

# INTELBRAS Access Controllers WIPS 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 WIPS.....	1
Network configuration.....	1
Restrictions and guidelines .....	2
Procedures .....	2
Configuring the AC.....	2
Configuring the switch .....	5
Verifying the configuration .....	5
Configuration files.....	6
Related documentation .....	8

# Introduction

The following information provides examples for configuring WIPS.

## Prerequisites

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

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

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

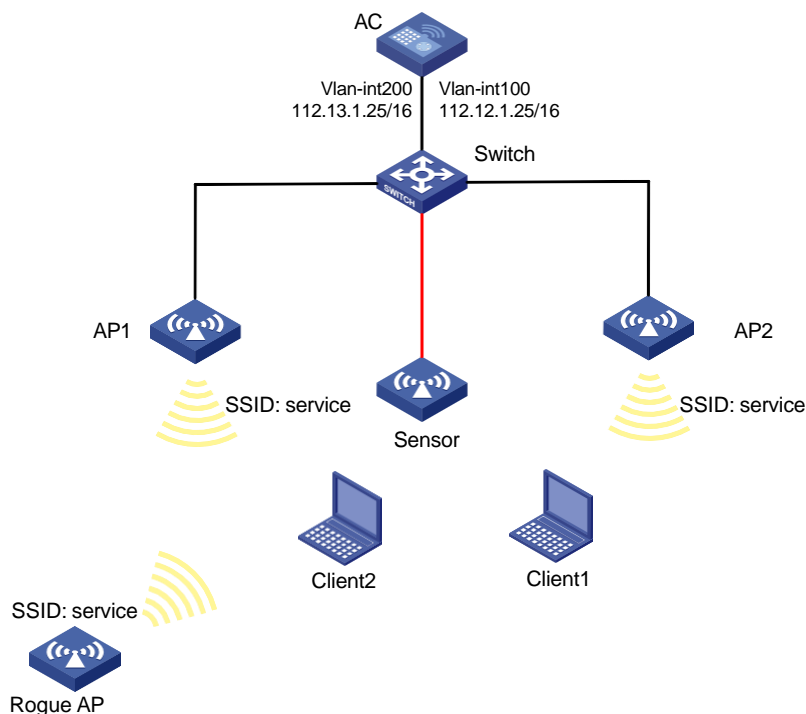
## Example: Configuring WIPS

### Network configuration

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

Enable WIPS on the sensor to take countermeasures against the rogue AP that uses the same SSID as AP 1 and AP 2.

**Figure 1 Network diagram**



# Restrictions and guidelines

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

## Procedures

### Configuring the AC

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

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

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

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

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

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

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

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

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

#### 2. Configure DHCP:

# Enable DHCP on the AC.

```
[AC] dhcp enable
```

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

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

# Specify gateway IP address 112.12.1.25 in the DHCP address pool.

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

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

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

# Specify gateway IP address 112.13.1.25 in the DHCP address pool.

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

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

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

### 3. Configure WIPS:

# Enter WIPS view.

```
[AC] wips
```

# Create AP classification rule 1 and configure the rule to match APs that use SSID **service**.

```
[AC-wips] ap-classification rule 1
[AC-wips-clr-rule-1] ssid equal service
[AC-wips-clr-rule-1] quit
```

# Create classification policy **class1**.

```
[AC-wips] classification policy class1
```

# Bind AP classification rule 1 to classification policy **class1**, and specify APs that match AP classification rule 1 as rogue APs.

```
[AC-wips-clr-class1] apply ap-classification rule 1 rogue-ap
[AC-wips-clr-class1] quit
```

# Create virtual security domain (VSD) **vsd1**, and apply classification policy **class1** to the VSD.

```
[AC-wips] virtual-security-domain vsd1
[AC-wips-vsd-1] apply classification policy class1
[AC-wips-vsd-1] quit
```

# Create countermeasure policy 1 and enable WIPS to take countermeasures against rogue APs.

```
[AC-wips] countermeasure policy 1
[AC-wips-cms-1] countermeasure rogue-ap
[AC-wips-cms-1] quit
```

# Apply countermeasure policy 1 to VSD **vsd1**.

```
[AC-wips] virtual-security-domain vsd1
[AC-wips-vsd-vsd1] apply countermeasure policy 1
[AC-wips-vsd-vsd1] quit
[AC-wips] quit
```

### 4. Configure the APs:

---

#### NOTE:

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

---

# Create service template **service** and set its SSID to **service**.

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

# Assign clients that come online through service template **service** to VLAN 200.

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

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

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

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

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

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

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

# Enable service template **service**.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

# Enable radio 1.

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

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

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

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

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

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

```
[AC-wlan-ap-sensor] serial-id 219801A28N819CE0004T
```

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

# Create AP group **group2** and add the AP to the AP group.

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

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

# Bind service template **service** to radio 1 in AP group **group2**.

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

```
[AC-wlan-ap-group-group2-ap-model-AP 3620] radio 1
```

# Enable radio 1.

```
[AC-wlan-ap-group-group2-ap-model-AP 3620-radio-1] radio enable
```

# Enable WIPS for the radio and add AP **sensor** to VSD **vsd1**.

```
[AC-wlan-ap-group-group2-ap-model-AP 3620-radio-1] wips
```

```
enable [AC-wlan-ap-group-group2-ap-model-AP 3620-radio-1]
```

```
quit
```

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

```
[AC-wlan-ap-group-group2] wips virtual-security-domain vsd1
```

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

## Configuring the switch

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

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

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

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

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

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

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

```
[Switch] interface gigabitethernet1/0/2
[Switch-GigabitEthernet1/0/2] port link-type access
[Switch-GigabitEthernet1/0/2] port access vlan 100
```

# Enable PoE on the access port.

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

# Configure GigabitEthernet 1/0/3 that connects the switch to AP **ap1** as an access port, and assign the port to VLAN 100.

```
[Switch] interface gigabitethernet1/0/3
[Switch-GigabitEthernet1/0/3] port link-type access
[Switch-GigabitEthernet1/0/3] port access vlan 100
```

# Enable PoE on the access port.

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

# Configure GigabitEthernet 1/0/4 that connects the switch to AP **ap2** as an access port, and assign the port to VLAN 100.

```
[Switch] interface gigabitethernet1/0/4
[Switch-GigabitEthernet1/0/4] port link-type access
[Switch-GigabitEthernet1/0/4] port access vlan 100
```

# Enable PoE on the access port.

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

## Verifying the configuration

1. Verify that WIPS has classified the AP that uses SSID **service** as a rogue AP and the service APs as authorized APs.

```
<AC> display wips virtual-security-domain vsd1 device
Total 3 detected devices in virtual-security-domain vsd1
```

Class: Auth - authorization; Ext - external; Mis - mistake;  
 Unauth - unauthorized; Uncate - uncategorized;  
 (A) - associate; (C) - config; (P) - potential

MAC address	Type	Class	Duration	Sensors	Channel	Status
000f-1111-0101	AP	Auth	00h 05m 24s 1		161	Active
000f-1111-0111	AP	Auth	00h 05m 26s 1		13	Active
000f-e200-1202	AP	Rogue	00h 05m 26s 1		161	Active

## 2. Verify that WIPS has taken countermeasures against the rogue AP.

```
<AC> display wips virtual-security-domain vsd1 countermeasure record
```

Total 1 times countermeasure, current 1 countermeasure record in  
 virtual-security-domain vsd1

Class: Auth - authorization; Ext - external; Mis - mistake;  
 Unauth - unauthorized; Uncate - uncategorized;  
 (A) - associate; (C) - config; (P) - potential

MAC address	Type	Class	Sensor name	Radio ID	Time
000f-e200-1202	AP	Rogue	sensor	1	2015-11-27/15:52:53

# Configuration files

- AC:
 

```
#
dhcp enable
#
vlan 100
#
vlan 200
#
dhcp server ip-pool vlan100
gateway-list 112.12.1.25
network 112.12.0.0 mask 255.255.0.0
#
dhcp server ip-pool vlan200
gateway-list 112.13.1.25
network 112.13.0.0 mask 255.255.0.0
dns-list 112.13.1.25
#
wlan service-template service
ssid service
vlan 200
client forwarding-location ac
akm mode psk
preshared-key pass-phrase cipher $c$3$j4R+Ff8S4XNa/uaUjAgwUO5fbtdy+yVXzC+Z
cipher-suite ccmp
security-ie rsn
```



```

    service-template enable
#
interface Vlan-interface100
    ip address 112.12.1.25 255.255.0.0
#
interface Vlan-interface200
    ip address 112.13.1.25 255.255.0.0
#
interface GigabitEthernet1/0/1
    port link-type trunk
    undo port trunk permit vlan 1
    port trunk permit vlan 100 200
#
wlan ap-group group1
    vlan 1
    ap ap1
    ap ap2
    ap-model AP 3620
        radio 1
            radio enable
            service-template service
        radio 2
            gigabitethernet 1
#
wlan ap-group group2
    vlan 1
    ap sensor
    wips virtual-security-domain vsd1
    ap-model AP 3620
        radio 1
            radio enable
            wips enable
        radio 2
            gigabitethernet 1
#
wlan ap ap1 model AP 3620
    serial-id 219801A2N819CE0002T
#
wlan ap ap2 model AP 3620
    serial-id 219801A2N819CE0004T
#
wlan ap sensor model AP 3620
    serial-id 219801A2N819CE0004T
#
wips
#
    ap-classification rule 1
        ssid equal service

```

```

#
classification policy class1
  apply ap-classification rule 1 rogue-ap
#
countermeasure policy 1
  countermeasure rogue-ap
#
virtual-security-domain vsd1
  apply classification policy class1
  apply countermeasure policy 1
#

```

- **Switch:**

```

#
vlan 100
#
vlan 200
#
interface GigabitEthernet1/0/1
  port link-type trunk
  undo port trunk permit vlan 1
  port trunk permit vlan 100
#
interface GigabitEthernet1/0/2
  port access vlan 100
poe enable
#
interface GigabitEthernet1/0/3
  port access vlan 100
poe enable
#
interface GigabitEthernet1/0/4
  port access vlan 100
poe enable
#

```

## Related documentation

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

# WIPS Countermeasures Against All SSIDs 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 WIPS countermeasures against all SSIDs .....	1
Network configuration .....	1
Procedures .....	2
Configuring the AC .....	2
Configuring the switch .....	5
Verifying the configuration .....	6
Configuration files .....	6
Related documentation .....	9

# Introduction

The following information provides examples for configuring WIPS countermeasures against all SSIDs.

## Prerequisites

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

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

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

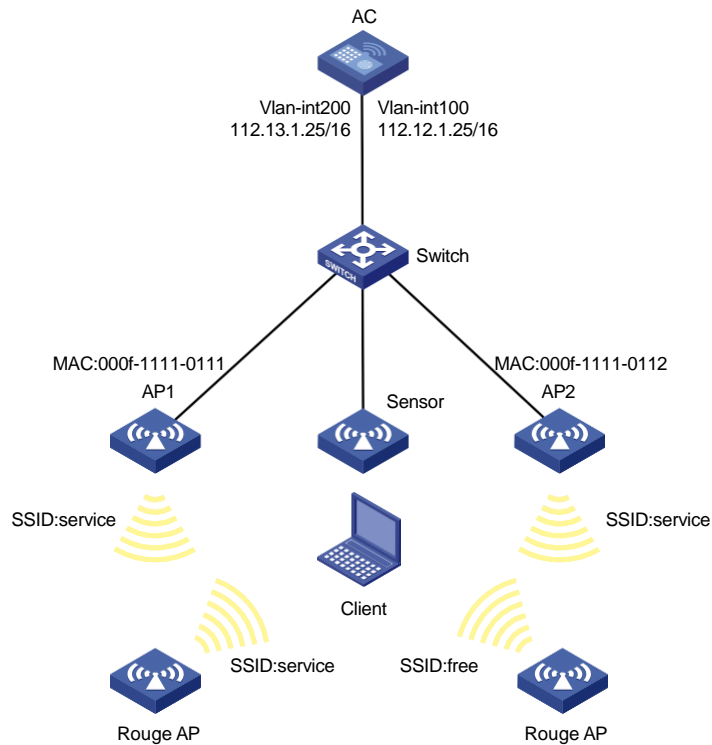
## Example: Configuring WIPS countermeasures against all SSIDs

### Network configuration

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

Enable WIPS on the sensor to take countermeasures against the rogue AP that uses SSID **service** and SSID **free**.

**Figure 1 Network diagram**



## Procedures

### Configuring the AC

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

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

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

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

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

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

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

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

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

## 2. Configure DHCP:

# Enable DHCP on the AC.

```
[AC] dhcp enable
```

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

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

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

# Specify gateway IP address 112.12.1.25 in the DHCP address pool.

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

```
[AC-dhcp-pool-vlan100] quit
```

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

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

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

# Specify gateway IP address 112.13.1.25 in the DHCP address pool.

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

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

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

```
[AC-dhcp-pool-vlan200] quit
```

## 3. Configure WIPS:

# Enter WIPS view.

```
[AC] wips
```

# Create AP classification rule 1 and configure the rule to match APs that use SSID **service**.

```
[AC-wips] ap-classification rule 1
```

```
[AC-wips-cls-rule-1] ssid equal service
```

```
[AC-wips-cls-rule-1] quit
```

# Create AP classification rule 2 and configure the rule to match APs that do not use SSID **service**.

```
[AC-wips] ap-classification rule 2
```

```
[AC-wips-cls-rule-2] ssid not equal service
```

```
[AC-wips-cls-rule-2] quit
```

# Create classification policy **class1**.

```
[AC-wips] classification policy class1
```

# Bind AP classification rule 1 to classification policy **class1**, specify APs that match AP classification rule 1 as rogue APs, and set the severity level to 100.

```
[AC-wips-cls-class1] apply ap-classification rule 1 rogue-ap severity-level 100
```

# Bind AP classification rule 2 to classification policy **class1**, specify APs that match AP classification rule 2 as rogue APs, and set the severity level to 100.

```
[AC-wips-cls-class1] apply ap-classification rule 2 rogue-ap severity-level 100
```

# Add MAC addresses 000f-1111-0111 and 000f-1111-0112 to the permitted device list.

```
[AC-wips-cls-class1] trust mac-address 000f-1111-0111
```

```
[AC-wips-cls-class1] trust mac-address 000f-1111-0112
```

```
[AC-wips-cls-class1] quit
```

# Create virtual security domain (VSD) **vsd1**, and apply classification policy **class1** to the VSD.

```
[AC-wips] virtual-security-domain vsd1
```

```
[AC-wips-vsd-1] apply classification policy class1
[AC-wips-vsd-1] quit
```

**# Create countermeasure policy 1 and enable WIPS to take countermeasures against rogue APs.**

```
[AC-wips] countermeasure policy 1
[AC-wips-cms-1] countermeasure rogue-ap
[AC-wips-cms-1] quit
```

**# Apply countermeasure policy 1 to VSD vsd1.**

```
[AC-wips] virtual-security-domain vsd1
[AC-wips-vsd-vsd1] apply countermeasure policy 1
[AC-wips-vsd-vsd1] quit
[AC-wips] quit
```

#### 4. Configure the APs:

---

##### NOTE:

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

---

**# Create service template **service** and set its SSID to **service**.**

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

**# Assign clients that come online through service template **service** to VLAN 200.**

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

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

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

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

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

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

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

**# Enable service template **service**.**

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

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

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

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

```
[AC] wlan ap ap2 model AP 3620
[AC-wlan-ap-ap2] serial-id 219801A28N819CE0003T
[AC-wlan-ap-ap2] quit
```

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

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

**# Bind service template **service** to radio 1 in **group1**.**

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



```

[AC-wlan-ap-group-group1-ap-model-AP 3620-radio-1] service-template service
# Enable radio 1.
[AC-wlan-ap-group-group1-ap-model-AP 3620-radio-1] radio
enable [AC-wlan-ap-group-group1-ap-model-AP 3620-radio-1] quit
[AC-wlan-ap-group-group1-ap-model-AP 3620]
quit [AC-wlan-ap-group-group1] quit
# Create AP sensor and specify its model and serial ID.
[AC] wlan ap sensor model AP 3620
[AC-wlan-ap-sensor] serial-id 219801A28N819CE0004T
[AC-wlan-ap-sensor] quit
# Create AP group group2 and add the AP to the AP group.
[AC] wlan ap-group group2
[AC-wlan-ap-group-group2] ap sensor
# Enable radio 1.
[AC-wlan-ap-group-group2] ap-model AP 3620
[AC-wlan-ap-group-group2-ap-model-AP 3620] radio 1
[AC-wlan-ap-group-group2-ap-model-AP 3620-radio-1] radio enable
# Enable WIPS for the radio and add AP sensor to VSD vsd1..
[AC-wlan-ap-group-group2-ap-model-AP 3620-radio-1] wips
enable [AC-wlan-ap-group-group2-ap-model-AP 3620-radio-1]
quit
[AC-wlan-ap-group-group2-ap-model-AP 3620] quit
[AC-wlan-ap-group-group2] wips virtual-security-domain vsd1
[AC-wlan-ap-group-group2] return

```

## Configuring the switch

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

```

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

```

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

```

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

```

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

```

[Switch-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[Switch-GigabitEthernet1/0/1] port trunk permit vlan 100 200

```

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

```

[Switch] interface gigabitethernet1/0/2
[Switch-GigabitEthernet1/0/2] port link-type access
[Switch-GigabitEthernet1/0/2] port access vlan 100

```

# Enable PoE on the access port.

```

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

```

# Configure GigabitEthernet 1/0/3 that connects the switch to AP **ap1** as an access port, and assign the port to VLAN 100.

```
[Switch] interface gigabitethernet1/0/3
[Switch-GigabitEthernet1/0/3] port link-type access
[Switch-GigabitEthernet1/0/3] port access vlan 100
```

# Enable PoE on the access port.

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

# Configure GigabitEthernet 1/0/4 that connects the switch to AP **ap2** as an access port, and assign the port to VLAN 100.

```
[Switch] interface gigabitethernet1/0/4
[Switch-GigabitEthernet1/0/4] port link-type access
[Switch-GigabitEthernet1/0/4] port access vlan 100
```

# Enable PoE on the access port.

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

## Verifying the configuration

1. Verify that WIPS has classified the AP that uses all SSIDs as a rogue AP and the service APs as authorized APs.

```
<AC> display wips virtual-security-domain vsd1 device
Total 3 detected devices in virtual-security-domain vsd1
```

```
Class: Auth - authorization; Ext - external; Mis - mistake;
Unauth - unauthorized; Uncate - uncategorized;
(A) - associate; (C) - config; (P) - potential
```

MAC address	Type	Class	Duration	Sensors	Channel	Status
000f-1111-0111	AP	Auth	00h 05m 26s 1	161		Active
000f-1111-0112	AP	Auth	00h 05m 26s 1	161		Active
000f-e200-1202	AP	Rogue	00h 05m 26s 1	161		Active
000f-e200-1222	AP	Rogue	00h 05m 26s 1	161		Active

2. Verify that WIPS has taken countermeasures against the rogue AP.

```
<AC> display wips virtual-security-domain vsd1 countermeasure record
Total 2 times countermeasure, current 2 countermeasure record in
virtual-security-domain vsd1
```

```
Reason: Attack; Ass - associated; Black - blacklist;
Class - classification; Manu - manual;
```

MAC address	Type	Reason	Countermeasure	AP	Radio ID	Time
000f-e200-1202	AP	Class	sensor		1	2019-09-20/07:20:38
000f-e200-1222	AP	Class	sensor		1	2019-09-20/07:20:38

## Configuration files

- AC:

```

#
dhcp enable
#
vlan 100
#
vlan 200
#
dhcp server ip-pool vlan100
    gateway-list 112.12.1.25
    network 112.12.0.0 mask 255.255.0.0
#
dhcp server ip-pool vlan200
    gateway-list 112.13.1.25
    network 112.13.0.0 mask 255.255.0.0
    dns-list 112.13.1.25
#
wlan service-template service
    ssid service
    vlan 200
    client forwarding-location ac
    akm mode psk
    preshared-key pass-phrase cipher $c$3$jJ5Vq5IaYJJP9g7gA9h4rbGHL1UK/iEIQ1FB
    cipher-suite ccmp
    security-ie rsn
    service-template enable
#
interface Vlan-interface100
    ip address 112.12.1.25 255.255.0.0
#
interface Vlan-interface200
    ip address 112.13.1.25 255.255.0.0
#
interface GigabitEthernet1/0/1
    port link-type trunk
    undo port trunk permit vlan 1
    port trunk permit vlan 100 200
#
wlan ap-group group1
    vlan 1
    ap ap1
    ap ap2
    ap-model AP 3620
        radio 1
            radio enable
            service-template service
        radio 2
            gigabitethernet 1
#

```

```

wlan ap-group group2
  vlan 1
  ap sensor
  wips virtual-security-domain vsd1
  ap-model AP 3620
    radio 1
      radio enable
      wips enable
    radio 2
  gigabitethernet 1
#
wlan ap ap1 model AP 3620
  serial-id 219801A2N819CE0002T
#
wlan ap ap2 model AP 3620
  serial-id 219801A2N819CE0003T
#
wlan ap sensor model 6320
  serial-id 219801A2N819CE0004T
#
wips
#
  ap-classification rule 1
    ssid equal service
#
  ap-classification rule 2
    ssid not equal service
#
  classification policy class1
    apply ap-classification rule 1 rogue-ap severity-level 100
    apply ap-classification rule 2 rogue-ap severity-level 100
    trust mac-address 000f-1111-0111
    trust mac-address 000f-1111-0112

#
  countermeasure policy 1
    countermeasure rogue-ap
#
  virtual-security-domain vsd1
    apply classification policy class1
    apply countermeasure policy 1
#
• Switch:
#
vlan 100
#
vlan 200
#

```

```
interface GigabitEthernet1/0/1
  port link-type trunk
  undo port trunk permit vlan 1
  port trunk permit vlan 100 200
#
interface GigabitEthernet1/0/2
  port access vlan 100
  poe enable
#
interface GigabitEthernet1/0/3
  port access vlan 100
  poe enable
#
interface GigabitEthernet1/0/4
  port access vlan 100
  poe enable
#
```

## Related documentation

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

# INTELBRAS Access Controllers IP Source Guard (IPv4) 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 IPv4SG .....	1
Network configuration .....	1
Restrictions and guidelines .....	1
Procedures .....	2
Configuring the AC .....	2
Configuring the switch .....	3
Verifying the configuration .....	4
Configuration files .....	5
Related documentation .....	7

# Introduction

The following information provides an example for configuring IPv4 source guard (IPv4SG).

## 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.

This document assumes that you have basic knowledge of IPv4SG and WLAN.

## Example: Configuring IPv4SG

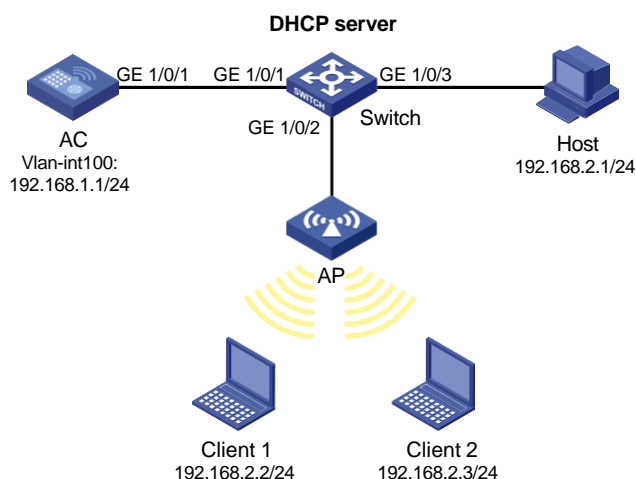
### Network configuration

As shown in [Figure 1](#), the DHCP server assigns IP addresses to Client 1 and the AP. Client 2 is assigned a static IPv4 address.

Configure network settings to meet the following requirements:

- Both of the clients access the same wireless network.
- Enable IPv4SG to generate IPv4SG bindings based on DHCP so that the AP forwards the packets only from Client 1.

**Figure 1 Network diagram**



### Restrictions and guidelines

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



# Procedures

## Configuring the AC

### 1. Configure interfaces on the AC:

# Create VLAN 100 and VLAN-interface 100, and assign IP address 192.168.1.1 to the VLAN interface. The AC will establish a CAPWAP tunnel with the AP in this VLAN.

```
<AC> system-view
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 192.168.1.1 24
[AC-Vlan-interface100] quit
```

# Create VLAN 200. The AC will use this VLAN for client access.

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

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

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

### 2. Configure a wireless service:

# Create service template 1 and enter its view.

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

# Set the SSID to **service**.

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

# Enable snooping DHCP packets on the service template.

```
[AC-wlan-st-1] client ipv4-snooping dhcp-learning enable
```

# Enable IPv4SG on the service template.

```
[AC-wlan-st-1] ip verify source
```

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

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

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

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

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

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

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

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

# Enable service template 1.

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

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

### 3. Configure AP settings:

---

**NOTE:**

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

---

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

```
[AC] wlan ap officeap model AP 3620
[AC-wlan-ap-officeap] serial-id 209801A28N819CE0002T
[AC-wlan-ap-officeap] quit
```

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

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

**# Bind service template 1 and VLAN 200 to radio 1 for AP group `group1`.**

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

**# Enable radio 1.**

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

## Configuring the switch

### 1. Configure switch interfaces:

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

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

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

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

**# Create VLAN-interface 100 that acts as a gateway and assign IP address 192.168.1.254 to the interface.**

```
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 192.168.1.254 24
[AC-Vlan-interface100] quit
```

**# Create VLAN-interface 200 that acts as a gateway and assign IP address 192.168.2.254 to the interface.**

```
[AC] interface vlan-interface 200
[AC-Vlan-interface200] ip address 192.168.2.254 24
[AC-Vlan-interface200] quit
```

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

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

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

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

**# Enable PoE on GigabitEthernet 1/0/2.**

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

**# Configure GigabitEthernet 1/0/3 (port that connects the switch and the host) as an access port, and assign the port to VLAN 200.**

```
[Switch] interface GigabitEthernet1/0/3
[Switch-GigabitEthernet1/0/3] port link-type access
[Switch-GigabitEthernet1/0/3] port access vlan 200
[Switch-GigabitEthernet1/0/3] quit
```

## 2. Configure the DHCP server:

**# Enable DHCP server.**

```
[Switch] dhcp enable
```

**# Create DHCP address pool 1 for dynamic IP allocation to the AP. Specify 192.168.1.0/24 as the subnet and 192.168.1.254 as the gateway address in the address pool.**

```
[Switch] dhcp server ip-pool 1
[Switch-dhcp-pool-1] network 192.168.1.0 mask 255.255.255.0
[Switch-dhcp-pool-1] gateway-list 192.168.1.254
```

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

```
[Switch-dhcp-pool-1] forbidden-ip 192.168.1.1
[Switch-dhcp-pool-1] quit
```

**# Create DHCP address pool 2 for dynamic IP allocation to Client 1 and the host. Specify 192.168.2.0/24 as the subnet and 192.168.2.254 as the gateway address in the address pool, and then specify the address of the DNS server. In this example, the gateway also acts as the DNS server.**

```
[Switch] dhcp server ip-pool 2
[Switch-dhcp-pool-2] network 192.168.2.0 mask 255.255.255.0
[Switch-dhcp-pool-2] gateway-list 192.168.2.254
[Switch-dhcp-pool-2] dns-list 192.168.2.254
[Switch-dhcp-pool-2] quit
```

## Verifying the configuration

**# Client 1 at MAC address 0024-d774-e6f4 comes online and obtains IP address 192.168.2.2/24 through DHCP. (Details not shown.)**

**# Client 2 at MAC address 0024-0130-696b comes online and obtains statically configured IP address 192.168.2.3/24. (Details not shown.)**

**# Verify that Client 1 can ping the host on the same subnet.**

```
C:\Users\>ping -S 192.168.2.2 192.168.2.1
```

```
Pinging 192.168.2.1 from 192.168.2.2 with 32 bytes of data:
```

```
Reply from 192.168.2.1 : time=22ms
```

```
Reply from 192.168.2.1 : time=61ms
```

```
Reply from 192.168.2.1 : time=32ms
```

```

Reply from 192.168.2.1 : time=16ms

Ping statistics for 192.168.2.1 :
    Packets: Sent = 4,Received = 4,Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 16ms, Maximum = 61ms, Average = 32ms

# Verify that Client 2 cannot ping the host.
C:\Users\>ping -S 192.168.2.3 192.168.2.1

Pinging 192.168.2.1 from 192.168.2.3 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.2.1 :
    Packets: Sent = 4,Received = 0,Lost = 4 (100% loss),

```

## Configuration files

```

• AC:
#
vlan 100
#
vlan 200
#
wlan service-template 1
    ssid service
    client forwarding-location ac
    akm mode psk
    preshared-key pass-phrase cipher $c$3$X2Rlx149vpJl58WfBfCMdjt0NpHVdUHApNcS
    cipher-suite ccmp
    security-ie rsn
    ip verify source
    client ipv4-snooping dhcp-learning enable

    service-template enable
#
interface Vlan-interface100
    ip address 192.168.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
    port link-type trunk
    undo port trunk permit vlan 1
    port trunk permit vlan 100 200
#
wlan ap-group group1
    ap officeap

```

```

ap-model AP 3620
  radio 1
    radio enable
    service-template 1 vlan 200
  radio 2
#
wlan ap officeap model AP 3620
  serial-id 209801A28N819CE0002T
#
●    Switch:
#
vlan 100
#
vlan 200
#
dhcp server ip-pool 1
  gateway-list 192.168.1.254
  network 192.168.1.0 mask 255.255.255.0
  forbidden-ip 192.168.1.1
#
dhcp server ip-pool 2
  gateway-list 192.168.2.254
  network 192.168.2.0 mask 255.255.255.0
  dns-list 192.168.2.254
#
interface Vlan-interface100
  ip address 192.168.1.254 255.255.255.0
#
interface Vlan-interface200
  ip address 192.168.2.254 255.255.255.0
#
interface GigabitEthernet1/0/1
  port link-mode bridge
  port link-type trunk
  port trunk permit vlan 100 200
#
interface GigabitEthernet1/0/2
  port link-mode bridge
  port access vlan 100
  poe enable
#
interface GigabitEthernet1/0/3
  port link-mode bridge
  port access vlan 200
#

```

# Related documentation

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

# INTELBRAS Access Controllers IP Source Guard (IPv6) Configuration Examples

---

Copyright © 2024 Intelbras S.A All rights reserved.

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

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

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

# Contents

Introduction .....	1
Prerequisites .....	1
Example: Configuring IPv6SG .....	1
Network configuration .....	1
Restrictions and guidelines .....	1
Procedures .....	2
Configuring the AC .....	2
Configuring the switch .....	3
Verifying the configuration .....	4
Configuration files .....	4
Related documentation .....	5



# Introduction

The following information provides an example for configuring IPv6 source guard (IPv6SG).

## 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.

This document assumes that you have basic knowledge of IPv6SG and WLAN.

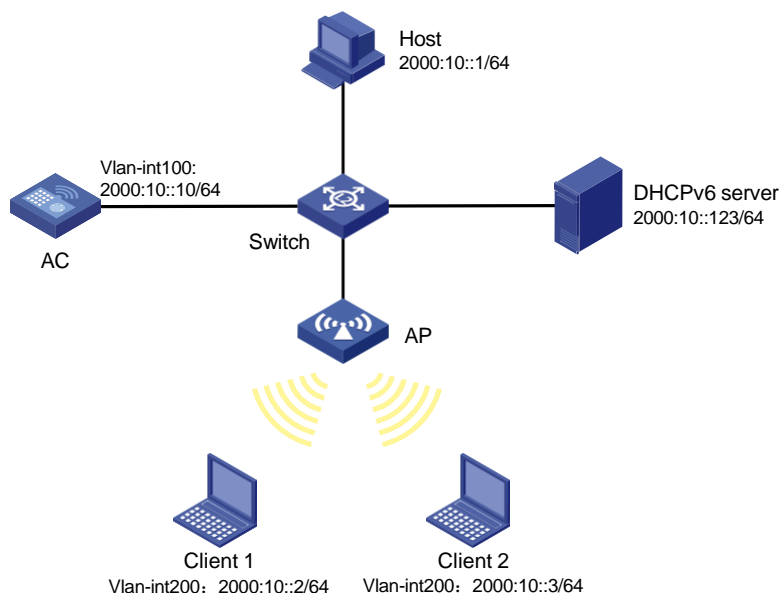
## Example: Configuring IPv6SG

### Network configuration

As shown in [Figure 1](#), Client 1 supports stateful IPv6 address configuration and obtains an IPv6 address through the DHCPv6 server. Client 2 is assigned a static IPv6 address. Both of the clients access the same wireless network.

Enable IPv6SG to generate IPv6SG bindings based on DHCPv6 so that the AP forwards the packets only from Client 1.

**Figure 1 Network diagram**



### Restrictions and guidelines

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

# Procedures

## Configuring the AC

### 1. Configure interfaces on the AC:

# Create VLAN 100 and VLAN-interface 100, and assign an IPv6 address to the VLAN interface. The AC will establish a CAPWAP tunnel with the AP in this VLAN.

```
[AC] vlan 100
[AC-vlan100] quit
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ipv6 address 2000:10::10/64
[AC-Vlan-interface100] quit
```

# Create VLAN 200. The AC will use this VLAN for client access.

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

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

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

### 2. Configure a wireless service:

# Create a service template named 1 and configure the SSID of the service template as **service**.

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

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

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

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

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

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

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

# Enable snooping DHCPv6 and ND packets on the service template.

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

# Enable IPv6SG on the service template.

```
[AC-wlan-st-1] ipv6 verify source
```

# Enable service template 1.

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

### 3. Configure an AP:

---

**NOTE:**

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

---

**# Create an AP named `officeap` with model `AP 3620`, and set its serial ID to `219801A28N819CE0002T`.**

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

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

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

**# Bind service template 1 and VLAN 200 to radio 1 for AP group `group1`.**

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

**# Enable radio 1.**

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

## Configuring the switch

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

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

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

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

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

```
[Switch] interface GigabitEthernet1/0/1
[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 (port that connects the switch and the AP) as an access port, and assign the access port to VLAN 100.**

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

**# Enable PoE on GigabitEthernet 1/0/2.**

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

# Verifying the configuration

# Client 1 at MAC address 0024-d774-e6f4 comes online and obtains IPv6 address 2000:10::2/64 through DHCP. (Details not shown.)

# Client 2 at MAC address 0024-0130-696b comes online and obtains statically configured IPv6 address 2000:10::3/64. (Details not shown.)

# Verify that Client 1 can ping the host on the same subnet.

```
C:\Users\>ping -S 2000:10::2 2000:10::1
```

```
Pinging 2000:10::1 from 2000:10::2 with 32 bytes of data:
```

```
Reply from 2000:10::1 : time=22ms
```

```
Reply from 2000:10::1 : time=61ms
```

```
Reply from 2000:10::1 : time=32ms
```

```
Reply from 2000:10::1 : time=16ms
```

```
Ping statistics for 2000:10::1 :
```

```
Packets: Sent = 4,Received = 4,Lost = 0 (0% loss),
```

```
Approximate round trip times in milli-seconds:
```

```
Minimum = 16ms,Maximum = 61ms,Average = 32ms
```

# Verify that Client 2 cannot ping the host.

```
C:\Users\>ping -S 2000:10::3 2000:10::1
```

```
Pinging 2000:10::1 from 2000:10::3 with 32 bytes of data:
```

```
Request timed out.
```

```
Request timed out.
```

```
Request timed out.
```

```
Request timed out.
```

```
Ping statistics for 2000: 10::1 :
```

```
Packets: Sent = 4,Received = 0,Lost = 4 (100% loss),
```

# Configuration files

- AC:

```
#
vlan 100
#
vlan 200
#
wlan service-template 1
ssid service
client forwarding-location ac
akm mode psk
preshared-key pass-phrase cipher $c$3$F+XVY6sHOZMICJgo1grWmp03hqIH31BV1i2F
cipher-suite ccmp
security-ie rsn
ipv6 verify source
```

```

client ipv6-snooping nd-learning enable
client ipv6-snooping dhcpv6-learning enable
service-template enable
#
interface Vlan-interface100
 ip address 2000:10::10/64
#
interface GigabitEthernet1/0/1
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 100 200
#
wlan ap-group group1
 ap officeap
 ap-model AP 3620
 radio 1
 radio enable
 service-template 1 vlan 200
 radio 2
 gigabitethernet 1
#
wlan ap officeap model AP 3620
 serial-id 219801A28N819CE0002T
#

```

- **Switch:**

```

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

```

## Related documentation

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

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