IP Theft

IP theft

An IP Theft feature is a wireless controller security mechanism that

- detects duplicate IP address usage among connected clients
- assigns precedence to clients based on a defined preference order, and
- blocks or excludes clients attempting to use IP addresses already assigned to others.

The IP Theft feature is enabled by default on the controller. If a wireless client tries to use an IP address assigned to a wired client, the controller marks it as a theft attempt.

Lower the idle timeout to prevent false IP theft

Lower the idle timeout for devices that may switch WLANs while out of range to prevent incorrect IP theft events.

When a device moves between WLANs while out of range of APs, it may retain the same IPv6 link-local address but present a different MAC address. Because the controller cannot immediately detect the move, it may interpret the reuse of the same IP address as an IP theft event.

To avoid this, lower the idle timeout value so the controller can promptly remove stale client entries from the original WLAN. This helps ensure that address reuse by legitimate roaming devices is not mistakenly treated as a theft attempt.

IP preference levels for IP theft detection

The controller uses IP preference levels to resolve conflicts when multiple clients claim the same IP address. These levels determine which client has priority based on the method used to learn the IP address. Preference order for IPv4 clients:

- DHCPv4
- ARP
- Data packets

Preference order for IPv6 clients:

- DHCPv6
- NDP (Neighbor Discovery Protocol)
- Data packets

Additional rules:

- Static wired clients always receive higher preference than dynamically assigned clients.
- Wired clients are prioritized over wireless clients when IP conflicts occur.

Configure IP theft (GUI)

Prevent unauthorized use or reuse of IP addresses by configuring IP theft protections.

Procedure

Step 1 Choose **Configuration** > **Security** > **Wireless Protection Policies** > **Client Exclusion Policies**.

Step 2 Check the **IP Theft or IP Reuse** check box.

Step 3 Click **Apply**.

Configure IP theft (CLI)

Enable IP theft detection and configure client exclusion policies using CLI.

Procedure

Step 1 Enter the global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure the client exclusion policy.

Example:

```
Device(config)# wireless wps client-exclusion ip-theft
```

Configure the IP theft exclusion timer (CLI)

Set the exclusion timer to temporarily block IP addresses suspected of theft on a WLAN.

Procedure

Step 1 Enter the global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure a WLAN policy profile and enter the wireless policy configuration mode.

Example:

```
Device(config)# wireless profile policy profile-policy default-policy-profile
```

Step 3 Specify the timeout, in seconds.

Example:

```
Device(config-wireless-policy)# exclusionlist timeout time-in-seconds
```

The valid range is from zero-2147483647. Enter zero for no timeout.

Add static entries for wired hosts (CLI)

Configure static wired bindings for devices on a VLAN to control IP address and interface assignment.

Note If you configure wired bindings and SVI IP addresses on the device, the device uses those instead of DHCP.

Procedure

Step 1 Enter the global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure the IPv4 or IPv6 static entry.

Example:

```
Device(config)# device-tracking binding vlan vlan-id 20 ipv4-address 20.20.20.5 interface
gigabitEthernet ge-intf-num 1 hardware-or-mac-address 0000.1111.2222
```

Example:

```
Device(config)# device-tracking binding vlan vlan-id 20 ipv6-address 2200:20:20::6 interface
 gigabitEthernet ge-intf-num 1 hardware-or-mac-address 0000.444.3333
```

Use the first option to configure an IPv4 static entry or the second option to create an IPv6 static entry.

Verify IP theft configuration

Use the command to check if the IP theft feature is enabled or not:

```
Device# show wireless wps summary

Client Exclusion Policy
  Excessive 802.11-association failures   : Enabled
  Excessive 802.11-authentication failures: Enabled
  Excessive 802.1x-authentication         : Enabled
  IP-theft                                : Enabled
  Excessive Web authentication failure    : Enabled
  Cids Shun failure                       : Enabled
  Misconfiguration failure                : Enabled
  Failed Qos Policy                       : Enabled
  Failed Epm                              : Enabled
```

Use the commands to view additional details about the IP theft feature:

```
Device# show wireless client summary

Number of Local Clients: 1

MAC Address    AP Name                WLAN State              Protocol Method     Role
-------------------------------------------------------------------------------------------
000b.bbb1.0001 SimAP-1                2    Run                11a      None       Local


Number of Excluded Clients: 1

MAC Address    AP Name                WLAN State              Protocol Method
-------------------------------------------------------------------------------------------
10da.4320.cce9 charlie2               2    Excluded           11ac     None
```

```
Device# show wireless device-tracking database ip

IP                              VLAN  STATE       DISCOVERY   MAC
  ------------------------------------------------------------------------------
  20.20.20.2                     20    Reachable   Local       001e.14cc.cbff
  20.20.20.6                     20    Reachable   IPv4 DHCP   000b.bbb1.0001


Device# show wireless exclusionlist

Excluded Clients

MAC Address       Description          Exclusion Reason               Time Remaining
-------------------------------------------------------------------------------------
10da.4320.cce9                         IP address theft                   59
```

Note Client exclusion timer deletes the entry from exclusion list with a granularity of 10 seconds. The entry is checked to retain or delete after every 10 seconds. There are chances that the running timer value for excluded clients might display negative values upto 10 seconds.

Note When you enable client exclusion, the system adds the client to the exclusion list. This feature does not prevent the client from being deleted.

```
Device# show wireless exclusionlist client mac 12da.4820.cce9 detail

Client State : Excluded
Client MAC Address : 12da.4820.cce9
Client IPv4 Address: 20.20.20.6
Client IPv6 Address: N/A
Client Username: N/A
Exclusion Reason : IP address theft
Authentication Method : None
Protocol: 802.11ac
AP MAC Address : 58ac.780e.08f0
AP Name: charlie2
AP slot : 1
Wireless LAN Id : 2
Wireless LAN Name: mhe-ewlc
VLAN Id : 20
```

Feature history for SAE client exclusion visibility

Table 1: Feature history

Feature Name	Release Information	Feature Description
SAE client exclusion visibility	Cisco IOS XE 17.18.2	The SAE authentication client exclusion feature overcomes the limitations of Flex central authentication deployments with SAE-enabled WLANs. The feature reports client authentication failures and exclusion data to the controller. It generates syslog messages for these events and allows administrators to configure the duration that a client remains excluded. It centralizes troubleshooting information that was previously only available on individual Access Points, reducing the need for manual log collection.

SAE client exclusion visibility

SAE client exclusion visibility is a feature that

- addresses a limitation in Flex central authentication deployments with SAE-enabled WLANs
- makes client exclusion list data available on the controller, and
- reduces manual log collection for customers.

In Flex central authentication deployments with SAE enabled WLANs, the controller does not have access to client exclusion list data because SAE authentication messages are processed at the AP, and authentication failures are not reported to the controller. As a result, you must collect logs manually, which increases operational costs. This feature provides a solution to this issue.

This feature addresses only Flex central authentication, WPA3 + SAE/FT-SAE/SAE-EXT-KEY/FT-SAE-EXT-KEY WLANs.

Configure client exclusion timeout (GUI)

To set the duration for which a client remains excluded from the system using the GUI.

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Policy**.

Step 2 In the **General** tab, specify the name and description for the policy profile.

Step 3 Click the **Advanced** tab.

Step 4 In the **WLAN Timeout** section, enter a value for the **Client Exclusion Timeout** field, in seconds. This option is enabled by default. The valid range is 0 to 2,147,483,647 seconds. The default is 60 seconds.

Step 5 Click **Apply to Device**.

The system enables and configures the SAE authentication client exclusion feature for the selected wireless policy profile.

What to do next

Monitor excluded clients.

Monitor client exclusion

Monitor excluded clients.

Procedure

Step 1 Choose **Monitoring** > **Wireless** > **Clients**.

Step 2 Click the **Excluded Clients** tab.
The excluded clients and their details are listed on this page. Additionally, you can add an excluded client by clicking the **Add** button and entering the MAC address and the description.

Configure client exclusion timeout (CLI)

Set the duration for which a client remains excluded from the system.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure a policy profile for the WLAN.

Example:

```
Device# wireless profile policy policy-profile-name
```

Replace `policy-profile-name` with the name of your wireless policy profile. For example, `flex-profile-policy`.

Step 3 Disable central DHCP for locally switched clients.

Example:

```
Device(config-wireless-policy)# no central dhcp
```

Step 4 Disable central switching.

Example:

```
Device(config-wireless-policy)# no central switching
```

Step 5 Enable or disable exclusion listing on the WLAN by setting the exclusion time for the client. This feature is enabled by default.

Example:

```
Device(config-wireless-policy)# [no] exclusionlist timeout seconds
```

The timeout is set in seconds. The default is 60 seconds. The valid range is from 0 to 2,147,483,647 seconds. If you set the value to 0, the client remains excluded indefinitely.

Use the **no** form of this command to disable the feature.

The specified exclusion timeout is applied to the WLAN policy profile. This duration determines how long the excluded clients remain unable to connect.

```
Device# configure terminal
Device(config)# wireless profile policy default-policy-profile
Device(config-wireless-policy)# no central dhcp
Device(config-wireless-policy)# no central switching
Device(config-wireless-policy)# [no] exclusionlist timeout 60
```

Verify client exclusion data

Verify client exclusion data using these commands.

Verify the wireless policy profile information, including the exclusion status and timeout for clients, using this command:

```
Device# show wireless profile policy detailed flex-profile-policy
WLAN Switching Policy
  Flex Central Switching            : DISABLED
  Flex Central Authentication       : ENABLED
  Flex Central DHCP                 : DISABLED
  Flex NAT PAT                      : DISABLED

Exclusionlist Params
  Exclusionlist                     : ENABLED
  Exclusion Timeout                 : 60
```

View a summary of wireless clients, including information about excluded clients, using this command:

```
Device# show wireless client summary
Number of Clients: 0
Number of Excluded Clients: 1
MAC Address AP Name Type ID State Protocol Method
 ------------------------------------------------------------------------------------------------

90XX.84XX.63XX WLAN 3 Excluded N/A None
```

Verify the list of excluded wireless clients using this command:

```
Device# show wireless exclusionlist
Number of Excluded Clients : 1
MAC Address Description Exclusion Reason Time Remaining
```

```
---------------------------------------------------------------------------------------------------

90XX.84XX.63XX          SAE authentication failure 49
```