200.

```
[Switch] interface vlan-interface 200
[Switch-Vlan-interface200] ip address 2.2.2.100 255.255.255.0
[Switch-Vlan-interface200] quit
```

Assign an IP address to VLAN-interface 2.

```
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] ip address 192.168.0.100 255.255.255.0
[Switch-Vlan-interface2] quit
```

Configuring the DHCP server

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

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

Assign an IP address to VLAN-interface 100.

```
[DHCP] interface vlan-interface 100
[DHCP-Vlan-interface100] ip address 2.2.1.200 255.255.255.0
[DHCP-Vlan-interface100] quit
```

Assign an IP address to VLAN-interface 200.

```
[DHCP] interface vlan-interface 200
[DHCP-Vlan-interface200] ip address 2.2.2.200 255.255.255.0
[DHCP-Vlan-interface200] quit
```

Enable DHCP.

```
[DHCP] dhcp enable
```

Create a DHCP address pool named **VLAN100**, specify the DHCP server as the gateway, specify subnet 2.2.1.0/24, and exclude AC addresses from dynamic allocation. The server will use this address pool to assign address to the AP.

```
[DHCP] dhcp server ip-pool VLAN100
[DHCP-dhcp-pool-vlan100] gateway-list 2.2.1.200
```



```
[DHCP-dhcp-pool-vlan100] network 2.2.1.0 mask 255.255.255.0
[DHCP-dhcp-pool-vlan100] forbidden-ip 2.2.1.1 2.2.1.2
[DHCP-dhcp-pool-vlan100] quit
```

Create a DHCP address pool named **VLAN200**, specify the switch as the gateway, specify subnet 2.2.2.0/24, specify the DNS server address as 8.8.8.8, and exclude AC and switch addresses from dynamic allocation. The server will use this address pool to assign address to the client.

```
[DHCP] dhcp server ip-pool VLAN200
[DHCP-dhcp-pool-vlan200] gateway-list 2.2.2.100
[DHCP-dhcp-pool-vlan200] network 2.2.2.0 mask 255.255.255.0
[DHCP-dhcp-pool-vlan200] dns-list 8.8.8.8
[DHCP-dhcp-pool-vlan200] forbidden-ip 2.2.2.100 2.2.2.1 2.2.2.2
[DHCP-dhcp-pool-vlan200] quit
```

Configuring the INC server

In this example, the INC server runs INC PLAT 7.3 (E0605) and INC IPM 7.3 (E0516).

The INC server configuration is the same for AC 1 and AC 2, except for the AC IP address. This section configures AC 1 as an example. Refer to AC 1 configuration when you configure AC 2 and remember to change the IP address setting for AC 2.

1. Add an access user:
 - a. Log in to INC and click the **Service** tab.
 - b. From the navigation tree, select **Intelligent Portal Management > User Management > Users**.
 - c. Click **Add** to open the **Add User** page.
 - d. Enter username **client** and password **admin@123**.
 - e. Use the default settings for other parameters.
 - f. Click **OK**.

Figure 2 Adding an access user

2. Add an authentication page template:
 - a. From the navigation tree, select **Intelligent Portal Management > Page Template List**.
 - b. Click **Add** to open the **Add Theme** page.
 - c. Enter template name **theme** in the **Theme Name** field.
 - d. Use the default settings for other parameters.
 - e. Click **OK** to open the page for editing the template.

Figure 3 Adding an authentication page template

Add Theme

Theme Name * ?

Custom Page: ☐ First ☒ Authentication ☒ Home ☐ Transparent Authentication

Type *

Description

- f. On the **theme** page, click the **Authentication** icon in the **Basic Controls** area.
- g. Click **Edit** in authentication edit area, select **Other** and **Account** in the **Authentication Method** area, click **OK**, and then click **Save Page**.
- h. Use the default settings for other configuration.
- i. Click **Confirm Release**.

Figure 4 Editing the template

Page Template List > Custom Template > theme

Basic Controls | **Authentication** | **Home** | **Page Preview** | **Save Page** | **Content Setting** | **Confirm Release** | **Page Preview**

Authentication Scrolling Pictures

Picture Rich Text

Two Pictures in Parallel Three Pictures in Parallel

Four Picture in Parallel Video

Menu Title

App Download Telephone

HTML background music

Authentication edit area

Authentication Method

☐ One-Click Login ☒ Other

☒ Account ☐ WeChat ☐ SMS Message ☐ Weibo ☐ QQ ☐ Facebook ☐ E-mail ☐ Ticket ☐ Machine

Account Authentication Settings

☐ Modify ☐ Password ☐ Forgot Password ☐ Generally registration ☐ Register By scanning the two-dimension code

Wi-Fi User Agreement

Select Agreements Required

☒ Free Wi-Fi User A... ☐

3. Add an authentication policy:
 - a. From the navigation tree, select **Intelligent Portal Management > Authentication Policies**.
 - b. Click **Add** to open the **Add Authentication Policy** page.
 - c. Enter authentication policy name **policy1**, and select **theme** from the **Page Template** list.
 - d. Select a transparent authentication period to enable portal transparent authentication (MAC-trigger authentication).
 - e. Use the default settings for other parameters.
 - f. Click **OK**.

Figure 5 Adding an authentication policy

The screenshot shows the 'Add Authentication Policy' form within the 'Intelligent Portal Management' interface. The breadcrumb navigation at the top reads 'Intelligent Portal Management > Add Authentication Policy'. The form title is 'Add Authentication Policy'. The form contains the following fields and controls:

- Name ***: A text input field containing 'policy1'.
- Description**: An empty text input field.
- Page Template ***: A dropdown menu showing 'theme'.
- Authentication Free**: A checkbox with a help icon (?).
- Only Mobile Endpoints**: A checkbox with a help icon (?).
- Transparent Authentication Period ***: A dropdown menu showing 'Today'.
- Match SSID for Transparent Authentication**: An unchecked checkbox.
- Idle Time Before Network Cut (Minutes) ***: A text input field containing '30'.
- Idle Traffic Before Network Cut (Bytes) ***: A text input field containing '10240'.
- Max. Online Duration Per Access (Seconds) ***: A text input field containing '0'.
- Maximum Online Duration Per Day (Seconds) ***: A text input field containing '0'.
- Maximum Traffic Per Day (MB) ***: A text input field containing '0'.

At the bottom right of the form, there are two buttons: 'OK' and 'Cancel'.

4. Add a site:
 - a. From the navigation tree, select **Intelligent Portal Management > Site Management**.
 - b. Click **Add** to open the **Add Site** page.
 - c. Enter the site name, the site address, the expected number of clients to be supported, and the telephone number.
 - d. Click **OK**.

Figure 6 Adding a site

Intelligent Portal Management > Site Management > Add Site

Site Basic Information

Site Name *

Site Address * ?

Expected Supported Number *

Telephone *

Site Introduction

Site Group *

User Group *

- e.** In the **Associated APs** area, click **Add** to associate an AP.
- f.** Enter the serial number and MAC address of the AP.
- g.** Click **OK**.

Figure 7 Adding an AP

Add

AP Serial Number * 219801A0CNC138011454

AP IP Address

AP MAC Address * 70F9-6DD7-D900

OK Cancel

- i. In the **Bind Authentication Policy** area, click **Add** to bind the AP to an authentication policy.
- j. Select authentication policy **policy1**.
- k. Use the default settings for other parameters.
- l. Click **OK**.

Figure 8 Binding the AP to an authentication policy

Bind to Authentication Policies

Authentication Policy policy1

SSID

Start Time

End Time

OK Cancel

Verifying the configuration

Make the AP come online.

Verify that the AP state is R/M on AC 1 and R/B on AC 2.

```
<AC1> display wlan ap all
Total number of APs: 1
Total number of connected APs: 1
Total number of connected manual APs: 1
Total number of connected auto APs: 0
Total number of connected common APs: 1
Total number of connected WTUs: 0
Total number of inside APs: 0
Maximum supported APs: 6144
Remaining APs: 6143
```

```

Total AP licenses: 2048
Local AP licenses: 2048
Server AP licenses: 0
Remaining Local AP licenses: 2047
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
office	1	R/M	AP 3620	219801A28N819CE0002T

```
<AC2> display wlan ap all
```

```

Total number of APs: 1
Total number of connected APs: 1
Total number of connected manual APs: 1
Total number of connected auto APs: 0
Total number of connected common APs: 1
Total number of connected WTUs: 0
Total number of inside APs: 0
Maximum supported APs: 6144
Remaining APs: 6143
Total AP licenses: 2048
Local AP licenses: 2048
Server AP licenses: 0
Remaining Local AP licenses: 2048
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
office	1	R/B	AP 3620	219801A28N819CE0002T

Verify that all Web requests are redirected to the portal authentication page (<http://192.168.0.111:8080/portal>) before you pass portal authentication, and you can access Internet resources after being authenticated.

View online port user information generated on the ACs. This example displays the command output on AC 1.

```
[AC1] display portal user all
```

```

Total portal users: 1
Username: client
  AP name: office
  Radio ID: 2
  SSID: service
  Portal server: newpt
  State: Online

```

VPN instance: N/A

MAC	IP	VLAN	Interface
0021-6330-0933	2.2.2.3	200	WLAN-BSS1/0/16

Authorization information:

DHCP IP pool: N/A

User profile: N/A

Session group profile: N/A

ACL number: N/A

Inbound CAR: N/A

Outbound CAR: N/A

Enable local forwarding. (Details not shown.)

Verify that you cannot view the ACL entries deployed by the portal server on AC 1 but can view the entries on the AP.

[AC1] display portal rule all ap office

Slot 1:

[AP] display portal rule all

IPv4 portal rules on WLAN-BSS1/0/16:

Rule 1:

Type	: Static
Action	: Permit
Protocol	: Any
Status	: Active
Source:	
IP	: 0.0.0.0
Mask	: 0.0.0.0
Port	: Any
MAC	: 0000-0000-0000
Interface	: WLAN-BSS1/0/16
VLAN	: Any
Destination:	
IP	: 192.168.0.111
Mask	: 255.255.255.255
Port	: Any

Rule 2:

Type	: Dynamic
Action	: Permit
Status	: Active
Source:	
IP	: 2.2.2.3
MAC	: 0021-6330-0933
Interface	: WLAN-BSS1/0/16
VLAN	: Any

Rule 3:

Type	: Static
Action	: Redirect

```
Status                : Active
Source:
  IP                   : 0.0.0.0
  Mask                 : 0.0.0.0
  Interface            : WLAN-BSS1/0/16
  VLAN                 : Any
  Protocol             : TCP
Destination:
  IP                   : 0.0.0.0
  Mask                 : 0.0.0.0
  Port                 : 443
```

```
Rule 4:
Type                  : Static
Action                : Redirect
Status                : Active
Source:
  IP                   : 0.0.0.0
  Mask                 : 0.0.0.0
  Interface            : WLAN-BSS1/0/16
  VLAN                 : Any
  Protocol             : TCP
Destination:
  IP                   : 0.0.0.0
  Mask                 : 0.0.0.0
  Port                 : 80
```

```
Rule 5:
Type                  : Static
Action                : Deny
Status                : Active
Source:
  IP                   : 0.0.0.0
  Mask                 : 0.0.0.0
  Interface            : WLAN-BSS1/0/16
  VLAN                 : Any
Destination:
  IP                   : 0.0.0.0
  Mask                 : 0.0.0.0
```

Configuration files

- AC 1:

```
#
wlan global-configuration
  nas-id wiportal
#
vlan 100
```



```

#
vlan 200
#
wlan service-template st1
    ssid service
    vlan 200
    client forwarding-location ap
akm mode psk
preshared-key pass-phrase cipher $c$3$oLf6pOZ6bxrf25nodjOJKYEfnZ6g6ErccHyQ
cipher-suite ccmp
security-ie rsn
portal enable method direct
portal domain dm1
portal bas-ip 2.2.2.1
portal apply web-server newpt
portal apply mac-trigger-server mts
portal temp-pass period 300 enable
service-template enable
#
interface Vlan-interface100
    ip address 2.2.1.1 255.255.255.0
#
interface Vlan-interface200
    ip address 2.2.2.1 255.255.255.0
#
interface GigabitEthernet1/0/1
    port link-type trunk
    port trunk permit vlan 1 100 200
#
ip route-static 192.168.0.0 16 2.2.2.100
#
radius session-control enable
#
domain dm1
    authentication portal none
    authorization portal none
    accounting portal none
#
portal host-check enable
portal client-gateway interface Vlan-interface200
portal free-rule 0 destination ip 192.168.0.111 255.255.255.255
portal free-rule 1 destination ip 2.2.2.1 255.255.255.255
portal free-rule 2 destination ip any udp 53
portal free-rule 3 destination ip any tcp 53
portal free-rule 4 destination ip 2.2.2.2 255.255.255.255
portal safe-redirect enable
portal safe-redirect method get post
portal safe-redirect user-agent CaptiveNetworkSupport

```

```

portal safe-redirect user-agent MicroMessenger
portal safe-redirect user-agent Mozilla
portal safe-redirect user-agent WeChat
portal safe-redirect user-agent iPhone
portal safe-redirect user-agent micromessenger
#
portal web-server newpt
    url http://192.168.0.111:8080/INC -
    WSMAuth/protocol captive-bypass ios optimize
    enable
    server-type oauth
#
portal local-web-server http
#
portal mac-trigger-server mts
    ip 192.168.0.111
    cloud-binding enable
#
wlan ap-group group1
    priority 7
    wlan tunnel-preempt enable
    backup-ac ip 2.2.1.2
    ap office
    ap-model AP 3620
map-configuration flash:/map.txt
radio 1
    radio 2
    radio enable
    service-template st1
#
wlan ap office model W6320
serial-id 219801A28N819CE0002T
#

```

- **AC 2:**

```

#
wlan global-configuration
    nas-id wiportal
#
vlan 100
#
vlan 200
#
wlan service-template st1
    ssid service
    vlan 200
    client forwarding-location ap
akm mode psk
    preshared-key pass-phrase cipher $c$3$oLf6pOZ6bxrf25nodjOJKYEfnZ6g6ErccHyQ
    cipher-suite ccmp

```

```

security-ie rsn
portal enable method direct
portal domain dm1
portal bas-ip 2.2.2.2
portal apply web-server newpt
portal mac-trigger-server mts
portal temp-pass period 300 enable
service-template enable
#
interface Vlan-interface100
ip address 2.2.1.2 255.255.255.0
#
interface Vlan-interface200
ip address 2.2.2.2 255.255.255.0
#
interface GigabitEthernet1/0/1
port link-type trunk
port trunk permit vlan 1 100 200
#
ip route-static 192.168.0.0 16 2.2.2.100
#
radius session-control enable
#
domain dm1
authentication portal none
authorization portal none
accounting portal none
#
portal host-check enable
portal client-gateway interface Vlan-interface200
portal free-rule 0 destination ip 192.168.0.111 255.255.255.255
portal free-rule 1 destination ip 2.2.2.1 255.255.255.255
portal free-rule 2 destination ip any udp 53
portal free-rule 3 destination ip any tcp 53
portal free-rule 4 destination ip 2.2.2.2 255.255.255.255
portal safe-redirect enable
portal safe-redirect method get post
portal safe-redirect user-agent CaptiveNetworkSupport
portal safe-redirect user-agent MicroMessenger
portal safe-redirect user-agent Mozilla
portal safe-redirect user-agent WeChat
portal safe-redirect user-agent iPhone
portal safe-redirect user-agent micromessenger
#
portal web-server newpt
url http://192.168.0.111:8080/INC -
WSMAuth/protocol captive-bypass ios optimize
enable
server-type oauth

```

```
#
portal local-web-server http
#
portal mac-trigger-server mts
  ip 192.168.0.111
  cloud-binding enable
#
wlan ap-group group1
  priority 6
  wlan tunnel-preempt enable
  backup-ac ip 2.2.1.1
  ap office
  ap-model AP 3620
map-configuration flash:/map.txt
radio 1
  radio 2
  radio enable
  service-template st1
#
wlan ap office model AP 3620
serial-id 219801A28N819CE0002T
#
```

- **Switch:**

```
#
vlan 2
#
vlan 100
#
vlan 200
#
interface Vlan-interface2
  ip address 192.168.0.100 255.255.255.0
#
interface Vlan-interface200
  ip address 2.2.2.100 255.255.255.0
#
interface GigabitEthernet1/0/1
  port link-type trunk
  port trunk permit vlan 1 100 200
#
interface GigabitEthernet1/0/2
  port link-type trunk
  port trunk pvid vlan 100
  port trunk permit vlan 100 200
  poe enable
#
interface GigabitEthernet1/0/3
  port link-type trunk
```

- ```

 port trunk permit vlan 100 200
#
interface GigabitEthernet1/0/4
 port link-type trunk
 port trunk permit vlan 1 100 200
#

```
- **DHCP server:**

```

#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 100 200
#
interface vlan-interface 100
 ip address 2.2.2.200 255.255.255.0
#
interface vlan-interface 200
 ip address 2.2.2.200 255.255.255.0
#
dhcp enable
#
dhcp server ip-pool VLAN100
 gateway-list 2.2.1.200
 network 2.2.1.0 mask 255.255.255.0
 forbidden-ip 2.2.1.1
 forbidden-ip 2.2.1.2
#
dhcp server ip-pool VLAN200
 gateway-list 2.2.2.100
 network 2.2.2.0 mask 255.255.255.0
 dns-list 8.8.8.8
 forbidden-ip 2.2.2.1
 forbidden-ip 2.2.2.2
 forbidden-ip 2.2.2.100
#

```

## Related documentation

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

# INTELBRAS Access Controllers

## Dual-Link Backup Remote Portal

## MAC-Trigger Authentication in Local

## Forwarding Configuration Examples

---

Copyright © 2024 Intelbras S.A All rights reserved.

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

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

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

# Contents

|                                                                                                                    |    |
|--------------------------------------------------------------------------------------------------------------------|----|
| Introduction .....                                                                                                 | 1  |
| Prerequisites .....                                                                                                | 1  |
| Example: Configuring remote portal MAC-trigger authentication for dual-link<br>AC backup and local forwarding..... | 1  |
| Network configuration.....                                                                                         | 1  |
| Analysis .....                                                                                                     | 2  |
| Restrictions and guidelines .....                                                                                  | 2  |
| Procedures .....                                                                                                   | 3  |
| Editing the AP configuration file.....                                                                             | 3  |
| Configuring AC 1 .....                                                                                             | 3  |
| Configuring AC 2 .....                                                                                             | 6  |
| Configuring the switch .....                                                                                       | 7  |
| Configuring the DHCP server .....                                                                                  | 8  |
| Configuring the INC server.....                                                                                    | 8  |
| Verifying the configuration .....                                                                                  | 14 |
| Verifying dual-link backup configuration .....                                                                     | 14 |
| Verifying portal MAC-trigger authentication configuration .....                                                    | 15 |
| Configuration files.....                                                                                           | 16 |
| Related documentation .....                                                                                        | 19 |

# Introduction

The following information provides an example for configuring remote portal MAC-trigger authentication with local forwarding.

## Prerequisites

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

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

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

## Example: Configuring remote portal MAC-trigger authentication for dual-link AC backup and local forwarding

### Network configuration

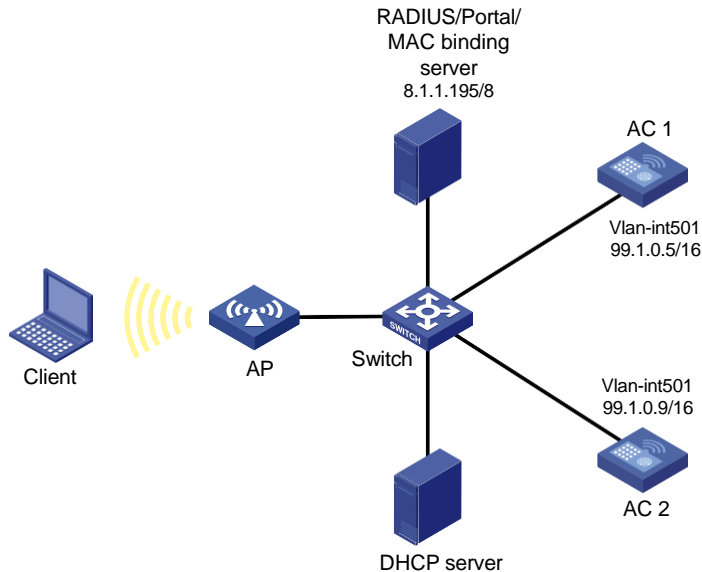
As shown in [Figure 1](#), the AP and the client obtain IP addresses from the DHCP server. The INC server acts as the portal authentication server, portal Web server, and RADIUS server.

Configure the devices to meet the following requirements:

- The AP associates with both ACs and the two ACs to back up each other. When the master AC (AC 1) fails, the backup AC (AC 2) takes over, and the AP can provide services correctly through the backup AC.
- Before passing portal authentication, the client can access only the portal Web server. After passing the authentication, the client can access other network resources.
- The AP forwards all the client traffic.
- The client can access network resources through any Layer 2 ports in its access VLAN without re-authentication.



**Figure 1 Network diagram**



## Analysis

- To allow an authenticated user to access network resources on any Layer 2 ports in its access VLAN without re-authentication, you must enable the portal roaming feature.
- To assign interface GigabitEthernet 1/0/1 on the AP to VLAN 600 for local forwarding, you must edit the configuration file of the AP and then upload the file to the storage medium of the AC.
- For dual-link backup to operate correctly, you must configure manual AP or auto AP settings on both ACs. This ensures that the AP can establish CAPWAP tunnels with both ACs.

## Restrictions and guidelines

When you configure remote portal MAC-trigger authentication for dual-link AC backup and local forwarding, follow these restrictions and guidelines:

- Use the actual serial ID of an AP to uniquely identify that AP.
- If you configure manual APs, make sure the manual APs configured on the two ACs have the same AP name and identifier (serial ID or MAC address).
- Portal authentication might fail if portal clients come online and go offline frequently during a short period. To resolve the issue, disable Rule ARP entry feature for portal clients.
- Make sure the two ACs have the same portal authentication settings, except for the portal Web server setting.
- Some clients are enabled with MAC randomization by default, which might cause seamless roaming failures. As a best practice, disable MAC randomization.
- You must upload the AP configuration file to both the master and backup ACs.

# Procedures

## Editing the AP configuration file

# Use a text editor to edit the AP configuration file, name the file **map.txt**, and then upload the file to the storage medium of the ACs. The file content and format are as follows:

```
system-view
vlan 600
interface gigabitethernet1/0/1
port link-type trunk
port trunk permit vlan 600
```

## Configuring AC 1

### 1. Configure dual-link backup:

# Create VLAN 501 and VLAN-interface 501. Assign the VLAN interface an IP address. The AC will use this IP address to establish a CAPWAP tunnel with the AP.

```
<AC1> system-view
[AC1] vlan 501
[AC1-vlan501] quit
[AC1] interface vlan-interface 501
[AC1-Vlan-interface501] ip address 99.1.0.5 16
[AC1-Vlan-interface501] quit
```

# Create VLAN 600. This VLAN will be used for wireless client access.

```
[AC1] vlan 600
[AC1-vlan600] quit
```

# Configure GigabitEthernet 1/0/1 that connects AC 1 to the switch as a trunk port, and assign the port to VLANs 501 and 600.

```
[AC1] interface gigabitethernet 1/0/1
[AC1-GigabitEthernet1/0/1] port link-type trunk
[AC1-GigabitEthernet1/0/1] port trunk permit vlan 501 600
[AC1-GigabitEthernet1/0/1] quit
```

### 2. Configure a static route to the INC server.

```
[AC1] ip route-static 8.0.0.0 255.0.0.0 99.1.0.100
```

### 3. Configure wireless services:

# Create service template **st1** and enter its view.

```
[AC1] wlan service-template st1
```

# Specify the SSID as **service**.

```
[AC1-wlan-st-st1] ssid service
```

# Assign clients coming online through the service template to VLAN 600.

```
[AC1-wlan-st-st1] vlan 600
```

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

```
[AC1-wlan-st-st1] akm mode psk
[AC1-wlan-st-st1] preshared-key pass-phrase simple 12345678
```

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

```
[AC1-wlan-st-st1] cipher-suite ccmp
[AC1-wlan-st-st1] security-ie rsn
```

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

```
[AC1-wlan-st-st1] client forwarding-location ap
[AC1-wlan-st-st1] quit
```

#### 4. Configure the AP:

---

**NOTE:**

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

---

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

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

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

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

# Set the AP connection priority to 7.

```
[AC1-wlan-ap-group-group1] priority 7
```

# Specify AC 2 as the backup AC for AC 1.

```
[AC1-wlan-ap-group-group1] backup-ac ip 99.1.0.9
```

# Enable master CAPWAP tunnel preemption.

```
[AC1-wlan-ap-group-group1] wlan tunnel-preempt enable
```

# Deploy configuration file **map.txt** to the AP in the AP model view of AP group **group1**.

```
[AC1-wlan-ap-group-group1] ap-model AP 3620
[AC1-wlan-ap-group-group1-ap-model-AP 3620] map-configuration map.txt
```

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

```
[AC1-wlan-ap-group-group1-ap-model-AP 3620] radio 2
[AC1-wlan-ap-group-group1-ap-model-AP 3620-radio-2] service-template st1
```

# Enable radio 2.

```
[AC1-wlan-ap-group-group1-ap-model-AP 3620-radio-2] radio
enable [AC1-wlan-ap-group-group1-ap-model-AP 3620-radio-2] quit
[AC1-wlan-ap-group-group1-ap-model-AP 3620]
quit [AC1-wlan-ap-group-group1] quit
```

#### 5. Configure a RADIUS scheme:

# Create RADIUS scheme **rs1**.

```
[AC1] radius scheme rs1
```

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

```
[AC1-radius-rs1] primary authentication 8.1.1.195
[AC1-radius-rs1] primary accounting 8.1.1.195
```

# Specify shared keys for RADIUS authentication and accounting.

```
[AC1-radius-rs1] key authentication simple radius
[AC1-radius-rs1] key accounting simple radius
```

# Configure AC 1 to remove the ISP domain name from the usernames sent to the RADIUS servers.

```
[AC1-radius-rs1] user-name-format without-domain
[AC1-radius-rs1] nas-ip 99.1.0.5
[AC1-radius-rs1] quit
```

# Enable RADIUS session-control.

```
[AC1] radius session-control enable
```

6. Configure the authentication domain:

# Create domain **dm1** and enter its view.

```
[AC1] domain dm1
```

# Configure the domain to use RADIUS scheme **rs1** for authentication, authorization, and accounting.

```
[AC1-isp-dm1] authentication portal radius-scheme rs1
```

```
[AC1-isp-dm1] authorization portal radius-scheme rs1
```

```
[AC1-isp-dm1] accounting portal radius-scheme rs1
```

# Set the client idle timeout to 15 minutes and set the minimum threshold to 1024 bytes for clients in ISP domain **dm1**.

```
[AC1-isp-dm1] authorization-attribute idle-cut 15 1024
```

```
[AC1-isp-dm1] quit
```

7. Configure portal authentication:

# Create the portal authentication server **newpt**, specify the server IP address as 8.1.1.195, and set the destination UDP port number to **50100** for the AC to send unsolicited portal packets to the portal authentication server.

```
[AC1] portal server newpt
```

```
[AC1-portal-server-newpt] ip 8.1.1.195 key simple portal
```

```
[AC1-portal-server-newpt] port 50100
```

```
[AC1-portal-server-newpt] quit
```

# Configure the URL for the portal Web server **newpt** as **http://8.1.1.195:8080/portal**.

```
[AC1] portal web-server newpt
```

```
[AC1-portal-websvr-newpt] url http://8.1.1.195:8080/portal
```

# Configure URL parameters **nasip** for the portal Web server **newpt**. Configure the value of the **nasip** parameter as 99.1.0.5.

```
[AC1-portal-websvr-newpt] url-parameter nasip value 99.1.0.5
```

```
[AC1-portal-websvr-newpt] quit
```

# Enable intra-VLAN roaming for portal users.

```
[AC1] portal roaming enable
```

# Disable the Rule ARP entry feature for portal clients.

```
[AC1] undo portal refresh arp enable
```

# Enable validity check on wireless portal clients.

```
[AC1] portal host-check enable
```

# Enable direct IPv4 portal authentication for service template **st1**.

```
[AC1] wlan service-template st1
```

```
[AC1-wlan-st-st1] portal enable method direct
```

# Configure the authentication domain for IPv4 portal users as **dm1** on service template **st1**.

```
[AC1-wlan-st-st1] portal domain dm1
```

# Specify portal Web server **newpt** as the backup portal Web server on service template **st1** for portal authentication.

```
[AC1-wlan-st-st1] portal apply web-server newpt
```

# On service template **st1**, configure the BAS-IP attribute as 99.1.0.5 for portal packets sent to the portal authentication server.

```
[AC1-wlan-st-st1] portal bas-ip 99.1.0.5
```

```
[AC1-wlan-st-st1] quit
```

# Configure IPv4-based portal-free rules to permit DNS server traffic.

```
[AC1] portal free-rule 1 destination ip any udp 53
```

```
[AC1] portal free-rule 2 destination ip any tcp 53
```

8. Configure MAC-trigger authentication:

# Create the MAC binding server **mts** and enter its view.

```
[AC1] portal mac-trigger-server mts
```

# Specify the IP address of the MAC binding server as **8.1.1.195**.

```
[AC1-portal-mac-trigger-server-mts] ip 8.1.1.195
```

```
[AC1-portal-mac-trigger-server-mts] quit
```

# Specify the MAC binding server **mts** on service template **st1**.

```
[AC1] wlan service-template st1
```

```
[AC1-wlan-st-st1] portal apply mac-trigger-server mts
```

# Enable the service template.

```
[AC1-wlan-st-st1] service-template enable
```

```
[AC1-wlan-st-st1] quit
```

## Configuring AC 2

1. Configure dual-link backup:

# Create VLAN-interface 501. Assign the VLAN interface an IP address. The AC will use this IP address to establish a CAPWAP tunnel with the AP.

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

```
[AC2] vlan 501
```

```
[AC2-vlan501] quit
```

```
[AC2] interface Vlan-interface 501
```

```
[AC2-Vlan-interface501] ip address 99.1.0.9 16
```

```
[AC2-Vlan-interface501] quit
```

# Configure GigabitEthernet 1/0/1 that connects AC 2 to the switch as a trunk port, and assign the port to VLANs 501 and 600.

```
[AC2] interface gigabitethernet 1/0/1
```

```
[AC2-GigabitEthernet1/0/1] port link-type trunk
```

```
[AC2-GigabitEthernet1/0/1] port trunk permit vlan 501 600
```

```
[AC2-GigabitEthernet1/0/1] quit
```

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

```
[AC2] wlan ap ap1 model AP 3620
```

```
[AC2-wlan-ap-ap1] serial-id 219801A28N819CE0002T
```

```
[AC2-wlan-ap-ap1] quit
```

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

```
[AC2] wlan ap-group group1
```

```
[AC2-wlan-ap-group-group1] ap ap1
```

# Set the AP connection priority to 5.

```
[AC2-wlan-ap-group-group1] priority 5
```

# Specify AC 1 as the backup AC for AC 2.

```
[AC2-wlan-ap-group-group1] backup-ac ip 99.1.0.5
```

# Enable master CAPWAP tunnel preemption.

```
[AC2-wlan-ap-group-group1] wlan tunnel-preempt enable
```

2. Configure AC 2 in the same way AC 1 was configured.

# Configuring the switch

**# Create VLAN 501. The VLAN will be used to forward traffic in the CAPWAP tunnels between the ACs and the AP.**

```
<Switch> system-view
[Switch] vlan 501
[Switch-vlan501] quit
```

**# Create VLAN 600. The VLAN will be used to forward client traffic.**

```
[Switch] vlan 600
[Switch-vlan600] quit
```

**# Create VLAN 2. The VLAN will be used to connect to the INC server.**

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

**# Assign the interface that connects the switch to the INC server to VLAN 2. (Details not shown.)**

**# Configure GigabitEthernet 1/0/1 that connects the switch to AC 1 as a trunk port, and assign the port to VLANs 501 and 600.**

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 501 600
[Switch-GigabitEthernet1/0/1] quit
```

**# Configure GigabitEthernet 1/0/3 that connects the switch to AC 2 as a trunk port, and assign the port to VLANs 501 and 600.**

```
[Switch] interface gigabitethernet 1/0/3
[Switch-GigabitEthernet1/0/3] port link-type trunk
[Switch-GigabitEthernet1/0/3] port trunk permit vlan 501 600
[Switch-GigabitEthernet1/0/3] quit
```

**# Configure GigabitEthernet 1/0/2 that connects the switch to the AP as a trunk port, assign the port to VLANs 501 and 600, and set the PVID to 501.**

```
[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] port link-type trunk
[Switch-GigabitEthernet1/0/2] port trunk permit vlan 501 600
[Switch-GigabitEthernet1/0/2] port trunk pvid vlan 501
```

**# Enable PoE.**

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

**# Configure GigabitEthernet 1/0/4 that connects the switch to the DHCP server as a trunk port, and assign the port to VLANs 501 and 600.**

```
[Switch] interface gigabitethernet 1/0/4
[Switch-GigabitEthernet1/0/4] port link-type trunk
[Switch-GigabitEthernet1/0/4] port trunk permit vlan 501 600
[Switch-GigabitEthernet1/0/4] quit
```

**# Assign an IP address to VLAN-interface 501.**

```
[Switch] interface vlan-interface 501
[Switch-Vlan-interface501] ip address 99.1.0.100 255.255.0.0
[Switch-Vlan-interface501] quit
```

**# Assign an IP address to VLAN-interface 600.**

```
[Switch] interface vlan-interface 600
```

```
[Switch-Vlan-interface600] ip address 99.100.0.100 255.255.0.0
[Switch-Vlan-interface600] quit
```

# Assign an IP address to VLAN-interface 2. The INC server will use this address as the gateway address.

```
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] ip address 8.1.1.190 255.0.0.0
[Switch-Vlan-interface2] quit
```

## Configuring the DHCP server

Details not shown.

## Configuring the INC server

In this example, the INC server runs INC PLAT 7.3 (E0504), INC INC - EIA 7.3 (E0503), and INC EIP 7.3 (E0503).

The INC server configuration is the same for AC 1 and AC 2, except for the AC IP address. This section configures AC 1 as an example. Refer to AC 1 configuration when you configure AC 2 and remember to change the IP address setting for AC 2.

### Configure the RADIUS server to add access devices

1. Log in to INC and click the **User** tab.
2. From the navigation pane, select **User Access Policy > Access Device Management > Access Device**.
3. Click **Add**.  
The **Add Access Device** page opens.
4. In the **Access Configuration** area, configure the following parameters:
  - o Enter **radius** in the **Shared Key** and **Confirm Shared Key** fields.
  - o Use the default values for other parameters.
5. In the **Device List** area, click **Select** or **Add Manually** to add the AC 1 at 99.1.0.5 as an access device.
6. Click **OK**.

**Figure 2 Adding an access device**

Navigation: User > User Access Policy > Access Device Management > Access Device > Add Access Device

**Access Configuration**

|                            |                                                                 |                      |           |
|----------------------------|-----------------------------------------------------------------|----------------------|-----------|
| Authentication Port *      | 1812                                                            | Accounting Port *    | 1813      |
| Service Type               | LAN Access Service                                              | Service Group        | Ungrouped |
| Access Device Type         | H3C(General)                                                    | Confirm Shared Key * | *****     |
| Shared Key *               | *****                                                           |                      |           |
| Access Device Group        | --                                                              |                      |           |
| Certificate Authentication | <input checked="" type="radio"/> None <input type="radio"/> EAP |                      |           |
| Certificate Type           | EAP-TLS Authn                                                   |                      |           |

**Device List**

Select Add Manually Clear All

| Device Name | Device IP | Device Model | Comments    | Delete |
|-------------|-----------|--------------|-------------|--------|
| wx5540h-lrf | 99.1.0.5  | wx5540h-lrf  | wx5540h-lrf |        |

Total Items: 1.

OK Cancel

## Configure the portal server:

1. Configure portal authentication:
  - a. Click the **User** tab.
  - b. Select **User Access Policy > Portal Service > Server** from the navigation tree to open the portal server configuration page.
  - c. Configure the portal server parameters as needed.  
This example uses the default settings.
  - d. Click **OK**.

**Figure 3 Portal authentication server configuration**

User > User Access Policy > Portal Service > Server

Portal Server

Basic Information

Log Level \* Info

Portal Server

Request Timeout(Seconds) \* 4

User Heartbeat Interval(Minutes) \* 5

Server Heartbeat Interval(Seconds) \* 20

LB Device Address

Portal Web

Request Timeout(Seconds) \* 15

Verify Endpoint Requests Yes

HTTP Heartbeat Display New Page

Packet Code

Use Cache Yes

HTTPS Heartbeat Display Original Page

Portal Page

http://8.1.1.195:8080/portal/  
https://8.1.1.195:8443/portal/  
http://[8:195]:8080/portal/  
https://[8:195]:8443/portal/

2. Configure the IP address group:
  - a. Select **User Access Policy > Portal Service > IP Group** from the navigation tree to open the portal IP address group configuration page.
  - b. Click **Add** to open the page as shown in [Figure 4](#).
  - c. Enter the IP group name. In this example, the name is w05995-wc5020-irf-ipaddgroup.
  - d. Enter the start IP address and end IP address of the IP group.  
Make sure the client IP address is in the IP group.
  - e. Select a service group.  
This example uses the default group **Ungrouped**.
  - f. Select **Normal** from the **Action** list.
  - g. Click **OK**.



**Figure 4 Adding an IP address group**

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

Add IP Group

IP Group Name \* w05995-wx5540h-irf-ipaddgroup

Start IP \* 99.100.0.1

End IP \* 99.100.0.255

Service Group Ungrouped

Action \* Normal

OK Cancel

**3. Add a portal device:**

- a. Select **User Access Policy > Portal Service > Device** from the navigation tree to open the portal device configuration page.
- b. Click **Add** to open the page as shown in [Figure 5](#).
- c. Enter the device name. In this example, the name is **WC5020-IRF**.
- d. Specify the version as **Portal 2.0**.
- e. Enter the IP address (99.1.0.5) of the AC's interface connected to the client.
- f. Set whether to support the portal server heartbeat and user heartbeat functions. In this example, select **No** for both **Support Server Heartbeat** and **Support User Heartbeat**.
- g. Enter the key, which must be the same as that configured on the AC.
- h. Select **Directly Connected** from the **Access Method** list.
- i. Use the default settings for other parameters.
- j. Click **OK**.

**Figure 5 Adding a portal device**

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

Add Device

Device Information

Device Name \* WC5020-IRF

Version \* Portal 2.0

Listening Port \* 2000

Authentication Retries \* 0

Support Server Heartbeat \* No

Key \* \*\*\*\*\*

Access Method \* Directly Connected

Device Description

Service Group \* Ungrouped

IP Address \* 99.1.0.5

Local Challenge \* No


Logout Retries \* 1

Support User Heartbeat \* No

Confirm Key \* \*\*\*\*\*

OK Cancel

**4. Associate the portal device with the IP address group:**

- a. As shown in [Figure 6](#), click the **Port Group Information Management** icon  for the device to open the port group configuration page.
- b. Click **Add** to open the page as shown in [Figure 7](#).
- c. Enter the port group name. In this example, the name is **w05995-wc5020-irf-portgroup**.

- d. Select the configured IP address group.  
The IP address used by the user to access the network must be within this IP address group.
- e. Select **Supported** for **Transparent Authentication**.
- f. Use the default settings for other parameters.
- g. Click **OK**.
- h. From the navigation tree, select **Intelligent Portal Management > User Management > Users**.

**Figure 6 Device list**

User > User Access Policy > Portal Service > Device

Query Devices

Device Name:  Version:   
 Deploy Result:  Service Group:

**Add**

| Device Name | Version    | Service Group | IP Address | Last Deployed at | Deploy Result | Operation |
|-------------|------------|---------------|------------|------------------|---------------|-----------|
| WX5540H-IRF | Portal 2.0 | Ungrouped     | 99.1.0.5   |                  | Not Deployed  |           |

**Figure 7 Adding a port group**

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

Add Port Group

|                               |                                                          |                                    |                                                            |
|-------------------------------|----------------------------------------------------------|------------------------------------|------------------------------------------------------------|
| Port Group Name *             | <input type="text" value="05995-wx5540h-irf-portgroup"/> | Language *                         | <input type="text" value="English"/>                       |
| Start Port *                  | <input type="text" value="0"/>                           | End Port *                         | <input type="text" value="ZZZZZ"/>                         |
| Protocol *                    | <input type="text" value="HTTP"/>                        | Quick Authentication *             | <input type="text" value="No"/>                            |
| NAT or Not *                  | <input type="text" value="No"/>                          | Error Transparent Transmission *   | <input type="text" value="Yes"/>                           |
| Authentication Type *         | <input type="text" value="PAP"/>                         | IP Group *                         | <input type="text" value="w05995-wx5540h-irf-ipaddgroup"/> |
| Heartbeat Interval(Minutes) * | <input type="text" value="0"/>                           | Heartbeat Timeout(Minutes) *       | <input type="text" value="0"/>                             |
| User Domain                   | <input type="text"/>                                     | Port Group Description             | <input type="text"/>                                       |
| Transparent Authentication    | <input type="text" value="Supported"/>                   | Client Protection Against Cracks * | <input type="text" value="No"/>                            |
| Page Push Policy              | <input type="text"/>                                     | Default Authentication Page        | <input type="text"/>                                       |

**OK** **Cancel**

5. Select **User Access Policy > Service Parameters > Validate System Configuration** from the navigation tree to make the configurations take effect.

## Configuring the MAC binding server

1. Add an access policy:
  - a. Select **User Access Policy > Access Policy** from the navigation tree to open the access policy page.
  - b. Click **Add** to open the page as shown in [Figure 8](#).
  - c. Enter the access policy name. In this example, the name is **w05995\_portal**.
  - d. Select a service group.
  - e. Use the default settings for other parameters.
  - f. Click **OK**.

**Figure 8 Adding an access policy**

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

**Basic Information**

Access Policy Name \* w05995\_portal

Service Group \* Ungrouped

Description

**Authorization Information**

Access Period None

Allocate IP \* No

Downstream Rate(Kbps)

Upstream Rate(Kbps)

Priority

Deploy VLAN

☐ Deploy User Profile

☐ Deploy ACL

Deploy User Group

2. Add an access service:
  - a. Select **User Access Policy > Access Service** from the navigation tree to open the access service page.
  - b. Click **Add** to open the page as shown in [Figure 9](#).
  - c. Enter the service name. In this example, the service name is w05995\_portal.
  - d. Select the **Transparent Authentication on Portal Endpoints** option.
  - e. Use the default settings for other parameters.
  - f. Click **OK**.

**Figure 9 Adding an access service**

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

**Basic Information**

Service Name \* w05995\_portal

Service Group \* Ungrouped

Default Proprietary Attribute Assignment Policy \* Do not use

Default Max. Number of Bound Endpoints \* 0

Description

☒ Available

Service Suffix

Default Access Policy \* w05995\_portal

Default Max. Number of Online Endpoints \* 0

☒ Transparent Authentication

3. Add an access user:
  - a. Select **Access User > All Access Users** from the navigation tree to open the access user page.
  - b. Click **Add** to open the page as shown in [Figure 10](#).
  - c. Select or add an access user. In this example, the account name is w05995.
  - d. Set the password. In this example, the password is w05995\_portal.
  - e. Select **Enable Password Strategy**.
  - f. Retain the default settings for other parameters.
  - g. Select the configured service.
  - h. Click **OK**.

**Figure 10 Adding an access user**

User > All Access Users > Add Access User

Access Information

User Name \* w05995 Select Add User

Account Name \* w05995\_portal

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

Password \* \*\*\*\*\* Confirm Password \* \*\*\*\*\*

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

Start Time [ ] End Time [ ]

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

Login Message [ ]

Access Service

| Service Name                                      | Service Suffix | Status    | Allocate IP |
|---------------------------------------------------|----------------|-----------|-------------|
| <input type="checkbox"/> MAC_server               |                | Available |             |
| <input type="checkbox"/> RadiusServer             |                | Available |             |
| <input checked="" type="checkbox"/> w05995_portal |                | Available |             |

4. Configure system parameters:
  - a. Select **User Access Policy > Service Parameters > System Settings** from the navigation tree to open the system settings page.
  - b. Click the **Configure** icon for **User Endpoint Settings** to open the page as shown in Figure 11.
  - c. Enable **Transparent MAC Authentication**.
  - d. Select whether to enable transparent portal authentication on non-smart devices.  
In this example, select **Enable** for **Non-Terminal Authentication**.
  - e. Click **OK**.
  - f. Click the **Configure** icon for **Endpoint Aging Time** to open the page as shown in Figure 12.
  - g. Set the endpoint aging time as needed.  
This example uses the default value.

**Figure 11 Configuring user endpoint settings**

User > User Access Policy > Service Parameters > System Settings > User Endpoint Settings

User Endpoint Settings

Transparent Authentication Enable Max. Devices for Single Account \* 10

Non-Terminal Authentication Permit Log off User with Endpoint Conflict No

OK Cancel

**Figure 12 Setting the endpoint aging time**

User > User Access Policy > Service Parameters > System Settings > Endpoint Aging Policy > Modify Endpoint Aging Policy

Modify Endpoint Aging Policy

Access Scenario \* Default Policy

Endpoint Aging Policy(Days) \* 7

Endpoint Aging Mode By Binding Time

OK Cancel

5. Select **User Access Policy > Service Parameters > Validate System Configuration** from the navigation tree to make the configurations take effect.

# Verifying the configuration

## Verifying dual-link backup configuration

# Make the AP come online.

# Verify that the AP first associates with AC 1. Shut down VLAN-interface 501 on AC 1, wait 3 minutes, and verify that the AP associates with AC 2 and the AP state on AC 2 is **R/M**.

```
[AC2] display wlan ap all
```

Total number of APs: 1

Total number of connected APs: 1

Total number of connected manual APs: 1

Total number of connected auto APs: 0

Total number of connected common APs: 1

Total number of connected WTUs: 0

Total number of inside APs: 0

Maximum supported APs: 10

Remaining APs: 9

Total AP licenses: 10

Local AP licenses: 10

Server AP licenses: 0

Remaining local AP licenses: 9

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            |
| apl               | 1               | R/M           | AP 3620                | 219801A28N819CE0002T |

# Bring up VLAN-interface 501 on AC 1. Verify that the AP state becomes R/M on AC 1 and R/B on AC 2.

```
[AC1] display wlan ap all
```

Total number of APs: 1

Total number of connected APs: 1

Total number of connected manual APs: 1

Total number of connected auto APs: 0

Total number of connected common APs: 1

Total number of connected WTUs: 0

Total number of inside APs: 0

Maximum supported APs: 10

Remaining APs: 9

Total AP licenses: 10

Local AP licenses: 10

Server AP licenses: 0

Remaining local AP licenses: 9

Sync AP licenses: 0

### AP information

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

| AP name | APID | State | Model   | Serial ID            |
|---------|------|-------|---------|----------------------|
| ap1     | 1    | R/M   | AP 3620 | 219801A28N819CE0002T |

```

[AC2] display wlan ap all
Total number of APs: 1
Total number of connected APs: 1
Total number of connected manual APs: 1
Total number of connected auto APs: 0
Total number of connected common APs: 1
Total number of connected WTUs: 0
Total number of inside APs: 0
Maximum supported APs: 10
Remaining APs: 9
Total AP licenses: 10
Local AP licenses: 10
Server AP licenses: 0
Remaining local AP licenses: 10
Sync AP licenses: 0

```

AP information

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

| AP name | APID | State | Model   | Serial ID            |
|---------|------|-------|---------|----------------------|
| ap1     | 1    | R/B   | AP 3620 | 219801A28N819CE0002T |

## Verifying portal MAC-trigger authentication configuration

# Display MAC binding server configuration.

```

[AC1] display portal mac-trigger-server name mts
Portal mac trigger server name: mts
Version : 1.0
Server type : INC
IP : 8.1.1.195
Port : 50100
VPN instance : Not configured
Aging time : 300 seconds
Free-traffic threshold : 0 bytes
NAS-Port-Type : Not configured
Binding retry times : 3
Binding retry interval : 1 seconds
Authentication timeout : 3 minutes

```

A user can perform portal authentication through a Web browser. Before passing the authentication, the user can access only the authentication page **<http://192.168.0.111:8080/portal>**. All Web requests from the user will be redirected to the authentication page. After passing the authentication, the user can access other network resources.

For the first portal authentication, the user is required to enter the username and password.

# Display portal user information.

```

[AC1] display portal user all
Total portal users: 1
Username: w05995_portal

```

```

AP name: ap1
Radio ID: 2
SSID: service
Portal server: newpt
State: Online
VPN instance: N/A
MAC IP VLAN Interface
a89c-ed90-7730 99.100.0.12 600 WLAN-BSS2/0/2121
Authorization information:
 DHCP IP pool: N/A
 User profile: N/A
 Session group profile: N/A
 ACL number: N/A
 Inbound CAR: N/A
 Outbound CAR: N/A

```

When the user goes offline and then accesses the network again, the user does not need to enter the authentication username and password.

#### # Display portal user information.

```

[AC1] display portal user all
Total portal users: 1
Username: A8:9C:ED:90:77:30
 AP name: ap1
 Radio ID: 2
 SSID: service
 Portal server: newpt
 State: Online
 VPN instance: N/A
 MAC IP VLAN Interface
 a89c-ed90-7730 99.100.0.12 600 WLAN-BSS2/0/2121
 Authorization information:
 DHCP IP pool: N/A
 User profile: N/A
 Session group profile: N/A
 ACL number: N/A
 Inbound CAR: N/A
 Outbound CAR: N/A

```

## Configuration files

- AC 1:
 

```

#
vlan 501
#
vlan 600
#
wlan service-template st1
 ssid service
 vlan 600

```

```

client forwarding-location ap
akm mode psk
preshared-key pass-phrase cipher c3$oLf6pOZ6bxrf25nodjOJKYEfnZ6g6ErccHyQ
cipher-suite ccmp
security-ie rsn
portal enable method direct
portal domain dml
portal bas-ip 99.1.0.5
portal apply web-server newpt
portal apply mac-trigger-server mts
service-template enable
#
interface Vlan-interface501
ip address 99.1.0.5 255.255.0.0
#
interface GigabitEthernet1/0/1
port link-type trunk
port trunk permit vlan 1 501 600
#
ip route-static 8.0.0.0 8 99.1.0.100
#
radius scheme rs1
primary authentication 8.1.1.195
primary accounting 8.1.1.195
key authentication cipher c3$/Mc+yQtK3k6E3L0TtJth+7Pel1EBrSZAmg==
key accounting cipher c3$WoQkH/FbIsUGadr043yY0MGAPHWTIQvUdA==
user-name-format without-domain
nas-ip 99.1.0.5
#
domain dml
authorization-attribute idle-cut 15 1024
authentication portal radius-scheme rs1
authorization portal radius-scheme rs1
accounting portal radius-scheme rs1
#
portal host-check enable
portal free-rule 1 destination ip any udp 53
portal free-rule 2 destination ip any tcp 53
#
portal web-server newpt
url http://8.1.1.195:8080/portal
url-parameter nasip value 99.1.0.5
#
portal server newpt
ip 8.1.1.195 key cipher c3$GZf8+GypB2tLYA25pKOLrJu3quh+vnFE1Q==
#
portal mac-trigger-server mts
ip 8.1.1.195

```



```
#
wlan ap-group group1
 priority 7
 wlan tunnel-preempt enable
 backup-ac ip 99.1.0.9
 ap ap1
 ap-model AP 3620
map-configuration flash:/map.txt
radio 1
 radio 2
 radio enable
 service-template st1
#
wlan ap ap1 model AP 3620
 serial-id 219801A28N819CE0002T
#
```

- **AC 2:**  
Similar as that on AC 1. (Details not shown.)
- **Switch:**

```
#
vlan 2
#
vlan 501
#
vlan 600
#
interface Vlan-interface2
 ip address 8.1.1.190 255.0.0.0
#
interface Vlan-interface501
 ip address 99.1.0.100 255.255.0.0
#
interface Vlan-interface600
 ip address 99.100.0.100 255.255.0.0
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 1 501 600
#
interface GigabitEthernet1/0/2
 port link-type trunk
 port trunk permit vlan 1 501 600
 port trunk pvid vlan 501
 poe enable
#
interface GigabitEthernet1/0/3
 port link-type trunk
 port trunk permit vlan 1 501 600
```

```
#
interface GigabitEthernet1/0/4
 port link-type trunk
 port trunk permit vlan 1 501 600
#
```

## Related documentation

- *AP Management Command Reference* in *INTELBRAS Access Controllers Command References*
- *AP Management Configuration Guide* in *INTELBRAS Access Controllers Configuration Guides*
- *Portal Authentication Command Reference* in *INTELBRAS Access Controllers Command References*
- *Portal Authentication Configuration Guide* in *INTELBRAS Access Controllers Configuration Guides*
- *WLAN Access Command Reference* in *INTELBRAS Access Controllers Command References*
- *WLAN Access Configuration Guide* in *INTELBRAS Access Controllers Configuration Guides*
- *WLAN High Availability Command Reference* in *INTELBRAS Access Controllers Command References*
- *WLAN High Availability Configuration Guide* in *INTELBRAS Access Controllers Configuration Guides*

# INTELBRAS Access Controllers

## Dual-Link Backup Remote Portal and MAC Transparent Authentication in Local Forwarding Configuration Examples

---

Copyright © 2024 Intelbras S.A All rights reserved.

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

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

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

# Contents

|                                                                                                                          |    |
|--------------------------------------------------------------------------------------------------------------------------|----|
| Introduction .....                                                                                                       | 1  |
| Prerequisites .....                                                                                                      | 1  |
| Example: Configuring remote portal and MAC transparent authentication for dual-link AC backup and local forwarding ..... | 1  |
| Network configuration .....                                                                                              | 1  |
| Analysis .....                                                                                                           | 2  |
| Restrictions and guidelines .....                                                                                        | 2  |
| Procedures .....                                                                                                         | 3  |
| Editing the AP configuration file .....                                                                                  | 3  |
| Configuring AC 1 .....                                                                                                   | 3  |
| Configuring AC 2 .....                                                                                                   | 6  |
| Configuring the switch .....                                                                                             | 10 |
| Configuring the DHCP server .....                                                                                        | 11 |
| Configuring the INC server .....                                                                                         | 11 |
| Verifying the configuration .....                                                                                        | 17 |
| Verifying dual-link backup configuration .....                                                                           | 17 |
| Verifying transparent authentication configuration .....                                                                 | 17 |
| Configuration files .....                                                                                                | 18 |
| Related documentation .....                                                                                              | 22 |

# Introduction

The following information provides an example for configuring remote portal and MAC transparent authentication with local forwarding.

## Prerequisites

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

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

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

## Example: Configuring remote portal and MAC transparent authentication for dual-link AC backup and local forwarding

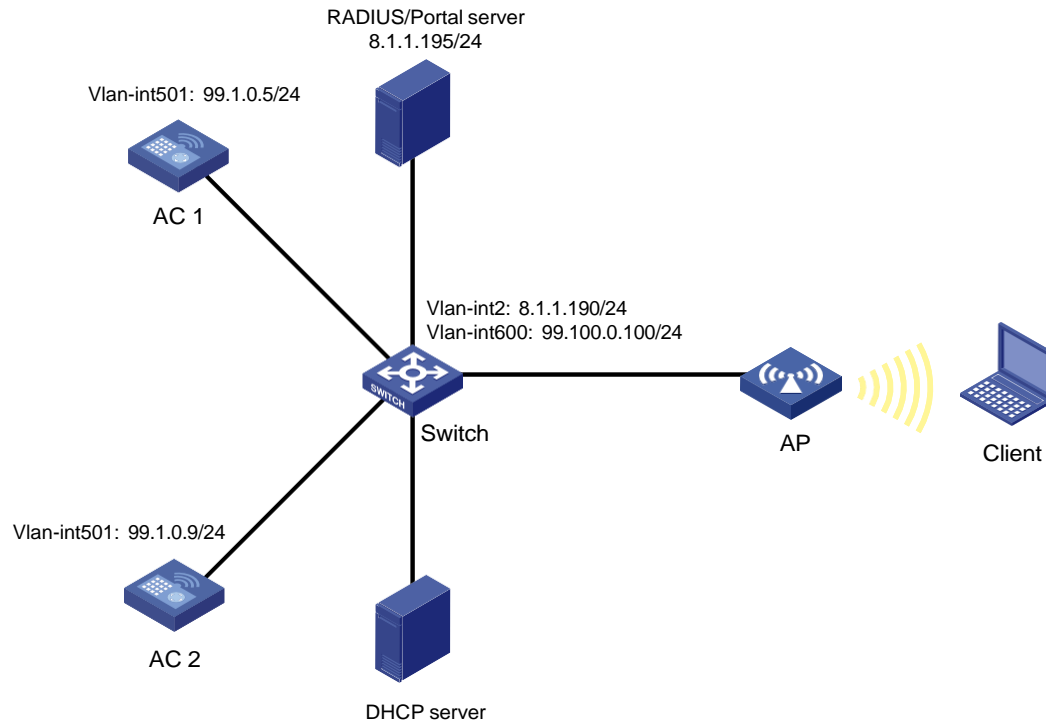
### Network configuration

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

Configure the devices to meet the following requirements:

- The AP associates with both ACs and the two ACs to back up each other. When the master AC (AC 1) fails, the backup AC (AC 2) takes over, and the AP can provide services correctly through the backup AC.
- Remote MAC authentication and direct portal authentication are used for wireless clients.
- Before passing portal authentication, the client can access only the portal Web server. After passing the authentication, the client can access other network resources.
- The AP forwards all the client traffic.
- The client can access network resources through any Layer 2 ports in its access VLAN without re-authentication.
- The authentication process is simplified and clients do not need to enter username and password every time a client attempts to access network resources.

**Figure 1 Network diagram**



## Analysis

- To allow an authenticated user to access network resources on any Layer 2 ports in its access VLAN without re-authentication, you must enable the portal roaming feature.
- To assign interface GigabitEthernet 1/0/1 on the AP to VLAN 600 for local forwarding, you must edit the configuration file of the AP and then upload the file to the storage medium of the AC.
- To allow clients whose MAC information has been recorded by the RADIUS server to access network resources directly without being portal authenticated, configure the AC to ignore MAC authentication failures.

## Restrictions and guidelines

When you configure MAC-based portal authentication for dual-link AC backup and local forwarding, follow these restrictions and guidelines:

- Use the actual serial ID of an AP to uniquely identify that AP.
- If you configure manual APs, make sure the manual APs configured on the two ACs have the same AP name and identifier (serial ID or MAC address).
- Make sure the two ACs are of the same version.
- Make sure the portal authentication server type and portal Web server type configured on the ACs are the same as the actual server type. This example uses an INC server.
- To avoid possible authentication failure caused by frequent logins and logouts of portal clients in a short time, disable the Rule ARP entry feature.
- To allow the RADIUS server to modify user authorization information and log off users, enable the RADIUS session-control feature.

- URLs redirected from the ACs to the portal Web server do not carry parameters by default. You can configure the parameters to carry as needed.
- If you enable portal authentication in VLAN interface view, only centralized forwarding is supported. If you enable portal authentication in service template view, both centralized forwarding and local forwarding are supported. This example enables portal authentication in service template view.
- In a local-forwarding WLAN, the AC does not keep ARP entries for portal clients. To ensure that valid users can perform portal authentication, you must enable wireless client validity check on the AC.
- Make sure the two ACs have the same portal-free rule settings, including the rule numbers.
- Make sure the two ACs have the same portal authentication settings, except for the portal Web server, portal BAS-IP, and interface used by clients to access the AC during portal authentication.
- Some clients are enabled with MAC randomization by default, which might cause seamless roaming failures. As a best practice, disable MAC randomization.
- You must upload the AP configuration file to both the master and backup ACs.

## Procedures

### Editing the AP configuration file

# Use a text editor to edit the AP configuration file, name the file **map.txt**, and then upload the file to the storage medium of the ACs. The file content and format are as follows:

```
system-view
vlan 600
interface gigabitethernet1/0/1
port link-type trunk
port trunk permit vlan 600
```

### Configuring AC 1

#### 1. Configure the VLAN interface:

# Create VLAN 501 and VLAN-interface 501. Assign the VLAN interface an IP address. The AC will use this IP address to establish a CAPWAP tunnel with the AP.

```
<AC1> system-view
[AC1] vlan 501
[AC1-vlan501] quit
[AC1] interface vlan-interface 501
[AC1-Vlan-interface501] ip address 99.1.0.5 24
[AC1-Vlan-interface501] quit
```

# Create VLAN 600. The client will use this VLAN to access the wireless network.

```
[AC1] vlan 600
[AC1-vlan600] quit
```

# Configure GigabitEthernet 1/0/1 that connects AC 1 to the switch as a trunk port, and assign the port to VLANs 501 and 600.

```
[AC1] interface gigabitethernet 1/0/1
[AC1-GigabitEthernet1/0/1] port link-type trunk
[AC1-GigabitEthernet1/0/1] port trunk permit vlan 501 600
[AC1-GigabitEthernet1/0/1] quit
```

2. Configure a static route to the INC server.

```
[AC1] ip route-static 8.1.1.0 255.255.255.0 99.1.0.100
```

3. Configure wireless services:

# Create service template **st1** and enter its view.

```
[AC1] wlan service-template st1
```

# Specify the SSID as **service**.

```
[AC1-wlan-st-st1] ssid service
```

# Assign clients coming online through the service template to VLAN 600.

```
[AC1-wlan-st-st1] vlan 600
```

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

```
[AC1-wlan-st-st1] akm mode psk
```

```
[AC1-wlan-st-st1] preshared-key pass-phrase simple 12345678
```

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

```
[AC1-wlan-st-st1] cipher-suite ccmp
```

```
[AC1-wlan-st-st1] security-ie rsn
```

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

```
[AC1-wlan-st-st1] client forwarding-location ap
```

```
[AC1-wlan-st-st1] quit
```

4. Configure the AP:

---

**NOTE:**

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

---

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

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

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

```
[AC1-wlan-ap-ap1] quit
```

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

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

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

# Set the AP connection priority to 7.

```
[AC1-wlan-ap-group-group1] priority 7
```

# Specify AC 2 as the backup AC for AC 1.

```
[AC1-wlan-ap-group-group1] backup-ac ip 99.1.0.9
```

# Enable master CAPWAP tunnel preemption.

```
[AC1-wlan-ap-group-group1] wlan tunnel-preempt enable
```

# Deploy configuration file **map.txt** to the AP in the AP model view of AP group **group1**.

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

```
[AC1-wlan-ap-group-group1-ap-model-AP 3620] map-configuration map.txt
```

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

```
[AC1-wlan-ap-group-group1-ap-model-AP 3620] radio 2
```

```
[AC1-wlan-ap-group-group1-ap-model-AP 3620-radio-2] service-template st1
```

# Enable radio 2.

```
[AC1-wlan-ap-group-group1-ap-model-AP 3620-radio-2] radio
```

```
enable [AC1-wlan-ap-group-group1-ap-model-AP 3620-radio-2] quit
```

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



- ```
[AC1-wlan-ap-group-group1] quit
```
5. Configure a RADIUS scheme:
 - # Create RADIUS scheme **rs1**.

```
[AC1] radius scheme rs1
```

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

```
[AC1-radius-rs1] primary authentication 8.1.1.195
[AC1-radius-rs1] primary accounting 8.1.1.195
```

 - # Specify shared keys for RADIUS authentication and accounting.

```
[AC1-radius-rs1] key authentication simple radius
[AC1-radius-rs1] key accounting simple radius
```

 - # Configure AC 1 to remove the ISP domain name from the usernames sent to the RADIUS servers.

```
[AC1-radius-rs1] user-name-format without-domain
[AC1-radius-rs1] nas-ip 99.1.0.5
[AC1-radius-rs1] quit
```

 - # Enable RADIUS session-control.

```
[AC1] radius session-control enable
```
 6. Configure the authentication domain for portal authentication:
 - # Create domain **dm1** and enter its view.

```
[AC1] domain dm1
```

 - # Configure the domain to use RADIUS scheme **rs1** for authentication, authorization, and accounting.

```
[AC1-isp-dm1] authentication portal radius-scheme rs1
[AC1-isp-dm1] authorization portal radius-scheme rs1
[AC1-isp-dm1] accounting portal radius-scheme rs1
```

 - # Set the client idle timeout to 15 minutes and set the minimum threshold to 1024 bytes for clients in ISP domain **dm1**.

```
[AC1-isp-dm1] authorization-attribute idle-cut 15 1024
[AC1-isp-dm1] quit
```
 7. Configure the authentication domain for MAC authentication:
 - # Create ISP domain **newpt** and enter its view.

```
[AC1] domain dm2
```

 - # Configure the domain to use RADIUS scheme **rs1** for authentication, authorization, and accounting for LAN users.

```
[AC1-isp-dm2] authentication lan-access radius-scheme rs1
[AC1-isp-dm2] authorization lan-access radius-scheme rs1
[AC1-isp-dm2] accounting lan-access radius-scheme rs1
[AC1-isp-dm2] quit
```
 8. Configure portal authentication:
 - # Create the portal authentication server **newpt**, specify the server IP address as 8.1.1.195, and set the destination UDP port number to **50100** for the AC to send unsolicited portal packets to the portal authentication server.

```
[AC1] portal server newpt
[AC1-portal-server-newpt] ip 8.1.1.195 key simple portal
[AC1-portal-server-newpt] port 50100
[AC1-portal-server-newpt] quit
```

 - # Configure the URL for the portal Web server **newpt** as **http://8.1.1.195:8080/portal**.

```
[AC1] portal web-server newpt
```

```
[AC1-portal-websvr-newpt] url http://8.1.1.195:8080/portal
# Configure URL parameters nasip for the portal Web server newpt. Configure the value of the
nasip parameter as 99.1.0.5.
[AC1-portal-websvr-newpt] url-parameter nasip value 99.1.0.5
[AC1-portal-websvr-newpt] quit
# Configure an IPv4-based portal-free rule to permit portal Web server traffic.
[AC1] portal free-rule 0 destination ip 8.1.1.195 24
# Configure IPv4-based portal-free rules to permit DNS server traffic.
[AC1] portal free-rule 1 destination ip any udp 53
[AC1] portal free-rule 2 destination ip any tcp 53
# Enable intra-VLAN roaming for portal users.
[AC1] portal roaming enable
# Disable the Rule ARP entry feature for portal clients.
[AC1] undo portal refresh arp enable
# Enable validity check on wireless portal clients.
[AC1] portal host-check enable
# Enable direct IPv4 portal authentication for service template st1.
[AC1] wlan service-template st1
[AC1-wlan-st-st1] portal enable method direct
# Configure the authentication domain for IPv4 portal users as dm1 on service template st1.
[AC1-wlan-st-st1] portal domain dm1
# Specify portal Web server newpt on service template st1 to redirect portal user HTTP or
HTTPS requests to the server.
[AC1-wlan-st-st1] portal apply web-server newpt
# Specify the BAS IP as the IP address of VLAN-interface 501, from which clients come online
from AC 1.
[AC1-wlan-st-st1] portal bas-ip 99.1.0.5
```

9. Configure MAC authentication:

```
# Set the authentication mode to mac.
[AC1-wlan-st-st1] client-security authentication-mode mac
# Configure the AC to ignore MAC authentication failures.
[AC1-wlan-st-st1] client-security ignore-authentication
# Specify ISP domain dm2 as the authentication domain for MAC authentication clients in
service template st1.
[AC1-wlan-st-st1] mac-authentication domain dm2
# Enable the service template.
[AC1-wlan-st-st1] service-template enable
[AC1-wlan-st-st1] quit
```

Configuring AC 2

1. Configure the VLAN interface:


```
# Create VLAN 501 and VLAN-interface 501. Assign the VLAN interface an IP address. The AC
will use this IP address to establish a CAPWAP tunnel with the AP.
<AC2> system-view
[AC2] vlan 501
[AC2-vlan501] quit
[AC2] interface Vlan-interface 501
```

```
[AC2-Vlan-interface501] ip address 99.1.0.9 24
[AC2-Vlan-interface501] quit
```

Create VLAN 600. The client will use this VLAN to access the wireless network.

```
[AC2] vlan 600
[AC2-vlan600] quit
```

Configure GigabitEthernet 1/0/1 that connects AC 2 to the switch as a trunk port, and assign the port to VLANs 501 and 600.

```
[AC2] interface gigabitethernet 1/0/1
[AC2-GigabitEthernet1/0/1] port link-type trunk
[AC2-GigabitEthernet1/0/1] port trunk permit vlan 501 600
[AC2-GigabitEthernet1/0/1] quit
```

2. Configure a static route to the INC server.

```
[AC2] ip route-static 8.1.1.0 255.255.255.0 99.1.0.100
```

3. Configure wireless services:

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

```
[AC2] wlan service-template st1
```

Specify the SSID as **service.**

```
[AC2-wlan-st-st1] ssid service
```

Assign clients coming online through the service template to VLAN 600.

```
[AC2-wlan-st-st1] vlan 600
```

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

```
[AC2-wlan-st-st1] akm mode psk
[AC2-wlan-st-st1] preshared-key pass-phrase simple 12345678
```

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

```
[AC2-wlan-st-st1] cipher-suite ccmp
[AC2-wlan-st-st1] security-ie rsn
```

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

```
[AC2-wlan-st-st1] client forwarding-location ap
[AC2-wlan-st-st1] quit
```

4. Configure the AP:

NOTE:

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

Create AP **ap1, and specify the AP name and serial ID.**

```
[AC2] wlan ap ap1 model AP 3620
[AC2-wlan-ap-ap1] serial-id 219801A28N819CE0002T
[AC2-wlan-ap-ap1] quit
```

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

```
[AC2] wlan ap-group group1
[AC2-wlan-ap-group-group1] ap ap1
```

Set the AP connection priority to 5.

```
[AC2-wlan-ap-group-group1] priority 5
```

Specify AC 1 as the backup AC for AC 2.

```
[AC2-wlan-ap-group-group1] backup-ac ip 99.1.0.5
```

Enable master CAPWAP tunnel preemption.

```
[AC2-wlan-ap-group-group1] wlan tunnel-preempt enable
```

Deploy configuration file **map.txt** to the AP in the AP model view of AP group **group1**.

```
[AC2-wlan-ap-group-group1] ap-model AP 3620
[AC2-wlan-ap-group-group1-ap-model-AP 3620] map-configuration map.txt
```

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

```
[AC2-wlan-ap-group-group1-ap-model-AP 3620] radio 2
[AC2-wlan-ap-group-group1-ap-model-AP 3620-radio-2] service-template st1
```

Enable radio 2.

```
[AC2-wlan-ap-group-group1-ap-model-AP 3620-radio-2] radio
enable [AC2-wlan-ap-group-group1-ap-model-AP 3620-radio-2] quit
[AC2-wlan-ap-group-group1-ap-model-AP 3620]
quit [AC2-wlan-ap-group-group1] quit
```

5. Configure a RADIUS scheme:

Create RADIUS scheme **rs1**.

```
[AC2] radius scheme rs1
```

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

```
[AC2-radius-rs1] primary authentication 8.1.1.195
[AC2-radius-rs1] primary accounting 8.1.1.195
```

Specify shared keys for RADIUS authentication and accounting.

```
[AC2-radius-rs1] key authentication simple radius
[AC2-radius-rs1] key accounting simple radius
```

Configure AC 1 to remove the ISP domain name from the usernames sent to the RADIUS servers.

```
[AC2-radius-rs1] user-name-format without-domain
[AC2-radius-rs1] nas-ip 99.1.0.9
[AC2-radius-rs1] quit
```

Enable RADIUS session-control.

```
[AC2] radius session-control enable
```

6. Configure the authentication domain for portal authentication:

Create domain **dm1** and enter its view.

```
[AC2] domain dm1
```

Configure the domain to use RADIUS scheme **rs1** for authentication, authorization, and accounting.

```
[AC2-isp-dm1] authentication portal radius-scheme rs1
[AC2-isp-dm1] authorization portal radius-scheme rs1
[AC2-isp-dm1] accounting portal radius-scheme rs1
```

Set the client idle timeout to 15 minutes and set the minimum threshold to 1024 bytes for clients in ISP domain **dm1**.

```
[AC2-isp-dm1] authorization-attribute idle-cut 15 1024
[AC2-isp-dm1] quit
```

7. Configure the authentication domain for MAC authentication:

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

```
[AC2] domain dm2
```

Configure the domain to use RADIUS scheme **rs1** for authentication, authorization, and accounting for LAN users.

```
[AC2-isp-dm2] authentication lan-access radius-scheme rs1
[AC2-isp-dm2] authorization lan-access radius-scheme rs1
[AC2-isp-dm2] accounting lan-access radius-scheme rs1
[AC2-isp-dm2] quit
```

8. Configure portal authentication:

Create the portal authentication server **newpt**, specify the server IP address as 8.1.1.195, and set the destination UDP port number to **50100** for the AC to send unsolicited portal packets to the portal authentication server.

```
[AC2] portal server newpt
[AC2-portal-server-newpt] ip 8.1.1.195 key simple portal
[AC2-portal-server-newpt] port 50100
[AC2-portal-server-newpt] quit
```

Configure the URL for the portal Web server **newpt** as **http://8.1.1.195:8080/portal**.

```
[AC2] portal web-server newpt
[AC2-portal-websvr-newpt] url http://8.1.1.195:8080/portal
```

Configure URL parameters **nasip** for the portal Web server **newpt**. Configure the value of the **nasip** parameter as 99.1.0.9.

```
[AC2-portal-websvr-newpt] url-parameter nasip value 99.1.0.9
[AC2-portal-websvr-newpt] quit
```

Configure an IPv4-based portal-free rule to permit portal Web server traffic.

```
[AC2] portal free-rule 0 destination ip 8.1.1.195 24
```

Configure IPv4-based portal-free rules to permit DNS server traffic.

```
[AC2] portal free-rule 1 destination ip any udp 53
[AC2] portal free-rule 2 destination ip any tcp 53
```

Enable intra-VLAN roaming for portal users.

```
[AC2] portal roaming enable
```

Disable the Rule ARP entry feature for portal clients.

```
[AC2] undo portal refresh arp enable
```

Enable validity check on wireless portal clients.

```
[AC2] portal host-check enable
```

Enable direct IPv4 portal authentication for service template **st1**.

```
[AC2] wlan service-template st1
[AC2-wlan-st-st1] portal enable method direct
```

Configure the authentication domain for IPv4 portal users as **dm1** on service template **st1**.

```
[AC2-wlan-st-st1] portal domain dm1
```

Specify portal Web server **newpt** on service template **st1** to redirect user HTTP or HTTPS requests to the server.

```
[AC2-wlan-st-st1] portal apply web-server newpt
```

Specify the BAS IP as the IP address of VLAN-interface 501, from which clients come online from AC 2.

```
[AC2-wlan-st-st1] portal bas-ip 99.1.0.9
```

9. Configure MAC authentication:

Set the authentication mode to **mac**.

```
[AC2-wlan-st-st1] client-security authentication-mode mac
```

Configure the AC to ignore MAC authentication failures.

```
[AC2-wlan-st-st1] client-security ignore-authentication
```

Specify ISP domain **dm2** as the authentication domain for MAC authentication clients in service template **st1**.

```
[AC2-wlan-st-st1] mac-authentication domain dm2
```

Enable the service template.

```
[AC2-wlan-st-st1] service-template enable
[AC2-wlan-st-st1] quit
```

Configuring the switch

Create VLAN 501 for forwarding CAPWAP tunnel traffic between AC and AP.

```
<Switch> system-view
[Switch] vlan 501
[Switch-vlan501] quit
```

Create VLAN 600 for forwarding client traffic.

```
[Switch] vlan 600
[Switch-vlan600] quit
```

Create VLAN 2 for connecting to the INC server.

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

Add the interface that connects the switch to the INC server to VLAN 2. (Details not shown.)

Configure GigabitEthernet 1/0/1 that connects the switch to AC 1 as a trunk port, and assign it to VLAN 501 and VLAN 600.

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port link-type trunk
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 501 600
[Switch-GigabitEthernet1/0/1] quit
```

Configure GigabitEthernet 1/0/3 that connects the switch to AC 2 as a trunk port, and assign it to VLAN 501 and VLAN 600.

```
[Switch] interface gigabitethernet 1/0/3
[Switch-GigabitEthernet1/0/3] port link-type trunk
[Switch-GigabitEthernet1/0/3] port trunk permit vlan 501 600
[Switch-GigabitEthernet1/0/3] quit
```

Configure GigabitEthernet 1/0/2 that connects the switch to the AP as a trunk port, and assign it to VLAN 501 and VLAN 600.

```
[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] port link-type trunk
[Switch-GigabitEthernet1/0/2] port trunk permit vlan 501 600
[Switch-GigabitEthernet1/0/2] port trunk pvid vlan 501
```

Enable PoE.

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

Configure GigabitEthernet 1/0/4 that connects the switch to the DHCP server as a trunk port, and assign it to VLAN 501 and VLAN 600.

```
[Switch] interface gigabitethernet 1/0/4
[Switch-GigabitEthernet1/0/4] port link-type trunk
[Switch-GigabitEthernet1/0/4] port trunk permit vlan 501 600
[Switch-GigabitEthernet1/0/4] quit
```

Assign an IP address to VLAN-interface 501.

```
[Switch] interface vlan-interface 501
[Switch-Vlan-interface501] ip address 99.1.0.100 255.255.255.0
[Switch-Vlan-interface501] quit
```

Assign an IP address to VLAN-interface 600.

```
[Switch] interface vlan-interface 600
```

```
[Switch-Vlan-interface600] ip address 99.100.0.100 255.255.255.0
[Switch-Vlan-interface600] quit
```

Assign an IP address to VLAN-interface 2. This address will be used as the gateway address for the INC server.

```
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] ip address 8.1.1.190 255.255.255.0
[Switch-Vlan-interface2] quit
```

Configuring the DHCP server

Details not shown.

Configuring the INC server

In this example, the INC server runs INC PLAT 7.3 (E0504), INC INC - EIA 7.3 (E0503), and INC EIP 7.3 (E0503).

Configure the RADIUS server

1. Add AC 1 as an access device:
 - a. Log in to INC and click the **User** tab.
 - b. From the navigation pane, select **User Access Policy > Access Device Management > Access Device**.
 - c. Click **Add**.
The **Add Access Device** page opens.
 - d. In the **Access Configuration** area, configure the following parameters:
 - Enter **radius** in the **Shared Key** and **Confirm Shared Key** fields. Make sure the key is the same as the key configured on the ACs.
 - Use the default values for other parameters.
 - e. In the **Device List** area, click **Select** or **Add Manually** to add AC 1 at 99.1.0.5 as an access device.
 - f. Click **OK**.

Figure 2 Adding an access device

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

Access Configuration

Authentication Port *	1812	Accounting Port *	1813
Service Type	LAN Access Service		
Access Device Type	H3C(General)	Service Group	Ungrouped
Shared Key *	radius	Confirm Shared Key *	radius
Access Device Group	--		
Certificate Authentication	<input checked="" type="radio"/> None <input type="radio"/> EAP		
Certificate Type	EAP-TLS Authn		

Device List

Select Add Manually Clear All

Device Name	Device IP	Device Model	Comments	Delete
wx5540h-lrf	99.1.0.5	wx5540h-lrf	wx5540h-lrf	

Total Items: 1.

OK Cancel

2. Repeat the previous step to add AC 2 as an access device.

The IP address of AC 2 is 99.1.0.9.

Configure the portal server

1. Configure portal authentication:
 - a. Click the **User** tab.
 - b. Select **User Access Policy > Portal Service > Server** from the navigation tree to open the portal server configuration page.
 - c. Configure the portal server parameters as needed.
This example uses the default settings.
 - d. Click **OK**.

Figure 3 Portal authentication server configuration

User > User Access Policy > Portal Service > Server

Portal Server

Basic Information

Log Level * Info

Portal Server

Request Timeout(Seconds) * 4

User Heartbeat Interval(Minutes) * 5

Server Heartbeat Interval(Seconds) * 20

LB Device Address

Portal Web

Request Timeout(Seconds) * 15

Verify Endpoint Requests Yes

HTTP Heartbeat Display New Page

Packet Code

Use Cache Yes

HTTPS Heartbeat Display Original Page

Portal Page

http://8.1.1.195:8080/portal/
https://8.1.1.195:8443/portal/
http://[8:195]:8080/portal/
https://[8:195]:8443/portal/

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

Figure 4 Adding an IP address group

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

Add IP Group

IP Group Name *	w05995-wx5540h-irf-ipaddgroup
Start IP *	99.100.0.1
End IP *	99.100.0.255
Service Group	Ungrouped
Action *	Normal

OK Cancel

3. Add AC 1 as a portal device:
 - a. Select **User Access Policy > Portal Service > Device** from the navigation tree to open the portal device configuration page.
 - b. Click **Add** to open the page as shown in [Figure 5](#).
 - c. Enter the device name.
 - d. Specify the version as **Portal 2.0**.
 - e. Enter the portal BAS-IP configured on AC 1 as the IP address.
 - f. Set whether to support the portal server heartbeat and user heartbeat functions.
In this example, select **No** for both **Support Server Heartbeat** and **Support User Heartbeat**.
 - g. Enter the key, which must be the same as that configured on the AC.
 - h. Select **Directly Connected** from the **Access Method** list.
 - i. Use the default settings for other parameters.
 - j. Click **OK**.

Figure 5 Adding a portal device


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

Add Device

Device Information

Device Name *	WX5540H-IRF	Service Group *	Ungrouped
Version *	Portal 2.0	IP Address *	99.1.0.5
Listening Port *	2000	Local Challenge *	No
Authentication Retries *	0	Logout Retries *	1
Support Server Heartbeat *	No	Support User Heartbeat *	No
Key *	*****	Confirm Key *	*****
Access Method *	Directly Connected		
Device Description			

OK Cancel

4. Repeat the previous step to add AC 2 as a portal device.
5. Associate AC 1 with the IP address group:
 - a. As shown in [Figure 6](#), click the **Port Group Information Management** icon  for the device to open the port group configuration page.
 - b. Click **Add** to open the page as shown in [Figure 7](#).

- c. Enter the port group name.
- d. Select the configured IP address group.
The IP address used by the user to access the network must be within this IP address group.
- e. Select **Supported** for **Transparent Authentication**.
- f. Use the default settings for other parameters.
- g. Click **OK**.

Figure 6 Device list

User > User Access Policy > Portal Service > Device

Query Devices

Device Name: Version:

Deploy Result: Service Group:

Add

Device Name	Version	Service Group	IP Address	Last Deployed at	Deploy Result	Operation
WX5540H-IRF	Portal 2.0	Ungrouped	99.1.0.5		Not Deployed	

Figure 7 Adding a port group

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

Add Port Group

Port Group Name: 05995-wx5540h-irf-portgroup Language: English

Start Port: 0 End Port: zzzzzz

Protocol: HTTP Quick Authentication: No

NAT or Not: No Error Transparent Transmission: Yes

Authentication Type: PAP IP Group: w05995-wx5540h-irf-ipaddgroup

Heartbeat Interval(Minutes): 0 Heartbeat Timeout(Minutes): 0

User Domain: Port Group Description:

Transparent Authentication: Supported Client Protection Against Cracks: No

Page Push Policy: Default Authentication Page:

OK Cancel

6. Repeat the previous step to associate AC 2 with the IP address group.

Configuring access settings

1. Add an access policy:
 - a. Select **User Access Policy > Access Policy** from the navigation tree to open the access policy page.
 - b. Click **Add** to open the page as shown in [Figure 8](#).
 - c. Enter the access policy name. In this example, the name is **w05995_portal**.
 - d. Select a service group.
 - e. Use the default settings for other parameters.
 - f. Click **OK**.

Figure 8 Adding an access policy

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

Basic Information

Access Policy Name * w05995_portal

Service Group * Ungrouped

Description

Authorization Information

Access Period None

Allocate IP * No

Downstream Rate(Kbps)

Upstream Rate(Kbps)

Priority

Deploy VLAN

☐ Deploy User Profile

☐ Deploy ACL

Deploy User Group

2. Add an access service:
 - a. Select **User Access Policy > Access Service** from the navigation tree to open the access service page.
 - b. Click **Add** to open the page as shown in [Figure 9](#).
 - c. Enter the service name. In this example, the service name is **w05995_portal**.
 - d. Select the **Transparent Authentication on Portal Endpoints** option.
 - e. Use the default settings for other parameters.
 - f. Click **OK**.

Figure 9 Adding an access service

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

Basic Information

Service Name * w05995_portal

Service Group * Ungrouped

Default Proprietary Attribute Assignment Policy * Do not use

Default Max. Number of Bound Endpoints * 0

Description

☒ Available

Service Suffix

Default Access Policy * w05995_portal

Default Max. Number of Online Endpoints * 0

☒ Transparent Authentication

3. Add an access user:
 - a. Select **Access User > All Access Users** from the navigation tree to open the access user page.
 - b. Click **Add** to open the page as shown in [Figure 10](#).
 - c. Select or add an access user.
 - d. Set the password. In this example, the password is w05995_portal.
 - e. Retain the default settings for other parameters.
 - f. Click **OK**.

Figure 10 Adding an access user

4. Configure system parameters:
 - a. Select **User Access Policy > Service Parameters > System Settings** from the navigation tree to open the system settings page.
 - b. Click the **Configure** icon for **User Endpoint Settings** to open the page as shown in [Figure 11](#).
 - c. Enable **Transparent MAC Authentication**.
 - d. Select whether to enable transparent portal authentication on non-smart devices. In this example, select **Enable** for **Non-Terminal Authentication**.
 - e. Click **OK**.
 - f. Click the **Configure** icon for **Endpoint Aging Time** to open the page as shown in [Figure 12](#).
 - g. Set the endpoint aging time as needed. This example uses the default value.

Figure 11 Configuring user endpoint settings

Figure 12 Setting the endpoint aging time

Verifying the configuration

Verifying dual-link backup configuration

Make the AP come online.

Verify that the AP first associates with AC 1. Shut down VLAN-interface 501 on AC 1, wait 3 minutes, and verify that the AP associates with AC 2 and the AP state on AC 2 is **R/M**.

Bring up VLAN-interface 501 on AC 1. Verify that the AP state becomes R/M on AC 1 and R/B on AC 2.

Verifying transparent authentication configuration

If user and client MAC address information is not recorded on the RADIUS server, MAC authentication fails. Verify that the AC ignores the authentication failure and triggers portal authentication.

```
[AC1] display portal user all
Total portal users: 1
Username: w05995_portal
  AP name: ap1
  Radio ID: 2
  SSID: service
  Portal server: newpt
  State: Online
  VPN instance: N/A
  MAC          IP          VLAN    Interface
a89c-ed90-7730 99.100.0.12 600     WLAN-BSS2/0/2141
Authorization information:
  DHCP IP pool: N/A
  User profile: N/A
  Session group profile: N/A
  ACL number: N/A
  Inbound CAR: N/A
  Outbound CAR: N/A
```

After portal authentication, the RADIUS server records user and client MAC address information. At next associations, the client can pass MAC authentication and access network resources without passing portal authentication.

Display MAC-authenticated user information.

```
[AC1] display mac-authentication connection
Total connections: 1
User MAC address      : c486-e95f-033f
AP name               : ap1
Radio ID              : 2
SSID                  : 05995-service-mac
BSSID                 : 600b-03fc-46d1
Username              : c486e95f033f
Authentication domain : dm2
```

```

Initial VLAN                : 600
Authorization VLAN          : 600
Authorization ACL number    : N/A
Authorization user profile   : N/A
Authorization CAR            : N/A
Authorization URL            : N/A
Termination action          : Default
Session timeout last from   : 2019/10/17 19:09:48
Session timeout period      : 86400 s
Online from                 : 2019/10/17 19:09:48
Online duration             : 0h 0m 20s

```

Configuration files

- AC 1:


```

#
vlan 501
#
vlan 600
#
wlan service-template st1
    ssid service
    vlan 600
    client forwarding-location ap
akm mode psk
preshared-key pass-phrase cipher $c$3$oLf6pOZ6bxrf25nodjOJKYEfnZ6g6ErccHyQ
cipher-suite ccmp
security-ie rsn
client-security authentication-mode mac
client-security ignore-authentication
mac-authentication domain dm2
portal enable method direct
portal domain dm1
portal bas-ip 99.1.0.5
portal apply web-server newpt
service-template enable
#
interface Bridge-Aggregation1
#
interface Vlan-interface501
    ip address 99.1.0.5 255.255.255.0
#
interface GigabitEthernet1/0/1
    port link-type trunk
    port trunk permit vlan 1 501 600
#
    ip route-static 8.1.1.0 24 99.1.0.100
#

```

```

radius session-control enable
#
radius scheme rs1
primary authentication 8.1.1.195
primary accounting 8.1.1.195
key authentication cipher $c$3$/Mc+yQtK3k6E3L0TtJth+7Pel1EBrSZAmg==
key accounting cipher $c$3$WoQkH/FblsUGadr043yY0MGAPHWTIQvUdA==
user-name-format without-domain
nas-ip 99.1.0.5
#
domain dm1
authorization-attribute idle-cut 15 1024
authentication portal radius-scheme rs1
authorization portal radius-scheme rs1
accounting portal radius-scheme rs1
#
domain dm2
authentication lan-access radius-scheme rs1
authorization lan-access radius-scheme rs1
accounting lan-access radius-scheme rs1
#
portal host-check enable
portal free-rule 0 destination ip 8.1.1.0 255.255.255.0
portal free-rule 1 destination ip any udp 53
portal free-rule 2 destination ip any tcp 53
#
portal web-server newpt
url http://8.1.1.195:8080/portal
url-parameter nasip value 99.1.0.5
#
portal server newpt
ip 8.1.1.195 key cipher $c$3$GZf8+GypB2tLYA25pKOLrJu3quh+vnFE1Q==
#
wlan ap-group group1
priority 7
wlan tunnel-preempt enable
backup-ac ip 99.1.0.9
ap ap1
ap-model AP 3620
map-configuration flash:/map.txt
radio 1
radio 2
radio enable
service-template st1
#
wlan ap ap1 model AP 3620
serial-id 219801A28N819CE0002T
#

```

- **AC 2:**

```
#
vlan 501
#
vlan 600
#
wlan service-template st1
    ssid service
    vlan 600
    client forwarding-location ap
akm mode psk
    preshared-key pass-phrase cipher $c$3$oLf6pOZ6bxrf25nodjOJKYEfnZ6g6ErccHyQ
    cipher-suite ccmp
    security-ie rsn
    client-security authentication-mode mac
    client-security ignore-authentication
    mac-authentication domain dm2
    portal enable method direct
    portal domain dm1
    portal bas-ip 99.1.0.9
    portal apply web-server newpt
    service-template enable
#
interface Bridge-Aggregation1
#
interface Vlan-interface501
    ip address 99.1.0.9 255.255.255.0
#
interface GigabitEthernet1/0/1
    port link-type trunk
    port trunk permit vlan 1 501 600
#
    ip route-static 8.1.1.0 24 99.1.0.100
#
    radius session-control enable
#
radius scheme rs1
    primary authentication 8.1.1.195
    primary accounting 8.1.1.195
    key authentication cipher $c$3$/Mc+yQtK3k6E3L0TtJth+7Pel1EBrsZAMg==
    key accounting cipher $c$3$WoQkH/FblsUGadr043yY0MGAPHWTIQvUdA==
    user-name-format without-domain
    nas-ip 99.1.0.9
#
domain dm1
    authorization-attribute idle-cut 15 1024
    authentication portal radius-scheme rs1
    authorization portal radius-scheme rs1
```



```

    accounting portal radius-scheme rs1
#
domain dm2
    authentication lan-access radius-scheme rs1
    authorization lan-access radius-scheme rs1
    accounting lan-access radius-scheme rs1
#
portal host-check enable
portal free-rule 0 destination ip 8.1.1.0 255.255.255.0
portal free-rule 1 destination ip any udp 53
portal free-rule 2 destination ip any tcp 53
#
portal web-server newpt
    url http://8.1.1.195:8080/portal
    url-parameter nasip value 99.1.0.9
#
portal server newpt
    ip 8.1.1.195 key cipher $c$3$GZf8+GypB2tLYA25pKOLrJu3quh+vnFE1Q==
#
wlan ap-group group1
    priority 5
    wlan tunnel-preempt enable
    backup-ac ip 99.1.0.5
    ap ap1
    ap-model AP 3620
map-configuration flash:/map.txt
radio 1
    radio 2
    radio enable
    service-template st1
#
wlan ap ap1 model AP 3620
    serial-id 219801A28N819CE0002T
#

```

- **Switch:**

```

#
vlan 2
#
vlan 501
#
vlan 600
#
interface Vlan-interface2
    ip address 8.1.1.190 255.255.255.0
#
interface Vlan-interface501
    ip address 99.1.0.100 255.255.255.0
#

```

```

interface Vlan-interface600
 ip address 99.100.0.100 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 1 501 600
#
interface GigabitEthernet1/0/2
 port link-type trunk
 port trunk permit vlan 1 501 600
 port trunk pvid vlan 501
 poe enable
#
interface GigabitEthernet1/0/3
 port link-type trunk
 port trunk permit vlan 1 501 600
#
interface GigabitEthernet1/0/4
 port link-type trunk
 port trunk permit vlan 1 501 600
#

```

Related documentation

- *AAA Management Command Reference* in *INTELBRAS Access Controllers Command References*
- *AAA Management Configuration Guide* in *INTELBRAS Access Controllers Configuration Guides*
- *AP Management Command Reference* in *INTELBRAS Access Controllers Command References*
- *AP Management Configuration Guide* in *INTELBRAS Access Controllers Configuration Guides*
- *Portal Authentication Command Reference* in *INTELBRAS Access Controllers Command References*
- *Portal Authentication Configuration Guide* in *INTELBRAS Access Controllers Configuration Guides*
- *WLAN Access Command Reference* in *INTELBRAS Access Controllers Command References*
- *WLAN Access Configuration Guide* in *INTELBRAS Access Controllers Configuration Guides*
- *WLAN High Availability Command Reference* in *INTELBRAS Access Controllers Command References*
- *WLAN High Availability Configuration Guide* in *INTELBRAS Access Controllers Configuration Guides*

INTELBRAS Access Controllers

Dual-Link Backup Remote Portal Authentication in Local Forwarding Configuration Examples

Copyright © 2024 Intelbras S.A All rights reserved.

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

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

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

Contents

Introduction	1
Prerequisites	1
Example: Configuring remote portal authentication for dual-link AC backup and local forwarding	1
Network configuration	1
Analysis	2
Restrictions and guidelines	2
Procedures	3
Editing the AP configuration file	3
Configuring AC 1	3
Configuring AC 2	6
Configuring the switch	9
Configuring the DHCP server	10
Configuring the INC server	11
Verifying the configuration	16
Configuration files	18
Related documentation	22

Introduction

The following information provides an example for configuring remote portal authentication with local forwarding.

Prerequisites

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

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

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

Example: Configuring remote portal authentication for dual-link AC backup and local forwarding

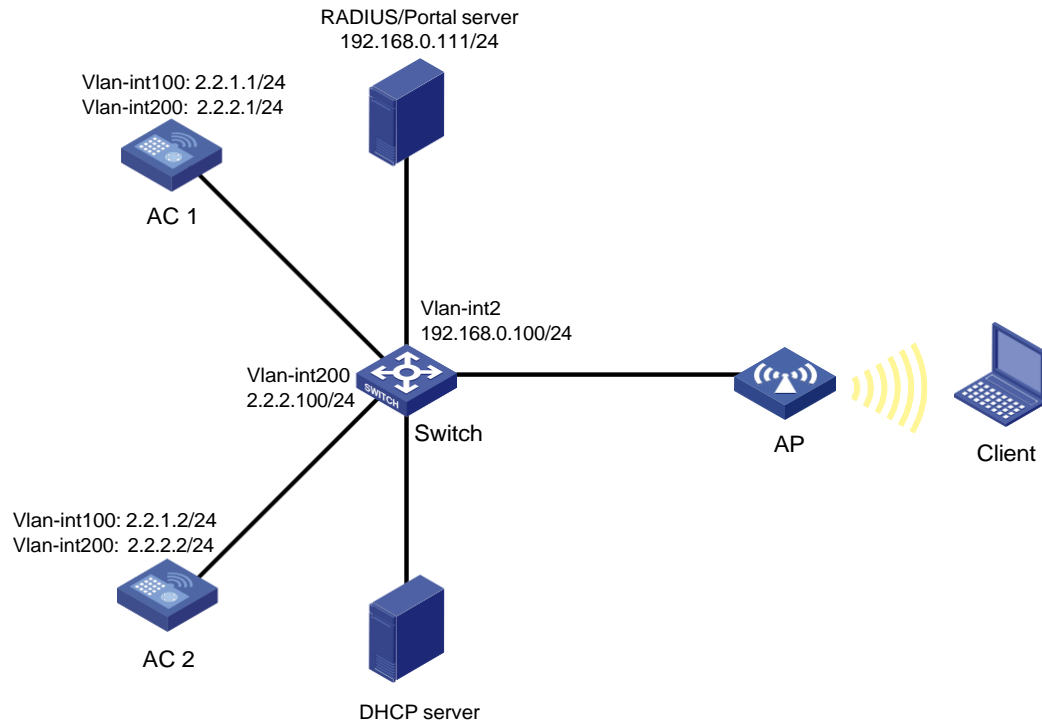
Network configuration

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

Configure the devices to meet the following requirements:

- The AP associates with both ACs and the two ACs to back up each other. When the master AC (AC 1) fails, the backup AC (AC 2) takes over, and the AP can provide services correctly through the backup AC.
- Direct portal authentication is used for wireless clients.
- Before passing portal authentication, the client can access only the portal Web server. After passing the authentication, the client can access other network resources.
- The AP forwards all the client traffic.
- The client can access network resources through any Layer 2 ports in its access VLAN without re-authentication.
- The INC server can dynamically modify user authorization information and log off clients.

Figure 1 Network diagram



Analysis

- To allow an authenticated user to access network resources on any Layer 2 ports in its access VLAN without re-authentication, you must enable the portal roaming feature.
- In a local-forwarding WLAN, the AC does not keep ARP entries for portal clients. To ensure that valid users can perform portal authentication, you must enable wireless client validity check on the AC.
- To avoid possible authentication failure caused by frequent logins and logouts of portal clients in a short time, disable the Rule ARP entry feature.
- To allow the RADIUS server to modify user authorization information and log off users, enable the RADIUS session-control feature.
- To assign interface GigabitEthernet 1/0/1 on the AP to VLAN 200 for local forwarding, you must edit the configuration file of the AP and then upload the file to the storage medium of the AC.

Restrictions and guidelines

When you configure remote portal authentication for dual-link AC backup and local forwarding, follow these restrictions and guidelines:

- Use the actual serial ID of an AP to uniquely identify that AP.
- If you configure manual APs, make sure the manual APs configured on the two ACs have the same AP name and identifier (serial ID or MAC address).
- Make sure the two ACs are of the same version.
- Make sure the portal authentication server type and portal Web server type configured on the ACs are the same as the actual server type. This example uses an INC server.

- To avoid possible authentication failure caused by frequent logins and logouts of portal clients in a short time, disable the Rule ARP entry feature.
- To allow the RADIUS server to modify user authorization information and log off users, enable the RADIUS session-control feature.
- URLs redirected from the ACs to the portal Web server do not carry parameters by default. You can configure the parameters to carry as needed.
- If you enable portal authentication in VLAN interface view, only centralized forwarding is supported. If you enable portal authentication in service template view, both centralized forwarding and local forwarding are supported. This example enables portal authentication in service template view.
- In a local-forwarding WLAN, the AC does not keep ARP entries for portal clients. To ensure that valid users can perform portal authentication, you must enable wireless client validity check on the AC.
- Make sure the two ACs have the same portal-free rule settings, including the rule numbers.
- Make sure the two ACs have the same portal authentication settings, except for the portal Web server, portal BAS-IP, and interface used by clients to access the AC during portal authentication.
- You must upload the AP configuration file to both the master and backup ACs.

Procedures

Editing the AP configuration file

Use a text editor to edit the AP configuration file, name the file **map.txt**, and then upload the file to the storage medium of the ACs. The file content and format are as follows:

```
system-view
vlan 600
interface gigabitethernet1/0/1
port link-type trunk
port trunk permit vlan 600
```

Configuring AC 1

1. Configure AC interfaces:

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

```
<AC1> system-view
[AC1] vlan 100
[AC1-vlan100] quit
[AC1] interface vlan-interface 100
[AC1-Vlan-interface100] ip address 2.2.1.1 24
[AC1-Vlan-interface100] quit
```

Create VLAN 200 and VLAN-interface 200. Assign the VLAN interface an IP address. Clients will use this VLAN to access the WLAN.

```
[AC1] vlan 200
[AC1-vlan200] quit
[AC1] interface vlan-interface 200
[AC1-Vlan-interface200] ip address 2.2.2.1 24
[AC1-Vlan-interface200] quit
```

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

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

2. Configure a static route to the INC server.

```
[AC1] ip route-static 192.168.0.0 255.255.255.0 2.2.2.100
```

3. Configure wireless services:

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

```
[AC1] wlan service-template st1
```

Specify the SSID as **service**.

```
[AC1-wlan-st-st1] ssid service
```

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

```
[AC1-wlan-st-st1] vlan 200
```

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

```
[AC1-wlan-st-st1] akm mode psk
```

```
[AC1-wlan-st-st1] preshared-key pass-phrase simple 12345678
```

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

```
[AC1-wlan-st-st1] cipher-suite ccmp
```

```
[AC1-wlan-st-st1] security-ie rsn
```

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

```
[AC1-wlan-st-st1] client forwarding-location ap
```

```
[AC1-wlan-st-st1] quit
```

4. Configure the AP:

NOTE:

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

Create AP **office**, and specify the AP model and serial ID.

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

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

```
[AC1-wlan-ap-office] quit
```

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

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

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

Set the AP connection priority to 7.

```
[AC1-wlan-ap-group-group1] priority 7
```

Specify AC 2 as the backup AC for AC 1.

```
[AC1-wlan-ap-group-group1] backup-ac ip 2.2.1.2
```

Enable master CAPWAP tunnel preemption.

```
[AC1-wlan-ap-group-group1] wlan tunnel-preempt enable
```

Deploy configuration file **map.txt** to the AP in the AP model view of AP group **group1**.

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

```
[AC1-wlan-ap-group-group1-ap-model-AP 3620] map-configuration map.txt
```

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

```
[AC1-wlan-ap-group-group1-ap-model-AP 3620] radio 2
```


- ```
[AC1-wlan-ap-group-group1-ap-model-AP 3620-radio-2] service-template st1
```
- # Enable radio 2.**
- ```
[AC1-wlan-ap-group-group1-ap-model-AP 3620-radio-2] radio
enable [AC1-wlan-ap-group-group1-ap-model-AP 3620-radio-2] quit
[AC1-wlan-ap-group-group1-ap-model-AP 3620]
quit [AC1-wlan-ap-group-group1] quit
```
- 5. Configure a RADIUS scheme:**
- # Create RADIUS scheme **rs1**.**
- ```
[AC1] radius scheme rs1
```
- # Specify the IP addresses of the primary authentication and accounting RADIUS servers.**
- ```
[AC1-radius-rs1] primary authentication 192.168.0.111
[AC1-radius-rs1] primary accounting 192.168.0.111
```
- # Specify shared keys for RADIUS authentication and accounting.**
- ```
[AC1-radius-rs1] key authentication simple radius
[AC1-radius-rs1] key accounting simple radius
```
- # Configure AC 1 to remove the ISP domain name from the usernames sent to the RADIUS servers.**
- ```
[AC1-radius-rs1] user-name-format without-domain
[AC1-radius-rs1] nas-ip 2.2.2.1
[AC1-radius-rs1] quit
```
- # Enable RADIUS session-control.**
- ```
[AC1] radius session-control enable
```
- 6. Configure the authentication domain:**
- # Create domain **dm1** and enter its view.**
- ```
[AC1] domain dm1
```
- # Configure the domain to use RADIUS scheme **rs1** for authentication, authorization, and accounting.**
- ```
[AC1-isp-dm1] authentication portal radius-scheme rs1
[AC1-isp-dm1] authorization portal radius-scheme rs1
[AC1-isp-dm1] accounting portal radius-scheme rs1
```
- # Set the client idle timeout to 15 minutes and set the minimum threshold to 1024 bytes for clients in ISP domain **dm1**.**
- ```
[AC1-isp-dm1] authorization-attribute idle-cut 15 1024
[AC1-isp-dm1] quit
```
- 7. Configure portal authentication:**
- # Create the portal authentication server **newpt**, specify the server IP address as 192.168.0.111, and set the destination UDP port number to **50100** for the AC to send unsolicited portal packets to the portal authentication server.**
- ```
[AC1] portal server newpt
[AC1-portal-server-newpt] ip 192.168.0.111 key simple radius
[AC1-portal-server-newpt] port 50100
```
- # Set the server type as INC.**
- ```
[AC1-portal-server-newpt] server-type iNC
[AC1-portal-server-newpt] quit
```
- # Configure the URL for the portal Web server **newpt** as **http://192.168.0.111:8080/portal**.**
- ```
[AC1] portal web-server newpt
[AC1-portal-websvr-newpt] url http://192.168.0.111:8080/portal
```

# Configure URL parameters **nasip** for the portal Web server **newpt**. Configure the value of the **nasip** parameter as 2.2.2.1.

```
[AC1-portal-websvr-newpt] url-parameter nasip value 2.2.2.1
[AC1-portal-websvr-newpt] quit
```

# Configure an IPv4-based portal-free rule to permit portal Web server traffic.

```
[AC1] portal free-rule 0 destination ip 192.168.0.111 24
```

# Configure IPv4-based portal-free rules to permit DNS server traffic.

```
[AC1] portal free-rule 1 destination ip any udp 53
[AC1] portal free-rule 2 destination ip any tcp 53
```

# Enable intra-VLAN roaming for portal users.

```
[AC1] portal roaming enable
```

# Disable the Rule ARP entry feature for portal clients.

```
[AC1] undo portal refresh arp enable
```

# Enable validity check on wireless portal clients.

```
[AC1] portal host-check enable
```

# Enable direct IPv4 portal authentication for service template **st1**.

```
[AC1] wlan service-template st1
[AC1-wlan-st-st1] portal enable method direct
```

# Configure the authentication domain for IPv4 portal users as **dm1** on service template **st1**.

```
[AC1-wlan-st-st1] portal domain dm1
```

# Specify portal Web server **newpt** on service template **st1** to redirect portal user HTTP or HTTPS requests to the server.

```
[AC1-wlan-st-st1] portal apply web-server newpt
```

# Specify the BAS IP as the IP address of VLAN-interface 200, from which clients come online from AC 1.

```
[AC1-wlan-st-st1] portal bas-ip 2.2.2.1
```

# Enable the service template.

```
[AC1-wlan-st-st1] service-template enable
[AC1-wlan-st-st1] quit
```

## 8. Configure MAC authentication:

# Set the authentication mode to **mac**.

```
[AC1-wlan-st-st1] client-security authentication-mode mac
```

# Configuring AC 2

## 1. Configure AC interfaces:

# Create VLAN 501 and VLAN-interface 100. Assign the VLAN interface an IP address. The AC will use this IP address to establish a CAPWAP tunnel with the AP.

```
<AC2> system-view
[AC2] vlan 100
[AC2-vlan100] quit
[AC2] interface vlan-interface 100
[AC2-Vlan-interface100] ip address 2.2.1.2 24
[AC2-Vlan-interface100] quit
```

# Create VLAN 200 and VLAN-interface 200. Assign the VLAN interface an IP address. Clients will use this VLAN to access the WLAN.

```
[AC2] vlan 200
[AC2-vlan200] quit
```

```
[AC2] interface vlan-interface 200
[AC2-Vlan-interface200] ip address 2.2.2.2 24
[AC2-Vlan-interface200] quit
```

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

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

**2. Configure a static route to the INC server.**

```
[AC2] ip route-static 192.168.0.0 255.255.255.0 2.2.2.100
```

**3. Configure wireless services:**

**# Create service template **st1** and enter its view.**

```
[AC2] wlan service-template st1
```

**# Specify the SSID as **service**.**

```
[AC2-wlan-st-st1] ssid service
```

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

```
[AC2-wlan-st-st1] vlan 200
```

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

```
[AC2-wlan-st-st1] akm mode psk
```

```
[AC2-wlan-st-st1] preshared-key pass-phrase simple 12345678
```

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

```
[AC2-wlan-st-st1] cipher-suite ccmp
```

```
[AC2-wlan-st-st1] security-ie rsn
```

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

```
[AC2-wlan-st-st1] client forwarding-location ap
```

```
[AC2-wlan-st-st1] quit
```

**4. Configure the AP:**

---

**NOTE:**

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

---

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

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

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

```
[AC2-wlan-ap-office] quit
```

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

```
[AC2] wlan ap-group group1
```

```
[AC2-wlan-ap-group-group1] ap office
```

**# Set the AP connection priority to 6.**

```
[AC2-wlan-ap-group-group1] priority 6
```

**# Specify AC 1 as the backup AC for AC 2.**

```
[AC2-wlan-ap-group-group1] backup-ac ip 2.2.1.1
```

**# Enable master CAPWAP tunnel preemption.**

```
[AC2-wlan-ap-group-group1] wlan tunnel-preempt enable
```

**# Deploy configuration file **map.txt** to the AP in the AP model view of AP group **group1**.**

```
[AC2-wlan-ap-group-group1] ap-model AP 3620
```

- ```
[AC2-wlan-ap-group-group1-ap-model-AP 3620] map-configuration map.txt
```
- # Bind service template **st1** to radio 2 in AP group **group1**.**
- ```
[AC2-wlan-ap-group-group1-ap-model-AP 3620] radio 2
[AC2-wlan-ap-group-group1-ap-model-AP 3620-radio-2] service-template st1
```
- # Enable radio 2.**
- ```
[AC2-wlan-ap-group-group1-ap-model-AP 3620-radio-2] radio
enable [AC2-wlan-ap-group-group1-ap-model-AP 3620-radio-2] quit
[AC2-wlan-ap-group-group1-ap-model-AP 3620]
quit [AC2-wlan-ap-group-group1] quit
```
- 5. Configure a RADIUS scheme:**
- # Create RADIUS scheme **rs1**.**
- ```
[AC2] radius scheme rs1
```
- # Specify the IP addresses of the primary authentication and accounting RADIUS servers.**
- ```
[AC2-radius-rs1] primary authentication 192.168.0.111
[AC2-radius-rs1] primary accounting 192.168.0.111
```
- # Specify shared keys for RADIUS authentication and accounting.**
- ```
[AC2-radius-rs1] key authentication simple radius
[AC2-radius-rs1] key accounting simple radius
```
- # Configure AC 1 to remove the ISP domain name from the usernames sent to the RADIUS servers.**
- ```
[AC2-radius-rs1] user-name-format without-domain
[AC2-radius-rs1] nas-ip 2.2.2.2
[AC2-radius-rs1] quit
```
- # Enable RADIUS session-control.**
- ```
[AC2] radius session-control enable
```
- 6. Configure the authentication domain for portal authentication:**
- # Create domain **dm1** and enter its view.**
- ```
[AC2] domain dm1
```
- # Configure the domain to use RADIUS scheme **rs1** for authentication, authorization, and accounting.**
- ```
[AC2-isp-dm1] authentication portal radius-scheme rs1
[AC2-isp-dm1] authorization portal radius-scheme rs1
[AC2-isp-dm1] accounting portal radius-scheme rs1
```
- # Set the client idle timeout to 15 minutes and set the minimum threshold to 1024 bytes for clients in ISP domain **dm1**.**
- ```
[AC2-isp-dm1] authorization-attribute idle-cut 15 1024
[AC2-isp-dm1] quit
```
- 7. Configure portal authentication:**
- # Create the portal authentication server **newpt**, specify the server IP address as 192.168.0.111, and set the destination UDP port number to **50100** for the AC to send unsolicited portal packets to the portal authentication server.**
- ```
[AC2] portal server newpt
[AC2-portal-server-newpt] ip 192.168.0.111 key simple radius
[AC2-portal-server-newpt] port 50100
```
- # Set the server type as INC.**
- ```
[AC2-portal-server-newpt] server-type inc
[AC2-portal-server-newpt] quit
```
- # Configure the URL for the portal Web server **newpt** as **http://192.168.0.111:8080/portal** .**

```

[AC2] portal web-server newpt
[AC2-portal-websvr-newpt] url http://192.168.0.111:8080/portal
# Configure URL parameters nasip for the portal Web server newpt. Configure the value of the
nasip parameter as 2.2.2.2.
[AC2-portal-websvr-newpt] url-parameter nasip value 2.2.2.2
[AC2-portal-websvr-newpt] quit
# Configure an IPv4-based portal-free rule to permit portal Web server traffic.
[AC2] portal free-rule 0 destination ip 192.168.0.111 24
# Configure IPv4-based portal-free rules to permit DNS server traffic.
[AC2] portal free-rule 1 destination ip any udp 53
[AC2] portal free-rule 2 destination ip any tcp 53
# Enable intra-VLAN roaming for portal users.
[AC2] portal roaming enable
# Disable the Rule ARP entry feature for portal clients.
[AC2] undo portal refresh arp enable
# Enable validity check on wireless portal clients.
[AC2] portal host-check enable
# Enable direct IPv4 portal authentication for service template st1.
[AC2] wlan service-template st1
[AC2-wlan-st-st1] portal enable method direct
# Configure the authentication domain for IPv4 portal users as dm1 on service template st1.
[AC2-wlan-st-st1] portal domain dml
# Specify portal Web server newpt on service template st1 to redirect user HTTP or HTTPS
requests to the server.
[AC2-wlan-st-st1] portal apply web-server newpt
# Specify the BAS IP as the IP address of VLAN-interface 200, from which clients come online
from AC 2.
[AC2-wlan-st-st1] portal bas-ip 2.2.2.2
# Enable the service template.
[AC2-wlan-st-st1] service-template enable
[AC2-wlan-st-st1] quit

```

Configuring the switch

```

# Create VLAN 100 for forwarding CAPWAP tunnel traffic between AC and AP.
<Switch> system-view
[Switch] vlan 100
[Switch-vlan100] quit
# Create VLAN 200 for forwarding client traffic.
[Switch] vlan 200
[Switch-vlan200] quit
# Create VLAN 2 for connecting to the INC server.
[Switch] vlan 2
[Switch-vlan2] quit
# Add the interface that connects the switch to the INC server to VLAN 2. (Details not shown.)
# Configure GigabitEthernet 1/0/1 that connects the switch to AC 1 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 1/0/4 that connects the switch to AC 2 as a trunk port, and assign it to VLAN 100 and VLAN 200.

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

Configure GigabitEthernet 1/0/2 that connects the switch to the AP as a trunk port, set the PVID to VLAN 100, and assign the interface 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 pvid vlan 100
[Switch-GigabitEthernet1/0/2] port trunk permit vlan 100 200
```

Enable PoE.

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

Configure GigabitEthernet 1/0/3 that connects the switch to the DHCP server as a trunk port, and assign it to VLAN 100 and VLAN 200.

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

Assign an IP address to VLAN-interface 200.

```
[Switch] interface vlan-interface 200
[Switch-Vlan-interface200] ip address 2.2.2.100 255.255.255.0
[Switch-Vlan-interface200] quit
```

Assign an IP address to VLAN-interface 2. This address will be used as the gateway address for the INC server.

```
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] ip address 192.168.0.100 255.255.255.0
[Switch-Vlan-interface2] quit
```

Configuring the DHCP server

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

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

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

```
[DHCP Server] vlan 100
[DHCP Server-vlan100] quit
[DHCP Server] interface vlan-interface 100
```

```
[DHCP Server-Vlan-interface100] ip address 2.2.1.200 255.255.255.0
[DHCP Server-Vlan-interface100] quit
```

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

```
[DHCP Server] vlan 200
[DHCP Server-vlan200] quit
[DHCP Server] interface vlan-interface 200
[DHCP Server-Vlan-interface200] ip address 2.2.2.200 255.255.255.0
[DHCP Server-Vlan-interface200] quit
```

Enable DHCP.

```
[DHCP Server] dhcp enable
```

Create a DHCP address pool named **VLAN100** for the AP, specify the DHCP server as the gateway, and exclude the IP addresses of AC 1, AC 2, and DHCP server from dynamic allocation.

```
[DHCP Server] dhcp server ip-pool VLAN100
[DHCP Server-dhcp-pool-vlan100] gateway-list 2.2.1.200
[DHCP Server-dhcp-pool-vlan100] network 2.2.1.0 mask 255.255.255.0
[DHCP Server-dhcp-pool-vlan100] forbidden-ip 2.2.1.200 2.2.1.1 2.2.1.2
[DHCP Server-dhcp-pool-vlan100] quit
```

Create a DHCP address pool named **VLAN200** for the client, specify the switch as the gateway, and exclude the IP addresses of AC 1, AC 2, and switch from dynamic allocation.

```
[DHCP Server] dhcp server ip-pool VLAN200
[DHCP Server-dhcp-pool-vlan200] gateway-list 2.2.2.100
[DHCP Server-dhcp-pool-vlan200] network 2.2.2.0 mask 255.255.255.0
[DHCP Server-dhcp-pool-vlan200] dns-list 8.8.8.8
[DHCP Server-dhcp-pool-vlan200] forbidden-ip 2.2.2.100 2.2.2.1 2.2.2.2
[DHCP Server-dhcp-pool-vlan200] quit
```

Configuring the INC server

In this example, the INC server runs INC PLAT 7.3 (E0605), INC INC - EIA 7.3 (E0512), and INC EIP 7.3 (E0512).

Configure the RADIUS server

1. Add AC 1 as an access device:
 - a. Log in to INC and click the **User** tab.
 - b. From the navigation pane, select **User Access Policy > Access Device Management > Access Device**.
 - c. Click **Add**.
The **Add Access Device** page opens.
 - d. In the **Access Configuration** area, configure the following parameters:
 - Enter **radius** in the **Shared Key** and **Confirm Shared Key** fields. Make sure the key is the same as the key configured on the ACs.
 - Use the default values for other parameters.
 - e. In the **Device List** area, click **Select** or **Add Manually** to add AC 1 at 2.2.2.1 as an access device.
 - f. Click **OK**.

Figure 2 Adding an access device

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

Access Configuration

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

Device List

Select Add Manually Clear All

Device Name	Device IP	Device Model	Comments	Delete
	2.2.2.1			

Total Items: 1.

OK Cancel

2. Repeat the previous step to add AC 2 as an access device.
The IP address of AC 2 is 2.2.2.2.
3. Add an access policy.
 - a. From the navigation pane, select **User Access Policy > Access Policy**.
 - b. Click **Add**.
 - c. Enter the access policy name. In this example, the name is AccessPolicy.
 - d. Select the **Ungrouped** service group.
 - e. Use the default settings for other parameters.

Figure 3 Adding an access policy

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

Basic Information

Access Policy Name *	AccessPolicy
Service Group *	Ungrouped
Description	

Authorization Information

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

4. Add an access service.

- a. From the navigation pane, select **User Access Policy > Access Service**.
- b. Click **Add**.
- c. Enter the service name. In this example, the service name is **RadiusServer**.
- d. Select **AccessPolicy**.
- e. Use the default settings for other parameters.
- f. Click **OK**.

Figure 4 Adding an access service

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

Basic Information

Service Name * Service Suffix

Service Group * Default Access Policy *

Default Proprietary Attribute Assignment Policy * ?

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

Description

☒ Available ? ☐ Transparent Authentication on Portal Endpoints ?

Access Scenario List

Add

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

OK **Cancel**

5. Add an access user.
 - a. From the navigation pane, select **Access User > All Access Users**.
 - b. Click **Add**.
 - c. Select an existing access user or click **Add User** to add a new access user.
 - d. Specify the account name. In this example, the name is **client**.
 - e. Set the password.
 - f. Select service **RadiusServer**.
 - g. Use the default settings for other parameters.
 - h. Click **OK**.

Figure 5 Adding an access user

User > All Access Users > Add Access User

Access Information

User Name * **Select** **Add User**

Account Name * ?

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

Password * Confirm Password *

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

Start Time End Time

Max. Idle Time (Minutes) Max. Concurrent Logins

Login Message

Access Service

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

Binding Information

OK **OK & Print** **Cancel**

Configure the portal server

1. Configure portal authentication:
 - a. Click the **User** tab.
 - b. Select **User Access Policy > Portal Service > Server** from the navigation tree to open the portal server configuration page.
 - c. Permit different ports to be bound to the same IP address group, and configure the other portal server parameters as needed.
This example uses the default settings.
 - d. Click **OK**.

Figure 6 Portal authentication server configuration

User > User Access Policy > Portal Service > Server

Portal Server

Basic Information

Log Level * Info

Portal Server

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

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

Portal Web

Request Timeout(Seconds) * 15 ? Packet Code ?

Verify Endpoint Requests Yes Use Cache Yes

HTTP Heartbeat Display New Page HTTPS Heartbeat Display Original Page

Portal Page

http://192.168.0.111:8080/portal/

192.168.0.111

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

Figure 7 Adding an IP address group

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

Add IP Group

IP Group Name * Portal_user

Start IP * 2.2.2.1

End IP * 2.2.2.255

Service Group Ungrouped

Action * Normal

OK Cancel

3. Add AC 1 as a portal device:
 - a. Select **User Access Policy > Portal Service > Device** from the navigation tree to open the portal device configuration page.
 - b. Click **Add** to open the page as shown in [Figure 8](#).
 - c. Enter the device name.
 - d. Specify the version as **Portal 2.0**.
 - e. Enter the portal BAS-IP configured on AC 1 as the IP address.
 - f. Set whether to support the portal server heartbeat and user heartbeat functions.
In this example, select **No** for both **Support Server Heartbeat** and **Support User Heartbeat**.
 - g. Enter the key, which must be the same as that configured on the AC.
 - h. Select **Directly Connected** from the **Access Method** list.
 - i. Use the default settings for other parameters.
 - j. Click **OK**.

Figure 8 Adding a portal device

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

Add Device

Device Information

Device Name * NAS

Version * Portal 2.0

Listening Port * 2000

Authentication Retries * 0

Support Server Heartbeat * No

Key * *****

Access Method * Directly Connected

Device Description

Service Group * Ungrouped

IP Address * 2.2.2.1


Local Challenge * No

Logout Retries * 1

Support User Heartbeat * No

Confirm Key * *****

OK Cancel

4. Repeat the previous step to add AC 2 as a portal device.
5. Associate AC 1 with the IP address group:
 - a. As shown in [Figure 9](#), click the **Port Group Information Management** icon  for the device to open the port group configuration page.

- b. Click **Add** to open the page as shown in [Figure 10](#).
- c. Enter the port group name. In this example, the name is **Portal_user**.
- d. Select the configured IP address group.
The IP address used by the user to access the network must be within this IP address group.
- e. Use the default settings for other parameters.
- f. Click **OK**.

Figure 9 Device list

Figure 10 Adding a port group

6. Repeat the previous step to associate AC 2 with the IP address group.

Verifying the configuration

Make the AP come online.

Verify that the AP first associates with AC 1. Shut down VLAN-interface 100 on AC 1, wait 3 minutes, and verify that the AP associates with AC 2 and the AP state on AC 2 is **R/M**.

Bring up VLAN-interface 100 on AC 1. Verify that the AP state becomes R/M on AC 1 and R/B on AC 2.

```
<AC1> display wlan ap all
Total number of APs: 1
Total number of connected APs: 1
Total number of connected manual APs: 1
Total number of connected auto APs: 0
Total number of connected common APs: 1
Total number of connected WTUs: 0
Total number of inside APs: 0
Maximum supported APs: 64
```

Remaining APs: 63
Total AP licenses: 16
Local AP licenses: 16
Server AP licenses: 0
Remaining Local AP licenses: 15
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
office	1	R/M	AP 3620	219801A28N819CE0002T

<AC2> display wlan ap all

Total number of APs: 1
Total number of connected APs: 1
Total number of connected manual APs: 1
Total number of connected auto APs: 0
Total number of connected common APs: 1
Total number of connected WTUs: 0
Total number of inside APs: 0
Maximum supported APs: 64
Remaining APs: 63
Total AP licenses: 16
Local AP licenses: 16
Server AP licenses: 0
Remaining Local AP licenses: 16
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
office	1	R/B	AP 3620	219801A28N819CE0002T

Verify that all Web requests are redirected to the portal authentication page (<http://192.168.0.111:8080/portal>) before you pass portal authentication, and you can access Internet resources after being authenticated.

View online port user information generated on AC 1.

[AC1] display portal user all

Total portal users: 1

Username: Client

AP name: office

Radio ID: 2

SSID: service

Portal server: newpt

State: Online

VPN instance: N/A

MAC	IP	VLAN	Interface
0021-6330-0933	2.2.2.3	200	WLAN-BSS1/0/16

Authorization information:

DHCP IP pool: N/A

User profile: N/A

Session group profile: N/A

ACL number: N/A

Inbound CAR: N/A

Outbound CAR: N/A

Configuration files

- AC 1:

```
#
vlan 100
#
vlan 200
#
wlan service-template st1
  ssid service
  vlan 200
  client forwarding-location ap
  akm mode psk
  preshared-key pass-phrase cipher $c$3$0Lf6pOZ6bxrf25nodjOJKYEfnZ6g6ErccHyQ
  cipher-suite ccmp
  security-ie rsn
  portal enable method direct
  portal domain dml
  portal bas-ip 2.2.2.1
  portal apply web-server newpt
  service-template enable
#
interface Vlan-interface100
  ip address 2.2.1.1 255.255.255.0
#
interface Vlan-interface200
  ip address 2.2.2.1 255.255.255.0
#
interface GigabitEthernet1/0/1
  port link-type trunk
  port trunk permit vlan 1 100 200
#
ip route-static 192.168.0.0 24 2.2.2.100
#
radius session-control enable
```

```

#
radius scheme rs1
  primary authentication 192.168.0.111
  primary accounting 192.168.0.111
  key authentication cipher $c$3$Sqqgz7lDs4XPnethmAgyAKVlke7qwEkYbQ==
  key accounting cipher $c$3$4J/JBRGwqB4F213furJmKB6JWYXBFjWE6g==
  user-name-format without-domain
  nas-ip 2.2.2.1
#
domain dml
  authorization-attribute idle-cut 15 1024
  authentication portal radius-scheme rs1
  authorization portal radius-scheme rs1
  accounting portal radius-scheme rs1
#
portal host-check enable
portal free-rule 0 destination ip 192.168.0.0 255.255.255.0
portal free-rule 1 destination ip any udp 53
portal free-rule 2 destination ip any tcp 53
#
portal web-server newpt
  url http://192.168.0.111:8080/portal
  url-parameter nasip value 2.2.2.1
#
portal server newpt
  ip 192.168.0.111 key cipher $c$3$AkTEB7OgMYnCqsfDeplhoAgXUek/rVrLZw==
#
wlan ap-group group1
  priority 7
  wlan tunnel-preempt enable
  backup-ac ip 2.2.1.2
  ap office
  ap-model AP 3620
map-configuration flash:/map.txt
radio 1
  radio 2
  radio enable
  service-template st1
#
wlan ap office model AP 3620
  serial-id 219801A28N819CE0002T
#
• AC 2:
#
vlan 100
#
vlan 200
#

```

```

wlan service-template st1
  ssid service
  vlan 200
  client forwarding-location ap
akm mode psk
  preshared-key pass-phrase cipher $c$3$oLf6pOZ6bxrf25nodjOJKYEfnZ6g6ErccHyQ
  cipher-suite ccmp
  security-ie rsn
  portal enable method direct
  portal domain dml
  portal bas-ip 2.2.2.2
  portal apply web-server newpt
  service-template enable
#
interface Vlan-interface100
  ip address 2.2.1.2 255.255.255.0
#
interface Vlan-interface200
  ip address 2.2.2.2 255.255.255.0
#
interface GigabitEthernet1/0/1
  port link-type trunk
  port trunk permit vlan 1 100 200
#
  ip route-static 192.168.0.0 24 2.2.2.100
#
  radius session-control enable
#
radius scheme rs1
  primary authentication 192.168.0.111
  primary accounting 192.168.0.111
  key authentication cipher $c$3$Sgqgz7lDs4XPnethmAgyAKVlke7qwEkYbQ==
  key accounting cipher $c$3$4J/JBRGwqB4F213furJmKB6JWYXBFjWE6g==
  user-name-format without-domain
  nas-ip 2.2.2.2
#
domain dml
  authorization-attribute idle-cut 15 1024
  authentication portal radius-scheme rs1
  authorization portal radius-scheme rs1
  accounting portal radius-scheme rs1
#
portal host-check enable
portal free-rule 0 destination ip 192.168.0.0 255.255.255.0
portal free-rule 1 destination ip any udp 53
portal free-rule 2 destination ip any tcp 53
#
portal web-server newpt

```



```

url http://192.168.0.111:8080/portal
url-parameter nasip value 2.2.2.2
#
portal server newpt
  ip 192.168.0.111 key cipher $c$3$AkTEB7OgMYnCqsfDeplhoAgXUek/rVrLZw==
#
wlan ap-group group1
  priority 6
  wlan tunnel-preempt enable
  backup-ac ip 2.2.1.1
  ap office
  ap-model AP 3620
map-configuration flash:/map.txt
radio 1
  radio 2
  radio enable
  service-template st1
#
wlan ap office model AP 3620
  serial-id 219801A28N819CE0002T
#

```

- **Switch:**

```

#
vlan 2
#
vlan 100
#
vlan 200
#
interface Vlan-interface2
  ip address 192.168.0.100 255.255.255.0
#
interface Vlan-interface200
  ip address 2.2.2.100 255.255.255.0
#
interface GigabitEthernet1/0/1
  port link-type trunk
  port trunk permit vlan 1 100 200
#
interface GigabitEthernet1/0/2
  port link-type trunk
  port trunk pvid vlan 100
  port trunk permit vlan 100 200
  poe enable
#
interface GigabitEthernet1/0/3
  port link-type trunk
  port trunk permit vlan 100 200

```

```
#
interface GigabitEthernet1/0/4
 port link-type trunk
 port trunk permit vlan 1 100 200
• DHCP server:
#
 dhcp enable
#
 vlan 100
#
 vlan 200
#
 dhcp server ip-pool VLAN100
 gateway-list 2.2.1.200
 network 2.2.1.0 mask 255.255.255.0
 forbidden-ip 2.2.1.1
 forbidden-ip 2.2.1.2
 forbidden-ip 2.2.1.200
#
 dhcp server ip-pool VLAN200
 gateway-list 2.2.2.100
 network 2.2.2.0 mask 255.255.255.0
 dns-list 8.8.8.8
 forbidden-ip 2.2.2.1
 forbidden-ip 2.2.2.2
 forbidden-ip 2.2.2.100
#
 interface Vlan-interface100
 ip address 2.2.1.200 255.255.255.0
#
 interface Vlan-interface200
 ip address 2.2.2.200 255.255.255.0
#
 interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 1 100 200
#
```

Related documentation

- *AAA Management Command Reference in INTELBRAS Access Controllers Command References*
- *AAA Management Configuration Guide in INTELBRAS Access Controllers Configuration Guides*
- *AP Management Command Reference in INTELBRAS Access Controllers Command References*
- *AP Management Configuration Guide in INTELBRAS Access Controllers Configuration Guides*
- *Portal Authentication Command Reference in INTELBRAS Access Controllers Command References*
- *Portal Authentication Configuration Guide in INTELBRAS Access Controllers Configuration*

Guides

- *WLAN Access Command Reference in INTELBRAS Access Controllers Command References*

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

INTELBRAS Access Controllers

Dual-Link Backup Remote Portal and MAC Transparent Authentication in Centralized Forwarding Configuration Examples

Copyright © 2024 Intelbras S.A All rights reserved.

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

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

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

Contents

Introduction	1
Prerequisites	1
Example: Configuring remote portal and MAC transparent authentication for dual-link AC backup and centralized forwarding	1
Network configuration	1
Analysis	2
Restrictions and guidelines	2
Procedures	3
Configuring AC 1	3
Configuring AC 2	6
Configuring the switch	10
Configuring the INC server	11
Verifying the configuration	17
Configuration files	18
Related documentation	22

Introduction

The following information provides an example for configuring remote portal and MAC transparent authentication with centralized forwarding.

Prerequisites

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

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

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

Example: Configuring remote portal and MAC transparent authentication for dual-link AC backup and centralized forwarding

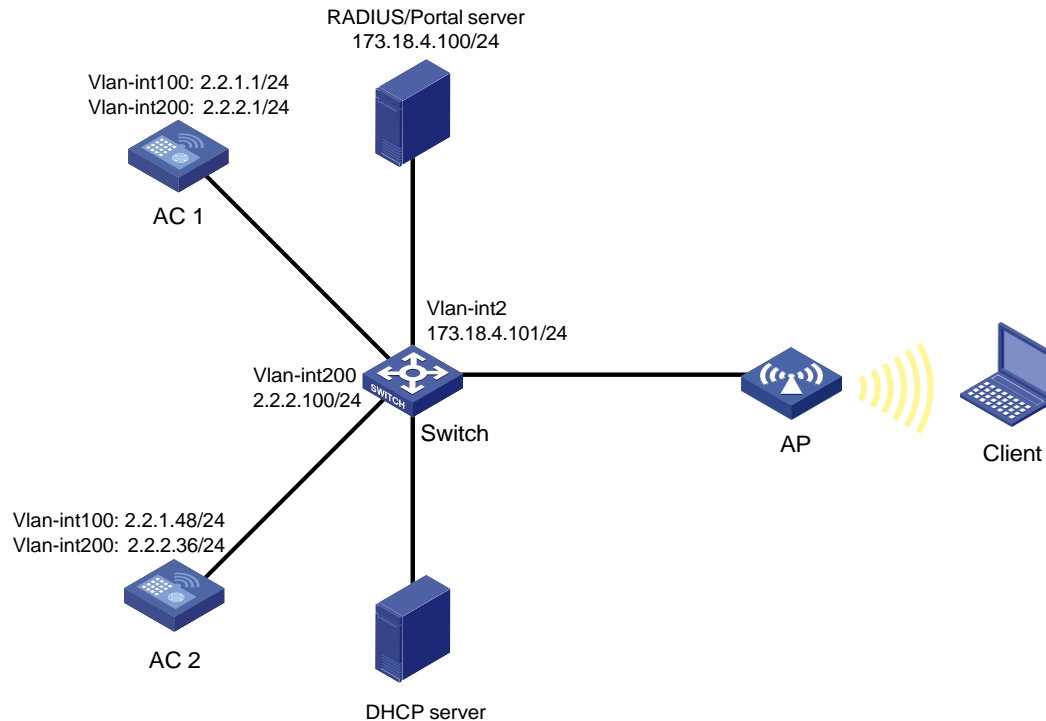
Network configuration

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

Configure the devices to meet the following requirements:

- The AP associates with both ACs and the two ACs to back up each other. When the master AC (AC 1) fails, the backup AC (AC 2) takes over, and the AP can provide services correctly through the backup AC.
- Remote MAC authentication and direct portal authentication are used for wireless clients.
- Before passing portal authentication, the client can access only the portal Web server. After passing the authentication, the client can access other network resources.
- The client can access network resources through any Layer 2 ports in its access VLAN without re-authentication.
- The INC server can dynamically modify user authorization information and log off clients.

Figure 1 Network diagram



Analysis

- To allow an authenticated user to access network resources on any Layer 2 ports in its access VLAN without re-authentication, you must enable the portal roaming feature.
- To allow the RADIUS server to modify user authorization information and log off users, enable the RADIUS session-control feature.
- To avoid allocation failures of dynamic authorization information during client association, configure RADIUS DAE.

Restrictions and guidelines

When you configure MAC-based portal authentication for dual-link AC backup and centralized forwarding, follow these restrictions and guidelines:

- Use the actual serial ID of an AP to uniquely identify that AP.
- If you configure manual APs, make sure the manual APs configured on the two ACs have the same AP name and identifier (serial ID or MAC address).
- Make sure the two ACs are of the same version.
- Make sure the portal authentication server type and portal Web server type configured on the ACs are the same as the actual server type.
- To avoid possible authentication failure caused by frequent logins and logouts of portal clients in a short time, disable the Rule ARP entry feature.
- To allow the RADIUS server to modify user authorization information and log off users, enable the RADIUS session-control feature.
- URLs redirected from the ACs to the portal Web server do not carry parameters by default. You can configure the parameters to carry as needed.

- If you enable portal authentication in VLAN interface view, only centralized forwarding is supported. If you enable portal authentication in service template view, both centralized forwarding and local forwarding are supported. This example enables portal authentication in service template view.
- Make sure the two ACs have the same portal-free rule settings, including the rule numbers.
- Some clients are enabled with MAC randomization by default, which might cause seamless roaming failures. As a best practice, disable MAC randomization.

Procedures

Configuring AC 1

1. Configure AC interfaces:

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

```
<AC1> system-view
[AC1] vlan 100
[AC1-vlan100] quit
[AC1] interface vlan-interface 100
[AC1-Vlan-interface100] ip address 2.2.1.1 24
[AC1-Vlan-interface100] quit
```

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

```
[AC1] vlan 200
[AC1-vlan200] quit
[AC1] interface vlan-interface 200
[AC1-Vlan-interface200] ip address 2.2.2.1 24
[AC1-Vlan-interface200] quit
```

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

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

2. Configure a static route to the INC server.

```
[AC1] ip route-static 173.18.4.0 255.255.255.0 2.2.2.100
```

3. Configure wireless services:

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

```
[AC1] wlan service-template st1
```

Specify the SSID as **service**.

```
[AC1-wlan-st-st1] ssid service
```

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

```
[AC1-wlan-st-st1] vlan 200
```

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

```
[AC1-wlan-st-st1] akm mode psk
```

```
[AC1-wlan-st-st1] preshared-key pass-phrase simple 12345678
```

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

```
[AC1-wlan-st-st1] cipher-suite ccmp
```

```
[AC1-wlan-st-st1] security-ie rsn
```

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

```
[AC1-wlan-st-st1] client forwarding-location ac
```

```
[AC1-wlan-st-st1] quit
```

4. Configure the AP:

NOTE:

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

Create AP **office**, and specify the AP name and serial ID.

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

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

```
[AC1-wlan-ap-office] quit
```

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

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

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

Set the AP connection priority to 7.

```
[AC1-wlan-ap-group-group1] priority 7
```

Specify AC 2 as the backup AC for AC 1. Set the backup AC address as the IP address of VLAN-interface 100 on AC 2.

```
[AC1-wlan-ap-group-group1] backup-ac ip 2.2.1.48
```

Enable master CAPWAP tunnel preemption.

```
[AC1-wlan-ap-group-group1] wlan tunnel-preempt enable
```

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

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

```
[AC1-wlan-ap-group-group1-ap-model-AP 3620] radio 2
```

```
[AC1-wlan-ap-group-group1-ap-model-AP 3620-radio-2] service-template st1
```

Enable radio 2.

```
[AC1-wlan-ap-group-group1-ap-model-AP 3620-radio-2] radio
```

```
enable [AC1-wlan-ap-group-group1-ap-model-AP 3620-radio-2] quit
```

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

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

5. Configure a RADIUS scheme:

Create RADIUS scheme **rs1**.

```
[AC1] radius scheme rs1
```

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

```
[AC1-radius-rs1] primary authentication 173.18.4.100
```

```
[AC1-radius-rs1] primary accounting 173.18.4.100
```

Specify shared keys for RADIUS authentication and accounting.

```
[AC1-radius-rs1] key authentication simple radius
```

```
[AC1-radius-rs1] key accounting simple radius
```

Configure AC 1 to remove the ISP domain name from the usernames sent to the RADIUS servers.

```
[AC1-radius-rs1] user-name-format without-domain
```

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

```
[AC1-radius-rs1] nas-ip 2.2.2.1
```

```
[AC1-radius-rs1] quit
```

Enable RADIUS session-control.

```
[AC1] radius session-control enable
```

Enable the RADIUS DAS feature and enter RADIUS DAS view.

```
[AC1] radius dynamic-author server
```

Specify the DAC as 10.110.1.2. Set the shared key to **123456** in plaintext form for secure communication between the DAS and DAC.

```
[AC1-radius-da-server] client ip 173.18.4.100 key simple radius
```

```
[AC1-radius-da-server] quit
```

6. Configure authentication domains:

Create domain **dm2** and enter its view.

```
[AC1] domain dm2
```

Configure the domain to use RADIUS scheme **rs1** for authentication, authorization, and accounting.

```
[AC1-isp-dm2] authentication lan-access radius-scheme rs1
```

```
[AC1-isp-dm2] authorization lan-access radius-scheme rs1
```

```
[AC1-isp-dm2] accounting lan-access radius-scheme rs1
```

```
[AC1-isp-dm2] quit
```

Create domain **dm1** and enter its view.

```
[AC1] domain dm1
```

Configure the domain to use RADIUS scheme **rs1** for authentication, authorization, and accounting.

```
[AC1-isp-dm1] authentication portal radius-scheme rs1
```

```
[AC1-isp-dm1] authorization portal radius-scheme rs1
```

```
[AC1-isp-dm1] accounting portal radius-scheme rs1
```

Set the client idle timeout to 15 minutes and set the minimum threshold to 1024 bytes for clients in ISP domain **dm1**.

```
[AC1-isp-dm1] authorization-attribute idle-cut 15 1024
```

```
[AC1-isp-dm1] quit
```

7. Configure portal authentication:

Create the portal authentication server **newpt**, specify the server IP address as 173.18.4.100, and set the destination UDP port number to **50100** for the AC to send unsolicited portal packets to the portal authentication server.

```
[AC1] portal server newpt
```

```
[AC1-portal-server-newpt] ip 173.18.4.100 key simple portal
```

```
[AC1-portal-server-newpt] port 50100
```

Set the server type to CMCC.

```
[AC1-portal-server-newpt] server-type cmcc
```

```
[AC1-portal-server-newpt] quit
```

Configure the URL for the portal Web server **newpt** as **http://173.18.4.100:8080/portal**.

```
[AC1] portal web-server newpt
```

```
[AC1-portal-websvr-newpt] url http://173.18.4.100:8080/portal
```

Configure URL parameters **ssid**, **wlanuserip**, **wlanacname**, and **nasip** for the portal Web server. Specify the AP's SSID, the IP address of the client, the AC's name, and NAS IP 2.2.2.1 as the values for the parameters, respectively. (The parameters are required to be carried in the URL of a portal Web server of the CMCC type.)

```
[AC1-portal-websvr-newpt] url-parameter ssid ssid
```

```
[AC1-portal-websvr-newpt] url-parameter wlanuserip source-address
```

```
[AC1-portal-websvr-newpt] url-parameter wlanacname value AC
```

```
[AC1-portal-websvr-newpt] url-parameter nasip value 2.2.2.1
```

```

# Set the portal Web server type to CMCC.
[AC1-portal-websvr-newpt] server-type cmcc
[AC1-portal-websvr-newpt] quit

# Configure an IPv4-based portal-free rule to permit portal Web server traffic.
[AC1] portal free-rule 0 destination ip 173.18.4.100 24

# Configure IPv4-based portal-free rules to permit DNS server traffic.
[AC1] portal free-rule 1 destination ip any udp 53
[AC1] portal free-rule 2 destination ip any tcp 53

# Enable intra-VLAN roaming for portal users.
[AC1] portal roaming enable

# Disable the Rule ARP entry feature for portal clients.
[AC1] undo portal refresh arp enable

# Enable validity check on wireless portal clients.
[AC1] portal host-check enable

# Enable direct IPv4 portal authentication for service template st1.
[AC1] wlan service-template st1
[AC1-wlan-st-st1] portal enable method direct

# Configure the authentication domain for IPv4 portal users as dm1 on service template st1.
[AC1-wlan-st-st1] portal domain dm1

# Specify portal Web server newpt on service template st1 to redirect portal user HTTP or
HTTPS requests to the server.
[AC1-wlan-st-st1] portal apply web-server newpt

# Specify the BAS IP as the IP address of VLAN-interface 200, from which clients come online
from AC 1.
[AC1-wlan-st-st1] portal bas-ip 2.2.2.1

# Configure MAC authentication and configure the AC to ignore MAC authentication failures.
[AC1-wlan-st-st1] client-security authentication-mode mac
[AC1-wlan-st-st1] client-security ignore-authentication

# Specify ISP domain dm2 as the authentication domain for MAC authentication clients in
service template st1.
[AC1-wlan-st-st1] mac-authentication domain dm2

# Enable the service template.
[AC1-wlan-st-st1] service-template enable
[AC1-wlan-st-st1] quit

```

Configuring AC 2

1. Configure AC interfaces:

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

```

<AC2> system-view
[AC2] vlan 100
[AC2-vlan100] quit
[AC2] interface vlan-interface 100
[AC2-Vlan-interface100] ip address 2.2.1.48 24
[AC2-Vlan-interface100] quit

```

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

```
[AC2] vlan 200
[AC2-vlan200] quit
[AC2] interface vlan-interface 200
[AC2-Vlan-interface200] ip address 2.2.2.36 24
[AC2-Vlan-interface200] quit
```

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

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

2. Configure a static route to the INC server.

```
[AC2] ip route-static 173.18.4.0 255.255.255.0 2.2.2.100
```

3. Configure wireless services:

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

```
[AC2] wlan service-template st1
```

Specify the SSID as **service.**

```
[AC2-wlan-st-st1] ssid service
```

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

```
[AC2-wlan-st-st1] vlan 200
```

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

```
[AC2-wlan-st-st1] akm mode psk
```

```
[AC2-wlan-st-st1] preshared-key pass-phrase simple 12345678
```

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

```
[AC2-wlan-st-st1] cipher-suite ccmp
```

```
[AC2-wlan-st-st1] security-ie rsn
```

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

```
[AC2-wlan-st-st1] client forwarding-location ac
```

```
[AC2-wlan-st-st1] quit
```

4. Configure the AP:

NOTE:

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

Create AP **office, and specify the AP name and serial ID.**

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

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

```
[AC2-wlan-ap-office] quit
```

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

```
[AC2] wlan ap-group group1
```

```
[AC2-wlan-ap-group-group1] ap office
```

Set the AP connection priority to 5.

```
[AC2-wlan-ap-group-group1] priority 5
```

Specify AC 1 as the backup AC for AC 2. Set the backup AC address as the IP address of VLAN-interface 100 on AC 1.

```
[AC2-wlan-ap-group-group1] backup-ac ip 2.2.1.1
```

Enable master CAPWAP tunnel preemption.

```
[AC2-wlan-ap-group-group1] wlan tunnel-preempt enable
# Bind service template st1 to radio 2 in AP group group1.
[AC2-wlan-ap-group-group1] ap-model AP 3620
[AC2-wlan-ap-group-group1-ap-model-AP 3620] radio 2
[AC2-wlan-ap-group-group1-ap-model-AP 3620-radio-2] service-template st1
# Enable radio 2.
[AC2-wlan-ap-group-group1-ap-model-AP 3620-radio-2] radio
enable [AC2-wlan-ap-group-group1-ap-model-AP 3620-radio-2] quit
[AC2-wlan-ap-group-group1-ap-model-AP 3620]
quit [AC2-wlan-ap-group-group1] quit
```

5. Configure a RADIUS scheme:

Create RADIUS scheme **rs1**.

```
[AC2] radius scheme rs1
# Specify the IP addresses of the primary authentication and accounting RADIUS servers.
```

```
[AC2-radius-rs1] primary authentication 173.18.4.100
```

```
[AC2-radius-rs1] primary accounting 173.18.4.100
```

Specify shared keys for RADIUS authentication and accounting.

```
[AC2-radius-rs1] key authentication simple radius
```

```
[AC2-radius-rs1] key accounting simple radius
```

Configure AC 2 to remove the ISP domain name from the usernames sent to the RADIUS servers.

```
[AC2-radius-rs1] user-name-format without-domain
```

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

```
[AC2-radius-rs1] nas-ip 2.2.2.36
```

```
[AC2-radius-rs1] quit
```

Enable RADIUS session-control.

```
[AC2] radius session-control enable
```

Enable the RADIUS DAS feature and enter RADIUS DAS view.

```
[AC2] radius dynamic-author server
```

Specify the DAC as 10.110.1.2. Set the shared key to **123456** in plaintext form for secure communication between the DAS and DAC.

```
[AC2-radius-da-server] client ip 173.18.4.100 key simple radius
```

```
[AC2-radius-da-server] quit
```

6. Configure authentication domains:

Create domain **dm2** and enter its view.

```
[AC2] domain dm2
```

Configure the domain to use RADIUS scheme **rs1** for authentication, authorization, and accounting.

```
[AC2-isp-dm2] authentication lan-access radius-scheme rs1
```

```
[AC2-isp-dm2] authorization lan-access radius-scheme rs1
```

```
[AC2-isp-dm2] accounting lan-access radius-scheme rs1
```

```
[AC2-isp-dm2] quit
```

Create domain **dm1** and enter its view.

```
[AC2] domain dm1
```

Configure the domain to use RADIUS scheme **rs1** for authentication, authorization, and accounting.

```
[AC2-isp-dm1] authentication portal radius-scheme rs1
```

```
[AC2-isp-dm1] authorization portal radius-scheme rs1
```

```
[AC2-isp-dm1] accounting portal radius-scheme rs1
```

Set the client idle timeout to 15 minutes and set the minimum threshold to 1024 bytes for clients in ISP domain **dm1**.

```
[AC2-isp-dm1] authorization-attribute idle-cut 15 1024
```

```
[AC2-isp-dm1] quit
```

7. Configure portal authentication:

Create the portal authentication server **newpt**, specify the server IP address as 173.18.4.100, and set the destination UDP port number to **50100** for the AC to send unsolicited portal packets to the portal authentication server.

```
[AC2] portal server newpt
```

```
[AC2-portal-server-newpt] ip 173.18.4.100 key simple portal
```

```
[AC2-portal-server-newpt] port 50100
```

Set the server type to CMCC.

```
[AC2-portal-server-newpt] server-type cmcc
```

```
[AC2-portal-server-newpt] quit
```

Configure the URL for the portal Web server **newpt** as <http://173.18.4.100:8080/portal>.

```
[AC2] portal web-server newpt
```

```
[AC2-portal-websvr-newpt] url http://173.18.4.100:8080/portal
```

Configure URL parameters **ssid**, **wlanuserip**, **wlanacname**, and **nasip** for the portal Web server. Specify the AP's SSID, the IP address of the client, the AC's name, and NAS IP 2.2.2.36 as the values for the parameters, respectively. (The parameters are required to be carried in the URL of a portal Web server of the CMCC type.)

```
[AC2-portal-websvr-newpt] url-parameter ssid ssid
```

```
[AC2-portal-websvr-newpt] url-parameter wlanuserip source-address
```

```
[AC2-portal-websvr-newpt] url-parameter wlanacname value AC
```

```
[AC2-portal-websvr-newpt] url-parameter nasip value 2.2.2.36
```

Set the portal Web server type to CMCC.

```
[AC2-portal-websvr-newpt] server-type cmcc
```

```
[AC2-portal-websvr-newpt] quit
```

Configure an IPv4-based portal-free rule to permit portal Web server traffic.

```
[AC2] portal free-rule 0 destination ip 173.18.4.100 24
```

Configure IPv4-based portal-free rules to permit DNS server traffic.

```
[AC2] portal free-rule 1 destination ip any udp 53
```

```
[AC2] portal free-rule 2 destination ip any tcp 53
```

Enable intra-VLAN roaming for portal users.

```
[AC2] portal roaming enable
```

Disable the Rule ARP entry feature for portal clients.

```
[AC2] undo portal refresh arp enable
```

Enable validity check on wireless portal clients.

```
[AC2] portal host-check enable
```

Enable direct IPv4 portal authentication for service template **st1**.

```
[AC2] wlan service-template st1
```

```
[AC2-wlan-st-st1] portal enable method direct
```

Configure the authentication domain for IPv4 portal users as **dm1** on service template **st1**.

```
[AC2-wlan-st-st1] portal domain dm1
```

Specify portal Web server **newpt** on service template **st1** to redirect portal user HTTP or HTTPS requests to the server.

```
[AC2-wlan-st-st1] portal apply web-server newpt
```

Specify the BAS IP as the IP address of VLAN-interface 200, from which clients come online from AC 2.

```
[AC2-wlan-st-st1] portal bas-ip 2.2.2.36
```

Configure MAC authentication and configure the AC to ignore MAC authentication failures.

```
[AC2-wlan-st-st1] client-security authentication-mode mac
```

```
[AC2-wlan-st-st1] client-security ignore-authentication
```

Specify ISP domain **dm2 as the authentication domain for MAC authentication clients in service template **st1**.**

```
[AC2-wlan-st-st1] mac-authentication domain dm2
```

Enable the service template.

```
[AC2-wlan-st-st1] service-template enable
```

```
[AC2-wlan-st-st1] quit
```

Configuring the switch

Create VLAN 100 for forwarding CAPWAP tunnel traffic between AC and AP.

```
<Switch> system-view
```

```
[Switch] vlan 100
```

```
[Switch-vlan100] quit
```

Create VLAN 200 for forwarding client traffic.

```
[Switch] vlan 200
```

```
[Switch-vlan200] quit
```

Create VLAN 2 for connecting to the INC server.

```
[Switch] vlan 2
```

```
[Switch-vlan2] quit
```

Add the interface that connects the switch to the INC server to VLAN 2. (Details not shown.)

Configure GigabitEthernet 1/0/1 that connects the switch to AC 1 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 1/0/3 that connects the switch to AC 2 as a trunk port, and assign it to VLAN 100 and VLAN 200.

```
[Switch] interface gigabitethernet 1/0/3
```

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

```
[Switch-GigabitEthernet1/0/3] port trunk permit vlan 100 200
```

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

Configure GigabitEthernet 1/0/2 that connects the switch to the AP as a trunk 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
```


Configure GigabitEthernet 1/0/4 that connects the switch to the DHCP server as a trunk port, and assign it to VLAN 100 and VLAN 200.

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

Assign an IP address to VLAN-interface 200.

```
[Switch] interface vlan-interface 200
[Switch-Vlan-interface200] ip address 2.2.2.100 255.255.255.0
[Switch-Vlan-interface200] quit
```

Assign an IP address to VLAN-interface 2. This address will be used as the gateway address for the INC server.

```
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] ip address 173.18.4.101 255.255.255.0
[Switch-Vlan-interface2] quit
```

Configuring the INC server

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

Configure the RADIUS server

1. Add AC 1 as an access device:
 - a. Log in to INC at 173.18.4.100:8080/INC and click the **User** tab.
 - b. From the navigation pane, select **User Access Policy > Access Device Management > Access Device**.
 - c. Click **Add**.
The **Add Access Device** page opens.
 - d. In the **Access Configuration** area, configure the following parameters:
 - Enter **radius** in the **Shared Key** and **Confirm Shared Key** fields. Make sure the key is the same as the key configured on the ACs.
 - Use the default values for other parameters.
 - e. In the **Device List** area, click **Select** or **Add Manually** to add AC 1 at 2.2.2.1 as an access device.
 - f. Click **OK**.

Figure 2 Adding an access device

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

Access Configuration

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

Device List

Select Add Manually Clear All

Device Name	Device IP	Device Model	Comments	Delete
	2.2.2.1			

Total Items: 1.

OK Cancel

2. Repeat the previous step to add AC 2 as an access device.

The IP address of AC 2 is 2.2.2.36.

Configure the portal server

1. Configure portal authentication:
 - a. Click the **User** tab.
 - b. Select **User Access Policy > Portal Service > Server** from the navigation tree to open the portal server configuration page.
 - c. Configure the portal server parameters as needed.
This example uses the default settings.
 - d. Click **OK**.

Figure 3 Portal authentication server configuration

User > User Access Policy > Portal Service > Server

Portal Server

Basic Information

Log Level * Info

Portal Server

Request Timeout(Seconds) *	4	Server Heartbeat Interval(Seconds) *	20
User Heartbeat Interval(Minutes) *	5	LB Device Address	

Portal Web

Request Timeout(Seconds) *	15	Packet Code	
Verify Endpoint Requests	Yes	Use Cache	Yes
HTTP Heartbeat Display	New Page	HTTPS Heartbeat Display	Original Page

Portal Page

<http://173.18.4.100:8080/portal/>
<https://173.18.4.100:8443/portal/>

2. Configure the IP address group:
 - a. Select **User Access Policy > Portal Service > IP Group** from the navigation tree to open the portal IP address group configuration page.
 - b. Click **Add** to open the page as shown in [Figure 4](#).

- c. Enter the IP group name. In this example, the name is **Portal_user**.
- d. Enter the start IP address and end IP address of the IP group.
Make sure the client IP address is in the IP group.
- e. Select a service group.
This example uses the default group **Ungrouped**.
- f. Select **Normal** from the **Action** list.
- g. Click **OK**.

Figure 4 Adding an IP address group

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

Add IP Group

IP Group Name *	Portal_user
Start IP *	2.2.2.1
End IP *	2.2.2.255
Service Group	Ungrouped ▼
Action *	Normal ▼

OK Cancel

3. Add AC 1 as a portal device:
 - a. Select **User Access Policy > Portal Service > Device** from the navigation tree to open the portal device configuration page.
 - b. Click **Add** to open the page as shown in [Figure 5](#).
 - c. Enter the device name.
 - d. Specify the version as **Portal 2.0**.
 - e. Enter the portal BAS-IP configured on AC 1 as the IP address.
 - f. Set whether to support the portal server heartbeat and user heartbeat functions.
In this example, select **No** for both **Support Server Heartbeat** and **Support User Heartbeat**.
 - g. Enter the key, which must be the same as that configured on the AC.
 - h. Select **Directly Connected** from the **Access Method** list.
 - i. Use the default settings for other parameters.
 - j. Click **OK**.

Figure 5 Adding a portal device


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

Add Device

Device Information

Device Name *	NAS	Service Group *	Ungrouped
Version *	Portal 2.0	IP Address *	2.2.2.1
Listening Port *	2000	Local Challenge *	No
Authentication Retries *	0	Logout Retries *	1
Support Server Heartbeat *	No	Support User Heartbeat *	No
Key *	*****	Confirm Key *	*****
Access Method *	Directly Conne		
Device Description			

OK Cancel

4. Repeat the previous step to add AC 2 as a portal device.
5. Associate AC 1 with the IP address group:
 - a. As shown in Figure 6, click the **Port Group Information Management** icon  for the device to open the port group configuration page.
 - b. Click **Add** to open the page as shown in Figure 7.
 - c. Enter the port group name.
 - d. Select the configured IP address group.

The IP address used by the user to access the network must be within this IP address group.
 - e. Select **Supported** for **Transparent Authentication**.
 - f. Use the default settings for other parameters.
 - g. Click **OK**.

Figure 6 Device list



User > User Access Policy > Portal Service > Device

Query Devices

Device Name: Version:
Deploy Result: Service Group:

Query Reset

Add

Device Name	Version	Service Group	IP Address	Last Deployed at	Deploy Result	Operation
NAS	Portal 2.0	Ungrouped	2.2.2.1		Not Deployed	 

1-1 of 1. Page 1 of 1.

Figure 7 Adding a port group

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

Add Port Group

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

OK Cancel

6. Repeat the previous step to associate AC 2 with the IP address group.

Configuring access settings

1. Add an access policy:
 - a. Select **User Access Policy > Access Policy** from the navigation tree to open the access policy page.
 - b. Click **Add** to open the page as shown in [Figure 8](#).
 - c. Enter the access policy name. In this example, the name is **AccessPolicy**.
 - d. Select **Ungrouped** from the service group list.
 - e. Use the default settings for other parameters.
 - f. Click **OK**.

Figure 8 Adding an access policy

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

Basic Information

Access Policy Name * AccessPolicy

Service Group * Ungrouped

Description

Authorization Information

Access Period None

Allocate IP * No

Downstream Rate(Kbps)

Upstream Rate(Kbps)

Priority

Deploy VLAN

☐ Deploy User Profile

☐ Deploy ACL

Deploy User Group

2. Add an access service:
 - a. Select **User Access Policy > Access Service** from the navigation tree to open the access service page.
 - b. Click **Add** to open the page as shown in [Figure 9](#).
 - c. Enter the service name. In this example, the service name is **MAC_server**.
 - d. Select the **Transparent Authentication on Portal Endpoints** option.
 - e. Use the default settings for other parameters.
 - f. Click **OK**.

Figure 9 Adding an access service

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

Basic Information

Service Name * MAC_server

Service Suffix

Service Group * Ungrouped

Default Access Policy * AccessPolicy

Default Proprietary Attribute Assignment Policy * Do not use

Default Max. Number of Bound Endpoints * 0

Default Max. Number of Online Endpoints * 0

Description

☒ Available

☒ Transparent Authentication

Access Scenario List

Add

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

OK Cancel

3. Add an access user:

- a. Select **Access User > All Access Users** from the navigation tree to open the access user page.
- b. Click **Add** to open the page as shown in [Figure 10](#).
- c. Select or add an access user.
- d. Specify the account name. In this example, the name is **client**.
- e. Set the password. In this example, the password is **1234567**.
- f. Select service **MAC_server**.
- g. Retain the default settings for other parameters.
- h. Click **OK**.

Figure 10 Adding an access user

User > All Access Users > Add Access User

Access Information

User Name * Client1 [Select] [Add User]

Account Name * client

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

Password * 1234567 Confirm Password * 1234567

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

Start Time [08:00] End Time [18:00]

Max. Idle Time(Minutes) [30] Max. Concurrent Logins [1]

Login Message []

Access Service

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

4. Configure system parameters:
 - a. Select **User Access Policy > Service Parameters > System Settings** from the navigation tree to open the system settings page.
 - b. Click the **Configure** icon for **User Endpoint Settings** to open the page as shown in [Figure 11](#).
 - c. Enable **Transparent MAC Authentication**.
 - d. Select whether to enable transparent portal authentication on non-smart devices. In this example, select **Enable** for **Non-Terminal Authentication**.
 - e. Click **OK**.
 - f. Click the **Configure** icon for **Endpoint Aging Time** to open the page as shown in [Figure 12](#).
 - g. Set the endpoint aging time as needed. This example uses the default value.

Figure 11 Configuring user endpoint settings

User > User Access Policy > Service Parameters > System Settings > User Endpoint Settings

User Endpoint Settings

Transparent Authentication [Enable]

Max. Devices for Single Account * [10]

Non-Terminal Authentication [Permit] ⓘ

Log off User with Endpoint Conflict [No]

[OK] [Cancel]

Figure 12 Setting the endpoint aging time

User > User Access Policy > Service Parameters > System Settings > Endpoint Aging Policy > Modify Endpoint Aging Policy

Modify Endpoint Aging Policy

Access Scenario * Default Policy

Endpoint Aging Policy(Days) * 7 ⓘ

Endpoint Aging Mode By Binding Time ▼

OK Cancel

Verifying the configuration

Make the AP come online.

Verify that the AP first associates with AC 1. Shut down VLAN-interface 100 on AC 1, wait 3 minutes, and verify that the AP associates with AC 2 and the AP state on AC 2 is **R/M**.

Bring up VLAN-interface 100 on AC 1. Verify that the AP state becomes R/M on AC 1 and R/B on AC 2.

If user and client MAC address information is not recorded on the RADIUS server, MAC authentication fails. Verify that the AC ignores the authentication failure and triggers portal authentication.

```
[AC1] display portal user all
Total portal users: 1
Username: client
  AP name: office
  Radio ID: 2
  SSID: service
  Portal server: newpt
  State: Online
  VPN instance: N/A
  MAC          IP          VLAN    Interface
  ---          -
  0021-6330-0933 2.2.2.2    200     WLAN-BSS1/0/2
Authorization information:
  DHCP IP pool: N/A
  User profile: N/A
  Session group profile: N/A
  ACL number: N/A
  Inbound CAR: N/A
  Outbound CAR: N/A
```

After portal authentication, the RADIUS server records user and client MAC address information. At next associations, the client can pass MAC authentication and access network resources without being portal reauthenticated.

Display MAC-authenticated user information.

```
[AC1] display mac-authentication connection
User MAC address      : 0021-6330-0933
AP name               : office
```

```

Radio ID                : 2
SSID                    : service
BSSID                   : 70ba-efaf-ddb0
Username                 : 002163300933
Authentication domain   : dm2
Initial VLAN            : 200
Authorization VLAN      : 200
Authorization ACL number : N/A
Authorization user profile : N/A
Termination action      : Default
Session timeout period   : 86401 s
Online from              : 2016/04/22 18:56:20

```

Configuration files

- AC 1:

```

#
vlan 100
#
vlan 200
#
wlan service-template st1
    ssid service
    vlan 200
client forwarding-location ac
akm mode psk
    preshared-key pass-phrase cipher $c$3$oLf6pOZ6bxrf25nodjOJKYEfnZ6g6ErccHyQ
    cipher-suite ccmp
    security-ie rsn
    client-security authentication-mode mac
    client-security ignore-authentication
    mac-authentication domain dm2
    portal enable method direct
    portal domain dm1
    portal bas-ip 2.2.2.1
    portal apply web-server newpt
    service-template enable
#
interface Vlan-interface100
    ip address 2.2.1.1 255.255.255.0
#
interface Vlan-interface200
    ip address 2.2.2.1 255.255.255.0
#
interface GigabitEthernet1/0/1
    port link-mode bridge
    port link-type trunk

```



```

port trunk permit vlan 1 100 200
#
ip route-static 173.18.4.0 24 2.2.2.100
#
radius session-control enable
#
radius scheme rs1
primary authentication 173.18.4.100
primary accounting 173.18.4.100
key authentication cipher $c$3$Sgqz7lDs4XPnethmAgyAKVlke7qwEkYbQ==
key accounting cipher $c$3$4J/JBRGwqB4F213furJmKB6JWYXBFjWE6g==
user-name-format without-domain
nas-ip 2.2.2.1
#
radius dynamic-author server
client ip 173.18.4.100 key cipher $c$3$AkTEB7OgMYnCqsfDeplhoAgXUek/rVrLZw==
#
domain dm1
authorization-attribute idle-cut 15 1024
authentication portal radius-scheme rs1
authorization portal radius-scheme rs1
accounting portal none
#
domain dm2
authorization-attribute idle-cut 15 1024
authentication lan-access radius-scheme rs1
authorization lan-access radius-scheme rs1
accounting lan-access radius-scheme rs1
#
portal host-check enable
portal free-rule 0 destination ip 192.168.0.0 255.255.255.0
portal free-rule 1 destination ip any udp 53
portal free-rule 2 destination ip any tcp 53
#
portal web-server newpt
url http://173.18.4.100:8080/portal
server-type cmcc
url-parameter nasip value 2.2.2.1
url-parameter ssid ssid
url-parameter wlanacname value AC
url-parameter wlanuserip source-address
#
portal server newpt
ip 173.18.4.100 key cipher $c$3$jiLQ5VIGG4TF7R3sHTT07bmV9rtisQYBzQ==
server-type cmcc
#
wlan ap-group group1
priority 7

```

```

wlan tunnel-preempt enable
backup-ac ip 2.2.1.48
ap office
ap-model AP 3620
radio 1
    radio 2
        radio enable
        service-template st1
#
wlan ap office model AP 3620
    serial-id 219801A28N819CE0002T
#

```

- **AC 2:**

```

#
vlan 100
#
vlan 200
#
wlan service-template st1
    ssid service
    vlan 200
client forwarding-location ac
akm mode psk
    preshared-key pass-phrase cipher $c$3$oLf6pOZ6bxrf25nodjOJKYEfnZ6g6ErccHyQ
    cipher-suite ccmp
    security-ie rsn
    client-security authentication-mode mac
    client-security ignore-authentication
    mac-authentication domain dm2
    portal enable method direct
    portal domain dm1
    portal bas-ip 2.2.2.36
    portal apply web-server newpt
    service-template enable
#
interface Vlan-interface100
    ip address 2.2.1.48 255.255.255.0
#
interface Vlan-interface200
    ip address 2.2.2.36 255.255.255.0
#
interface GigabitEthernet1/0/1
    port link-mode bridge
    port link-type trunk
    port trunk permit vlan 1 100 200
#
ip route-static 173.18.4.0 24 2.2.2.100
#

```

```

radius session-control enable
#
radius scheme rs1
primary authentication 173.18.4.100
primary accounting 173.18.4.100
key authentication cipher $c$3$Sqqqz7lDs4XPnethmAgyAKVlke7qwEkYbQ==
key accounting cipher $c$3$4J/JBRGwqB4F213furJMkB6JWYXBFjWE6g==
user-name-format without-domain
nas-ip 2.2.2.36
#
radius dynamic-author server
client ip 173.18.4.100 key cipher $c$3$AkTEB7OgMYnCqsfDeplhoAgXUek/rVrLZw==
#
domain dm1
authorization-attribute idle-cut 15 1024
authentication portal radius-scheme rs1
authorization portal radius-scheme rs1
accounting portal none
#
domain dm2
authorization-attribute idle-cut 15 1024
authentication lan-access radius-scheme rs1
authorization lan-access radius-scheme rs1
accounting lan-access radius-scheme rs1
#
portal host-check enable
portal free-rule 0 destination ip 192.168.0.0 255.255.255.0
portal free-rule 1 destination ip any udp 53
portal free-rule 2 destination ip any tcp 53
#
portal web-server newpt
url http://173.18.4.100:8080/portal
server-type cmcc
url-parameter nasip value 2.2.2.36
url-parameter ssid ssid
url-parameter wlanacname value AC
url-parameter wlanuserip source-address
#
portal server newpt
ip 173.18.4.100 key cipher $c$3$jilQ5VIGG4TF7R3sHTT07bmV9rtiSQYBzQ==
server-type cmcc
#
wlan ap-group group1
priority 5
wlan tunnel-preempt enable
backup-ac ip 2.2.1.1
ap office
ap-model AP 3620

```

```

radio 1
    radio 2
    radio enable
    service-template st1
#
wlan ap office model AP 3620
    serial-id 219801A28N819CE0002T
#
• Switch:
#
vlan 2
#
vlan 100
#
vlan 200
#
interface Vlan-interface2
    ip address 173.18.4.101 255.255.255.0
#
interface Vlan-interface200
    ip address 2.2.2.100 255.255.255.0
#
interface GigabitEthernet1/0/1
    port link-type trunk
    port trunk permit vlan 1 100 200
#
interface GigabitEthernet1/0/2
    port link-type access
    port access vlan 100
    poe enable
#
interface GigabitEthernet1/0/3
    port link-type trunk
    port trunk permit vlan 1 100 200
#
interface GigabitEthernet1/0/4
    port link-type trunk
    port trunk permit vlan 1 100 200

```

Related documentation

- *AAA Management Command Reference in INTELBRAS Access Controllers Command References*
- *AAA Management Configuration Guide in INTELBRAS Access Controllers Configuration Guides*
- *AP Management Command Reference in INTELBRAS Access Controllers Command References*
- *AP Management Configuration Guide in INTELBRAS Access Controllers Configuration Guides*
- *Portal Authentication Command Reference in INTELBRAS Access Controllers Command References*

- *Portal Authentication Configuration Guide in INTELBRAS Access Controllers Configuration Guides*

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

INTELBRAS Access Controllers

Dual-Link Backup Remote Portal Authentication in Centralized Forwarding Configuration Examples

Copyright © 2024 Intelbras S.A All rights reserved.

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

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

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

Contents

Introduction	1
Prerequisites	1
Example: Configuring remote portal authentication for dual-link AC backup and centralized forwarding	1
Network configuration	1
Analysis	2
Restrictions and guidelines	2
Procedures	3
Configuring AC 1	3
Configuring AC 2	6
Configuring the switch	9
Configuring the DHCP server	10
Configuring the INC server	11
Verifying the configuration	16
Configuration files	17
Related documentation	22

Introduction

The following information provides an example for configuring remote portal authentication with centralized forwarding.

Prerequisites

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

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

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

Example: Configuring remote portal authentication for dual-link AC backup and centralized forwarding

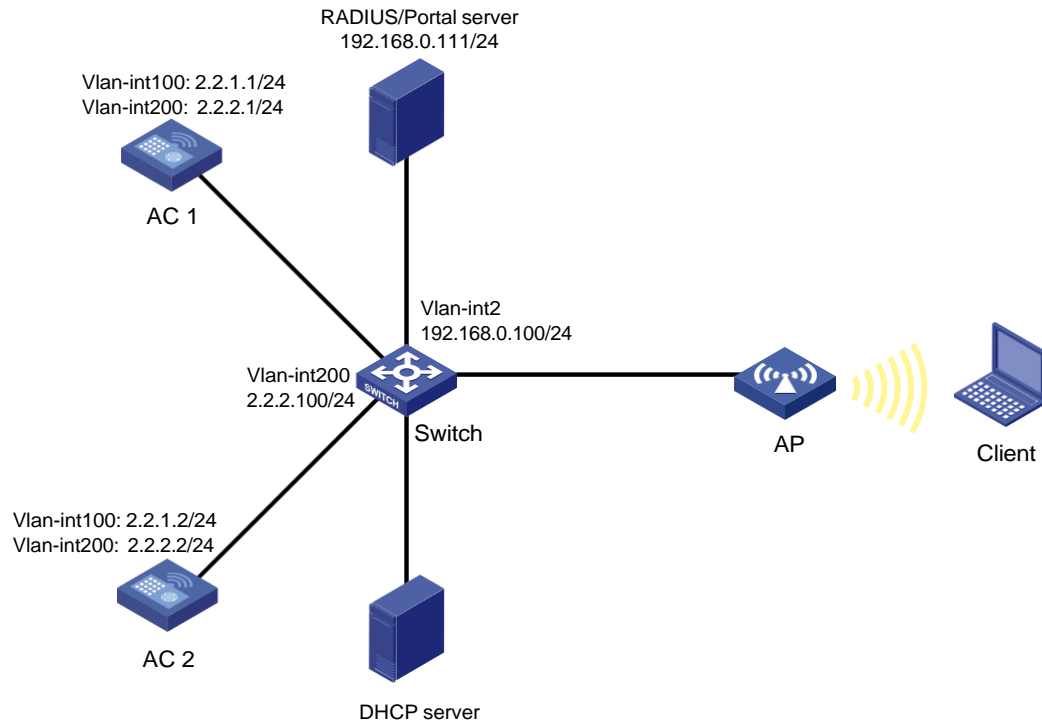
Network configuration

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

Configure the devices to meet the following requirements:

- The AP associates with both ACs and the two ACs to back up each other. When the master AC (AC 1) fails, the backup AC (AC 2) takes over, and the AP can provide services correctly through the backup AC.
- Direct portal authentication is used for wireless clients.
- Before passing portal authentication, the client can access only the portal Web server. After passing the authentication, the client can access other network resources.
- The client can access network resources through any Layer 2 ports in its access VLAN without re-authentication.
- The INC server can dynamically modify user authorization information and log off clients.

Figure 1 Network diagram



Analysis

- To allow an authenticated user to access network resources on any Layer 2 ports in its access VLAN without re-authentication, you must enable the portal roaming feature.
- To avoid possible authentication failure caused by frequent logins and logouts of portal clients in a short time, disable the Rule ARP entry feature.
- To allow the RADIUS server to modify user authorization information and log off users, enable the RADIUS session-control feature.

Restrictions and guidelines

When you configure remote portal authentication for dual-link AC backup and centralized forwarding, follow these restrictions and guidelines:

- Use the actual serial ID of an AP to uniquely identify that AP.
- If you configure manual APs, make sure the manual APs configured on the two ACs have the same AP name and identifier (serial ID or MAC address).
- Make sure the two ACs are of the same version.
- Make sure the portal authentication server type and portal Web server type configured on the ACs are the same as the actual server type. This example uses an INC server.
- To avoid possible authentication failure caused by frequent logins and logouts of portal clients in a short time, disable the Rule ARP entry feature.
- To allow the RADIUS server to modify user authorization information and log off users, enable the RADIUS session-control feature.
- URLs redirected from the ACs to the portal Web server do not carry parameters by default. You can configure the parameters to carry as needed.

- If you enable portal authentication in VLAN interface view, only centralized forwarding is supported. If you enable portal authentication in service template view, both centralized forwarding and local forwarding are supported. This example enables portal authentication in service template view.
- Make sure the two ACs have the same portal-free rule settings, including the rule numbers.

Procedures

Configuring AC 1

1. Configure AC interfaces:

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

```
<AC1> system-view
[AC1] vlan 100
[AC1-vlan100] quit
[AC1] interface vlan-interface 100
[AC1-Vlan-interface100] ip address 2.2.1.1 24
[AC1-Vlan-interface100] quit
```

Create VLAN 200 and VLAN-interface 200. Assign the VLAN interface an IP address. Clients will use this VLAN to access the WLAN.

```
[AC1] vlan 200
[AC1-vlan200] quit
[AC1] interface vlan-interface 200
[AC1-Vlan-interface200] ip address 2.2.2.1 24
[AC1-Vlan-interface200] quit
```

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

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

2. Configure a static route to the INC server.

```
[AC1] ip route-static 192.168.0.0 255.255.0.0 2.2.2.100
```

3. Configure wireless services:

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

```
[AC1] wlan service-template st1
```

Specify the SSID as **service**.

```
[AC1-wlan-st-st1] ssid service
```

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

```
[AC1-wlan-st-st1] vlan 200
```

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

```
[AC1-wlan-st-st1] akm mode psk
```

```
[AC1-wlan-st-st1] preshared-key pass-phrase simple 12345678
```

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

```
[AC1-wlan-st-st1] cipher-suite ccmp
```

```
[AC1-wlan-st-st1] security-ie rsn
```

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

```
[AC1-wlan-st-st1] client forwarding-location ac
[AC1-wlan-st-st1] quit
```

4. Configure the AP:

NOTE:

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

Create AP **office**, and specify the AP model and serial ID.

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

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

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

Set the AP connection priority to 7.

```
[AC1-wlan-ap-group-group1] priority 7
```

Specify AC 2 as the backup AC for AC 1. Set the backup AC address as the IP address of VLAN-interface 100 on AC 2.

```
[AC1-wlan-ap-group-group1] backup-ac ip 2.2.1.2
```

Enable master CAPWAP tunnel preemption.

```
[AC1-wlan-ap-group-group1] wlan tunnel-preempt enable
```

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

```
[AC1-wlan-ap-group-group1] ap-model AP 3620
[AC1-wlan-ap-group-group1-ap-model-AP 3620] radio 2
[AC1-wlan-ap-group-group1-ap-model-AP 3620-radio-2] service-template st1
```

Enable radio 2.

```
[AC1-wlan-ap-group-group1-ap-model-AP 3620-radio-2] radio
enable [AC1-wlan-ap-group-group1-ap-model-AP 3620-radio-2] quit
[AC1-wlan-ap-group-group1-ap-model-AP 3620]
quit [AC1-wlan-ap-group-group1] quit
```

5. Configure a RADIUS scheme:

Create RADIUS scheme **rs1**.

```
[AC1] radius scheme rs1
```

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

```
[AC1-radius-rs1] primary authentication 192.168.0.111
[AC1-radius-rs1] primary accounting 192.168.0.111
```

Specify shared keys for RADIUS authentication and accounting.

```
[AC1-radius-rs1] key authentication simple radius
[AC1-radius-rs1] key accounting simple radius
```

Configure AC 1 to remove the ISP domain name from the usernames sent to the RADIUS servers.

```
[AC1-radius-rs1] user-name-format without-domain
[AC1-radius-rs1] nas-ip 2.2.2.1
[AC1-radius-rs1] quit
```

Enable RADIUS session-control.

```
[AC1] radius session-control enable
```

6. Configure the authentication domain:

Create domain **dm1** and enter its view.

```
[AC1] domain dm1
```

Configure the domain to use RADIUS scheme **rs1** for authentication, authorization, and accounting.

```
[AC1-isp-dm1] authentication portal radius-scheme rs1
```

```
[AC1-isp-dm1] authorization portal radius-scheme rs1
```

```
[AC1-isp-dm1] accounting portal radius-scheme rs1
```

Set the client idle timeout to 15 minutes and set the minimum threshold to 1024 bytes for clients in ISP domain **dm1**.

```
[AC1-isp-dm1] authorization-attribute idle-cut 15 1024
```

```
[AC1-isp-dm1] quit
```

7. Configure portal authentication:

Create the portal authentication server **newpt**, specify the server IP address as 192.168.0.111, and set the destination UDP port number to **50100** for the AC to send unsolicited portal packets to the portal authentication server.

```
[AC1] portal server newpt
```

```
[AC1-portal-server-newpt] ip 192.168.0.111 key simple radius
```

```
[AC1-portal-server-newpt] port 50100
```

```
[AC1-portal-server-newpt] quit
```

Configure the URL for the portal Web server **newpt** as **http://192.168.0.111:8080/portal**.

```
[AC1] portal web-server newpt
```

```
[AC1-portal-websvr-newpt] url http://192.168.0.111:8080/portal
```

Configure URL parameters **nasip** for the portal Web server **newpt**. Configure the value of the **nasip** parameter as 2.2.2.1.

```
[AC1-portal-websvr-newpt] url-parameter nasip value 2.2.2.1
```

```
[AC1-portal-websvr-newpt] quit
```

Configure an IPv4-based portal-free rule to permit portal Web server traffic.

```
[AC1] portal free-rule 0 destination ip 192.168.0.111 24
```

Configure IPv4-based portal-free rules to permit DNS server traffic.

```
[AC1] portal free-rule 1 destination ip any udp 53
```

```
[AC1] portal free-rule 2 destination ip any tcp 53
```

Enable intra-VLAN roaming for portal users.

```
[AC1] portal roaming enable
```

Disable the Rule ARP entry feature for portal clients.

```
[AC1] undo portal refresh arp enable
```

Enable validity check on wireless portal clients.

```
[AC1] portal host-check enable
```

Enable direct IPv4 portal authentication for service template **st1**.

```
[AC1] wlan service-template st1
```

```
[AC1-wlan-st-st1] portal enable method direct
```

Configure the authentication domain for IPv4 portal users as **dm1** on service template **st1**.

```
[AC1-wlan-st-st1] portal domain dm1
```

Specify portal Web server **newpt** on service template **st1** to redirect portal user HTTP or HTTPS requests to the server.

```
[AC1-wlan-st-st1] portal apply web-server newpt
```

Specify the BAS IP as the IP address of VLAN-interface 200, from which clients come online from AC 1.

```
[AC1-wlan-st-st1] portal bas-ip 2.2.2.1
# Enable the service template.
[AC1-wlan-st-st1] service-template enable
[AC1-wlan-st-st1] quit
```

Configuring AC 2

1. Configure AC interfaces:

Create VLAN 501 and VLAN-interface 100. Assign the VLAN interface an IP address. The AC will use this IP address to establish a CAPWAP tunnel with the AP.

```
<AC2> system-view
[AC2] vlan 100
[AC2-vlan100] quit
[AC2] interface vlan-interface 100
[AC2-Vlan-interface100] ip address 2.2.1.2 24
[AC2-Vlan-interface100] quit
```

Create VLAN 200 and VLAN-interface 200. Assign the VLAN interface an IP address. Clients will use this VLAN to access the WLAN.

```
[AC2] vlan 200
[AC2-vlan200] quit
[AC2] interface vlan-interface 200
[AC2-Vlan-interface200] ip address 2.2.2.2 24
[AC2-Vlan-interface200] quit
```

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

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

2. Configure a static route to the INC server.

```
[AC2] ip route-static 192.168.0.0 255.255.0.0 2.2.2.100
```

3. Configure wireless services:

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

```
[AC2] wlan service-template st1
```

Specify the SSID as **service.**

```
[AC2-wlan-st-st1] ssid service
```

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

```
[AC2-wlan-st-st1] vlan 200
```

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

```
[AC2-wlan-st-st1] akm mode psk
```

```
[AC2-wlan-st-st1] preshared-key pass-phrase simple 12345678
```

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

```
[AC2-wlan-st-st1] cipher-suite ccmp
```

```
[AC2-wlan-st-st1] security-ie rsn
```

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

```
[AC2-wlan-st-st1] client forwarding-location ac
```

```
[AC2-wlan-st-st1] quit
```

4. Configure the AP:

NOTE:

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

Create AP *office*, and specify the AP model and serial ID.

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

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

```
[AC2] wlan ap-group group1
[AC2-wlan-ap-group-group1] ap office
```

Set the AP connection priority to 6.

```
[AC2-wlan-ap-group-group1] priority 6
```

Specify AC 1 as the backup AC for AC 2. Set the backup AC address as the IP address of VLAN-interface 100 on AC 1.

```
[AC2-wlan-ap-group-group1] backup-ac ip 2.2.1.1
```

Enable master CAPWAP tunnel preemption.

```
[AC2-wlan-ap-group-group1] wlan tunnel-preempt enable
```

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

```
[AC2-wlan-ap-group-group1] ap-model AP 3620
[AC2-wlan-ap-group-group1-ap-model-AP 3620] radio 2
[AC2-wlan-ap-group-group1-ap-model-AP 3620-radio-2] service-template st1
```

Enable radio 2.

```
[AC2-wlan-ap-group-group1-ap-model-AP 3620-radio-2] radio
enable [AC2-wlan-ap-group-group1-ap-model-AP 3620-radio-2] quit
[AC2-wlan-ap-group-group1-ap-model-AP 3620]
quit [AC2-wlan-ap-group-group1] quit
```

5. Configure a RADIUS scheme:

Create RADIUS scheme *rs1*.

```
[AC2] radius scheme rs1
```

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

```
[AC2-radius-rs1] primary authentication 192.168.0.111
[AC2-radius-rs1] primary accounting 192.168.0.111
```

Specify shared keys for RADIUS authentication and accounting.

```
[AC2-radius-rs1] key authentication simple radius
[AC2-radius-rs1] key accounting simple radius
```

Configure AC 1 to remove the ISP domain name from the usernames sent to the RADIUS servers.

```
[AC2-radius-rs1] user-name-format without-domain
[AC2-radius-rs1] nas-ip 2.2.2.2
[AC2-radius-rs1] quit
```

Enable RADIUS session-control.

```
[AC2] radius session-control enable
```

6. Configure the authentication domain:

Create domain *dm1* and enter its view.

```
[AC2] domain dm1
```

Configure the domain to use RADIUS scheme **rs1** for authentication, authorization, and accounting.

```
[AC2-isp-dm1] authentication portal radius-scheme rs1
[AC2-isp-dm1] authorization portal radius-scheme rs1
[AC2-isp-dm1] accounting portal radius-scheme rs1
```

Set the client idle timeout to 15 minutes and set the minimum threshold to 1024 bytes for clients in ISP domain **dm1**.

```
[AC2-isp-dm1] authorization-attribute idle-cut 15 1024
[AC2-isp-dm1] quit
```

7. Configure portal authentication:

Create the portal authentication server **newpt**, specify the server IP address as 192.168.0.111, and set the destination UDP port number to **50100** for the AC to send unsolicited portal packets to the portal authentication server.

```
[AC2] portal server newpt
[AC2-portal-server-newpt] ip 192.168.0.111 key simple radius
[AC2-portal-server-newpt] port 50100
[AC2-portal-server-newpt] quit
```

Configure the URL for the portal Web server **newpt** as **http://192.168.0.111:8080/portal**.

```
[AC2] portal web-server newpt
[AC2-portal-websvr-newpt] url http://192.168.0.111:8080/portal
```

Configure URL parameters **nasip** for the portal Web server **newpt**. Configure the value of the **nasip** parameter as 2.2.2.2.

```
[AC2-portal-websvr-newpt] url-parameter nasip value 2.2.2.2
[AC2-portal-websvr-newpt] quit
```

Configure an IPv4-based portal-free rule to permit portal Web server traffic.

```
[AC2] portal free-rule 0 destination ip 192.168.0.111 24
```

Configure IPv4-based portal-free rules to permit DNS server traffic.

```
[AC2] portal free-rule 1 destination ip any udp 53
[AC2] portal free-rule 2 destination ip any tcp 53
```

Enable intra-VLAN roaming for portal users.

```
[AC2] portal roaming enable
```

Disable the Rule ARP entry feature for portal clients.

```
[AC2] undo portal refresh arp enable
```

Enable validity check on wireless portal clients.

```
[AC2] portal host-check enable
```

Enable direct IPv4 portal authentication for service template **st1**.

```
[AC2] wlan service-template st1
[AC2-wlan-st-st1] portal enable method direct
```

Configure the authentication domain for IPv4 portal users as **dm1** on service template **st1**.

```
[AC2-wlan-st-st1] portal domain dm1
```

Specify portal Web server **newpt** on service template **st1** to redirect user HTTP or HTTPS requests to the server.

```
[AC2-wlan-st-st1] portal apply web-server newpt
```

Specify the BAS IP as the IP address of VLAN-interface 200, from which clients come online from AC 2.

```
[AC2-wlan-st-st1] portal bas-ip 2.2.2.2
```

Enable the service template.

```
[AC2-wlan-st-st1] service-template enable
```



```
[AC2-wlan-st-st1] quit
```

Configuring the switch

Create VLAN 100 for forwarding CAPWAP tunnel traffic between AC and AP.

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

Create VLAN 200 for forwarding client traffic.

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

Create VLAN 2 for connecting to the INC server.

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

Add the interface that connects the switch to the INC server to VLAN 2. (Details not shown.)

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

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

Enable PoE.

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

Configure GigabitEthernet 1/0/3 that connects the switch to AC 2 as a trunk port, and assign it to VLAN 100 and VLAN 200.

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

Configure GigabitEthernet 1/0/4 that connects the switch to the DHCP server as a trunk port, and assign it to VLAN 100 and VLAN 200.

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

Assign an IP address to VLAN-interface 200.

```
[Switch] interface vlan-interface 200
[Switch-Vlan-interface200] ip address 2.2.2.100 255.255.255.0
[Switch-Vlan-interface200] quit
```

Assign an IP address to VLAN-interface 2. This address will be used as the gateway address for the INC server.

```
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] ip address 192.168.0.100 255.255.255.0
[Switch-Vlan-interface2] quit
```

Configuring the DHCP server

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

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

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

```
[DHCP Server] vlan 100
[DHCP Server-vlan100] quit
[DHCP Server] interface vlan-interface 100
[DHCP Server-Vlan-interface100] ip address 2.2.1.200 255.255.255.0
[DHCP Server-Vlan-interface100] quit
```

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

```
[DHCP Server] vlan 200
[DHCP Server-vlan200] quit
[DHCP Server] interface vlan-interface 200
[DHCP Server-Vlan-interface200] ip address 2.2.2.200 255.255.255.0
[DHCP Server-Vlan-interface200] quit
```

Enable DHCP.

```
[DHCP Server] dhcp enable
```

Create a DHCP address pool named **VLAN100** for the AP, specify the DHCP server as the gateway, and exclude the IP addresses of AC 1, AC 2, and DHCP server from dynamic allocation.

```
[DHCP Server] dhcp server ip-pool VLAN100
[DHCP Server-dhcp-pool-vlan100] gateway-list 2.2.1.200
[DHCP Server-dhcp-pool-vlan100] network 2.2.1.0 mask 255.255.255.0
[DHCP Server-dhcp-pool-vlan100] forbidden-ip 2.2.1.200 2.2.1.1 2.2.1.2
[DHCP Server-dhcp-pool-vlan100] quit
```

Create a DHCP address pool named **VLAN200** for the client, specify the switch as the gateway, specify the DNS server address as 8.8.8.8, and exclude the IP addresses of AC 1, AC 2, and switch from dynamic allocation.

```
[DHCP Server] dhcp server ip-pool VLAN200
[DHCP Server-dhcp-pool-vlan200] gateway-list 2.2.2.100
[DHCP Server-dhcp-pool-vlan200] network 2.2.2.0 mask 255.255.255.0
[DHCP Server-dhcp-pool-vlan200] dns-list 8.8.8.8
[DHCP Server-dhcp-pool-vlan200] forbidden-ip 2.2.2.100 2.2.2.1 2.2.2.2
[DHCP Server-dhcp-pool-vlan200] quit
```

Configuring the INC server

In this example, the INC server runs INC PLAT 7.3 (E0605), INC INC - EIA 7.3 (E0512), and INC EIP 7.3 (E0512).

Configure the RADIUS server

1. Add AC 1 as an access device:
 - a. Log in to INC and click the **User** tab.
 - b. From the navigation pane, select **User Access Policy > Access Device Management > Access Device**.
 - c. Click **Add**.
The **Add Access Device** page opens.
 - d. In the **Access Configuration** area, configure the following parameters:
 - Enter **radius** in the **Shared Key** and **Confirm Shared Key** fields. Make sure the key is the same as the key configured on the ACs.
 - Use the default values for other parameters.
 - e. In the **Device List** area, click **Select** or **Add Manually** to add AC 1 at 2.2.2.1 as an access device.
 - f. Click **OK**.

Figure 2 Adding an access device

Navigation: User > User Access Policy > Access Device Management > Access Device > Add Access Device

Access Configuration

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

Device List

Select Add Manually Clear All

Device Name	Device IP	Device Model	Comments	Delete
	2.2.2.1			

Total Items: 1.

OK Cancel

2. Repeat the previous step to add AC 2 as an access device.
The IP address of AC 2 is 2.2.2.2.
3. Add an access policy.
 - a. From the navigation pane, select **User Access Policy > Access Policy**.
 - b. Click **Add**.
 - c. Enter the access policy name. In this example, the name is **AccessPolicy**.
 - d. Select the **Ungrouped** service group.
 - e. Use the default settings for other parameters.

Figure 3 Adding an access policy

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

Basic Information

Access Policy Name *

Service Group *

Description

Authorization Information

Access Period

Downstream Rate(Kbps)

Priority

Certificate Authentication ☒ None ☐ EAP

Certificate Type

Deploy VLAN

☐ Deploy User Profile

☐ Deploy ACL

Allocate IP *

Upstream Rate(Kbps)

☐ RSA Authentication

Deploy User Group

4. Add an access service.
 - a. From the navigation pane, select **User Access Policy > Access Service**.
 - b. Click **Add**.
 - c. Enter the service name. In this example, the service name is **RadiusServer**.
 - d. Select **AccessPolicy**.
 - e. Use the default settings for other parameters.
 - f. Click **OK**.

Figure 4 Adding an access service

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

Basic Information

Service Name *

Service Group *

Default Proprietary Attribute Assignment Policy *

Default Max. Number of Bound Endpoints *

Description

☒ Available

Service Suffix

Default Access Policy *

Default Max. Number of Online Endpoints *

☐ Transparent Authentication on Portal Endpoints

Access Scenario List

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

5. Add an access user.
 - a. From the navigation pane, select **Access User > All Access Users**.
 - b. Click **Add**.
 - c. Select an existing access user or click **Add User** to add a new access user.

- d. Specify the account name. In this example, the name is **client**.
- e. Set the password. In this example, the password is **1234567**.
- f. Select service **RadiusServer**.
- g. Use the default settings for other parameters.
- h. Click **OK**.

Figure 5 Adding an access user

The screenshot shows the 'Add Access User' configuration page. The 'Access Information' section includes fields for 'User Name' (client1), 'Account Name' (client), 'Password' (1234567), and 'Confirm Password'. There are checkboxes for 'Trial Account', 'Default BYOD User', 'MAC Authentication User', 'Computer User', 'Fast Access User', 'Allow User to Change Password', 'Enable Password Strategy', and 'Modify Password at Next Login'. The 'Access Service' section shows a table with 'RadiusServer' selected. The 'Binding Information' section has 'OK', 'OK & Print', and 'Cancel' buttons.

Configure the portal server

1. Configure portal authentication:
 - a. Click the **User** tab.
 - b. Select **User Access Policy > Portal Service > Server** from the navigation tree to open the portal server configuration page.
 - c. Permit different ports to be bound to the same IP address group, and configure the other portal server parameters as needed.
This example uses the default settings.
 - d. Click **OK**.

Figure 6 Portal authentication server configuration

The screenshot shows the 'Portal Server' configuration page. The 'Basic Information' section has 'Log Level' set to 'Info'. The 'Portal Server' section includes 'Request Timeout(Seconds)' (4), 'Server Heartbeat Interval(Seconds)' (20), 'User Heartbeat Interval(Minutes)' (5), and 'LB Device Address'. The 'Portal Web' section includes 'Request Timeout(Seconds)' (15), 'Verify Endpoint Requests' (Yes), 'HTTP Heartbeat Display' (New Page), 'Packet Code', 'Use Cache' (Yes), and 'HTTPS Heartbeat Display' (Original Page). The 'Portal Page' section shows the URL 'http://192.168.0.111:8080/portal/'.

192.168.0.111

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

Figure 7 Adding an IP address group

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

Add IP Group

IP Group Name *	<input type="text" value="Portal_user"/>
Start IP *	<input type="text" value="2.2.2.1"/>
End IP *	<input type="text" value="2.2.2.255"/>
Service Group	<input type="text" value="Ungrouped"/>
Action *	<input type="text" value="Normal"/>

OK Cancel

3. Add AC 1 as a portal device:
 - a. Select **User Access Policy > Portal Service > Device** from the navigation tree to open the portal device configuration page.
 - b. Click **Add** to open the page as shown in [Figure 8](#).
 - c. Enter the device name.
 - d. Specify the version as **Portal 2.0**.
 - e. Enter the portal BAS-IP configured on AC 1 as the IP address.
 - f. Set whether to support the portal server heartbeat and user heartbeat functions.
In this example, select **No** for both **Support Server Heartbeat** and **Support User Heartbeat**.
 - g. Enter the key, which must be the same as that configured on the AC.
 - h. Select **Directly Connected** from the **Access Method** list.
 - i. Use the default settings for other parameters.
 - j. Click **OK**.

Figure 8 Adding a portal device


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

Add Device

Device Information

Device Name *	NAS	Service Group *	Ungrouped
Version *	Portal 2.0	IP Address *	2.2.2.1
Listening Port *	2000	Local Challenge *	No
Authentication Retries *	0	Logout Retries *	1
Support Server Heartbeat *	No	Support User Heartbeat *	No
Key *	*****	Confirm Key *	*****
Access Method *	Directly Conne		
Device Description			

OK Cancel

4. Repeat the previous step to add AC 2 as a portal device.
5. Associate AC 1 with the IP address group:
 - a. As shown in Figure 9, click the **Port Group Information Management** icon  for the device to open the port group configuration page.
 - b. Click **Add** to open the page as shown in Figure 10.
 - c. Enter the port group name. In this example, the name is **Portal_user**.
 - d. Select the configured IP address group.

The IP address used by the user to access the network must be within this IP address group.
 - e. Use the default settings for other parameters.
 - f. Click **OK**.

Figure 9 Device list

User > User Access Policy > Portal Service > Device

Query Devices

Device Name: Version: Deploy Result: Service Group: Query Reset

Add

Device Name	Version	Service Group	IP Address	Last Deployed at	Deploy Result	Operation
NAS	Portal 2.0	Ungrouped	2.2.2.1		Not Deployed	

1-1 of 1, Page 1 of 1

Figure 10 Adding a port group

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

Add Port Group

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

OK Cancel

6. Repeat the previous step to associate AC 2 with the IP address group.

Verifying the configuration

Make the AP come online.

Verify that the AP first associates with AC 1. Shut down VLAN-interface 100 on AC 1, wait 3 minutes, and verify that the AP associates with AC 2 and the AP state on AC 2 is **R/M**.

Bring up VLAN-interface 100 on AC 1. Verify that the AP state becomes R/M on AC 1 and R/B on AC 2.

```
<AC1> display wlan ap all
```

Total number of APs: 1

Total number of connected APs: 1

Total number of connected manual APs: 1

Total number of connected auto APs: 0

Total number of connected common APs: 1

Total number of connected WTUs: 0

Total number of inside APs: 0

Maximum supported APs: 64

Remaining APs: 63

Total AP licenses: 16

Local AP licenses: 16

Server AP licenses: 0

Remaining Local AP licenses: 15

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
office	1	R/M	AP 3620	219801A28N819CE0002T

```
<AC2> display wlan ap all
```

Total number of APs: 1

Total number of connected APs: 1

Total number of connected manual APs: 1

Total number of connected auto APs: 0

Total number of connected common APs: 1

Total number of connected WTUs: 0

Total number of inside APs: 0

Maximum supported APs: 64

Remaining APs: 63

Total AP licenses: 16

Local AP licenses: 16

Server AP licenses: 0

Remaining Local AP licenses: 16

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
office           1      R/B   AP 3620      219801A28N819CE0002T
# Verify that all Web requests are redirected to the portal authentication page
(http://192.168.0.111:8080/portal) before you pass portal authentication, and you can access
Internet resources after being authenticated.
# View online port user information generated on AC 1.
[AC1] display portal user all
Total portal users: 1
Username: Client
  AP name: office
  Radio ID: 2
  SSID: service
  Portal server: newpt
  State: Online
  VPN instance: N/A
  MAC          IP          VLAN    Interface
0021-6330-0933 2.2.2.3      200     WLAN-BSS1/0/3
Authorization information:
  DHCP IP pool: N/A
  User profile: N/A
  Session group profile: N/A
  ACL number: N/A
  Inbound CAR: N/A
  Outbound CAR: N/A
```

Configuration files

- AC 1:

```
#
vlan 100
#
vlan 200
#
wlan service-template st1
  ssid service
  vlan 200
client forwarding-location ac
  akm mode psk
  preshared-key pass-phrase cipher $c$3$0Lf6p0Z6bxrf25nodjOJKYEfnZ6g6ErccHyQ
  cipher-suite ccmp
  security-ie rsn
portal enable method direct
portal domain dm1
```

```

portal bas-ip 2.2.2.1
portal apply web-server newpt
service-template enable
#
interface Vlan-interface100
ip address 2.2.1.1 255.255.255.0
#
interface Vlan-interface200
ip address 2.2.2.1 255.255.255.0
#
interface gigabitethernet 1/0/1
port link-type trunk
port trunk permit vlan 1 100 200
#
ip route-static 192.168.0.0 16 2.2.2.100
#
radius session-control enable
#
radius scheme rs1
primary authentication 192.168.0.111
primary accounting 192.168.0.111
key authentication cipher $c$3$Sggqz7lDs4XPnethmAgyAKVlke7qwEkYbQ==
key accounting cipher $c$3$4J/JBRGwqB4F213furJMkB6JWYXBFjWE6g==
user-name-format without-domain
nas-ip 2.2.2.1
#
domain dml
authorization-attribute idle-cut 15 1024
authentication portal radius-scheme rs1
authorization portal radius-scheme rs1
accounting portal radius-scheme rs1
#
portal host-check enable
portal free-rule 0 destination ip 192.168.0.0 255.255.255.0
portal free-rule 1 destination ip any udp 53
portal free-rule 2 destination ip any tcp 53
#
portal web-server newpt
url http://192.168.0.111:8080/portal
url-parameter nasip value 2.2.2.1
#
portal server newpt
ip 192.168.0.111 key cipher $c$3$AkTEB7OgMYnCqsfDeplhoAgXUek/rVrLZw==
#
wlan ap-group group1
priority 7
wlan tunnel-preempt enable
backup-ac ip 2.2.1.2

```

```

ap office
ap-model AP 3620
radio 1
    radio 2
    radio enable
    service-template st1
#
wlan ap office model AP 3620
    serial-id 219801A28N819CE0002T
#

```

- **AC 2:**

```

#
vlan 100
#
vlan 200
#
wlan service-template st1
    ssid service
    vlan 200
client forwarding-location ac
    akm mode psk
    preshared-key pass-phrase cipher $c$3$0Lf6pOZ6bxrf25nodjOJKYEfnZ6g6ErccHyQ
    cipher-suite ccmp
    security-ie rsn
portal enable method direct
    portal domain dm1
    portal bas-ip 2.2.2.2
    portal apply web-server newpt
    service-template enable
#
interface Vlan-interface100
    ip address 2.2.1.2 255.255.255.0
#
interface Vlan-interface200
    ip address 2.2.2.2 255.255.255.0
#
interface gigabitethernet 1/0/1
port link-type trunk
port trunk permit vlan 1 100 200
#
ip route-static 192.168.0.0 16 2.2.2.100
#
radius session-control enable
#
radius scheme rs1
    primary authentication 192.168.0.111
    primary accounting 192.168.0.111
    key authentication cipher $c$3$Sggqz7lDs4XPnethmAgyAKVlke7qwEkYbQ==

```

```

key accounting cipher $c$3$4J/JBRGwqB4F213furJMkB6JWYXBFjWE6g==
user-name-format without-domain
nas-ip 2.2.2.2
#
domain dml
    authorization-attribute idle-cut 15 1024
    authentication portal radius-scheme rs1
    authorization portal radius-scheme rs1
    accounting portal radius-scheme rs1
#
portal host-check enable
portal free-rule 0 destination ip 192.168.0.0 255.255.255.0
portal free-rule 1 destination ip any udp 53
portal free-rule 2 destination ip any tcp 53
#
portal web-server newpt
    url http://192.168.0.111:8080/portal
    url-parameter nasip value 2.2.2.2
#
portal server newpt
    ip 192.168.0.111 key cipher $c$3$AkTEB7OgMYnCqsfDeplhoAgXUek/rVrLZw==
#
wlan ap-group group1
    priority 6
    wlan tunnel-preempt enable
    backup-ac ip 2.2.1.1
    ap office
    ap-model AP 3620
radio 1
    radio 2
        radio enable
        service-template st1
#
wlan ap office model AP 3620
    serial-id 219801A28N819CE0002T
#

```

- **Switch:**

```

#
vlan 2
#
vlan 100
#
vlan 200
#
interface Vlan-interface2
    ip address 192.168.0.100 255.255.255.0
#
interface Vlan-interface200

```

```

ip address 2.2.2.100 255.255.255.0
#
interface GigabitEthernet1/0/1
port link-type trunk
port trunk permit vlan 1 100 200
#
interface GigabitEthernet1/0/2
port link-type access
port access vlan 100
poE enable
#
interface GigabitEthernet1/0/3
port link-type trunk
port trunk permit vlan 1 100 200
#
interface GigabitEthernet1/0/4
port link-type trunk
port trunk permit vlan 1 100 200

```

- **DHCP server:**

```

#
dhcp enable
#
vlan 100
#
vlan 200
#
dhcp server ip-pool VLAN100
gateway-list 2.2.1.200
network 2.2.1.0 mask 255.255.255.0
forbidden-ip 2.2.1.1
forbidden-ip 2.2.1.2
forbidden-ip 2.2.1.200
#
dhcp server ip-pool VLAN200
gateway-list 2.2.2.100
network 2.2.2.0 mask 255.255.255.0
dns-list 8.8.8.8
forbidden-ip 2.2.2.1
forbidden-ip 2.2.2.2
forbidden-ip 2.2.2.100
#
interface Vlan-interface100
ip address 2.2.1.200 255.255.255.0
#
interface Vlan-interface200
ip address 2.2.2.200 255.255.255.0
#
interface GigabitEthernet1/0/1

```

```
port link-type trunk
port trunk permit vlan 1 100 200
#
```

Related documentation

- *AAA Management Command Reference in INTELBRAS Access Controllers Command References*
- *AAA Management Configuration Guide in INTELBRAS Access Controllers Configuration Guides*
- *AP Management Command Reference in INTELBRAS Access Controllers Command References*
- *AP Management Configuration Guide in INTELBRAS Access Controllers Configuration Guides*
- *Portal Authentication Command Reference in INTELBRAS Access Controllers Command References*
- *Portal Authentication Configuration Guide in INTELBRAS Access Controllers Configuration Guides*
- *WLAN Access Command Reference in INTELBRAS Access Controllers Command References*
- *WLAN Access Configuration Guide in INTELBRAS Access Controllers Configuration Guides*
- *WLAN High Availability Command Reference in INTELBRAS Access Controllers Command References*
- *WLAN High Availability Configuration Guide in INTELBRAS Access Controllers Configuration Guides*

INTELBRAS Access Controllers

Dual-Link Backup OAuth-Based Portal Authentication in Centralized Forwarding Configuration Examples

Copyright © 2024 Intelbras S.A All rights reserved.

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

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

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

Contents

Introduction	1
Prerequisites	1
Example: Configuring OAuth-based portal authentication for dual-link AC backup and centralized forwarding	1
Network configuration	1
Analysis	2
Restrictions and guidelines	2
Procedures	3
Configuring AC 1	3
Configuring AC 2	6
Configuring the switch	9
Configuring the DHCP server	10
Configuring the INC server	11
Verifying the configuration	15
Configuration files	17
Related documentation	22

Introduction

The following information provides an example for configuring OAuth-based portal authentication in a dual-link backup network enabled with centralized forwarding.

Prerequisites

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

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

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

Example: Configuring OAuth-based portal authentication for dual-link AC backup and centralized forwarding

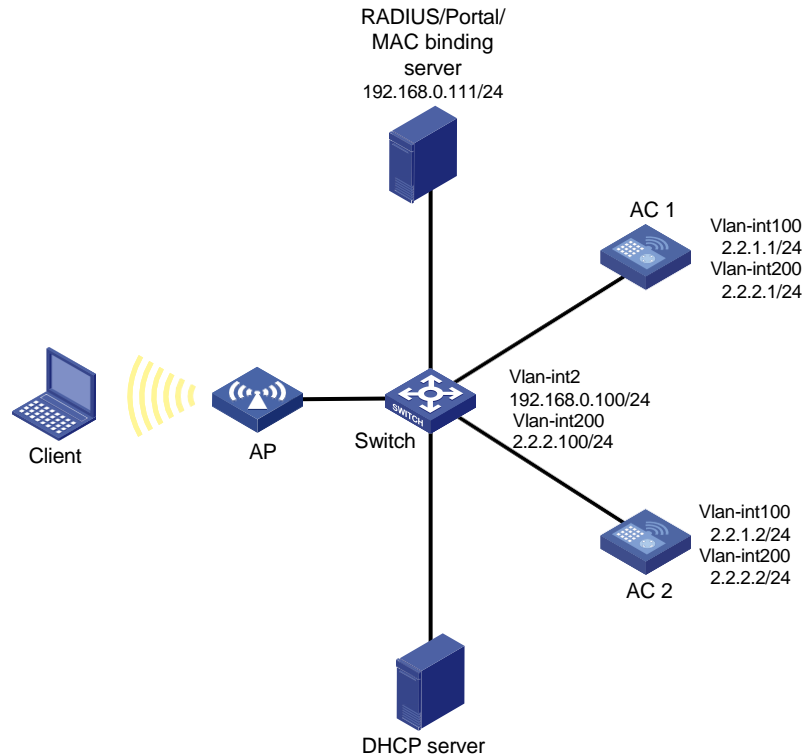
Network configuration

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

Configure the devices to meet the following requirements:

- Before passing portal authentication, the client can access only the portal Web server. After passing the authentication, the client can access other network resources.
- The AC forwards all the client traffic.
- The client can access network resources through any Layer 2 ports in its access VLAN without re-authentication.
- The INC server can dynamically modify user authorization information and log off clients.

Figure 1 Network diagram



Analysis

- To allow an authenticated user to access network resources on any Layer 2 ports in its access VLAN without re-authentication, you must enable the portal roaming feature.
- To avoid possible authentication failure caused by frequent logins and logouts of portal clients in a short time, disable the Rule ARP entry feature.
- To allow the RADIUS server to modify user authorization information and log off users, enable the RADIUS session-control feature.
- For dual-link backup to operate correctly, you must configure manual AP or auto AP settings on both ACs. This ensures that the AP can establish CAPWAP tunnels with both ACs.
- For MAC-trigger authentication to use OAuth, you must execute the **cloud-binding enable** command.

Restrictions and guidelines

When you configure OAuth-based portal authentication for dual-link AC backup and centralized forwarding, follow these restrictions and guidelines:

- Use the actual serial ID of an AP to uniquely identify that AP.
- If you configure manual APs, make sure the manual APs configured on the two ACs have the same AP name and identifier (serial ID or MAC address).
- For portal-free rules to take effect, you must configure DNS on the ACs.
- Some clients are enabled with MAC randomization by default, which might cause seamless roaming failures. As a best practice, disable MAC randomization.

Procedures

Configuring AC 1

1. Configure AC interfaces:

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

```
<AC1> system-view
[AC1] vlan 100
[AC1-vlan100] quit
[AC1] interface vlan-interface 100
[AC1-Vlan-interface100] ip address 2.2.1.1 24
[AC1-Vlan-interface100] quit
```

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

```
[AC1] vlan 200
[AC1-vlan200] quit
[AC1] interface vlan-interface 200
[AC1-Vlan-interface200] ip address 2.2.2.1 24
[AC1-Vlan-interface200] quit
```

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

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

2. Configure a static route to the INC server.

```
[AC1] ip route-static 192.168.0.0 255.255.0.0 2.2.2.100
```

3. Configure DNS server settings. (Details not shown.)

4. Configure wireless services:

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

```
[AC1] wlan service-template st1
```

Specify the SSID as **service**.

```
[AC1-wlan-st-st1] ssid service
```

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

```
[AC1-wlan-st-st1] vlan 200
```

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

```
[AC1-wlan-st-st1] akm mode psk
```

```
[AC1-wlan-st-st1] preshared-key pass-phrase simple 12345678
```

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

```
[AC1-wlan-st-st1] cipher-suite ccmp
```

```
[AC1-wlan-st-st1] security-ie rsn
```

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

```
[AC1-wlan-st-st1] client forwarding-location ac
```

```
[AC1-wlan-st-st1] quit
```

5. Configure the AP:

NOTE:

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

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

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

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

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

Set the AP connection priority to 7.

```
[AC1-wlan-ap-group-group1] priority 7
```

Specify AC 2 as the backup AC for AC 1. Set the backup AC address as the IP address of VLAN-interface 100 on AC 2.

```
[AC1-wlan-ap-group-group1] backup-ac ip 2.2.1.2
```

Enable master CAPWAP tunnel preemption.

```
[AC1-wlan-ap-group-group1] wlan tunnel-preempt enable
```

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

```
[AC1-wlan-ap-group-group1] ap-model AP 3620
[AC1-wlan-ap-group-group1-ap-model-AP 3620] radio 2
[AC1-wlan-ap-group-group1-ap-model-AP 3620-radio-2] service-template st1
```

Enable radio 2.

```
[AC1-wlan-ap-group-group1-ap-model-AP 3620-radio-2] radio
enable [AC1-wlan-ap-group-group1-ap-model-AP 3620-radio-2] quit
[AC1-wlan-ap-group-group1-ap-model-AP 3620]
quit [AC1-wlan-ap-group-group1] quit
```

6. Configure portal authentication:

Create domain **dm1** and enter its view.

```
[AC1] domain dm1
```

Configure the authentication, authorization, and accounting methods as none for portal users.

```
[AC1-isp-dm1] authentication portal none
[AC1-isp-dm1] authorization portal none
[AC1-isp-dm1] accounting portal none
[AC1-isp-dm1] quit
```

Create a portal Web server named **newpt**, specify the server's URL as **http://192.168.0.111/INC - WSMAuth/protocol**, and specify the server type as OAuth.

```
[AC1] portal web-server newpt
[AC1-portal-websvr-newpt] url http://192.168.0.111:8080/INC -
WSMAuth/protocol [AC1-portal-websvr-newpt] server-type oauth
```

Enable the optimized captive-bypass feature for iOS users.

```
[AC1-portal-websvr-newpt] captive-bypass ios optimize enable
[AC1-portal-websvr-newpt] quit
```

Create an HTTP-based local portal Web service and enter its view.

```
[AC1] portal local-web-server http
[AC1-portal-local-websvr-http] quit
```

Configure destination-based portal-free rule to permit traffic to the DNS server.

```
[AC1] portal free-rule 2 destination ip any udp 53
```

```
[AC1] portal free-rule 3 destination ip any tcp 53
```

Configure portal safe-redirect to reduce the workload of the authentication server.

```
[AC1] portal safe-redirect enable
```

```
[AC1] portal safe-redirect method get post
```

```
[AC1] portal safe-redirect user-agent CaptiveNetworkSupport
```

```
[AC1] portal safe-redirect user-agent MicroMessenger
```

```
[AC1] portal safe-redirect user-agent Mozilla
```

```
[AC1] portal safe-redirect user-agent WeChat
```

```
[AC1] portal safe-redirect user-agent iPhone
```

```
[AC1] portal safe-redirect user-agent micromessenger
```

Specify the NAS-ID. Make sure the NAS-ID is the same as the ID in file
iNC\client\conf\wiportal\conf.properties.

```
[AC1] wlan global-configuration
```

```
[AC1-wlan-global-configuration] nas-id wiportal
```

```
[AC1-wlan-global-configuration] quit
```

Set the user synchronization interval to 60 seconds for portal authentication using OAuth.

```
[AC1] portal oauth user-sync interval 60
```

Configure a destination-based portal-free rule: specify the rule number as **0** and IP address as **192.168.0.111**. This rule allows users to reach the portal Web server.

```
[AC1] portal free-rule 0 destination ip 192.168.0.111 32
```

Configure a destination-based portal-free rule: specify the rule number as **1** and IP address as **2.2.2.1**. This rule allows users to reach AC 1.

```
[AC1] portal free-rule 1 destination ip 2.2.2.1 32
```

Configure a destination-based portal-free rule: specify the rule number as **4** and IP address as **2.2.2.2**. This rule allows users to reach AC 2.

```
[AC1] portal free-rule 4 destination ip 2.2.2.2 32
```

Enable intra-VLAN roaming for portal users.

```
[AC1] portal roaming enable
```

Disable the Rule ARP entry feature for portal clients.

```
[AC1] undo portal refresh arp enable
```

Enable RADIUS session control.

```
[AC1] radius session-control enable
```

Enable direct IPv4 portal authentication for service template **st1**.

```
[AC1] wlan service-template st1
```

```
[AC1-wlan-st-st1] portal enable method direct
```

Configure the authentication domain for IPv4 portal users as **dm1** on service template **st1**.

```
[AC1-wlan-st-st1] portal domain dm1
```

Apply portal Web server **newpt** to service template **st1**.

```
[AC1-wlan-st-st1] portal apply web-server newpt
```

Enable portal temporary pass and set the temporary pass period to 300 seconds.

```
[AC1-wlan-st-st1] portal temp-pass period 300 enable
```

On the service template, configure the BAS-IP attribute as **2.2.2.1** for portal packets sent to the portal authentication server.

```
[AC1-wlan-st-st1] portal bas-ip 2.2.2.1
```

7. Configure MAC-based quick portal authentication:

Create MAC binding server **mts** and enter its view.

```
[AC1] portal mac-trigger-server mts
```

Specify the IP address of the MAC binding server as 192.168.0.111.

```
[AC1-portal-mac-trigger-server-mts] ip 192.168.0.111
# Enable cloud MAC-trigger authentication.
[AC1-portal-mac-trigger-server-mts] cloud-binding enable
[AC1-portal-mac-trigger-server-mts] quit
# Specify MAC binding server mts on service template st.
[AC1] wlan service-template st1
[AC1-wlan-st-st1] portal apply mac-trigger-server mts
# Enable the service template.
[AC1-wlan-st-st1] service-template enable
[AC1-wlan-st-st1] quit
```

Configuring AC 2

1. Configure AC interfaces:

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

```
<AC2> system-view
[AC2] vlan 100
[AC2-vlan100] quit
[AC2] interface vlan-interface 100
[AC2-Vlan-interface100] ip address 2.2.1.2 24
[AC2-Vlan-interface100] quit
```

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

```
[AC2] vlan 200
[AC2-vlan200] quit
[AC2] interface vlan-interface 200
[AC2-Vlan-interface200] ip address 2.2.2.2 24
[AC2-Vlan-interface200] quit
```

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

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

2. Configure a static route to the INC server.

```
[AC2] ip route-static 192.168.0.0 255.255.0.0 2.2.2.100
```

3. Configure DNS server settings. (Details not shown.)

4. Configure wireless services:

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

```
[AC2] wlan service-template st1
```

Specify the SSID as **service**.

```
[AC2-wlan-st-st1] ssid service
```

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

```
[AC2-wlan-st-st1] vlan 200
```

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

```
[AC2-wlan-st-st1] akm mode psk
```

```
[AC2-wlan-st-st1] preshared-key pass-phrase simple 12345678
```

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

```
[AC2-wlan-st-st1] cipher-suite ccmp
```

```
[AC2-wlan-st-st1] security-ie rsn
```

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

```
[AC2-wlan-st-st1] client forwarding-location ac
```

```
[AC2-wlan-st-st1] quit
```

5. Configure the AP:

NOTE:

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

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

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

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

```
[AC2-wlan-ap-office] quit
```

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

```
[AC2] wlan ap-group group1
```

```
[AC2-wlan-ap-group-group1] ap office
```

Set the AP connection priority to 6.

```
[AC2-wlan-ap-group-group1] priority 6
```

Specify AC 1 as the backup AC for AC 2. Set the backup AC address as the IP address of VLAN-interface 100 on AC 1.

```
[AC2-wlan-ap-group-group1] backup-ac ip 2.2.1.1
```

Enable master CAPWAP tunnel preemption.

```
[AC2-wlan-ap-group-group1] wlan tunnel-preempt enable
```

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

```
[AC2-wlan-ap-group-group1] ap-model AP 3620
```

```
[AC2-wlan-ap-group-group1-ap-model-AP 3620] radio 2
```

```
[AC2-wlan-ap-group-group1-ap-model-AP 3620-radio-2] service-template st1
```

Enable radio 2.

```
[AC2-wlan-ap-group-group1-ap-model-AP 3620-radio-2] radio
```

```
enable [AC2-wlan-ap-group-group1-ap-model-AP 3620-radio-2] quit
```

```
[AC2-wlan-ap-group-group1-ap-model-AP 3620]
```

```
quit [AC2-wlan-ap-group-group1] quit
```

6. Configure portal authentication:

Create domain **dm1** and enter its view.

```
[AC2] domain dm1
```

Configure the authentication, authorization, and accounting methods as none for portal users.

```
[AC2-isp-dm1] authentication portal none
```

```
[AC2-isp-dm1] authorization portal none
```

```
[AC2-isp-dm1] accounting portal none
```

```
[AC2-isp-dm1] quit
```

Create a portal Web server named **newpt**, specify the server's URL as **http://192.168.0.111/INC - WSMAuth/protocol**, and specify the server type as OAuth.

```
[AC2] portal web-server newpt
```

```
[AC2-portal-websvr-newpt] url http://192.168.0.111:8080/INC -  
WSMAuth/protocol [AC2-portal-websvr-newpt] server-type oauth
```

Enable the optimized captive-bypass feature for iOS users.

```
[AC2-portal-websvr-newpt] captive-bypass ios optimize enable
[AC2-portal-websvr-newpt] quit
```

Create an HTTP-based local portal Web service and enter its view.

```
[AC2] portal local-web-server http
[AC2-portal-local-websvr-http] quit
```

Configure destination-based portal-free rule to permit traffic to the DNS server.

```
[AC2] portal free-rule 2 destination ip any udp 53
[AC2] portal free-rule 3 destination ip any tcp 53
```

Configure portal safe-redirect to reduce the workload of the authentication server.

```
[AC2] portal safe-redirect enable
[AC2] portal safe-redirect method get post
[AC2] portal safe-redirect user-agent CaptiveNetworkSupport
[AC2] portal safe-redirect user-agent MicroMessenger
[AC2] portal safe-redirect user-agent Mozilla
[AC2] portal safe-redirect user-agent WeChat
[AC2] portal safe-redirect user-agent iPhone
[AC2] portal safe-redirect user-agent micromessenger
```

Specify the NAS-ID. Make sure the NAS-ID is the same as the ID in file `iNC\client\conf\wportal\conf.properties`.

```
[AC2] wlan global-configuration
[AC2-wlan-global-configuration] nas-id wportal
[AC2-wlan-global-configuration] quit
```

Set the user synchronization interval to 60 seconds for portal authentication using OAuth.

```
[AC2] portal oauth user-sync interval 60
```

Configure a destination-based portal-free rule: specify the rule number as **0** and IP address as **192.168.0.111**. This rule allows users to reach the portal Web server.

```
[AC2] portal free-rule 0 destination ip 192.168.0.111 24
```

Configure a destination-based portal-free rule: specify the rule number as **1** and IP address as **2.2.2.1**. This rule allows users to reach AC 1.

```
[AC2] portal free-rule 1 destination ip 2.2.2.1 32
```

Configure a destination-based portal-free rule: specify the rule number as **4** and IP address as **2.2.2.2**. This rule allows users to reach AC 2.

```
[AC2] portal free-rule 4 destination ip 2.2.2.2 32
```

Enable intra-VLAN roaming for portal users.

```
[AC2] portal roaming enable
```

Disable the Rule ARP entry feature for portal clients.

```
[AC2] undo portal refresh arp enable
```

Enable RADIUS session control.

```
[AC2] radius session-control enable
```

Enable direct IPv4 portal authentication for service template **st1**.

```
[AC2] wlan service-template st1
[AC2-wlan-st-st1] portal enable method direct
```

Configure the authentication domain for IPv4 portal users as **dm1** on service template **st1**.

```
[AC2-wlan-st-st1] portal domain dm1
```

Apply portal Web server **newpt** to service template **st1**.

```
[AC2-wlan-st-st1] portal apply web-server newpt
```

Enable portal temporary pass and set the temporary pass period to 300 seconds.


```
[AC2-wlan-st-st1] portal temp-pass period 300 enable
```

On the service template, configure the BAS-IP attribute as **2.2.2.1** for portal packets sent to the portal authentication server.

```
[AC2-wlan-st-st1] portal bas-ip 2.2.2.2
```

7. Configure MAC-based quick portal authentication:

Create MAC binding server **mts** and enter its view.

```
[AC2] portal mac-trigger-server mts
```

Specify the IP address of the MAC binding server as 192.168.0.111.

```
[AC2-portal-mac-trigger-server-mts] ip 192.168.0.111
```

Enable cloud MAC-trigger authentication.

```
[AC2-portal-mac-trigger-server-mts] cloud-binding enable
```

```
[AC2-portal-mac-trigger-server-mts] quit
```

Specify MAC binding server **mts** on service template **st**.

```
[AC2] wlan service-template st1
```

```
[AC2-wlan-st-st1] portal apply mac-trigger-server mts
```

Enable the service template.

```
[AC2-wlan-st-st1] service-template enable
```

```
[AC2-wlan-st-st1] quit
```

Configuring the switch

Create VLAN 100 for forwarding CAPWAP tunnel traffic between AC and AP.

```
<Switch> system-view
```

```
[Switch] vlan 100
```

```
[Switch-vlan100] quit
```

Create VLAN 200 for forwarding client traffic.

```
[Switch] vlan 200
```

```
[Switch-vlan200] quit
```

Create VLAN 2 for forwarding client traffic.

```
[Switch] vlan 2
```

```
[Switch-vlan2] quit
```

Add the interface that connects the switch to the INC server to VLAN 2. (Details not shown.)

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

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

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

```
[Switch-GigabitEthernet1/0/2] port trunk permit vlan 100 200
```

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

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

```

[Switch] interface gigabitethernet 1/0/3
[Switch-GigabitEthernet1/0/3] port link-type access
[Switch-GigabitEthernet1/0/3] port access vlan 100
# Enable PoE on GigabitEthernet 1/0/3.
[Switch-GigabitEthernet1/0/3] poe enable
[Switch-GigabitEthernet1/0/3] quit

# Configure GigabitEthernet 1/0/4 that connects the switch to the DHCP server as a trunk port, and assign the interface to VLAN 100 and VLAN 200.
[Switch] interface gigabitethernet 1/0/4
[Switch-GigabitEthernet1/0/4] port link-type trunk
[Switch-GigabitEthernet1/0/4] port trunk permit vlan 100 200
[Switch-GigabitEthernet1/0/4] quit

# Assign an IP address to VLAN-interface 2.
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] ip address 192.168.0.100 255.255.255.0
[Switch-Vlan-interface2] quit

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

```

Configuring the DHCP server

```

# Configure GigabitEthernet 1/0/1 that connects the server to the switch as a trunk port, and assign the interface to VLAN 100 and VLAN 200.
[DHCP] interface gigabitethernet 1/0/1
[DHCP-GigabitEthernet1/0/1] port link-type trunk
[DHCP-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[DHCP-GigabitEthernet1/0/1] quit

# Assign an IP address to VLAN-interface 100.
[DHCP] interface vlan-interface 100
[DHCP-Vlan-interface100] ip address 2.2.1.200 255.255.255.0
[DHCP-Vlan-interface100] quit

# Assign an IP address to VLAN-interface 200.
[DHCP] interface vlan-interface 200
[DHCP-Vlan-interface200] ip address 2.2.2.200 255.255.255.0
[DHCP-Vlan-interface200] quit

# Enable DHCP.
[DHCP] dhcp enable

# Create a DHCP address pool named VLAN100, specify the DHCP server as the gateway, and exclude AC and DHCP server addresses from dynamic allocation. The server will use this address pool to assign address to the AP.
[DHCP] dhcp server ip-pool VLAN100
[DHCP-dhcp-pool-vlan100] network 2.2.1.0 mask 255.255.255.0
[DHCP-dhcp-pool-vlan100] forbidden-ip 2.2.1.1 2.2.1.2
[DHCP-dhcp-pool-vlan100] quit

```

Create a DHCP address pool named **VLAN200**, specify the switch as the gateway, specify the DNS server address as 8.8.8.8, and exclude AC and DHCP server addresses from dynamic allocation. The server will use this address pool to assign address to the client.

```
[DHCP] dhcp server ip-pool VLAN200
[DHCP-dhcp-pool-vlan200] gateway-list 2.2.2.100
[DHCP-dhcp-pool-vlan200] network 2.2.2.0 mask 255.255.255.0
[DHCP-dhcp-pool-vlan200] dns-list 8.8.8.8
[DHCP-dhcp-pool-vlan200] forbidden-ip 2.2.2.100 2.2.2.1 2.2.2.2
[DHCP-dhcp-pool-vlan200] quit
```

Configuring the INC server

In this example, the INC server runs INC PLAT 7.3 (E0605) and INC IPM 7.3 (E0516).

To configure the INC server:

1. Add an access user:
 - a. Log in to INC and click the **Service** tab.
 - b. From the navigation tree, select **Intelligent Portal Management > User Management > Users**.
 - c. Click **Add** to open the **Add User** page.
 - d. Enter username **Client** and password **admin@123**.
 - e. Use the default settings for other parameters.
 - f. Click **OK**.

Figure 2 Adding an access user

The screenshot shows the 'Add User' form in the INC server interface. The form is titled 'Add User' and contains several input fields and dropdown menus. The 'Username' field is filled with 'client'. The 'User Group' dropdown is set to 'Ungrouped'. The 'User Password' and 'Confirm Password' fields are filled with '*****'. The 'Identity Number' and 'Telephone Number' fields are empty. The 'Set Online User Count' dropdown is set to 'By User Group'. The 'Start Time' and 'End Time' fields are empty. The 'Remark' field is empty. At the bottom right, there are 'OK' and 'Cancel' buttons.

2. Add an authentication page template:
 - a. From the navigation tree, select **Intelligent Portal Management > Page Template List**.

- b. Click **Add** to open the **Add Theme** page.
- c. Enter template name **theme** in the **Theme Name** field.
- d. Use the default settings for other parameters.
- e. Click **OK** to open the page for editing the template.

Figure 3 Adding an authentication page template

Add Theme

Theme Name * ?

Custom Page: ☐ First ☒ Authentication ☒ Home ☐ Transparent Authentication

Type *

Description ?


- f. On the **theme** page, click the **Authentication** icon  in the **Basic Controls** area.
- g. Click **Edit** in authentication edit area, select **Other** and **Account** in the **Authentication Method** area, click **OK**, and then click **Save Page**.
- h. Use the default settings for other configuration.
- i. Click **Confirm Release**.

Figure 4 Editing the template

Page Template List > Custom Template > theme

Basic Controls **Authentication** **Home** **Page Preview** **Save Page** **Content Setting** **Confirm Release** **Page Preview**

Authentication Scrolling Pictures

Picture Rich Text

Two Pictures in Parallel Three Pictures in Parallel

Four Picture in Parallel Video

Menu Title

App Download Telephone

HTML background music

Authentication edit area

Authentication Method

☒ One-Click Login ☒ Other

☒ Account ☒ Preferred

☐ WeChat

☐ SMS Message

☐ Weibo

☐ QQ

☐ Facebook

☐ E-mail

☐ Ticket

☐ Machine

Account Authentication Settings

☐ Modify

☐ Password

☐ Forgot

☐ Password

☐ Generally registration

☐ Register By scanning the two-dimension code

Wi-Fi User Agreement

Select Agreements Required

☒ Free Wi-Fi User A... ☐

3. Add an authentication policy:

- a. From the navigation tree, select **Intelligent Portal Management > Authentication Policies**.
- b. Click **Add** to open the **Add Authentication Policy** page.
- c. Enter authentication policy name **policy1**, and select **theme** from the **Page Template** list.
- d. Select a transparent authentication period to enable portal transparent authentication (MAC-trigger authentication).
- e. Use the default settings for other parameters.
- f. Click **OK**.

Figure 5 Adding an authentication policy

Intelligent Portal Management > Add Authentication Policy

Add Authentication Policy

Name *	policy1
Description	
Page Template *	theme
Authentication Free	<input type="checkbox"/> ?
Only Mobile Endpoints	<input type="checkbox"/> ?
Transparent Authentication Period *	Today
Match SSID for Transparent Authentication	<input type="checkbox"/>
Idle Time Before Network Cut (Minutes) *	30 ?
Idle Traffic Before Network Cut (Bytes) *	10240 ?
Max. Online Duration Per Access (Seconds) *	0 ?
Maximum Online Duration Per Day (Seconds) *	0 ?
Maximum Traffic Per Day (MB) *	0 ?

OK Cancel

4. Add a site:
 - a. From the navigation tree, select **Intelligent Portal Management > Site Management**.
 - b. Click **Add** to open the **Add Site** page.
 - c. Enter the site name, the site address, the expected number of clients to be supported, and the telephone number.
 - d. Click **OK**.

Figure 6 Adding a site

Intelligent Portal Management > Site Management > Add Site

Site Basic Information

Site Name * userspot

Site Address * useraddress ?

Expected Supported Number * 2

Telephone * 81819999

Site Introduction

Site Group * Ungrouped ▼

User Group * Ungrouped ▼

- e. In the **Associated APs** area, click **Add** to associate an AP.
- f. Enter the serial number and MAC address of the AP.
- g. Click **OK**.

Figure 7 Adding an AP

Add

AP Serial Number * 219801A0CNC138011454

AP IP Address

AP MAC Address * 70F9-6DD7-D900

OK Cancel

- i. In the **Bind Authentication Policy** area, click **Add** to bind the AP to an authentication policy.
- j. Select authentication policy **policy1**.
- k. Use the default settings for other parameters.
- l. Click **OK**.

Figure 8 Binding the AP to an authentication policy

Bind to Authentication Policies

Authentication Policy policy1

SSID

Start Time

End Time

OK Cancel

Verifying the configuration

Make the AP come online.

Verify that the AP state is R/M on AC 1 and R/B on AC 2.

```
<AC1> display wlan ap all
Total number of APs: 1
Total number of connected APs: 1
Total number of connected manual APs: 1
Total number of connected auto APs: 0
Total number of connected common APs: 1
Total number of connected WTUs: 0
Total number of inside APs: 0
Maximum supported APs: 10
Remaining APs: 9
```

```

Total AP licenses: 10
Local AP licenses: 10
Server AP licenses: 0
Remaining Local AP licenses: 9
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
office           1      R/M   AP 3620      219801A28N819CE0002T
<AC2> display wlan ap all
Total number of APs: 1
Total number of connected APs: 1
Total number of connected manual APs: 1
Total number of connected auto APs: 0
Total number of connected common APs: 1
Total number of connected WTUs: 0
Total number of inside APs: 0
Maximum supported APs: 10
Remaining APs: 9
Total AP licenses: 10
Local AP licenses: 10
Server AP licenses: 0
Remaining Local AP licenses: 10
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
office           1      R/B   AP 3620      219801A28N819CE0002T

```

Verify that all Web requests are redirected to the portal authentication page (<http://192.168.0.111:8080/portal>) before you pass portal authentication, and you can access Internet resources after being authenticated.

View online port user information generated on the ACs. This example displays the command output on AC 1.

```

[AC1] display portal user all
Total portal users: 1
Username:client
  AP name: office
  Radio ID: 2
  SSID: service
  Portal server: newpt
  State: Online
  VPN instance: N/A

```


MAC	IP	VLAN	Interface
d4bb-c85b-9d3f	2.2.2.3	200	WLAN-BSS1/0/4

Authorization information:

DHCP IP pool: N/A
 User profile: N/A
 Session group profile: N/A
 ACL number: N/A
 Inbound CAR: N/A

Delete portal users from AC 1. Verify that the client can still access the external network.

Verify that a portal user still exists on AC 1 but the username is the MAC address of the client.

[AC1] display portal user all

Total portal users: 1

Username: D4:BB:C8:5B:9D:3F

AP name: office
 Radio ID: 2
 SSID: service
 Portal server: newpt
 State: Online
 VPN instance: N/A

MAC	IP	VLAN	Interface
d4bb-c85b-9d3f	2.2.2.3	200	WLAN-BSS1/0/4

Authorization information:

DHCP IP pool: N/A
 User profile: N/A
 Session group profile: N/A
 ACL number: N/A
 Inbound CAR: N/A

Configuration files

- AC 1:


```
#
vlan 100
#
vlan 200
#
wlan service-template st1
  ssid service
  vlan 200
client forwarding-location ac
  akm mode psk
  preshared-key pass-phrase cipher $c$3$0Lf6p0Z6bxrf25nodjOJKYEfnZ6g6ErcchYQ
  cipher-suite ccmp
  security-ie rsn
portal enable method direct
portal domain dml
portal bas-ip 2.2.2.1
```

```

portal apply web-server newpt
portal apply mac-trigger-server mts
portal temp-pass period 300 enable
service-template enable
#
interface Vlan-interface100
ip address 2.2.1.1 255.255.255.0
#
interface Vlan-interface200
ip address 2.2.2.1 255.255.255.0
#
interface gigabitethernet 1/0/1
port link-type trunk
port trunk permit vlan 100 200
#
ip route-static 192.168.0.0 16 2.2.2.100
#
radius session-control enable
#
domain dml
authentication portal none
authorization portal none
accounting portal none
#
portal free-rule 0 destination ip 192.168.0.111 255.255.255.255
portal free-rule 1 destination ip 2.2.2.1 255.255.255.255
portal free-rule 2 destination ip any udp 53
portal free-rule 3 destination ip any tcp 53
portal free-rule 4 destination ip 2.2.2.2 255.255.255.255
portal safe-redirect enable
portal safe-redirect method get post
portal safe-redirect user-agent CaptiveNetworkSupport
portal safe-redirect user-agent MicroMessenger
portal safe-redirect user-agent Mozilla
portal safe-redirect user-agent WeChat
portal safe-redirect user-agent iPhone
portal safe-redirect user-agent micromessenger
#
portal web-server newpt
url http://192.168.0.111:8080/INC -
WSMAuth/protocol captive-bypass ios optimize
enable
service-type oauth
#
portal local-web-server http
#
portal mac-trigger-server mts
ip 192.168.0.111
cloud-binding enable

```

```
#
wlan ap-group group1
  priority 7
  wlan tunnel-preempt enable
  backup-ac ip 2.2.1.2
  ap office
  ap-model AP 3620
radio 1
  radio 2
    radio enable
    service-template st1
#
wlan ap office model AP 3620
serial-id 219801A28N819CE0002T
#
```

- **AC 2:**

```
#
vlan 100
#
vlan 200
#
wlan service-template st1
  ssid service
  vlan 200
client forwarding-location ac
  akm mode psk
  preshared-key pass-phrase cipher $c$3$oLf6pOZ6bxrf25nodjOJKYEfnZ6g6ErccHyQ
  cipher-suite ccmp
  security-ie rsn
  portal enable method direct
  portal domain dm1
  portal bas-ip 2.2.2.2
  portal apply web-server newpt
  portal apply mac-trigger-server mts
  portal temp-pass period 300 enable
  service-template enable
#
interface Vlan-interface100
  ip address 2.2.1.2 255.255.255.0
#
interface Vlan-interface200
  ip address 2.2.2.2 255.255.255.0
#
interface gigabitethernet 1/0/1
  port link-type trunk
  port trunk permit vlan 100 200
#
ip route-static 192.168.0.0 16 2.2.2.100
```

```

#
radius session-control enable
#
domain dml
authentication portal none
authorization portal none
accounting portal none
#
portal free-rule 0 destination ip 192.168.0.111 255.255.255.255
portal free-rule 1 destination ip 2.2.2.1 255.255.255.255
portal free-rule 2 destination ip any udp 53
portal free-rule 3 destination ip any tcp 53
portal free-rule 4 destination ip 2.2.2.2 255.255.255.255
portal safe-redirect enable
portal safe-redirect method get post
portal safe-redirect user-agent CaptiveNetworkSupport
portal safe-redirect user-agent MicroMessenger
portal safe-redirect user-agent Mozilla
portal safe-redirect user-agent WeChat
portal safe-redirect user-agent iPhone
portal safe-redirect user-agent micromessenger
#
portal web-server newpt
url http://192.168.0.111:8080/INC -
WSMAuth/protocol captive-bypass ios optimize
enable
service-type oauth
#
portal local-web-server http
#
portal mac-trigger-server mts
ip 192.168.0.111
cloud-binding enable
#
wlan ap-group group1
priority 6
wlan tunnel-preempt enable
backup-ac ip 2.2.1.1
ap office
ap-model AP 3620
radio 1
radio 2
radio enable
service-template st1
#
wlan ap office model AP 3620
serial-id 219801A28N819CE0002T
#

```

- Switch:

```

#
vlan 2
#
vlan 100
#
vlan 200
#
interface Vlan-interface2
 ip address 192.168.0.100 255.255.255.0
#
interface Vlan-interface200
 ip address 2.2.2.100 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 1 100 200
#
interface GigabitEthernet1/0/2
 port link-type trunk
 port trunk permit vlan 1 100 200
#
interface GigabitEthernet1/0/3
 port link-type access
 port access vlan 100
 poe enable
#
interface GigabitEthernet1/0/4
 port link-type trunk
 port trunk permit vlan 1 100 200
#

```

- **DHCP server:**

```

#
vlan 100
#
vlan 200
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 100 200
#
interface vlan-interface 100
 ip address 2.2.1.200 255.255.255.0
#
interface vlan-interface 200
 ip address 2.2.2.200 255.255.255.0
#
dhcp enable
#

```

```
dhcp server ip-pool vlan100
network 2.2.1.0 mask 255.255.255.0
forbidden-ip 2.2.1.1
forbidden-ip 2.2.1.2
#
dhcp server ip-pool vlan200
gateway-list 2.2.2.100
network 2.2.2.0 mask 255.255.255.0
dns-list 8.8.8.8
forbidden-ip 2.2.2.1
forbidden-ip 2.2.2.2
forbidden-ip 2.2.2.100
#
```

Related documentation

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

INTELBRAS Access Controllers

Dual-Link Backup OAuth-Based Portal Authentication in Centralized Forwarding Configuration Examples

Copyright © 2024 Intelbras S.A All rights reserved.

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

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

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

Contents

Introduction	1
Prerequisites	1
Example: Configuring OAuth-based portal authentication for dual-link AC backup and centralized forwarding	1
Network configuration	1
Analysis	2
Restrictions and guidelines	2
Procedures	2
Configuring AC 1	2
Configuring AC 2	5
Configuring the switch	8
Configuring the DHCP server	9
Configuring the INC server	10
Verifying the configuration	15
Configuration files	17
Related documentation	21

Introduction

The following information provides an example for configuring OAuth-based portal authentication in a dual-link backup network enabled with centralized forwarding.

Prerequisites

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

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

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

Example: Configuring OAuth-based portal authentication for dual-link AC backup and centralized forwarding

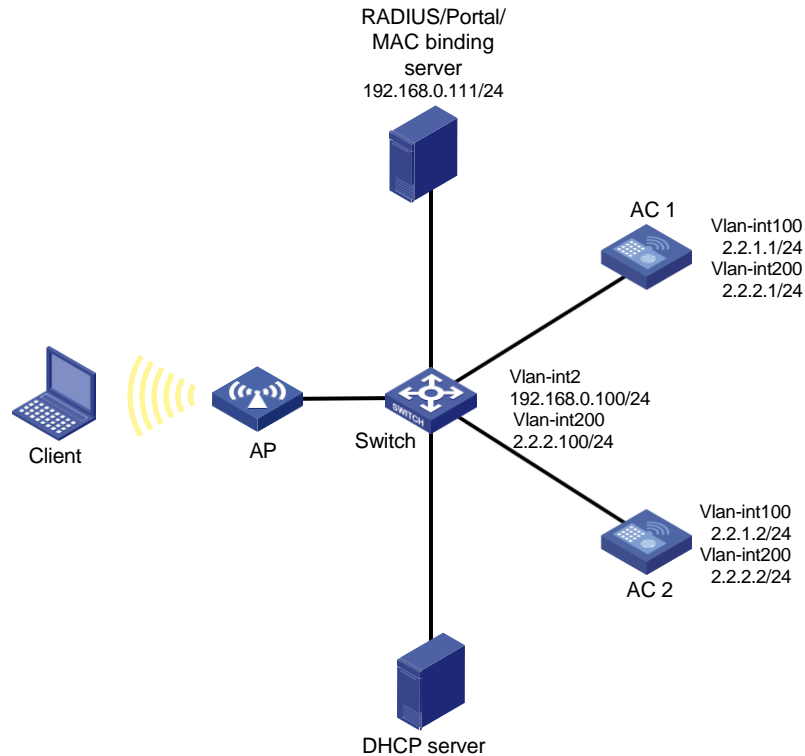
Network configuration

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

Configure the devices to meet the following requirements:

- The AP associates with both ACs and the two ACs to back up each other. When the master AC fails, the backup AC takes over, and the AP can provide services correctly through the backup AC.
- Before passing portal authentication, the client can access only the portal Web server. After passing the authentication, the client can access other network resources.
- The client can access network resources through any Layer 2 ports in its access VLAN without re-authentication.
- The INC server can dynamically modify user authorization information and log off clients.

Figure 1 Network diagram



Analysis

- To allow an authenticated user to access network resources on any Layer 2 ports in its access VLAN without re-authentication, you must enable the portal roaming feature.
- To avoid possible authentication failure caused by frequent logins and logouts of portal clients in a short time, disable the Rule ARP entry feature.
- To allow the RADIUS server to modify user authorization information and log off users, enable the RADIUS session-control feature.
- For dual-link backup to operate correctly, you must configure manual AP or auto AP settings on both ACs. This ensures that the AP can establish CAPWAP tunnels with both ACs.

Restrictions and guidelines

When you configure OAuth-based portal authentication for dual-link AC backup and centralized forwarding, follow these restrictions and guidelines:

- Use the actual serial ID of an AP to uniquely identify that AP.
- If you configure manual APs, make sure the manual APs configured on the two ACs have the same AP name and identifier (serial ID or MAC address).

Procedures

Configuring AC 1

1. Configure VLANs and interfaces:

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

```
<AC1> system-view
[AC1] vlan 100
[AC1-vlan100] quit
[AC1] interface vlan-interface 100
[AC1-Vlan-interface100] ip address 2.2.1.1 24
[AC1-Vlan-interface100] quit
```

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

```
[AC1] vlan 200
[AC1-vlan200] quit
[AC1] interface vlan-interface 200
[AC1-Vlan-interface200] ip address 2.2.2.1 24
[AC1-Vlan-interface200] quit
```

2. Configure a static route to the INC server.

```
[AC1] ip route-static 192.168.0.0 255.255.0.0 2.2.2.100
```

3. Configure DNS server settings. (Details not shown.)

4. Configure wireless services:

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

```
[AC1] wlan service-template st1
```

Specify the SSID as **service**.

```
[AC1-wlan-st-st1] ssid service
```

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

```
[AC1-wlan-st-st1] vlan 200
```

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

```
[AC1-wlan-st-st1] akm mode psk
```

```
[AC1-wlan-st-st1] preshared-key pass-phrase simple 12345678
```

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

```
[AC1-wlan-st-st1] cipher-suite ccmp
```

```
[AC1-wlan-st-st1] security-ie rsn
```

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

```
[AC1-wlan-st-st1] client forwarding-location ac
```

```
[AC1-wlan-st-st1] quit
```

5. Configure the AP:

NOTE:

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

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

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

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

```
[AC1-wlan-ap-office] quit
```

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

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

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

Set the AP connection priority to 7.

```
[AC1-wlan-ap-group-group1] priority 7
# Specify AC 2 as the backup AC for AC 1. Set the backup AC address as the IP address of
VLAN-interface 100 on AC 2.
[AC1-wlan-ap-group-group1] backup-ac ip 2.2.1.2
# Enable master CAPWAP tunnel preemption.
[AC1-wlan-ap-group-group1] wlan tunnel-preempt enable
# Bind service template st1 to radio 2 in AP group group1.
[AC1-wlan-ap-group-group1] ap-model AP 3620
[AC1-wlan-ap-group-group1-ap-model-AP 3620] radio 2
[AC1-wlan-ap-group-group1-ap-model-AP 3620-radio-2] service-template st1
# Enable radio 2.
[AC1-wlan-ap-group-group1-ap-model-AP 3620-radio-2] radio
enable [AC1-wlan-ap-group-group1-ap-model-AP 3620-radio-2] quit
[AC1-wlan-ap-group-group1-ap-model-AP 3620]
quit [AC1-wlan-ap-group-group1] quit
```

6. Configure portal authentication:

Create domain **dm1 and enter its view.**

```
[AC1] domain dm1
```

Configure the authentication, authorization, and accounting methods as none for portal users.

```
[AC1-isp-dm1] authentication portal none
[AC1-isp-dm1] authorization portal none
[AC1-isp-dm1] accounting portal none
[AC1-isp-dm1] quit
```

Create a portal Web server named **newpt, specify the server's URL as **http://192.168.0.111/INC - WSMAuth/protocol**, and specify the server type as OAuth.**

```
[AC1] portal web-server newpt
[AC1-portal-websvr-newpt] url http://192.168.0.111:8080/INC -
WSMAuth/protocol [AC1-portal-websvr-newpt] server-type oauth
```

Enable the optimized captive-bypass feature for iOS users.

```
[AC1-portal-websvr-newpt] captive-bypass ios optimize enable
[AC1-portal-websvr-newpt] quit
```

Create an HTTP-based local portal Web service and enter its view.

```
[AC1] portal local-web-server http
[AC1-portal-local-websvr-http] quit
```

Configure destination-based portal-free rule to permit traffic to the DNS server.

```
[AC1] portal free-rule 2 destination ip any udp 53
[AC1] portal free-rule 3 destination ip any tcp 53
```

Configure portal safe-redirect to reduce the workload of the authentication server.

```
[AC1] portal safe-redirect enable
[AC1] portal safe-redirect method get post
[AC1] portal safe-redirect user-agent CaptiveNetworkSupport
[AC1] portal safe-redirect user-agent MicroMessenger
[AC1] portal safe-redirect user-agent Mozilla
[AC1] portal safe-redirect user-agent WeChat
[AC1] portal safe-redirect user-agent iPhone
[AC1] portal safe-redirect user-agent micromessenger
```

Specify the NAS-ID. Make sure the NAS-ID is the same as the ID in file **INC\client\conf\portal\conf.properties.**

```

[AC1] wlan global-configuration
[AC1-wlan-global-configuration] nas-id wiportal
[AC1-wlan-global-configuration] quit
# Set the user synchronization interval to 60 seconds for portal authentication using OAuth.
[AC1] portal oauth user-sync interval 60
# Configure a destination-based portal-free rule: specify the rule number as 0 and IP address as
192.168.0.111. This rule allows users to reach the portal Web server.
[AC1] portal free-rule 0 destination ip 192.168.0.111 32
# Configure a destination-based portal-free rule: specify the rule number as 1 and IP address as
2.2.2.1. This rule allows users to reach AC 1.
[AC1] portal free-rule 1 destination ip 2.2.2.1 32
# Configure a destination-based portal-free rule: specify the rule number as 4 and IP address as
2.2.2.2. This rule allows users to reach AC 2.
[AC1] portal free-rule 4 destination ip 2.2.2.2 32
# Enable intra-VLAN roaming for portal users.
[AC1] portal roaming enable
# Disable the Rule ARP entry feature for portal clients.
[AC1] undo portal refresh arp enable
# Enable RADIUS session control.
[AC1] radius session-control enable
# Enable direct IPv4 portal authentication for service template st1.
[AC1] wlan service-template st1
[AC1-wlan-st-st1] portal enable method direct
# Configure the authentication domain for IPv4 portal users as dm1 on service template st1.
[AC1-wlan-st-st1] portal domain dml
# Apply portal Web server newpt to service template st1.
[AC1-wlan-st-st1] portal apply web-server newpt
# Enable portal temporary pass and set the temporary pass period to 300 seconds.
[AC1-wlan-st-st1] portal temp-pass period 300 enable
# On the service template, configure the BAS-IP attribute as 2.2.2.1 for portal packets sent to
the portal authentication server.
[AC1-wlan-st-st1] portal bas-ip 2.2.2.1
# Enable the service template.
[AC1-wlan-st-st1] service-template enable
[AC1-wlan-st-st1] quit

```

Configuring AC 2

1. Configure VLANs and interfaces:

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

```

<AC2> system-view
[AC2] vlan 100
[AC2-vlan100] quit
[AC2] interface vlan-interface 100
[AC2-Vlan-interface100] ip address 2.2.1.2 24
[AC2-Vlan-interface100] quit

```

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

```
[AC2] vlan 200
[AC2-vlan200] quit
[AC2] interface vlan-interface 200
[AC2-Vlan-interface200] ip address 2.2.2.2 24
[AC2-Vlan-interface200] quit
```

2. Configure a static route to the INC server.

```
[AC2] ip route-static 192.168.0.0 255.255.0.0 2.2.2.100
```

3. Configure DNS server settings. (Details not shown.)

4. Configure wireless services:

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

```
[AC2] wlan service-template st1
```

Specify the SSID as **service**.

```
[AC2-wlan-st-st1] ssid service
```

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

```
[AC2-wlan-st-st1] vlan 200
```

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

```
[AC2-wlan-st-st1] akm mode psk
```

```
[AC2-wlan-st-st1] preshared-key pass-phrase simple 12345678
```

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

```
[AC2-wlan-st-st1] cipher-suite ccmp
```

```
[AC2-wlan-st-st1] security-ie rsn
```

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

```
[AC2-wlan-st-st1] client forwarding-location ac
```

```
[AC2-wlan-st-st1] quit
```

5. Configure the AP:

NOTE:

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

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

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

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

```
[AC2-wlan-ap-office] quit
```

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

```
[AC2] wlan ap-group group1
```

```
[AC2-wlan-ap-group-group1] ap office
```

Set the AP connection priority to 6.

```
[AC2-wlan-ap-group-group1] priority 6
```

Specify AC 1 as the backup AC for AC 2. Set the backup AC address as the IP address of VLAN-interface 100 on AC 1.

```
[AC2-wlan-ap-group-group1] backup-ac ip 2.2.1.1
```

Enable master CAPWAP tunnel preemption.

```
[AC2-wlan-ap-group-group1] wlan tunnel-preempt enable
```

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

```
[AC2-wlan-ap-group-group1] ap-model AP 3620
```

```
[AC2-wlan-ap-group-group1-ap-model-AP 3620] radio 2
[AC2-wlan-ap-group-group1-ap-model-AP 3620-radio-2] service-template st1
```

Enable radio 2.

```
[AC2-wlan-ap-group-group1-ap-model-AP 3620-radio-2] radio
enable [AC2-wlan-ap-group-group1-ap-model-AP 3620-radio-2] quit
[AC2-wlan-ap-group-group1-ap-model-AP 3620]
quit [AC2-wlan-ap-group-group1] quit
```

6. Configure portal authentication:

Create domain **dm1** and enter its view.

```
[AC2] domain dm1
```

Configure the authentication, authorization, and accounting methods as none for portal users.

```
[AC2-isp-dm1] authentication portal none
[AC2-isp-dm1] authorization portal none
[AC2-isp-dm1] accounting portal none
[AC2-isp-dm1] quit
```

Create a portal Web server named **newpt**, specify the server's URL as **http://192.168.0.111/INC - WSMAuth/protocol**, and specify the server type as OAuth. (The URL is for illustration only.)

```
[AC2] portal web-server newpt
[AC2-portal-websvr-newpt] url http://192.168.0.111:8080/INC -
WSMAuth/protocol [AC2-portal-websvr-newpt] server-type oauth =
```

Enable the optimized captive-bypass feature for iOS users.

```
[AC2-portal-websvr-newpt] captive-bypass ios optimize enable
[AC2-portal-websvr-newpt] quit
```

Create an HTTP-based local portal Web service and enter its view.

```
[AC2] portal local-web-server http
[AC2-portal-local-websvr-http] quit
```

Configure destination-based portal-free rule to permit traffic to the DNS server.

```
[AC2] portal free-rule 2 destination ip any udp 53
[AC2] portal free-rule 3 destination ip any tcp 53
```

Configure portal safe-redirect to reduce the workload of the authentication server.

```
[AC2] portal safe-redirect enable
[AC2] portal safe-redirect method get post
[AC2] portal safe-redirect user-agent CaptiveNetworkSupport
[AC2] portal safe-redirect user-agent MicroMessenger
[AC2] portal safe-redirect user-agent Mozilla
[AC2] portal safe-redirect user-agent WeChat
[AC2] portal safe-redirect user-agent iPhone
[AC2] portal safe-redirect user-agent micromessenger
```

Specify the NAS-ID. Make sure the NAS-ID is the same as the ID in file **INC\client\conf\wportal\conf.properties**.

```
[AC2] wlan global-configuration
[AC2-wlan-global-configuration] nas-id wportal
[AC2-wlan-global-configuration] quit
```

Set the user synchronization interval to 60 seconds for portal authentication using OAuth.

```
[AC2] portal oauth user-sync interval 60
```

Configure a destination-based portal-free rule: specify the rule number as **0** and IP address as **192.168.0.111**. This rule allows users to reach the portal Web server.

```

[AC2] portal free-rule 0 destination ip 192.168.0.111 32
# Configure a destination-based portal-free rule: specify the rule number as 1 and IP address as
2.2.2.1. This rule allows users to reach AC 1.
[AC2] portal free-rule 1 destination ip 2.2.2.1 32
# Configure a destination-based portal-free rule: specify the rule number as 4 and IP address as
2.2.2.2. This rule allows users to reach AC 2.
[AC2] portal free-rule 4 destination ip 2.2.2.2 32
# Enable intra-VLAN roaming for portal users.
[AC2] portal roaming enable
# Disable the Rule ARP entry feature for portal clients.
[AC2] undo portal refresh arp enable
# Enable validity check on wireless portal clients.
[AC2] radius session-control enable
# Enable direct IPv4 portal authentication for service template st1.
[AC2] wlan service-template st1
[AC2-wlan-st-st1] portal enable method direct
# Configure the authentication domain for IPv4 portal users as dm1 on service template st1.
[AC2-wlan-st-st1] portal domain dm1
# Apply portal Web server newpt to service template st1.
[AC2-wlan-st-st1] portal apply web-server newpt
# Enable portal temporary pass and set the temporary pass period to 300 seconds.
[AC2-wlan-st-st1] portal temp-pass period 300 enable
# On the service template, configure the BAS-IP attribute as 2.2.2.2 for portal packets sent to
the portal authentication server.
[AC2-wlan-st-st1] portal bas-ip 2.2.2.2
# Enable the service template.
[AC2-wlan-st-st1] service-template enable
[AC2-wlan-st-st1] quit

```

Configuring the switch

```

# Create VLAN 100 for forwarding CAPWAP tunnel traffic between AC and AP.
<Switch> system-view
[Switch] vlan 100
[Switch-vlan100] quit
# Create VLAN 200 for forwarding client traffic.
[Switch] vlan 200
[Switch-vlan200] quit
# Create VLAN 2 for forwarding client traffic.
[Switch] vlan 2
[Switch-vlan2] quit
# Add the interface that connects the switch to the INC server to VLAN 2. (Details not shown.)
# Configure GigabitEthernet 1/0/1 that connects the switch to AC 1 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 1/0/2 that connects the switch to the AP as an access port, and assign the interface to VLAN 100.

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

Enable PoE on GigabitEthernet 1/0/2.

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

Configure GigabitEthernet 1/0/3 that connects the switch to the AC 2 as a trunk port, and assign the interface to VLAN 100 and VLAN 200.

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

Configure GigabitEthernet 1/0/4 that connects the switch to the DHCP server as a trunk port, and assign it to VLAN 100 and VLAN 200.

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

Assign an IP address to VLAN-interface 200.

```
[Switch] interface vlan-interface 200
[Switch-Vlan-interface200] ip address 2.2.2.100 255.255.255.0
[Switch-Vlan-interface200] quit
```

Assign an IP address to VLAN-interface 2.

```
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] ip address 192.168.0.100 255.255.255.0
[Switch-Vlan-interface2] quit
```

Configuring the DHCP server

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

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

Assign an IP address to VLAN-interface 100.

```
[DHCP] interface vlan-interface 100
[DHCP-Vlan-interface100] ip address 2.2.1.200 255.255.255.0
[DHCP-Vlan-interface100] quit
```

Assign an IP address to VLAN-interface 200.

```
[DHCP] interface vlan-interface 200
[DHCP-Vlan-interface200] ip address 2.2.2.200 255.255.255.0
[DHCP-Vlan-interface200] quit
```

Enable DHCP.

```
[DHCP] dhcp enable
```

Create a DHCP address pool named **VLAN100**, specify the DHCP server as the gateway, and exclude AC and DHCP server addresses from dynamic allocation. The server will use this address pool to assign address to the AP.

```
[DHCP] dhcp server ip-pool VLAN100
[DHCP-dhcp-pool-vlan100] gateway-list 2.2.1.200
[DHCP-dhcp-pool-vlan100] network 2.2.1.0 mask 255.255.255.0
[DHCP-dhcp-pool-vlan100] forbidden-ip 2.2.1.1 2.2.1.2
[DHCP-dhcp-pool-vlan100] quit
```

Create a DHCP address pool named **VLAN200**, specify the switch as the gateway, specify the DNS server address as 8.8.8.8, and exclude AC and DHCP server addresses from dynamic allocation. The server will use this address pool to assign address to the client.

```
[DHCP] dhcp server ip-pool VLAN200
[DHCP-dhcp-pool-vlan200] gateway-list 2.2.2.100
[DHCP-dhcp-pool-vlan200] network 2.2.2.0 mask 255.255.255.0
[DHCP-dhcp-pool-vlan200] dns-list 8.8.8.8
[DHCP-dhcp-pool-vlan200] forbidden-ip 2.2.2.100 2.2.2.1 2.2.2.2
[DHCP-dhcp-pool-vlan200] quit
```

Configuring the INC server

In this example, the INC server runs INC PLAT 7.3 (E0605) and INC IPM 7.3 (E0516).

To configure the INC server:

1. Add an access user:
 - a. Log in to INC and click the **Service** tab.
 - b. From the navigation tree, select **Intelligent Portal Management > User Management > Users**.
 - c. Click **Add** to open the **Add User** page.
 - d. Enter username **Client** and password **admin@123**.
 - e. Use the default settings for other parameters.
 - f. Click **OK**.

Figure 2 Adding an access user

Add User

Username * client ?

User Group Ungrouped

User Password * ***** ?

Confirm Password * *****

Identity Number

Telephone Number

Set Online User Count By User Group

Start Time

End Time

Remark

OK Cancel

2. Add an authentication page template:
 - a. From the navigation tree, select **Intelligent Portal Management > Page Template List**.
 - b. Click **Add** to open the **Add Theme** page.
 - c. Enter template name **theme** in the **Theme Name** field.
 - d. Use the default settings for other parameters.
 - e. Click **OK** to open the page for editing the template.

Figure 3 Adding an authentication page template

Add Theme

Theme Name * theme ?

Custom Page: ☐ First ☒ Authentication ☒ Home ☐ Transparent Authentication

Type * Phone

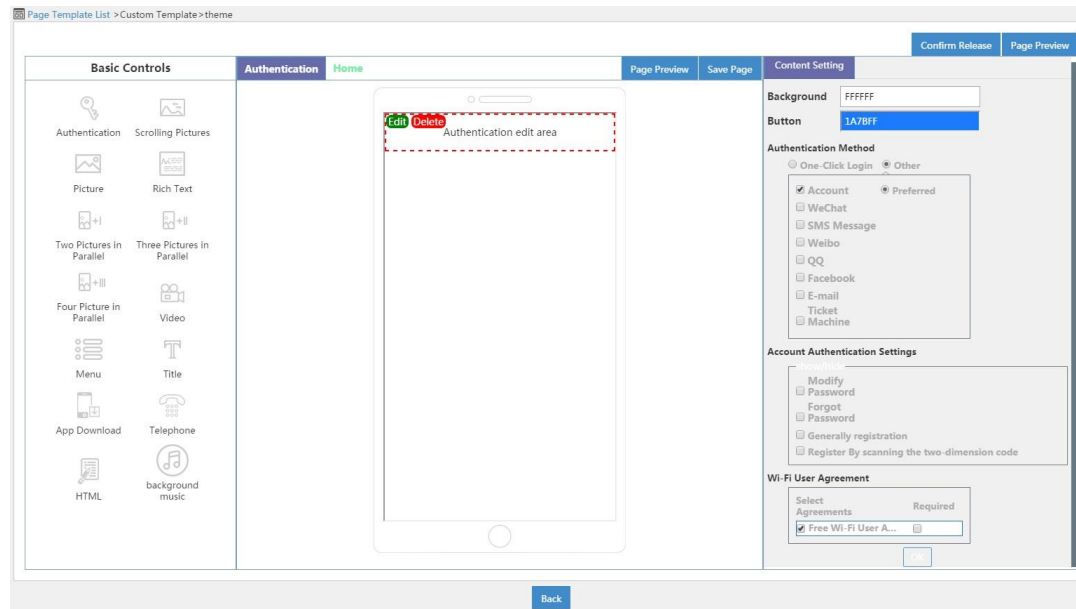
Description

OK Cancel

- f. On the **theme** page, click the **Authentication** icon  in the **Basic Controls** area.

- g. Click **Edit** in authentication edit area, select **Other** and **Account** in the **Authentication Method** area, click **OK**, and then click **Save Page**.
- h. Use the default settings for other configuration.
- i. Click **Confirm Release**.

Figure 4 Editing the template



3. Add an authentication policy:
 - a. From the navigation tree, select **Intelligent Portal Management > Authentication Policies**.
 - b. Click **Add** to open the **Add Authentication Policy** page.
 - c. Enter authentication policy name **policy1**, and select **theme** from the **Page Template** list.
 - d. Use the default settings for other parameters.
 - e. Click **OK**.

Figure 5 Adding an authentication policy

The screenshot shows the 'Add Authentication Policy' form within the 'Intelligent Portal Management' application. The breadcrumb navigation at the top reads 'Intelligent Portal Management > Add Authentication Policy'. The form title is 'Add Authentication Policy'. The form contains the following fields and controls:

- Name ***: A text input field containing 'policy1'.
- Description**: An empty text input field.
- Page Template ***: A dropdown menu with 'theme' selected.
- Authentication Free**: A checkbox with a help icon (?).
- Only Mobile Endpoints**: A checkbox with a help icon (?).
- Transparent Authentication Period ***: A dropdown menu with 'Today' selected.
- Match SSID for Transparent Authentication**: An unchecked checkbox.
- Idle Time Before Network Cut (Minutes) ***: A text input field containing '30' with a help icon (?).
- Idle Traffic Before Network Cut (Bytes) ***: A text input field containing '10240' with a help icon (?).
- Max. Online Duration Per Access (Seconds) ***: A text input field containing '0' with a help icon (?).
- Maximum Online Duration Per Day (Seconds) ***: A text input field containing '0' with a help icon (?).
- Maximum Traffic Per Day (MB) ***: A text input field containing '0' with a help icon (?).

At the bottom right of the form, there are two buttons: 'OK' and 'Cancel'.

4. Add a site:
 - a. From the navigation tree, select **Intelligent Portal Management > Site Management**.
 - b. Click **Add** to open the **Add Site** page.
 - c. Enter the site name, the site address, the expected number of clients to be supported, and the telephone number.
 - d. Click **OK**.

Figure 6 Adding a site

Intelligent Portal Management > Site Management > Add Site

Site Basic Information

Site Name * userspot

Site Address * useraddress ?

Expected Supported Number * 2

Telephone * 81819999

Site Introduction

Site Group * Ungrouped ▼

User Group * Ungrouped ▼

- e. In the **Associated APs** area, click **Add** to associate an AP.
- f. Enter the serial number and MAC address of the AP.
- g. Click **OK**.

Figure 7 Adding an AP

Add

AP Serial Number * 219801A0CNC138011454

AP IP Address

AP MAC Address * 70F9-6DD7-D900

OK Cancel

- i. In the **Bind Authentication Policy** area, click **Add** to bind the AP to an authentication policy.
- j. Select authentication policy **policy1**.
- k. Use the default settings for other parameters.
- l. Click **OK**.

Figure 8 Binding the AP to an authentication policy

Bind to Authentication Policies

Authentication Policy policy1

SSID

Start Time

End Time

OK Cancel

Verifying the configuration

Make the AP come online.

Verify that the AP state is R/M on AC 1 and R/B on AC 2.

```
<AC1> display wlan ap all
Total number of APs: 1
Total number of connected APs: 1
Total number of connected manual APs: 1
Total number of connected auto APs: 0
Total number of connected common APs: 1
Total number of connected WTUs: 0
Total number of inside APs: 0
Maximum supported APs: 10
Remaining APs: 9
```

```

Total AP licenses: 10
Local AP licenses: 10
Server AP licenses: 0
Remaining Local AP licenses: 9
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
office       1      R/M   AP 3620    219801A28N819CE0002T

```

```
<AC2> display wlan ap all
```

```

Total number of APs: 1
Total number of connected APs: 1
Total number of connected manual APs: 1
Total number of connected auto APs: 0
Total number of connected common APs: 1
Total number of connected WTUs: 0
Total number of inside APs: 0
Maximum supported APs: 10
Remaining APs: 9
Total AP licenses: 10
Local AP licenses: 10
Server AP licenses: 0
Remaining Local AP licenses: 10
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
office       1      R/B   AP 3620    219801A28N819CE0002T

```

Verify that all Web requests are redirected to the portal authentication page (<http://192.168.0.111:8080/portal>) before you pass portal authentication, and you can access Internet resources after being authenticated.

View online port user information generated on the ACs. This example displays the command output on AC 1.

```
[AC1] display portal user all
```

```

Total portal users: 1
Username: Client
  AP name: office
  Radio ID: 2
  SSID: service
  Portal server: newpt
  State: Online
  VPN instance: N/A

```


MAC	IP	VLAN	Interface
0021-6330-0933	2.2.2.3	200	WLAN-BSS1/0/4

Authorization information:

DHCP IP pool: N/A
 User profile: N/A
 Session group profile: N/A
 ACL number: N/A
 Inbound CAR: N/A
 Outbound CAR: N/A

Configuration files

- AC 1:

```
#
vlan 100
#
vlan 200
#
wlan service-template st1
  ssid service
  vlan 200
client forwarding-location ac
  akm mode psk
  preshared-key pass-phrase cipher $c$3$0Lf6pOZ6bxrf25nodjOJKYEfnZ6g6ErccHyQ
  cipher-suite ccmp
  security-ie rsn
  portal enable method direct
  portal domain dm1
  portal bas-ip 2.2.2.1
  portal apply web-server newpt
  portal temp-pass period 300 enable
  service-template enable
#
interface Vlan-interface100
  ip address 2.2.1.1 255.255.255.0
#
interface Vlan-interface200
  ip address 2.2.2.1 255.255.255.0
#
interface gigabitethernet 1/0/1
  port link-type trunk
  port trunk permit vlan 100 200
#
ip route-static 192.168.0.0 16 2.2.2.100
#
radius session-control enable
#
```

```

domain dm1
  authentication portal none
  authorization portal none
  accounting portal none
#
portal free-rule 0 destination ip 192.168.0.111 255.255.255.255
portal free-rule 1 destination ip 2.2.2.1 255.255.255.255
portal free-rule 2 destination ip any udp 53
portal free-rule 3 destination ip any tcp 53
portal free-rule 4 destination ip 2.2.2.2 255.255.255.255
portal safe-redirect enable
portal safe-redirect method get post
portal safe-redirect user-agent CaptiveNetworkSupport
portal safe-redirect user-agent MicroMessenger
portal safe-redirect user-agent Mozilla
portal safe-redirect user-agent WeChat
portal safe-redirect user-agent iPhone
portal safe-redirect user-agent micromessenger
#
portal web-server newpt
  url http://192.168.0.111:8080/INC -
  WSMAuth/protocol captive-bypass ios optimize
  enable
  service-type oauth
#
portal local-web-server http
#
wlan ap-group group1
  priority 7
  wlan tunnel-preempt enable
  backup-ac ip 2.2.1.2
  ap office
  ap-model AP 3620
radio 1
  radio 2
  radio enable
  service-template st1
#
wlan ap office model AP 3620
serial-id 219801A28N819CE0002T
#

```

- **AC 2:**

```

#
vlan 100
#
vlan 200
#
wlan service-template st1
  ssid service

```

```

vlan 200
client forwarding-location ac
akm mode psk
preshared-key pass-phrase cipher $c$3$0Lf6pOZ6bxrf25nodjOJKYEfnZ6g6ErccHyQ
cipher-suite ccmp
security-ie rsn
portal enable method direct
portal domain dml
portal bas-ip 2.2.2.2
portal apply web-server newpt
portal temp-pass period 300 enable
service-template enable
#
interface Vlan-interface100
ip address 2.2.1.2 255.255.255.0
#
interface Vlan-interface200
ip address 2.2.2.2 255.255.255.0
#
ip route-static 192.168.0.0 16 2.2.2.100
#
radius session-control enable
#
domain dml
authentication portal none
authorization portal none
accounting portal none
#
portal free-rule 0 destination ip 192.168.0.111 255.255.255.255
portal free-rule 1 destination ip 2.2.2.1 255.255.255.255
portal free-rule 2 destination ip any udp 53
portal free-rule 3 destination ip any tcp 53
portal free-rule 4 destination ip 2.2.2.2 255.255.255.255
portal safe-redirect enable
portal safe-redirect method get post
portal safe-redirect user-agent CaptiveNetworkSupport
portal safe-redirect user-agent MicroMessenger
portal safe-redirect user-agent Mozilla
portal safe-redirect user-agent WeChat
portal safe-redirect user-agent iPhone
portal safe-redirect user-agent micromessenger
#
portal web-server newpt
url http://192.168.0.111:8080/INC -
WSMAuth/protocol captive-bypass ios optimize
enable
service-type oauth
#
portal local-web-server http

```

```
#
wlan ap-group group1
  priority 6
  wlan tunnel-preempt enable
  backup-ac ip 2.2.1.1
  ap office
  ap-model AP 3620
radio 1
  radio 2
    radio enable
    service-template st1
#
wlan ap office model AP 3620
serial-id 219801A28N819CE0002T
#
```

- **Switch:**

```
#
vlan 2
#
vlan 100
#
vlan 200
#
interface Vlan-interface2
  ip address 192.168.0.100 255.255.255.0
#
interface Vlan-interface200
  ip address 2.2.2.100 255.255.255.0
#
interface GigabitEthernet1/0/1
  port link-type trunk
  port trunk permit vlan 1 100 200
#
interface GigabitEthernet1/0/2
  port link-type access
  port access vlan 100
  poe enable
#
interface GigabitEthernet1/0/3
  port link-type trunk
  port trunk permit vlan 100 200
#
interface GigabitEthernet1/0/4
  port link-type trunk
  port trunk permit vlan 100 200
#
```

- **DHCP server:**

```
#
```

```

interface GigabitEthernet1/0/1
  port link-type trunk
  port trunk permit vlan 100 200
#
interface vlan-interface 100
  ip address 2.2.2.200 255.255.255.0
#
interface vlan-interface 200
  ip address 2.2.2.200 255.255.255.0
#
dhcp enable
#
dhcp server ip-pool vlan100
  network 2.2.1.0 mask 255.255.255.0
  forbidden-ip 2.2.1.1
  forbidden-ip 2.2.1.2
#
dhcp server ip-pool vlan200
  gateway-list 2.2.2.100
  network 2.2.2.0 mask 255.255.255.0
  dns-list 8.8.8.8
  forbidden-ip 2.2.2.1
  forbidden-ip 2.2.2.2
  forbidden-ip 2.2.2.100
#

```

Related documentation

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

INTELBRAS Access Controllers

Dual-Link Backup Remote Portal

MAC-Trigger Authentication in Centralized

Forwarding Configuration Examples

Copyright © 2024 Intelbras S.A All rights reserved.

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

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

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

Contents

Introduction	1
Prerequisites	1
Example: Configuring remote portal MAC-trigger authentication for dual-link AC backup and centralized forwarding	1
Network configuration	1
Analysis	2
Restrictions and guidelines	2
Procedures	3
Configuring AC 1	3
Configuring AC 2	6
Configuring the switch	10
Configuring the INC server	11
Verifying the configuration	16
Configuration files	18
Related documentation	23

Introduction

The following information provides an example for configuring remote portal MAC-trigger authentication with centralized forwarding.

Prerequisites

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

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

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

Example: Configuring remote portal MAC-trigger authentication for dual-link AC backup and centralized forwarding

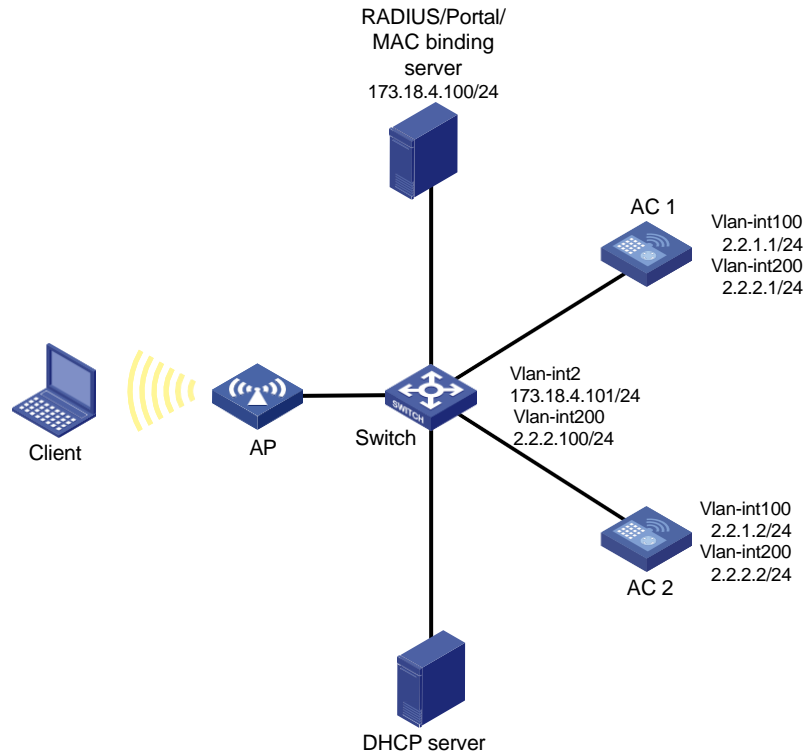
Network configuration

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

Configure the devices to meet the following requirements:

- The AP associates with both ACs and the two ACs to back up each other. When the master AC (AC 1) fails, the backup AC (AC 2) takes over, and the AP can provide services correctly through the backup AC.
- Before passing portal authentication, the client can access only the portal Web server. After passing the authentication, the client can access other network resources.
- The client can access network resources through any Layer 2 ports in its access VLAN without re-authentication.
- The INC server can dynamically modify user authorization information and log off clients.

Figure 1 Network diagram



Analysis

- To allow an authenticated user to access network resources on any Layer 2 ports in its access VLAN without re-authentication, you must enable the portal roaming feature.
- To allow the RADIUS server to modify user authorization information and log off users, enable the RADIUS session-control feature.
- To avoid allocation failures of dynamic authorization information during client association, configure RADIUS DAE.
- For dual-link backup to operate correctly, you must configure manual AP or auto AP settings on both ACs. This ensures that the AP can establish CAPWAP tunnels with both ACs.

Restrictions and guidelines

When you configure remote portal MAC-trigger authentication for dual-link AC backup and centralized forwarding, follow these restrictions and guidelines:

- Use the actual serial ID of an AP to uniquely identify that AP.
- Make sure the portal authentication server type, portal Web server type, and MAC binding server type configured on the ACs are the same as the actual server type.
- URLs redirected from the ACs to the portal Web server do not carry parameters by default. You can configure the parameters to carry as needed.
- To avoid possible authentication failure caused by frequent logins and logouts of portal clients in a short time, disable the Rule ARP entry feature.
- If you configure manual APs, make sure the manual APs configured on the two ACs have the same AP name and identifier (serial ID or MAC address).

- Make sure the two ACs are of the same version.
- Some clients are enabled with MAC randomization by default, which might cause seamless roaming failures. As a best practice, disable MAC randomization.

Procedures

Configuring AC 1

1. Configure AC interfaces:

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

```
<AC1> system-view
[AC1] vlan 100
[AC1-vlan100] quit
[AC1] interface vlan-interface 100
[AC1-Vlan-interface100] ip address 2.2.1.1 24
[AC1-Vlan-interface100] quit
```

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

```
[AC1] vlan 200
[AC1-vlan200] quit
[AC1] interface vlan-interface 200
[AC1-Vlan-interface200] ip address 2.2.2.1 24
[AC1-Vlan-interface200] quit
```

Configure GigabitEthernet1/0/1 that connects AC 1 to the switch as a trunk port, and assign it to VLAN 100 and VLAN 200.

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

2. Create a static route to the INC server.

```
[AC1] ip route-static 173.18.4.0 255.255.255.0 2.2.2.100
```

3. Configure wireless services:

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

```
[AC1] wlan service-template st1
```

Specify the SSID as **service**.

```
[AC1-wlan-st-st1] ssid service
```

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

```
[AC1-wlan-st-st1] vlan 200
```

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

```
[AC1-wlan-st-st1] akm mode psk
```

```
[AC1-wlan-st-st1] preshared-key pass-phrase simple 12345678
```

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

```
[AC1-wlan-st-st1] cipher-suite ccmp
```

```
[AC1-wlan-st-st1] security-ie rsn
```

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

```
[AC1-wlan-st-st1] client forwarding-location ac
```

```
[AC1-wlan-st-st1] quit
```

4. Configure the AP:

NOTE:

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

Create AP *office*, and specify the AP name and serial ID.

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

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

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

Set the AP connection priority to 7.

```
[AC1-wlan-ap-group-group1] priority 7
```

Specify AC 2 as the backup AC for AC 1. Set the backup AC address as the IP address of VLAN-interface 100 on AC 2.

```
[AC1-wlan-ap-group-group1] backup-ac ip 2.2.1.2
```

Enable master CAPWAP tunnel preemption.

```
[AC1-wlan-ap-group-group1] wlan tunnel-preempt enable
```

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

```
[AC1-wlan-ap-group-group1] ap-model AP 3620
[AC1-wlan-ap-group-group1-ap-model-AP 3620] radio 2
[AC1-wlan-ap-group-group1-ap-model-AP 3620-radio-2] service-template st1
```

Enable radio 2.

```
[AC1-wlan-ap-group-group1-ap-model-AP 3620-radio-2] radio
enable [AC1-wlan-ap-group-group1-ap-model-AP 3620-radio-2] quit
[AC1-wlan-ap-group-group1-ap-model-AP 3620]
quit [AC1-wlan-ap-group-group1] quit
```

5. Configure a RADIUS scheme:

Create RADIUS scheme *rs1*.

```
[AC1] radius scheme rs1
```

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

```
[AC1-radius-rs1] primary authentication 173.18.4.100
[AC1-radius-rs1] primary accounting 173.18.4.100
```

Specify shared keys for RADIUS authentication and accounting.

```
[AC1-radius-rs1] key authentication simple radius
[AC1-radius-rs1] key accounting simple radius
```

Configure AC 1 to remove the ISP domain name from the usernames sent to the RADIUS servers.

```
[AC1-radius-rs1] user-name-format without-domain
[AC1-radius-rs1] nas-ip 2.2.2.1
[AC1-radius-rs1] quit
```

Enable RADIUS session-control.

```
[AC1] radius session-control enable
```

Enable the RADIUS DAS feature and enter RADIUS DAS view.

```
[AC1] radius dynamic-author server
```

Specify the DAC as 173.18.4.100. Set the shared key to **radius** in plaintext form for secure communication between the DAS and DAC.

```
[AC1-radius-da-server] client ip 173.18.4.100 key simple radius
[AC1-radius-da-server] quit
```

6. Configure the authentication domain:

Create domain **dm1** and enter its view.

```
[AC1] domain dm1
```

Configure the domain to use RADIUS scheme **rs1** for authentication, authorization, and accounting.

```
[AC1-isp-dm1] authentication portal radius-scheme rs1
[AC1-isp-dm1] authorization portal radius-scheme rs1
[AC1-isp-dm1] accounting portal radius-scheme rs1
```

Set the client idle timeout to 15 minutes and set the minimum threshold to 1024 bytes for clients in ISP domain **dm1**.

```
[AC1-isp-dm1] authorization-attribute idle-cut 15 1024
[AC1-isp-dm1] quit
```

7. Configure portal authentication:

Create the portal authentication server **newpt**, specify the server IP address as 173.18.4.100, and set the destination UDP port number to **50100** for the AC to send unsolicited portal packets to the portal authentication server.

```
[AC1] portal server newpt
[AC1-portal-server-newpt] ip 173.18.4.100 key simple newpt
[AC1-portal-server-newpt] port 50100
```

Specify the portal authentication server type as CMCC.

```
[AC1-portal-server-newpt] server-type cmcc
[AC1-portal-server-newpt] quit
```

Configure the URL for the portal Web server **newpt** as **http://173.18.4.100:8080/portal**.

```
[AC1] portal web-server newpt
[AC1-portal-websvr-newpt] url http://173.18.4.100:8080/portal
```

Configure URL parameters **ssid**, **wlanuserip**, and **wlanacname**, and **nasip** for the portal Web server. Specify the AP's SSID, the IP address of the client, the AC's name, and NAS IP 2.2.2.1 as the values for the parameters, respectively. (The parameters are required to be carried in the URL of a portal Web server of the CMCC type.)

```
[AC1-portal-websvr-newpt] url-parameter ssid ssid
[AC1-portal-websvr-newpt] url-parameter wlanuserip source-address
[AC1-portal-websvr-newpt] url-parameter wlanacname value AC
[AC1-portal-websvr-newpt] url-parameter nasip value 2.2.2.1
```

Specify the portal Web server type as CMCC.

```
[AC1-portal-websvr-newpt] server-type cmcc
[AC1-portal-websvr-newpt] quit
```

Configure an IPv4-based portal-free rule to permit portal Web server traffic.

```
[AC1] portal free-rule 0 destination ip 173.18.4.100 24
```

Configure an IPv4-based portal-free rule to permit traffic from the aggregate interface.

```
[AC1] portal free-rule 1 source interface Bridge-Aggregation 1
```

Configure IPv4-based portal-free rules to permit DNS server traffic.

```
[AC1] portal free-rule 2 destination ip any udp 53
[AC1] portal free-rule 3 destination ip any tcp 53
```

Enable intra-VLAN roaming for portal users.

```
[AC1] portal roaming enable
```

Disable the Rule ARP entry feature for portal clients.

```
[AC1] undo portal refresh arp enable
```

Enable direct IPv4 portal authentication for service template **st1**.

```
[AC1] wlan service-template st1
```

```
[AC1-wlan-st-st1] portal enable method direct
```

Configure the authentication domain for IPv4 portal users as **dm1** on service template **st1**.

```
[AC1-wlan-st-st1] portal domain dm1
```

Specify portal Web server **newpt** as the backup portal Web server on service template **st1** for portal authentication.

```
[AC1-wlan-st-st1] portal apply web-server newpt
```

```
[AC1-wlan-st-st1] quit
```

8. Configure MAC-based quick portal authentication:

Create the MAC binding server **mts** and enter its view.

```
[AC1] portal mac-trigger-server mts
```

Specify the IP address of the MAC binding server as **173.18.4.100**.

```
[AC1-portal-mac-trigger-server-mts] ip 173.18.4.100
```

Specify the MAC binding server type as CMCC.

```
[AC1-portal-mac-trigger-server-mts] server-type cmcc
```

```
[AC1-portal-mac-trigger-server-mts] quit
```

Specify the MAC binding server **mts** on service template **st1**.

```
[AC1] wlan service-template st1
```

```
[AC1-wlan-st-st1] portal apply mac-trigger-server mts
```

Specify the portal BAS-IP as 2.2.2.1.

```
[AC1-wlan-st-st1] portal bas-ip 2.2.2.1
```

Enable the service template.

```
[AC1-wlan-st-st1] service-template enable
```

```
[AC1-wlan-st-st1] quit
```

Configuring AC 2

1. Configure AC interfaces:

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

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

```
[AC2] vlan 100
```

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

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

```
[AC2-Vlan-interface100] ip address 2.2.1.2 24
```

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

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

```
[AC2] vlan 200
```

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

```
[AC2] interface vlan-interface 200
```

```
[AC2-Vlan-interface200] ip address 2.2.2.2 24
```

```
[AC2-Vlan-interface200] quit
```

Configure GigabitEthernet1/0/1 that connects AC 2 to the switch as a trunk port, and assign it to VLAN 100 and VLAN 200.

```
[AC2] interface gigabitethernet 1/0/1
```

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

2. Create a static route to the INC server.

```
[AC2] ip route-static 173.18.4.0 255.255.255.0 2.2.2.100
```

3. Configure wireless services:

Create service template *st1* and enter its view.

```
[AC2] wlan service-template st1
```

Specify the SSID as *service*.

```
[AC2-wlan-st-st1] ssid service
```

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

```
[AC2-wlan-st-st1] vlan 200
```

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

```
[AC2-wlan-st-st1] akm mode psk
```

```
[AC2-wlan-st-st1] preshared-key pass-phrase simple 12345678
```

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

```
[AC2-wlan-st-st1] cipher-suite ccmp
```

```
[AC2-wlan-st-st1] security-ie rsn
```

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

```
[AC2-wlan-st-st1] client forwarding-location ac
```

```
[AC2-wlan-st-st1] quit
```

4. Configure the AP:

NOTE:

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

Create AP *office*, and specify the AP name and serial ID.

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

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

```
[AC2-wlan-ap-office] quit
```

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

```
[AC2] wlan ap-group group1
```

```
[AC2-wlan-ap-group-group1] ap office
```

Set the AP connection priority to 5.

```
[AC2-wlan-ap-group-group1] priority 5
```

Specify AC 1 as the backup AC for AC 2.

```
[AC2-wlan-ap-group-group1] backup-ac ip 2.2.1.1
```

Enable master CAPWAP tunnel preemption.

```
[AC2-wlan-ap-group-group1] wlan tunnel-preempt enable
```

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

```
[AC2-wlan-ap-group-group1] ap-model AP 3620
```

```
[AC2-wlan-ap-group-group1-ap-model-AP 3620] radio 2
```

```
[AC2-wlan-ap-group-group1-ap-model-AP 3620-radio-2] service-template st1
```

Enable radio 2.

```
[AC2-wlan-ap-group-group1-ap-model-AP 3620-radio-2] radio
```

```
enable [AC2-wlan-ap-group-group1-ap-model-AP 3620-radio-2] quit
```

```
[AC2-wlan-ap-group-group1-ap-model-AP 3620] quit
```

- ```
[AC2-wlan-ap-group-group1] quit
```
5. Configure a RADIUS scheme:
    - # Create RADIUS scheme **rs1**.

```
[AC2] radius scheme rs1
```

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

```
[AC2-radius-rs1] primary authentication 173.18.4.100
[AC2-radius-rs1] primary accounting 173.18.4.100
```

    - # Specify shared keys for RADIUS authentication and accounting.

```
[AC2-radius-rs1] key authentication simple radius
[AC2-radius-rs1] key accounting simple radius
```

    - # Configure AC 2 to remove the ISP domain name from the usernames sent to the RADIUS servers.

```
[AC2-radius-rs1] user-name-format without-domain
[AC2-radius-rs1] nas-ip 2.2.2.2
[AC2-radius-rs1] quit
```

    - # Enable RADIUS session-control.

```
[AC2] radius session-control enable
```

    - # Enable the RADIUS DAS feature and enter RADIUS DAS view.

```
[AC2] radius dynamic-author server
```

    - # Specify the DAC as 173.18.4.100. Set the shared key to **radius** in plaintext form for secure communication between the DAS and DAC.

```
[AC2-radius-da-server] client ip 173.18.4.100 key simple radius
[AC2-radius-da-server] quit
```
  6. Configure the authentication domain:
    - # Create domain **dm1** and enter its view.

```
[AC2] domain dm1
```

    - # Configure the domain to use RADIUS scheme **rs1** for authentication, authorization, and accounting.

```
[AC2-isp-dm1] authentication portal radius-scheme rs1
[AC2-isp-dm1] authorization portal radius-scheme rs1
[AC2-isp-dm1] accounting portal radius-scheme rs1
```

    - # Set the client idle timeout to 15 minutes and set the minimum threshold to 1024 bytes for clients in ISP domain **dm1**.

```
[AC2-isp-dm1] authorization-attribute idle-cut 15 1024
[AC2-isp-dm1] quit
```
  7. Configure portal authentication:
    - # Create the portal authentication server **newpt**, specify the server IP address as 173.18.4.100, and set the destination UDP port number to **50100** for the AC to send unsolicited portal packets to the portal authentication server.

```
[AC2] portal server newpt
[AC2-portal-server-newpt] ip 173.18.4.100 key simple newpt
[AC2-portal-server-newpt] port 50100
```

    - # Specify the portal authentication server type as CMCC.

```
[AC2-portal-server-newpt] server-type cmcc
[AC2-portal-server-newpt] quit
```

    - # Configure the URL for the portal Web server **newpt** as **http://173.18.4.100:8080/portal**.

```
[AC2] portal web-server newpt
[AC2-portal-websvr-newpt] url http://173.18.4.100:8080/portal
```

# Configure URL parameters **ssid**, **wlanuserip**, **wlanacname**, and **nasip** for the portal Web server. Specify the AP's SSID, the IP address of the client, the AC's name, and NAS IP 2.2.2.2 as the values for the parameters, respectively. (The parameters are required to be carried in the URL of a portal Web server of the CMCC type.)

```
[AC2-portal-websvr-newpt] url-parameter ssid ssid
[AC2-portal-websvr-newpt] url-parameter wlanuserip source-address
[AC2-portal-websvr-newpt] url-parameter wlanacname value AC
[AC2-portal-websvr-newpt] url-parameter nasip value 2.2.2.2
```

# Specify the portal Web server type as CMCC.

```
[AC2-portal-websvr-newpt] server-type cmcc
[AC2-portal-websvr-newpt] quit
```

# Configure an IPv4-based portal-free rule to permit portal Web server traffic.

```
[AC2] portal free-rule 0 destination ip 173.18.4.100 24
```

# Configure an IPv4-based portal-free rule to permit traffic from the aggregate interface.

```
[AC2] portal free-rule 1 source interface Bridge-Aggregation 1
```

# Configure IPv4-based portal-free rules to permit DNS server traffic.

```
[AC2] portal free-rule 2 destination ip any udp 53
[AC2] portal free-rule 3 destination ip any tcp 53
```

# Enable intra-VLAN roaming for portal users.

```
[AC2] portal roaming enable
```

# Disable the Rule ARP entry feature for portal clients.

```
[AC2] undo portal refresh arp enable
```

# Enable direct IPv4 portal authentication for service template **st1**.

```
[AC2] wlan service-template st1
[AC2-wlan-st-st1] portal enable method direct
```

# Configure the authentication domain for IPv4 portal users as **dm1** on service template **st1**.

```
[AC2-wlan-st-st1] portal domain dm1
```

# Specify portal Web server **newpt** as the backup portal Web server on service template **st1** for portal authentication.

```
[AC2-wlan-st-st1] portal apply web-server newpt
[AC2-wlan-st-st1] quit
```

## 8. Configure MAC-based quick portal authentication:

# Create the MAC binding server **mts** and enter its view.

```
[AC2] portal mac-trigger-server mts
```

# Specify the IP address of the MAC binding server as **173.18.4.100**.

```
[AC2-portal-mac-trigger-server-mts] ip 173.18.4.100
```

# Specify the MAC binding server type as CMCC.

```
[AC2-portal-mac-trigger-server-mts] server-type cmcc
[AC2-portal-mac-trigger-server-mts] quit
```

# Specify the MAC binding server **mts** on service template **st1**.

```
[AC2] wlan service-template st1
[AC2-wlan-st-st1] portal apply mac-trigger-server mts
```

# Specify the portal BAS-IP as 2.2.2.2.

```
[AC2-wlan-st-st1] portal bas-ip 2.2.2.2
```

# Enable the service template.

```
[AC2-wlan-st-st1] service-template enable
[AC2-wlan-st-st1] quit
```



# Configuring the switch

**# Create VLAN 100 for forwarding CAPWAP tunnel traffic between AC and AP.**

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

**# Create VLAN 200 for forwarding client traffic.**

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

**# Create VLAN 2 for connecting to the INC server.**

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

**# Add the interface that connects the switch to the INC server to VLAN 2. (Details not shown.)**

**# Configure the interface that connects the switch to the DHCP server. (Details not shown.)**

**# Configure GigabitEthernet 1/0/1 that connects the switch to AC 1 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 1/0/3 that connects the switch to AC 2 as a trunk port, and assign it to VLAN 100 and VLAN 200.**

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

**# Configure GigabitEthernet 1/0/2 that connects the switch 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
```

**# Assign an IP address to VLAN-interface 200.**

```
[Switch] interface vlan-interface 200
[Switch-Vlan-interface200] ip address 2.2.2.100 255.255.255.0
[Switch-Vlan-interface200] quit
```

**# Assign an IP address to VLAN-interface 2. This address will be used as the gateway address for the INC server.**

```
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] ip address 173.18.4.101 255.255.255.0
[Switch-Vlan-interface2] quit
```

# Configuring the INC server

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

The INC server configuration is the same for AC 1 and AC 2, except for the AC IP address. This section configures AC 1 as an example. Refer to AC 1 configuration when you configure AC 2 and remember to change the IP address setting for AC 2.

## Configure the RADIUS server to add access devices

1. Log in to INC and click the **User** tab.
2. From the navigation pane, select **User Access Policy > Access Device Management > Access Device**.
3. Click **Add**.  
The **Add Access Device** page opens.
4. In the **Access Configuration** area, configure the following parameters:
  - o Enter **radius** in the **Shared Key** and **Confirm Shared Key** fields.
  - o Use the default values for other parameters.
5. In the **Device List** area, click **Select** or **Add Manually** to add the AC 1 at 2.2.2.1 as an access device.
6. Click **OK**.

**Figure 2 Adding an access device**

The screenshot shows the 'Add Access Device' page. The breadcrumb navigation at the top is: User > User Access Policy > Access Device Management > Access Device > Add Access Device.

**Access Configuration**

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

**Device List**

Buttons: Select, Add Manually, Clear All

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

Total Items: 1.

Buttons: OK, Cancel

## Configure the portal server

1. Configure portal authentication:
  - a. Click the **User** tab.
  - b. Select **User Access Policy > Portal Service > Server** from the navigation tree to open the portal server configuration page.
  - c. Configure the portal server parameters as needed.  
This example uses the default settings.
  - d. Click **OK**.

**Figure 3 Portal authentication server configuration**

User > User Access Policy > Portal Service > Server

Portal Server

Basic Information

Log Level \* Info

Portal Server

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

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

Portal Web

Request Timeout(Seconds) \* 15 Packet Code

Verify Endpoint Requests Yes Use Cache Yes

HTTP Heartbeat Display New Page HTTPS Heartbeat Display Original Page

Portal Page

http://173.18.4.100:8080/portal/  
https://173.18.4.100:8443/portal/

2. Configure the IP address group:

- Select **User Access Policy > Portal Service > IP Group** from the navigation tree to open the portal IP address group configuration page.
- Click **Add** to open the page as shown in [Figure 4](#).
- Enter the IP group name. In this example, the name is Portal\_user.
- Enter the start IP address and end IP address of the IP group.  
Make sure the client IP address is in the IP group.
- Select a service group.  
This example uses the default group **Ungrouped**.
- Select **Normal** from the **Action** list.
- Click **OK**.

**Figure 4 Adding an IP address group**

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

Add IP Group

IP Group Name \* Portal\_user

Start IP \* 2.2.2.1

End IP \* 2.2.2.255

Service Group Ungrouped

Action \* Normal

OK Cancel

3. Add a portal device:

- Select **User Access Policy > Portal Service > Device** from the navigation tree to open the portal device configuration page.
- Click **Add** to open the page as shown in [Figure 5](#).
- Enter the device name. In this example, the name is NAS.
- Specify the version as **Portal 2.0**.
- Enter the IP address (2.2.2.1) of the AC's interface connected to the client.
- Set whether to support the portal server heartbeat and user heartbeat functions.

In this example, select **No** for both **Support Server Heartbeat** and **Support User Heartbeat**.

- g. Enter the key, which must be the same as that configured on the AC.
- h. Select **Directly Connected** from the **Access Method** list.
- i. Use the default settings for other parameters.
- j. Click **OK**.

**Figure 5 Adding a portal device**


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

Add Device

Device Information

|                            |                    |                          |           |
|----------------------------|--------------------|--------------------------|-----------|
| Device Name *              | NAS                | Service Group *          | Ungrouped |
| Version *                  | Portal 2.0         | IP Address *             | 2.2.2.1   |
| Listening Port *           | 2000               | Local Challenge *        | No        |
| Authentication Retries *   | 0                  | Logout Retries *         | 1         |
| Support Server Heartbeat * | No                 | Support User Heartbeat * | No        |
| Key *                      | *****              | Confirm Key *            | *****     |
| Access Method *            | Directly Connected |                          |           |
| Device Description         |                    |                          |           |

OK Cancel

4. Associate the portal device with the IP address group:
  - a. As shown in [Figure 6](#), click the **Port Group Information Management** icon  for the device to open the port group configuration page.
  - b. Click **Add** to open the page as shown in [Figure 7](#).
  - c. Enter the port group name. In this example, the name is **group**.
  - d. Select the configured IP address group.
 

The IP address used by the user to access the network must be within this IP address group.
  - e. Select **Supported** for **Transparent Authentication**.
  - f. Use the default settings for other parameters.
  - g. Click **OK**.
  - h. From the navigation tree, select **Intelligent Portal Management > User Management > Users**.

**Figure 6 Device list**

User > User Access Policy > Portal Service > Device



Query Devices

Device Name:  Version:

Deploy Result:  Service Group:

Query Reset

Add

| Device Name | Version    | Service Group | IP Address | Last Deployed at | Deploy Result | Operation                                                                                                                                                                   |
|-------------|------------|---------------|------------|------------------|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| NAS         | Portal 2.0 | Ungrouped     | 2.2.2.1    |                  | Not Deployed  |   |

1-1 of 1. Page 1 of 1.

Navigation: < 1 > 50

**Figure 7 Adding a port group**

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

Add Port Group

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

OK Cancel

5. Select **User Access Policy > Service Parameters > Validate System Configuration** from the navigation tree to make the configurations take effect.

## Configuring the MAC binding server

1. Add an access policy:
  - a. Select **User Access Policy > Access Policy** from the navigation tree to open the access policy page.
  - b. Click **Add** to open the page as shown in [Figure 8](#).
  - c. Enter the access policy name. In this example, the name is **AccessPolicy**.
  - d. Select **Ungrouped** from the service group list.
  - e. Use the default settings for other parameters.
  - f. Click **OK**.

**Figure 8 Adding an access policy**

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

Basic Information

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

Authorization Information

|                                              |      |                     |    |
|----------------------------------------------|------|---------------------|----|
| Access Period                                | None | Allocate IP *       | No |
| Downstream Rate(Kbps)                        |      | Upstream Rate(Kbps) |    |
| Priority                                     |      |                     |    |
| Deploy VLAN                                  |      |                     |    |
| <input type="checkbox"/> Deploy User Profile |      | Deploy User Group   |    |
| <input type="checkbox"/> Deploy ACL          |      |                     |    |

2. Add an access service:
  - a. Select **User Access Policy > Access Service** from the navigation tree to open the access service page.
  - b. Click **Add** to open the page as shown in [Figure 9](#).
  - c. Enter the service name. In this example, the service name is **MAC\_server**.
  - d. Select the **Transparent Authentication on Portal Endpoints** option.
  - e. Use the default settings for other parameters.
  - f. Click **OK**.

**Figure 9 Adding an access service**

3. Add an access user:
  - a. Select **Access User > All Access Users** from the navigation tree to open the access user page.
  - b. Click **Add** to open the page as shown in [Figure 10](#).
  - c. Select or add an access user. In this example, the account name is **client**.
  - d. Set the password. In this example, the password is **wireless**.
  - e. Bind a portal service. In this example, portal service **MAC\_server** is used.
  - f. Specify the number of limited online clients.
  - g. Retain the default settings for other parameters.
  - h. Select the configured service.
  - i. Click **OK**.

**Figure 10 Adding an access user**

4. Configure system parameters:
  - a. Select **User Access Policy > Service Parameters > System Settings** from the navigation tree to open the system settings page.
  - b. Click the **Configure** icon for **User Endpoint Settings** to open the page as shown in [Figure 11](#).
  - c. Enable **Transparent MAC Authentication**.
  - d. Select whether to enable transparent portal authentication on non-smart devices. In this example, select **Enable** for **Non-Terminal Authentication**.
  - e. Click **OK**.
  - f. Click the **Configure** icon for **Endpoint Aging Time** to open the page as shown in [Figure 12](#).

- g. Set the endpoint aging time as needed.  
This example uses the default value.

**Figure 11 Configuring user endpoint settings**

**Figure 12 Setting the endpoint aging time**

5. Select **User Access Policy > Service Parameters > Validate System Configuration** from the navigation tree to make the configurations take effect.

## Verifying the configuration

# Make the AP come online.

# Verify that the AP first associates with AC 1. Shut down VLAN-interface 100 on AC 1, wait 3 minutes, and verify that the AP associates with AC 2 and the AP state on AC 2 is **R/M**.

```
[AC2] display wlan ap all
```

```
Total number of APs: 1
```

```
Total number of connected APs: 1
```

```
Total number of connected manual APs: 1
```

```
Total number of connected auto APs: 0
```

```
Total number of connected common APs: 1
```

```
Total number of connected WTUs: 0
```

```
Total number of inside APs: 0
```

```
Maximum supported APs: 10
```

```
Remaining APs: 9
```

```
Total AP licenses: 10
```

```
Local AP licenses: 10
```

```
Server AP licenses: 0
```

```
Remaining Local AP licenses: 9
```

```
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            |
|---------|------|-------|---------|----------------------|
| office  | 1    | R/M   | AP 3620 | 219801A28N819CE0002T |

**# Bring up VLAN-interface 100 on AC 1. Verify that the AP state becomes R/M on AC 1 and R/B on AC 2.**

```
[AC1] display wlan ap all
Total number of APs: 1
Total number of connected APs: 1
Total number of connected manual APs: 1
Total number of connected auto APs: 0
Total number of connected common APs: 1
Total number of connected WTUs: 0
Total number of inside APs: 0
Maximum supported APs: 10
Remaining APs: 9
Total AP licenses: 10
Local AP licenses: 10
Server AP licenses: 0
Remaining Local AP licenses: 9
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            |
|---------|------|-------|---------|----------------------|
| office  | 1    | R/M   | AP 3620 | 219801A28N819CE0002T |

```
[AC2] display wlan ap all
Total number of APs: 1
Total number of connected APs: 1
Total number of connected manual APs: 1
Total number of connected auto APs: 0
Total number of connected common APs: 1
Total number of connected WTUs: 0
Total number of inside APs: 0
Maximum supported APs: 10
Remaining APs: 9
Total AP licenses: 10
Local AP licenses: 10
Server AP licenses: 0
Remaining Local AP licenses: 10
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            |
| office  | 1    | R/B   | AP 3620 | 219801A28N819CE0002T |

#### # Display MAC binding server configuration.

```
[AC1] display portal mac-trigger-server name mts
```

```
Portal mac trigger server name: mts
```

```

Version : 1.0
Server type : CMCC
IP : 173.18.4.100
Port : 50100
VPN instance : Not configured
Aging time : 300 seconds
Free-traffic threshold : 0 bytes
NAS-Port-Type : Not configured
Binding retry times : 3
Binding retry interval : 1 seconds
Authentication timeout : 3 minutes

```

A user can perform portal authentication through a Web browser. Before passing the authentication, the user can access only the authentication page **<http://173.18.4.100:8080/portal>**. All Web requests from the user will be redirected to the authentication page. After passing the authentication, the user can access other network resources.

For the first portal authentication, the user is required to enter the username and password.

#### # Display portal user information.

```
[AC1] display portal user all
```

```
Total portal users: 1
```

```
Username: Client
```

```
AP name: office
```

```
Radio ID: 2
```

```
SSID: service
```

```
Portal server: newpt
```

```
State: Online
```

```
VPN instance: N/A
```

|                |         |      |               |
|----------------|---------|------|---------------|
| MAC            | IP      | VLAN | Interface     |
| 0021-6330-0933 | 2.2.2.3 | 200  | WLAN-BSS1/0/3 |

```
Authorization information:
```

```
DHCP IP pool: N/A
```

```
User profile: N/A
```

```
Session group profile: N/A
```

```
ACL number: N/A
```

```
Inbound CAR: N/A
```

```
Outbound CAR: N/A
```

## Configuration files

- AC 1:
- #

```

vlan 100
#
vlan 200
#
wlan service-template st1
 ssid service
 vlan 200
client forwarding-location ac
 akm mode psk
 preshared-key pass-phrase cipher c3$oLf6pOZ6bxrf25nodjOJKYEfnZ6g6ErccHyQ
 cipher-suite ccmp
 security-ie rsn
 portal enable method direct
 portal domain dml
 portal bas-ip 2.2.2.1
 portal apply web-server newpt
 portal apply mac-trigger-server mts
 service-template enable
#
interface Vlan-interface100
 ip address 2.2.1.1 255.255.255.0
#
interface Vlan-interface200
 ip address 2.2.2.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 100 200
#
 ip route-static 173.18.4.0 24 2.2.2.100
#
 radius session-control enable
#
radius scheme rs1
 primary authentication 173.18.4.100
 primary accounting 173.18.4.100
 key authentication cipher c3$Sggqz7lDs4XPnethmAgyAKVlke7qwEkYbQ==
 key accounting cipher c3$4J/JBRGwqB4F213furJmKB6JWYXBFjWE6g==
 user-name-format without-domain
 nas-ip 2.2.2.1
#
radius dynamic-author server
 client ip 173.18.4.100 key cipher c3$AkTEB7OgMYnCqsfDeplhoAgXUek/rVrLZw==
#
domain dml
 authorization-attribute idle-cut 15 1024
 authentication portal radius-scheme rs1
 authorization portal radius-scheme rs1

```

```

 accounting portal radius-scheme rs1
#
portal free-rule 0 destination ip 173.18.4.0 255.255.255.0
portal free-rule 1 source interface Bridge-Aggregation 1
portal free-rule 2 destination ip any udp 53
portal free-rule 3 destination ip any tcp 53
#
portal web-server newpt
url http://173.18.4.100:8080/portal
server-type cmcc
url-parameter nasip value 2.2.2.1
url-parameter ssid ssid
url-parameter wlanacname value AC
url-parameter wlanuserip source-address
#
portal server newpt
ip 173.18.4.100 key cipher c3$AkTEB7OgMYnCqsfDeplhoAgXUek/rVrLZw==
server-type cmcc
#
portal mac-trigger-server mts
ip 173.18.4.100
server-type cmcc
#
wlan ap-group group1
priority 7
wlan tunnel-preempt enable
backup-ac ip 2.2.1.2
ap office
ap-model AP 3620
radio 1
 radio 2
 radio enable
 service-template st1
#
wlan ap office model AP 3620
serial-id 219801A28N819CE0002T
#

```

- **AC 2:**

```

#
vlan 100
#
vlan 200
#
wlan service-template st1
ssid service
vlan 200
client forwarding-location ac
akm mode psk

```

```

preshared-key pass-phrase cipher c3$0Lf6pOZ6bxrf25nodjOJKYEfnZ6g6ErccHyQ
cipher-suite ccmp
security-ie rsn
portal enable method direct
portal domain dml
portal bas-ip 2.2.2.2
portal apply web-server newpt
portal apply mac-trigger-server mts
service-template enable
#
interface Vlan-interface100
ip address 2.2.1.2 255.255.255.0
#
interface Vlan-interface200
ip address 2.2.2.2 255.255.255.0
#
interface GigabitEthernet1/0/1
port link-type trunk
port trunk permit vlan 100 200
#
ip route-static 173.18.4.0 16 2.2.2.100
#
radius session-control enable
#
radius scheme rs1
primary authentication 173.18.4.100
primary accounting 173.18.4.100
key authentication cipher c3$Sggqz7lDs4XPnethmAgyAKVlke7qwEkYbQ==
key accounting cipher c3$4J/JBRGwqB4F213furJMkB6JWYXBFjWE6g==
user-name-format without-domain
nas-ip 2.2.2.2
#
radius dynamic-author server
client ip 173.18.4.100 key cipher c3$AkTEB7OgMYnCqsfDeplhoAgXUek/rVrLZw==
#
domain dml
authorization-attribute idle-cut 15 1024
authentication portal radius-scheme rs1
authorization portal radius-scheme rs1
accounting portal radius-scheme rs1
#
portal free-rule 0 destination ip 173.18.4.0 255.255.255.0
portal free-rule 1 source interface Bridge-Aggregation 1
portal free-rule 2 destination ip any udp 53
portal free-rule 3 destination ip any tcp 53
#
portal web-server newpt
url http://173.18.4.100:8080/portal

```

```

server-type cmcc
url-parameter nasip value 2.2.2.2
url-parameter ssid ssid
url-parameter wlanacname value AC
url-parameter wlanuserip source-address
#
portal server newpt
ip 173.18.4.100 key cipher c3$AkTEB7OgMYnCqsfDeplhoAgXUek/rVrLZw==
server-type cmcc
#
portal mac-trigger-server mts
ip 173.18.4.100
server-type cmcc
#
wlan ap-group group1
priority 5
wlan tunnel-preempt enable
backup-ac ip 2.2.1.1
ap office
ap-model AP 3620
radio 1
radio 2
radio enable
service-template st1
#
wlan ap office model AP 3620
serial-id 219801A28N819CE0002T
#

```

- **Switch:**

```

#
vlan 2
#
vlan 100
#
vlan 200
#
interface Vlan-interface2
ip address 173.18.4.101 255.255.255.0
#
interface Vlan-interface200
ip address 2.2.2.100 255.255.255.0
#
interface GigabitEthernet1/0/1
port link-type trunk
port trunk permit vlan 1 100 200
#
interface GigabitEthernet1/0/2
port link-type access

```

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

## Related documentation

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

# INTELBRAS Access Controllers

## Remote 802.1X Authentication on a Dual-Link AC Backup Network 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  |
| General restrictions and guidelines .....                                                | 1  |
| Example: Configuring remote 802.1X authentication on a dual-link AC backup network ..... | 1  |
| Network configuration .....                                                              | 1  |
| Restrictions and guidelines .....                                                        | 2  |
| Procedures .....                                                                         | 2  |
| Configuring AC 1 .....                                                                   | 2  |
| Configuring AC 2 .....                                                                   | 4  |
| Configuring the switch .....                                                             | 7  |
| Configuring the RADIUS server .....                                                      | 8  |
| Configuring the client .....                                                             | 10 |
| Verifying the configuration .....                                                        | 11 |
| Configuration files .....                                                                | 14 |
| Related documentation .....                                                              | 17 |



# Introduction

The following information provides an example of configuring remote 802.1X authentication for clients on a dual-link AC backup 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 WLAN access, WLAN user security, WLAN user access authentication, 802.1X, AAA, and WLAN high availability features.

## General restrictions and guidelines

Make sure the master and backup ACs have the same RADIUS, service template, and radio settings.

Make sure the master and backup ACs use the same version of software.

## Example: Configuring remote 802.1X authentication on a dual-link AC backup network

### Network configuration

As shown in [Figure 1](#):

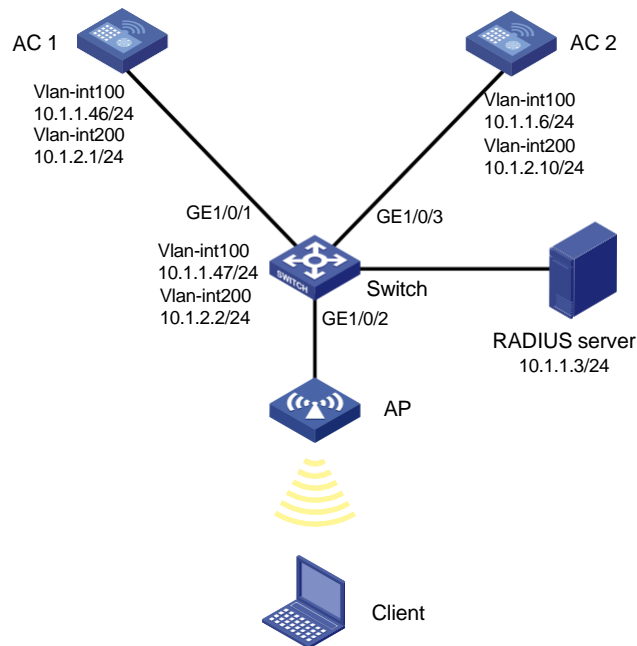
- The AP is attached to a switch dual-homed to AC 1 (the master AC) and AC 2 (the backup AC).
- The switch acts as a DHCP server to assign IP addresses to the AP and the client.
- The network deploys a RADIUS server that runs INC for 802.1X authentication.

Configure the devices to meet the following requirements:

- The ACs operate in active/standby mode to provide centralized forwarding. When AC 1 fails, the AP associates with AC 2. When AC 1 recovers, the AP re-associates with AC 1.
- The ACs act as the authenticator and use the RADIUS server to perform authentication, authorization, and accounting for the client.
- The client accesses the wireless network through VLAN 200 and performs RADIUS-based 802.1X authentication.
- Open system authentication is used to authenticate the client at the data link layer. This is the default authentication method.
- The 802.1X AKM mode is used to secure data transmission between the client and the AP.

- The cipher suite used for frame encryption is CCMP.

**Figure 1 Network diagram**



## Restrictions and guidelines

When you configure remote 802.1X authentication on a dual-link AC backup network, follow these restrictions and guidelines:

- Use the actual serial ID of an AP to uniquely identify that AP.
- For the INC server to dynamically change client authorization information or forcibly disconnect a client, enable the RADIUS session-control feature on the ACs.
- To avoid dynamic authorization failures, configure the RADIUS Dynamic Authorization Extensions Server (DAS) feature.

## Procedures

### Configuring AC 1

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 the master CAPWAP control and data tunnels with the AP.

```
<AC1> system-view
[AC1] vlan 100
[AC1-vlan100] quit
[AC1] interface vlan-interface 100
[AC1-Vlan-interface100] ip address 10.1.1.46 24
[AC1-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.

```
[AC1] vlan 200
[AC1-vlan200] quit
[AC1] interface vlan-interface 200
[AC1-Vlan-interface200] ip address 10.1.2.1 24
[AC1-Vlan-interface200] quit
```

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

```
[AC1] interface gigabitethernet1/0/1
[AC1-GigabitEthernet1/0/1] port link-type trunk
[AC1-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[AC1-GigabitEthernet1/0/1] quit
```

## 2. Configure RADIUS-based 802.1X authentication:

**# Create RADIUS scheme **radius1** and enter its view.**

```
[AC1] radius scheme radius1
```

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

```
[AC1-radius-radius1] primary authentication 10.1.1.3
[AC1-radius-radius1] primary accounting 10.1.1.3
```

**# Specify the shared keys for RADIUS authentication and accounting.**

```
[AC1-radius-radius1] key authentication simple 12345
[AC1-radius-radius1] key accounting simple 12345
```

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

```
[AC1-radius-radius1] nas-ip 10.1.2.1
[AC1-radius-radius1] quit
```

**# Create ISP domain **dom1** and enter its view.**

```
[AC1] domain dom1
```

**# Configure the ISP domain to use RADIUS scheme **radius1** for 802.1X user authentication, authorization, and accounting.**

```
[AC1-isp-dom1] authentication lan-access radius-scheme radius1
[AC1-isp-dom1] authorization lan-access radius-scheme radius1
[AC1-isp-dom1] accounting lan-access radius-scheme radius1
[AC1-isp-dom1] quit
```

**# Enable RADIUS session-control.**

```
[AC1] radius session-control enable
```

**# Enable RADIUS DAS and enter its view.**

```
[AC1] radius dynamic-author server
```

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

```
[AC1-radius-da-server] client ip 10.1.1.3 key simple 12345
[AC1-radius-da-server] quit
```

## 3. Configure 802.1X authentication:

**# Configure EAP relay as the method for the AC to exchange packets with the RADIUS server.**

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

## 4. Configure a service template:

**# Create service template **service** and enter its view.**

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

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

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

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

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

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

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

# Set the AKM mode to 802.1X.

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

# Specify the CCMP cipher suite and enable the RSN IE in beacon and probe responses.

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

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

# Set the access authentication mode to 802.1X authentication.

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

# Specify ISP domain **dom1** as the 802.1X authentication domain.

```
[AC1-wlan-st-service] dot1x domain dom1
```

# Enable the service template.

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

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

## 5. Configure the AP:

---

### NOTE:

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

---

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

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

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

```
[AC1-wlan-ap-ap1] quit
```

# Create AP group **group1**.

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

# Configure an AP grouping rule by AP name to add AP named **ap1** to the group.

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

# Set the AP connection priority to 7.

```
[AC1-wlan-ap-group-group1] priority 7
```

# Specify AC 2 as the backup AC.

```
[AC1-wlan-ap-group-group1] backup-ac ip 10.1.1.6
```

# Enable master CAPWAP tunnel preemption.

```
[AC1-wlan-ap-group-group1] wlan tunnel-preempt enable
```

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

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

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

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

# Enable radio 1.

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

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

## Configuring AC 2

### 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 the backup CAPWAP control and data tunnels with the AP.

```
<AC2> system-view
[AC2] vlan 100
[AC2-vlan100] quit
[AC2] interface vlan-interface 100
[AC2-Vlan-interface100] ip address 10.1.1.6 24
[AC2-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.

```
[AC2] vlan 200
[AC2-vlan200] quit
[AC2] interface vlan-interface 200
[AC2-Vlan-interface200] ip address 10.1.2.10 24
[AC2-Vlan-interface200] quit
```

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

```
[AC2] interface gigabitethernet1/0/1
[AC2-GigabitEthernet1/0/1] port link-type trunk
[AC2-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[AC2-GigabitEthernet1/0/1] quit
```

## 2. Configure RADIUS-based 802.1X authentication:

# Create RADIUS scheme **radius1** and enter its view.

```
[AC2] radius scheme radius1
```

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

```
[AC2-radius-radius1] primary authentication 10.1.1.3
[AC2-radius-radius1] primary accounting 10.1.1.3
```

# Specify the shared keys for RADIUS authentication and accounting.

```
[AC2-radius-radius1] key authentication simple 12345
[AC2-radius-radius1] key accounting simple 12345
```

# Specify IP address 10.1.2.10 as the source IP address for outgoing RADIUS packets.

```
[AC2-radius-radius1] nas-ip 10.1.2.10
[AC2-radius-radius1] quit
```

# Create ISP domain **dom1** and enter its view.

```
[AC2] domain dom1
```

# Configure the ISP domain to use RADIUS scheme **radius1** for 802.1X user authentication, authorization, and accounting.

```
[AC2-isp-dom1] authentication lan-access radius-scheme radius1
[AC2-isp-dom1] authorization lan-access radius-scheme radius1
[AC2-isp-dom1] accounting lan-access radius-scheme radius1
[AC2-isp-dom1] quit
```

# Enable RADIUS session-control.

```
[AC2] radius session-control enable
```

# Enable RADIUS DAS and enter its view.

```
[AC2] radius dynamic-author server
```

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

```
[AC2-radius-da-server] client ip 10.1.1.3 key simple 12345
[AC2-radius-da-server] quit
```

**3. Configure 802.1X authentication:**

**# Configure EAP relay as the method for the AC to exchange packets with the RADIUS server.**

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

**4. Configure a service template:**

**# Create service template **service** and enter its view.**

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

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

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

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

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

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

```
[AC2-wlan-st-service] vlan 200
```

**# Set the AKM mode to 802.1X.**

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

**# Specify the CCMP cipher suite and enable the RSN IE in beacon and probe responses.**

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

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

**# Set the access authentication mode to 802.1X authentication.**

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

**# Specify ISP domain **dom1** as the 802.1X authentication domain.**

```
[AC2-wlan-st-service] dot1x domain dom1
```

**# Enable the service template.**

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

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

**5. Configure the AP:**

---

**NOTE:**

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

---

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

```
[AC2] wlan ap ap1 model AP 3620
```

```
[AC2-wlan-ap-ap1] serial-id 219801A28N819CE0002T
```

```
[AC2-wlan-ap-ap1] quit
```

**# Create AP group **group1**.**

```
[AC2] wlan ap-group group1
```

**# Configure an AP grouping rule by AP name to add AP named **ap1** to the group.**

```
[AC2-wlan-ap-group-group1] ap ap1
```

**# Set the AP connection priority to 5.**

```
[AC2-wlan-ap-group-group1] priority 5
```

**# Specify AC 1 as the backup AC.**

```
[AC2-wlan-ap-group-group1] backup-ac ip 10.1.1.46
```

**# Enable master CAPWAP tunnel preemption.**

```
[AC2-wlan-ap-group-group1] wlan tunnel-preempt enable
```

```

Bind service template service to radio 1.
[AC2-wlan-ap-group-group1] ap-model AP 3620
[AC2-wlan-ap-group-group1-ap-model-AP 3620] radio 1
[AC2-wlan-ap-group-group1-ap-model-AP 3620-radio-1] service-template service

Enable radio 1.
[AC2-wlan-ap-group-group1-ap-model-AP 3620-radio-1] radio
enable [AC2-wlan-ap-group-group1-ap-model-AP 3620-radio-1] quit

```

## Configuring the switch

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

```

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

```

**# Create VLAN 200.** The switch will use this VLAN to forward packets for the client.

```

[Switch] vlan 200
[Switch-vlan200] quit

```

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

```

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

```

**# Configure GigabitEthernet 1/0/3 (the port connected to AC 2) as a trunk port, and assign the trunk port to VLANs 100 and 200.**

```

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

```

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

```

[Switch] interface 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

```

**# Assign an IP address to VLAN-interface 100.**

```

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

```

**# Assign an IP address to VLAN-interface 200.**

```

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

```

**# Configure DHCP address pool 100.** The switch will use this pool to assign an IP address to the AP.

```
[Switch] dhcp server ip-pool 100
[Switch-dhcp-pool-100] network 10.1.1.0 mask 255.255.255.0
[Switch-dhcp-pool-100] gateway-list 10.1.1.47
[Switch-dhcp-pool-100] quit
```

# Configure DHCP address pool **200**. The switch will use this pool to assign an IP address to the client. In this example, the address of the DNS server is 10.1.2.2 (the gateway address). You must replace it with the actual address of the DNS server on your network.

```
[Switch] dhcp server ip-pool 200
[Switch-dhcp-pool-200] network 10.1.2.0 mask 255.255.255.0
[Switch-dhcp-pool-200] gateway-list 10.1.2.2
[Switch-dhcp-pool-200] dns-list 10.1.2.2
[Switch-dhcp-pool-200] quit
```

#### # Enable DHCP

```
[Switch] dhcp enable
```

## Configuring the RADIUS server

In this example, the RADIUS server runs INC PLAT 7.3 (E0605) and INC UAM 7.1 (E0302).

### Adding AC 1 and AC 2 to INC as access devices

This example only illustrates the process to add AC 1 to INC as an access device. You can add access device AC 2 to INC in the same way AC 1 is added to INC as an access device.

To add AC 1 to INC as an access device:

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

**Figure 2 Adding an access device**

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

Access Configuration

|                       |               |                      |                 |
|-----------------------|---------------|----------------------|-----------------|
| Authentication Port * | 1812          | Accounting Port *    | 1813            |
| Service Type          | Unlimited     | Forcible Logout Type | Disconnect user |
| Access Device Type    | H3C (General) | Service Group        | Ungrouped       |
| Shared Key *          | 12345         | Confirm Shared Key * | 12345           |
| Access Location Group | ..            |                      |                 |

Device List

Select Add Manually Clear All

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

Total Items: 1.

OK Cancel



## Adding an access policy

1. Click the **User** tab.
2. From the navigation tree, select **User Access Policy > Access Policy**.
3. Click **Add**.
4. On the **Add Access Policy** page, configure the following parameters, as shown in [Figure 3](#):
  - o Enter **dot1x** in the **Access Policy Name** field.
  - o Select **EAP-PEAP** from the **Preferred EAP Type** list, and select **EAP-MSCHAPv2** from the **Subtype** list.

The certificate subtype on the INC server must be the same as the identity authentication method configured on the client.
5. Click **OK**.

**Figure 3 Adding an access policy**

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

Basic Information

Access Policy Name \* dot1x

Service Group \* Ungrouped

Description

Authorization Information

Access Period None

Downstream Rate (Kbps)

Priority

Preferred EAP Type EAP-PEAP

EAP Auto Negotiate Enable

Deploy Address Pool

☐ Deploy User Profile

☐ Deploy ACL

Offline Check Period (Hours)

Allocate IP \* No

Upstream Rate (Kbps)

Deploy User Group

Subtype EAP-MSCHAPv2

Maximum Online Duration for a Logon (Minutes)

Deploy VLAN

Deploy VSI name

Authentication Password Account Password

## Adding an access service

1. Click the **User** tab.
2. From the navigation tree, select **User Access Policy > Access Service**.
3. Click **Add**.
4. On the **Add Access Service** page, configure the following parameters, as shown in [Figure 4](#):
  - o Enter **dot1x** in the **Service Name** field.
  - o Select **dot1x** from the **Default Access Policy** list.
5. Click **OK**.

**Figure 4 Adding an access service**

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

Basic Information

Service Name \* dot1x

Service Group \* Ungrouped

Default Proprietary Attribute Assignment Policy \* Do not use

Default Max. Devices for Single Account \* 0

Daily Max. Online Duration \* 0

Description

☒ Available

Service Suffix

Default Access Policy \* dot1x Add

Default Max. Number of Online Endpoints \* 0

☒ Transparent Authentication

Access Scenario List

Add

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

OK Cancel

## Adding an access user

1. Click the **User** tab.
2. From the navigation tree, select **Access User > Access User**.  
The access user list opens.
3. Click **Add**.  
The **Add Access User** page opens.
4. In the **Access Information** area, configure the following parameters, as shown in [Figure 5](#):
  - a. Click **Select** or **Add User** to associate the user with INC Platform user **user**.
  - b. Enter **dot1x** in the **Account Name** field.
  - c. Enter **dot1x123** in the **Password** and **Confirm Password** fields.
5. In the **Access Service** area, select **dot1x** from the list.
6. Click **OK**.

**Figure 5 Adding an access user account**

The screenshot shows the 'Add Access User' configuration page. The 'Access Information' section includes fields for 'User Name' (set to 'user'), 'Account Name' (set to 'dot1x'), 'Password' (set to 'dot1x123'), and 'Confirm Password' (set to 'dot1x123'). There are checkboxes for 'Trial Account', 'Default BYOD User', 'MAC Authentication User' (checked), 'Computer User', and 'Fast Access User'. There are also fields for 'Start Time', 'End Time', 'Max. Idle Time (Minutes)', 'Max. Concurrent Logins' (set to 1), and 'Login Message'. The 'Access Service' section shows a table with two rows: 'dot1x' (checked) and 'MAC\_server'.

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

## Configuring the client

### Prerequisites

Make sure the client has been installed with the EAP-PEAP certificate.

This example uses Windows 7 Service Pack 1 to describe the procedure.

### Procedure

Perform the following tasks to create wireless network **service** and configure properties for the wireless network:

1. Click **Start**, and then select **Control Panel**.
2. In the control panel, click **View network status and tasks** below **Network and Internet**.
3. Click **Manage wireless networks**.
4. Click **Add**.
5. Click **Manually create a network profile**.
6. Configure the wireless network profile:
  - o Set the network name to **service**. (The network name is the same as the SSID in the service template on the ACs.)
  - o Set the security type to **WPA2-Enterprise**.
  - o Set the encryption type to **AES**.
  - o Retain the default settings for other parameters.

7. Click **Next**.
8. After the wireless network is added successfully, click **Change connection settings**.
9. In the wireless network properties dialog box, click the **Security** tab.
10. Select **Microsoft: Protected EAP (PEAP)** as the network authentication method, and clear the **Remember my credentials for this connection each time I'm logged on** option.
11. Click **Settings** next to **Microsoft: Protected EAP (PEAP)**.
12. In the **Protected EAP Properties** dialog box that opens, configure the following parameters:
  - a. Clear the **Validate server certificate** and **Enable Fast Reconnect** options.
  - b. Set the authentication method to **Secured password (EAP MSCHAP v2)**.
  - c. Click **Configure** next to **Secured password (EAP MSCHAP v2)**.
  - d. In the **EAP MSCHAPv2 Properties** dialog box that opens, clear the **Automatically use my Windows logon name and password (and domain if any)** option, and then click **OK**.
  - e. Click **OK**.
13. In the wireless network properties dialog box, click **Advanced settings**.
14. On the **802.1X settings** tab, select user authentication as the authentication mode.
15. On the **802.11 settings** tab, clear the **Enable Pairwise Master Key (PMK) caching** option, and then click **OK**.
16. Click **OK**.

## Verifying the configuration

1. Verify the AC backup and switchover functionality:
  - # Verify that the AP associates with AC 1 and comes online. (Details not shown.)
  - # Shut down VLAN-interface 100 on AC 1. (Details not shown.)
  - # Verify that the AP automatically associates with AC 2 and comes online in less than 3 minutes, during which traffic is interrupted. The state of the AP changes to **R/M (Run/Master)** on AC 2 after it comes up.

```
[AC2] display wlan ap all
Total number of APs: 1
Total number of connected APs: 1
Total number of connected manual APs: 1
Total number of connected auto APs: 0
Total number of connected common APs: 1
Total number of connected WTUs: 0
Total number of inside APs: 0
Maximum supported APs: 512
Remaining APs: 511
Total AP licenses: 128
Local AP licenses: 128
Server AP licenses: 0
Remaining local 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 | APID | State | Model   | Serial ID            |
|---------|------|-------|---------|----------------------|
| ap1     | 2    | R/M   | AP 3620 | 219801A28N819CE0002T |

# Bring up VLAN-interface 100 on AC 1. (Details not shown.)

# Verify that the AP re-associates with AC 1 and its state changes to **R/M (Run/Master)** on AC 1 after a successful association. At the same time, the state of the AP changes to **R/B** on AC 2.

```
[AC1] display wlan ap all
```

```
...
```

```
[AC2] display wlan ap all
```

```
Total number of APs: 1
```

```
Total number of connected APs: 1
```

```
Total number of connected manual APs: 1
```

```
Total number of connected auto APs: 0
```

```
Total number of connected common APs: 1
```

```
Total number of connected WTUs: 0
```

```
Total number of inside APs: 0
```

```
Maximum supported APs: 512
```

```
Remaining APs: 511
```

```
Total AP licenses: 128
```

```
Local AP licenses: 128
```

```
Server AP licenses: 0
```

```
Remaining local AP licenses: 128
```

```
Sync AP licenses: 0
```

#### AP information

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

| AP name | APID | State | Model   | Serial ID            |
|---------|------|-------|---------|----------------------|
| ap1     | 2    | R/B   | AP 3620 | 219801A28N819CE0002T |

2. Connect the client to the wireless network. (Details not shown.)

3. On AC 1, perform the following tasks to verify that the client has passed authentication and come online:

# Display detailed WLAN client information.

```
[AC1] display wlan client verbose
```

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

|              |                  |
|--------------|------------------|
| MAC address  | : cc3a-61a8-fb8c |
| IPv4 address | : 10.1.2.3       |
| IPv6 address | : N/A            |
| Username     | : dot1x          |
| AID          | : 1              |
| AP ID        | : 2              |
| AP name      | : ap1            |
| Radio ID     | : 1              |
| SSID         | : service        |
| BSSID        | : 741f-4ad4-1fe0 |
| VLAN ID      | : 200            |
| Sleep count  | : 0              |

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

#### # Display online 802.1X user information.

[AC1] display dot1x connection

Total connections: 1

|                       |                  |
|-----------------------|------------------|
| User MAC address      | : cc3a-61a8-fb8c |
| AP name               | : ap1            |
| Radio ID              | : 1              |
| SSID                  | : service        |
| BSSID                 | : 741f-4ad4-1fe0 |
| <b>Username</b>       | <b>: dot1x</b>   |
| Authentication domain | : dom1           |
| IPv4 address          | : 10.1.2.3       |
| Authentication method | : EAP            |
| Initial VLAN          | : 200            |

```
Authorization VLAN : 200
Authorization ACL number : N/A
Authorization user profile : N/A
Termination action : Default
Session timeout period : 36000001 s
Online from : 2015/12/21 11:27:11
Online duration : 0h 1m 1s
```

## Configuration files

- AC 1:

```
#
dot1x authentication-method eap
#
vlan 1
#
vlan 100
#
vlan 200
#
wlan service-template service
 ssid service
 vlan 200
 akm mode dot1x
 cipher-suite ccmp
 security-ie rsn
 client-security authentication-mode dot1x
 dot1x domain dom1
 client forwarding-location ac
 service-template enable
#
interface Vlan-interface100
 ip address 10.1.1.46 255.255.255.0
#
interface Vlan-interface200
 ip address 10.1.2.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 1 100 200
#
radius scheme radius1
 primary authentication 10.1.1.3
 primary accounting 10.1.1.3
 key authentication cipher c3$Bb61SHV2ZsVYPJU2+RFB/8ntk0uCQkmxDA==
 key accounting cipher c3$w03NfxnBmfDuedv9/xo7ESnoxKjowmmX9A==
nas-ip 10.1.2.1
#
```

```

radius dynamic-author server
 client ip 10.1.1.3 key cipher c3$AkTEB7OgMYnCqsfDeplhoAgXUek/rVrLZw==
#
domain dom1
 authentication lan-access radius-scheme radius1
 authorization lan-access radius-scheme radius1
 accounting lan-access radius-scheme radius1
#
wlan ap ap1 model AP 3620
 serial-id 219801A28N819CE0002T
#
wlan ap-group group1
ap ap1
wlan tunnel-preempt enable
 priority 7
 backup-ac ip 10.1.1.6
ap-model AP 3620
 radio 1
 radio enable
 service-template service
#

```

- **AC 2:**

```

#
 dot1x authentication-method eap
#
vlan 1
#
vlan 100
#
vlan 200
#
wlan service-template service
 ssid service
 vlan 200
 akm mode dot1x
 cipher-suite ccmp
 security-ie rsn
 client-security authentication-mode dot1x
 dot1x domain dom1
 client forwarding-location ac
 service-template enable
#
interface Vlan-interface100
 ip address 10.1.1.6 255.255.255.0
#
interface Vlan-interface200
 ip address 10.1.2.10 255.255.255.0
#

```

```

interface GigabitEthernet1/0/3
 port link-type trunk
 port trunk permit vlan 1 100 200
#
radius scheme radius1
 primary authentication 10.1.1.3
 primary accounting 10.1.1.3
 key authentication cipher c3$Bb61SHV2ZsVYPJU2+RFB/8ntk0uCQkmxDA==
 key accounting cipher c3$w03NfxnBmfDuedv9/xo7ESnoxKjowmmX9A==
nas-ip 10.1.2.10
#
radius dynamic-author server
 client ip 10.1.1.3 key cipher c3$AkTEB7OgMYnCqsfDeplhoAgXUek/rVrLZw==
#
domain dom1
 authentication lan-access radius-scheme radius1
 authorization lan-access radius-scheme radius1
 accounting lan-access radius-scheme radius1
#
wlan ap ap1 model AP 3620
 serial-id 219801A28N819CE0002T
#
wlan ap-group group1
ap ap1
wlan tunnel-preempt enable
 priority 5
 backup-ac ip 10.1.1.46
ap-model AP 3620
 radio 1
 radio enable
 service-template service
#

```

- **Switch:**

```

#
 dhcp enable
#
vlan 1
#
vlan 100
#
vlan 200
#
dhcp server ip-pool 100
 gateway-list 10.1.1.47
 network 10.1.1.0 mask 255.255.255.0

#
dhcp server ip-pool 200

```



```

gateway-list 10.1.2.2
dns-list 10.1.2.2
network 10.1.2.0 mask 255.255.255.0
#
interface Vlan-interface100
ip address 10.1.1.47 255.255.255.0
#
interface Vlan-interface200
ip address 10.1.2.2 255.255.255.0
#
interface GigabitEthernet1/0/1
port link-type trunk
port trunk permit vlan 1 100 200
#
interface GigabitEthernet1/0/2
port link-type access
port access vlan 100
poe enable
#
#
interface GigabitEthernet1/0/3
port link-type trunk
port trunk permit vlan 1 100 200
#

```

## Related documentation

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

# INTELBRAS Access Controllers

## Remote MAC Authentication on a Dual-Link AC Backup Network 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  |
| General restrictions and guidelines .....                                             | 1  |
| Example: Configuring remote MAC authentication on a dual-link AC backup network ..... | 1  |
| Network configuration .....                                                           | 1  |
| Restrictions and guidelines .....                                                     | 2  |
| Procedures .....                                                                      | 2  |
| Configuring AC 1 .....                                                                | 2  |
| Configuring AC 2 .....                                                                | 4  |
| Configuring the switch .....                                                          | 7  |
| Configuring the RADIUS server .....                                                   | 8  |
| Verifying the configuration .....                                                     | 11 |
| Configuration files .....                                                             | 12 |
| Related documentation .....                                                           | 16 |

# Introduction

The following information provides an example of configuring remote MAC authentication for clients on a dual-link AC backup network that uses shared key authentication for Pre-RSNA.

## 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 user access authentication, WLAN user security, and WLAN high availability features.

## General restrictions and guidelines

Make sure the master and backup ACs have the same RADIUS, service template, and radio settings.

Make sure the master and backup ACs use the same version of software.

## Example: Configuring remote MAC authentication on a dual-link AC backup network

### Network configuration

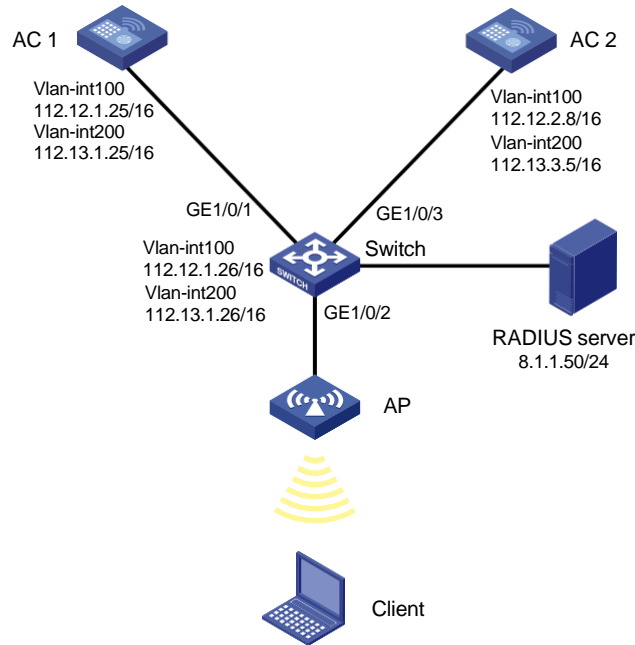
As shown in [Figure 1](#):

- The AP is attached to a switch dual-homed to AC 1 (the master AC) and AC 2 (the backup AC).
- The switch acts as a DHCP server to assign IP addresses to the AP and the client.
- The network deploys a RADIUS server for MAC authentication.

Configure the devices to meet the following requirements:

- The ACs operate in active/standby mode to provide centralized forwarding. When AC 1 fails, the AP associates with AC 2. When AC 1 recovers, the AP re-associates with AC 1.
- The ACs act as the authenticator and use the RADIUS server to perform authentication, authorization, and accounting for the client.
- The client accesses the wireless network through VLAN 200 and performs RADIUS-based MAC authentication.
- The PSK AKM mode is used to secure data transmission between the client and the AP.

**Figure 1 Network diagram**



## Restrictions and guidelines

On each AC, specify the user account format for MAC authentication. This example uses the MAC address of the client as the username and password. Make sure the RADIUS server has the same username and password settings as the ACs for the client.

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

Some endpoints by default use random MAC addresses. To ensure successful MAC authentication for such an endpoint, disable the endpoint from using a random MAC address.

## Procedures

### Configuring AC 1

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 the master CAPWAP control and data tunnels with the AP.

```
<AC1> system-view
[AC1] vlan 100
[AC1-vlan100] quit
[AC1] interface vlan-interface 100
[AC1-Vlan-interface100] ip address 112.12.1.25 16
[AC1-Vlan-interface100] quit
```

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

```
[AC1] vlan 200
[AC1-vlan200] quit
```

```
[AC1] interface vlan-interface 200
[AC1-Vlan-interface200] ip address 112.13.1.25 16
[AC1-Vlan-interface200] quit
```

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

```
[AC1] interface gigabitethernet1/0/1
[AC1-GigabitEthernet1/0/1] port link-type trunk
[AC1-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[AC1-GigabitEthernet1/0/1] quit
```

## 2. Configure RADIUS-based MAC authentication:

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

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

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

```
[AC1-radius-office] primary authentication 8.1.1.50
[AC1-radius-office] primary accounting 8.1.1.50
```

**# Specify the shared keys for RADIUS authentication and accounting.**

```
[AC1-radius-office] key authentication simple 123456789
[AC1-radius-office] key accounting simple 123456789
```

**# Exclude the ISP domain name from the usernames sent to the RADIUS servers.**

```
[AC1-radius-office] user-name-format without-domain
```

**# Specify IP address 112.12.1.25 as the source IP address for outgoing RADIUS packets.**

```
[AC1-radius-office] nas-ip 112.12.1.25
[AC1-radius-office] quit
```

**# Create ISP domain **office1** and enter its view.**

```
[AC1] domain office1
```

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

```
[AC1-isp-office1] authentication lan-access radius-scheme office
[AC1-isp-office1] authorization lan-access radius-scheme office
[AC1-isp-office1] accounting lan-access radius-scheme office
```

**# Set the idle-cut timer to 15 minutes and set the minimum number of bytes that a client must generate before the timer expires to 1024 bytes. The AC will disconnect a client if it has received traffic less than 1024 bytes from that client before the timer expires.**

```
[AC1-isp-office1] authorization-attribute idle-cut 15 1024
[AC1-isp-office1] quit
```

**# Configure MAC authentication to use MAC-based accounts. The MAC addresses are in hexadecimal notation without hyphens, and letters are in lower case. (This step is optional. The configuration in this step is the default configuration.)**

```
[AC1] mac-authentication user-name-format mac-address without-hyphen lowercase
```

## 3. Configure a service template:

**# Create service template **1** and enter its view.**

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

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

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

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

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

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

```
[AC1-wlan-st-1] client forwarding-location ac
Set the access authentication mode to MAC authentication.
[AC1-wlan-st-1] client-security authentication-mode mac
Specify ISP domain office1 as the MAC authentication domain.
[AC1-wlan-st-1] mac-authentication domain office1
```

4. Configure the AKM mode in the service template:

```
Set the AKM mode to PSK.
[AC1-wlan-st-1] akm mode psk
Set the PSK to 123456789 in plain text.
[AC1-wlan-st-1] preshared-key pass-phrase simple 123456789
Configure CCMP as the cipher suite and enable the RSN IE in beacon and probe responses.
[AC1-wlan-st-1] cipher-suite ccmp
[AC1-wlan-st-1] security-ie rsn
Enable the service template.
[AC1-wlan-st-1] service-template enable
[AC1-wlan-st-1] quit
```

5. Configure a manual AP:

---

**NOTE:**

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

---

```
Create manual AP ap1 and specify the AP model and serial ID.
[AC1] wlan ap ap1 model AP 3620
[AC1-wlan-ap-ap1] serial-id 219801A28N819CE0002T
[AC1-wlan-ap-ap1] quit
Create AP group group1 and create a grouping rule by AP name to add the AP named ap1 to the group.
[AC1] wlan ap-group group1
[AC1-wlan-ap-group-group1] ap ap1
Set the AP connection priority to 7.
[AC1-wlan-ap-group-group1] priority 7
Specify AC 2 as the backup AC.
[AC1-wlan-ap-group-group1] backup-ac ip 112.12.2.8
Enable master CAPWAP tunnel preemption.
[AC1-wlan-ap-group-group1] wlan tunnel-preempt enable
Bind service template 1 to radio 2.
[AC1-wlan-ap-group-group1] ap-model AP 3620
[AC1-wlan-ap-group-group1-ap-model-AP 3620] radio 2
[AC1-wlan-ap-group-group1-ap-model-AP 3620-radio-2] service-template 1
Enable radio 2.
[AC1-wlan-ap-group-group1-ap-model-AP 3620-radio-2] radio
enable [AC1-wlan-ap-group-group1-ap-model-AP 3620-radio-2] quit
```

## Configuring AC 2

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 the backup CAPWAP control and data tunnels with the AP.

```
<AC2> system-view
[AC2] vlan 100
[AC2-vlan100] quit
[AC2] interface vlan-interface 100
[AC2-Vlan-interface100] ip address 112.12.2.8 16
[AC2-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.

```
[AC2] vlan 200
[AC2-vlan200] quit
[AC2] interface vlan-interface 200
[AC2-Vlan-interface200] ip address 112.13.3.5 16
[AC2-Vlan-interface200] quit
```

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

```
[AC2] interface gigabitethernet1/0/1
[AC2-GigabitEthernet1/0/1] port link-type trunk
[AC2-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[AC2-GigabitEthernet1/0/1] quit
```

## 2. Configure RADIUS-based MAC authentication:

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

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

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

```
[AC2-radius-office] primary authentication 8.1.1.50
[AC2-radius-office] primary accounting 8.1.1.50
```

# Specify the shared keys for RADIUS authentication and accounting.

```
[AC2-radius-office] key authentication simple 123456789
[AC2-radius-office] key accounting simple 123456789
```

# Exclude the ISP domain name from the usernames sent to the RADIUS servers.

```
[AC2-radius-office] user-name-format without-domain
```

# Specify IP address 112.12.2.8 as the source IP address for outgoing RADIUS packets.

```
[AC2-radius-office] nas-ip 112.12.2.8
[AC2-radius-office] quit
```

# Create ISP domain **office1** and enter its view.

```
[AC2] domain office1
```

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

```
[AC2-isp-office1] authentication lan-access radius-scheme office
[AC2-isp-office1] authorization lan-access radius-scheme office
[AC2-isp-office1] accounting lan-access radius-scheme office
```

# Set the idle-cut timer to 15 minutes and set the minimum number of bytes that a client must generate before the timer expires to 1024 bytes. The AC will disconnect a client if it has received traffic less than 1024 bytes from that client before the timer expires.

```
[AC2-isp-office1] authorization-attribute idle-cut 15 1024
[AC2-isp-office1] quit
```



# Configure MAC authentication to use MAC-based accounts. The MAC addresses are in hexadecimal notation without hyphens, and letters are in lower case. (This step is optional. The configuration in this step is the default configuration.)

```
[AC2] mac-authentication user-name-format mac-address without-hyphen lowercase
```

**3. Configure a service template:**

# Create service template **1** and enter its view.

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

# Set the SSID to **service**.

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

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

```
[AC2-wlan-st-1] vlan 200
```

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

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

# Set the access authentication mode to MAC authentication.

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

# Specify ISP domain **office1** as the MAC authentication domain.

```
[AC2-wlan-st-1] mac-authentication domain office1
```

**4. Configure the AKM mode in the service template:**

# Set the AKM mode to PSK.

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

# Set the PSK to **123456789** in plain text.

```
[AC2-wlan-st-1] preshared-key pass-phrase simple 123456789
```

# Configure CCMP as the cipher suite and enable the RSN IE in beacon and probe responses.

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

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

# Enable the service template.

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

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

**5. Configure a manual AP:**

---

**NOTE:**

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

---

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

```
[AC2] wlan ap ap1 model AP 3620
```

```
[AC2-wlan-ap-ap1] serial-id 219801A28N819CE0002T
```

```
[AC2-wlan-ap-ap1] quit
```

# Create AP group **group1** and create a grouping rule by AP name to add the AP named **ap1** to the group.

```
[AC2] wlan ap-group group1
```

```
[AC2-wlan-ap-group-group1] ap ap1
```

# Set the AP connection priority to 5.

```
[AC2-wlan-ap-group-group1] priority 5
```

# Specify AC 1 as the backup AC.

```
[AC2-wlan-ap-group-group1] backup-ac ip 112.12.1.25
```

# Enable master CAPWAP tunnel preemption.

```

[AC2-wlan-ap-group-group1] wlan tunnel-preempt enable
Bind service template 1 to radio 2.
[AC2-wlan-ap-group-group1] ap-model AP 3620
[AC2-wlan-ap-group-group1-ap-model-AP 3620] radio 2
[AC2-wlan-ap-group-group1-ap-model-AP 3620-radio-2] service-template 1
Enable radio 2.
[AC2-wlan-ap-group-group1-ap-model-AP 3620-radio-2] radio
enable [AC2-wlan-ap-group-group1-ap-model-AP 3620-radio-2] quit

```

## Configuring the switch

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

```

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

```

**# Create VLAN 200. The switch will use this VLAN to forward packets for the wireless client.**

```

[Switch] vlan 200
[Switch-vlan200] quit

```

**# Configure GigabitEthernet 1/0/1 (the port connected to AC 1) 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 1/0/3 (the port connected to AC 2) as a trunk port, and assign the trunk port to VLAN 100 and VLAN 200.**

```

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

```

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

```

[Switch] interface 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

```

**# Assign an IP address to VLAN-interface 100.**

```

[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ip address 112.12.1.26 16
[Switch-Vlan-interface100] quit

```

**# Assign an IP address to VLAN-interface 200.**

```

[Switch] interface vlan-interface 200
[Switch-Vlan-interface200] ip address 112.13.1.26 16
[Switch-Vlan-interface200] quit

```

# Configure DHCP address pool **100**. The switch will use this pool to assign an IP address to the AP.

```
[Switch] dhcp server ip-pool 100
[Switch-dhcp-pool-100] network 112.12.0.0 mask 255.255.0.0
[Switch-dhcp-pool-100] gateway-list 112.12.1.26
[Switch-dhcp-pool-100] quit
```

# Configure DHCP address pool **200**. The switch will use this pool to assign an IP address to the client. In this example, the address of the DNS server is 112.13.1.26 (the gateway address). You must replace it with the actual address of the DNS server on your network.

```
[Switch] dhcp server ip-pool 200
[Switch-dhcp-pool-200] network 112.13.0.0 mask 255.255.0.0
[Switch-dhcp-pool-200] gateway-list 112.13.1.26
[Switch-dhcp-pool-200] dns-list 112.13.1.26
[Switch-dhcp-pool-200] quit
```

# Enable DHCP

```
[Switch] dhcp enable
```

## Configuring the RADIUS server

In this example, the RADIUS server runs INC PLAT 7.3 (E0605) and INC UAM 7.1 (E0302).

### Adding AC 1 and AC 2 to INC as access devices

This example only illustrates the process to add AC 1 to INC as an access device. You can add access device AC 2 to INC in the same way AC 1 is added to INC as an access device.

To add AC 1 to INC as an access device:

1. Log in to INC and click the **User** tab.
2. From the navigation tree, select **User Access Policy > Access Device Management > Access Device**.
3. Click **Add**.  
The **Add Access Device** page opens.
4. In the **Device List** area, click **Add Manually** to add AC 1 at 112.12.1.25 as an access device. This IP address is the source IP address specified on the AC for outgoing RADIUS packets.
5. In the **Access Configuration** area, configure the following parameters, as shown in [Figure 2](#):
  - Enter **123456789** in the **Shared Key** and **Confirm Shared Key** fields.  
The key is consistent with the shared key configured on the AC.
  - Use the default values for other parameters.
6. Click **OK**.

**Figure 2 Adding an access device**

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

Access Configuration

Authentication Port \* 1812 Accounting Port \* 1813

Service Type Unlimited Forcible Logout Type Disconnect user

Access Device Type H3C (General) Service Group Ungrouped

Shared Key \* \*\*\*\*\* Confirm Shared Key \* \*\*\*\*\*

Access Location Group ---

Device List

Select Add Manually Clear All

| Device Name | Device IP   | Device Model | Comments | Delete |
|-------------|-------------|--------------|----------|--------|
|             | 112.12.1.25 |              |          |        |

Total Items: 1.

OK Cancel

## Adding an access policy

1. Click the **User** tab.
2. From the navigation tree, select **User Access Policy > Access Policy**.
3. Click **Add**.
4. On the **Add Access Policy** page, configure the following parameters, as shown in [Figure 3](#):
  - o Enter **office** in the **Access Policy Name** field.
  - o Use the default values for other parameters.
5. Click **OK**.

**Figure 3 Adding an access policy**

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

Basic Information

Access Policy Name \* office

Service Group \* Ungrouped

Description

Authorization Information

Access Period None Allocate IP \* No

Downstream Rate (Kbps) Upstream Rate (Kbps)

Priority Deploy User Group

Preferred EAP Type EAP-MD5

EAP Auto Negotiate Enable

Maximum Online Duration for a Logon (Minutes)

Deploy Address Pool

Deploy User Profile

Deploy VLAN

Deploy VSI name

Authentication Password Account Password

Offline Check Period (Hours)

## Adding an access service

1. Click the **User** tab.
2. From the navigation tree, select **User Access Policy > Access Service**.
3. Click **Add**.
4. On the **Add Access Service** page, configure the following parameters, as shown in [Figure 4](#):
  - o Enter **office\_mac** in the **Service Name** field.
  - o Select **office** from the **Default Access Policy** list.
  - o Use the default values for other parameters.
5. Click **OK**.

**Figure 4 Adding an access service**

## Adding an access user

1. Click the **User** tab.
2. From the navigation tree, select **Access User > Access User**.  
The access user list opens.
3. Click **Add**.  
The **Add Access User** page opens.
4. In the **Access Information** area, add a user, as shown in [Figure 5](#):
  - a. Click **Add User**.
  - b. On the dialog box that opens, enter **adm\_office\_mac** in the **User Name** and **Identity Number** fields.
  - c. Click **Check Availability** to verify the validity of the username and identity number.
  - d. Click **OK**.
5. In the **Access Information** area, configure the following parameters, as shown in [Figure 6](#):
  - o Enter **3891d5833b20** in the **Account Name** field.
  - o Enter **3891d5833b20** in the **Password** and **Confirm Password** fields.
6. In the **Access Service** area, select **office\_mac** from the list.
7. Click **OK**.

**Figure 5 Adding a user**

**Figure 6 Adding an access user account**

User > All Access Users > Add Access User

Access Information

User Name \*  Select Add User

Account Name \*

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

Password \*  Confirm Password \*

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

Start Time  End Time

Max. Idle Time (Minutes)  Max. Concurrent Logins

Login Message

Access Service

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

## Verifying the configuration

1. Verify the AC backup and switchover functionality:

# Verify that the AP associates with AC 1 and comes online. (Details not shown.)

# Shut down VLAN-interface 100 on AC 1. (Details not shown.)

# Verify that the AP automatically associates with AC 2 and comes online in less than 3 minutes, during which traffic is interrupted. The state of the AP changes to **R/M (Run/Master)** on AC 2 after it comes up.

```
[AC2] display wlan ap all
```

```
Total number of APs: 1
```

```
Total number of connected APs: 1
```

```
Total number of connected manual APs: 1
```

```
Total number of connected auto APs: 0
```

```
Total number of connected common APs: 1
```

```
Total number of connected WTUs: 0
```

```
Total number of inside APs: 0
```

```
Maximum supported APs: 512
```

```
Remaining APs: 511
```

```
Total AP licenses: 128
```

```
Local AP licenses: 128
```

```
Server AP licenses: 0
```

```
Remaining local 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 | APID | State | Model   | Serial ID            |
|---------|------|-------|---------|----------------------|
| ap1     | 2    | R/M   | AP 3620 | 219801A28N819CE0002T |

# Bring up VLAN-interface 100 on AC 1. (Details not shown.)

# Verify that the AP re-associates with AC 1 and its state changes to **R/M (Run/Master)** on AC 1 after a successful association. At the same time, the state of the AP changes to **R/B** on AC 2.

```
[AC1] display wlan ap all
```

```
...
```

```
[AC2] display wlan ap all
```

```
Total number of APs: 1
```

```
Total number of connected APs: 1
```

```
Total number of connected manual APs: 1
```

```
Total number of connected auto APs: 0
```

```
Total number of connected common APs: 1
```

```
Total number of connected WTUs: 0
```

```
Total number of inside APs: 0
```

```
Maximum supported APs: 512
```

```
Remaining APs: 511
```

```
Total AP licenses: 128
```

```
Local AP licenses: 128
```

```
Server AP licenses: 0
```

```
Remaining local AP licenses: 128
```

```
Sync AP licenses: 0
```

#### AP information

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

| AP name | APID | State | Model   | Serial ID            |
|---------|------|-------|---------|----------------------|
| ap1     | 2    | R/B   | AP 3620 | 219801A28N819CE0002T |

2. Connect the client to the wireless network. (Details not shown.)
3. On AC 1, verify that the client has passed MAC authentication and PSK authentication and come online in VLAN 200.

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

```
Total Number of Clients : 1
```

| MAC address    | Username     | AP name | RID | IP address | IPv6 address | VLAN |
|----------------|--------------|---------|-----|------------|--------------|------|
| 3891-d583-3b20 | 3891d5833b20 | ap1     | 2   | 112.13.0.2 | N/A          | 200  |

## Configuration files

- AC 1:

```
#
dhcp enable
#
vlan 1
#
vlan 100
#
vlan 200

#
wlan service-template 1
 ssid service
```

```

vlan 200
client forwarding-location ac
akm mode psk
preshared-key pass-phrase cipher c3$heDUT35pq2/Zmsuy18nxS3vSHAeolC6kobTrDA==
cipher-suite ccmp
security-ie rsn
client-security authentication-mode mac
mac-authentication domain officel
service-template enable
#
interface Vlan-interface100
ip address 112.12.1.25 255.255.0.0
#
interface Vlan-interface200
ip address 112.13.1.25 255.255.0.0
#
interface GigabitEthernet1/0/1
port link-type trunk
port trunk permit vlan 100 200
#
radius scheme office
primary authentication 8.1.1.50
primary accounting 8.1.1.50
key authentication cipher c3$o/3Ueu4pLSdJ0r1kLdAwzJU/AaBGCxnGuBXHmQ==
key accounting cipher c3$oKqS/GRbPQc8AG+Vp+bJO4ZPK1k5+ceFuye/tQ==
user-name-format without-domain
nas-ip 112.12.1.25
#
domain officel
authorization-attribute idle-cut 15 1024
authentication lan-access radius-scheme office
authorization lan-access radius-scheme office
accounting lan-access radius-scheme office
#
wlan ap ap1 model AP 3620
serial-id 219801A28N819CE0002T
#
wlan ap-group group1
ap ap1
wlan tunnel-preempt enable
priority 7
backup-ac ip 112.12.2.8
ap-model AP 3620
radio 1
radio 2
radio enable
service-template 1
#

```



- AC 2:

```
#
dhcp enable
#
vlan 1
#
vlan 100
#
vlan 200

#
wlan service-template 1
 ssid service
 vlan 200
 client forwarding-location ac
 akm mode psk
 preshared-key pass-phrase cipher c3$heDUT35pq2/Zmsuy18nxS3vSHAeolC6kobTrDA==
 cipher-suite ccmp
 security-ie rsn
 client-security authentication-mode mac
 mac-authentication domain officel
 service-template enable
#
interface Vlan-interface100
 ip address 112.12.2.8 255.255.0.0
#
interface Vlan-interface200
 ip address 112.13.3.5 255.255.0.0
#
interface GigabitEthernet1/0/1
port link-type trunk
 port trunk permit vlan 100 200
#
radius scheme office
 primary authentication 8.1.1.50
 primary accounting 8.1.1.50
 key authentication cipher c3$o/3Ueu4pLSdJ0r1kLdAwzJU/AaBGCxnGuBXHmQ==
 key accounting cipher c3$oKqS/GRbPQc8AG+Vp+bJO4ZPK1k5+ceFuye/tQ==
 user-name-format without-domain
 nas-ip 112.12.2.8
#
domain officel
 authorization-attribute idle-cut 15 1024
 authentication lan-access radius-scheme office
 authorization lan-access radius-scheme office
 accounting lan-access radius-scheme office
#
wlan ap ap1 model AP 3620
```

```

 serial-id 219801A28N819CE0002T
#
wlan ap-group group1
ap ap1
wlan tunnel-preempt enable
 priority 5
 backup-ac 112.12.1.25
ap-model AP 3620
 radio 1
 radio 2
 radio enable
 service-template 1
#
● Switch:
#
vlan 1
#
vlan 100
#
vlan 200
#
dhcp server ip-pool 100
 gateway-list 112.12.1.26
 network 112.12.0.0 mask 255.255.0.0
#
dhcp server ip-pool 200
 gateway-list 112.13.1.26
 dns-list 112.13.1.26
 network 112.13.0.0 mask 255.255.0.0
#
interface Vlan-interface100
 ip address 112.12.1.26 255.255.0.0
#
interface Vlan-interface200
 ip address 112.13.1.26 255.255.0.0
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 100 200
#
interface GigabitEthernet1/0/3
 port link-type trunk
 port trunk permit vlan 100 200
#
interface GigabitEthernet1/0/2
 port access vlan 100
 poe enable
#

```

# Related documentation

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