



CHAPTER 43

Tracking Host Aging

This chapter describes how to configure IP device tracking with 802.1x, MAC authentication bypass, Web-proxy based authentication and EoU on the Catalyst 6500 series switches.



Note For complete syntax and usage information for the commands that are used in this chapter, refer to the *Catalyst 6500 Series Switch Command Reference* publication.



Note For information on configuring IEEE 802.1X authentication, see [Chapter 40, “Configuring 802.1X Authentication.”](#)



Note For information on configuring MAC Authentication Bypass, see [Chapter 41, “Configuring MAC Authentication Bypass.”](#)



Note For information on configuring Web-Based Proxy Authentication, see [Chapter 42, “Configuring Web-Based Proxy Authentication.”](#)



Note For information on configuring EoU, see [Chapter 44, “Configuring Network Admission Control.”](#)

This chapter consists of the following sections:

- [Understanding How Host Aging is Tracked, page 43-2](#)
- [Configuring IP Device Tracking Globally, page 43-2](#)
- [Enabling or Disabling IP Device Tracking on a Port with 802.1x Authentication, page 43-4](#)
- [Enabling or Disabling IP Device Tracking on a Port with MAC Authentication Bypass, page 43-4](#)
- [Enabling or Disabling IP Device Tracking on a Port with Web-Based Proxy Authentication, page 43-5](#)

Understanding How Host Aging is Tracked

Layer 2 authentication features, 802.1x, and MAC authentication bypass install entries into the CAM table to ensure packet switching in the hardware. The CAM entries are static and it cannot be ensured that they are current. The entries age with the hardware if they are not removed by the authentication feature at the end of the session. If a host leaves before the authentication session expires or if the authentication manager is not notified about removing the CAM entry, the stale entry remains in the hardware switching table. Even the Layer 3 protocols, LAN port IP and Web-based proxy authentication have no method to age out the CAM entry if the host leaves before the session expires.

The IP device-tracking feature, which is included in the authentication manager, tracks the existence of the host and removes aged entries in the CAM table. The device-tracking feature ensures that the hardware entries and authentication sessions get aged out. As a result of aging, the hosts are removed from the EARL.

Configuring IP Device Tracking Globally

When enabled, the IP device tracking feature sends out a probe to check if the host is still present. The probe can be sent out at regular intervals for a specified number of times. The default is enabled.

To enable or disable IP device tracking globally, perform this task in privileged mode:

Task	Command
Enable or disable IP device tracking globally.	set ip device-tracking {disable enable}

This example shows how to enable IP device tracking globally:

```
Console> (enable) set ip device-tracking enable
Successfully enabled device tracking.
Console> (enable)
```

This example shows how to display the current global configuration of IP device tracking:

```
Console> (enable) show ip device-tracking
Device tracking mode      : Enabled
Device tracking count    : 3
Device tracking timeout  : 30
Console> (enable)
```

The following sections describe how to set the probe interval and probe count values:

- [Specifying the IP Device Tracking Interval, page 43-2](#)
- [Specifying the IP Device Tracking Count, page 43-3](#)



Note

The **probe interval** and **probe count** values can only be set globally and are common for all types of authentication methods.

Specifying the IP Device Tracking Interval

You can set IP device tracking to send a probe at regular intervals (in seconds). The range is from 5 to 65535 seconds. The default is 30 seconds.

To specify the probe interval, perform this task in privileged mode:

Task	Command
Specify the time period in seconds to send a probe.	set ip device-tracking probe interval <i>interval</i>

This example shows how to set the IP device tracking interval:

```
Console> (enable) set ip device-tracking probe interval 45
Device tracking probe interval set to 45 secs.
Console> (enable)
```

Specifying the IP Device Tracking Count

You can configure IP device tracking to send 1 to 10 probes after the host becomes idle. The default is 3 probes.

To set the probe count, perform this task in privileged mode:

Task	Command
Specify the number of times to check for the existence of a host.	set ip device-tracking probe count <i>count</i>

This example shows how to set the IP device tracking probe count:

```
Console> (enable) set ip device-tracking probe count 5
Device tracking probe count set to 5.
Console> (enable)
```

Configuring IP Device Tracking on a Port

The following topics describe how to configure IP device tracking on a port:

- [Enabling or Disabling IP Device Tracking on a Port with 802.1x Authentication, page 43-4](#)
- [Enabling or Disabling IP Device Tracking on a Port with MAC Authentication Bypass, page 43-4](#)
- [Enabling or Disabling IP Device Tracking on a Port with Web-Based Proxy Authentication, page 43-5](#)
- [Enabling or Disabling IP Device Tracking on a Port with EoU, page 43-6](#)

Enabling or Disabling IP Device Tracking on a Port with 802.1x Authentication

To enable or disable IP device tracking on a module or port with 802.1x authentication, perform this task in privileged mode:

Task	Command
Enable or disable IP device tracking on a module or port with 802.1x authentication. The default is disabled.	set port dot1x <i>mod/port</i> ip-device-tracking {disable enable}

This example shows how to enable IP device tracking on a port with 802.1x authentication:

```
Console> (enable) set port dot1x 3/1 ip-device-tracking enable
Port 3/1 ip-device-tracking option is enabled.
Console> (enable)
```

This example shows how to view the current configuration of IP device tracking on a port with 802.1x authentication:

```
Console> (enable) show port dot1x 3/13
Port  Auth-State      BEnd-State  Port-Control  Port-Status
-----
 3/13  authenticated      idle        auto          authorized

Port  Port-Mode      Re-authentication  Shutdown-timeout  Control-Mode
-----
 3/13  SingleAuth     enabled           disabled          Both      Both

Port  Posture-Token  Critical-Status  Termination action  Session-timeout
-----
 3/13  Healthy        no               Initialize          3600

Port  Session-Timeout-Override  Url-Redirect
-----
 3/13  disabled                -

Port  Critical  ReAuth-When  IP-Device-Tracking
-----
 3/13  disabled  105          enabled
Console> (enable)
```

Enabling or Disabling IP Device Tracking on a Port with MAC Authentication Bypass

To enable or disable IP device tracking on a module or port with MAC authentication bypass, perform this task in privileged mode:

Task	Command
Enable or disable IP device tracking on a module or port with MAC authentication bypass. The default is disabled.	set port mac-auth-bypass <i>mod/port</i> ip-device-tracking {disable enable}

This example shows how to enable IP device tracking on a port with MAC authentication bypass:

```
Console> (enable) set port mac-auth-bypass 3/1 ip-device-tracking enable
Port 3/1 ip-device-tracking option is enabled.
Console> (enable)
```

This example shows how to view the current configuration of IP device tracking on a port with MAC authentication bypass:

```
Console> (enable) show port mac-auth-bypass 3/1
Port  Mac-Auth-Bypass State MAC Address      Auth-State      Vlan
-----
3/1 Enabled                00-00-00-00-00-00 waiting          1

Port  Termination action Session Timeout Shutdown/Time-Left
-----
3/1 initialize            300             NO              -

Port  PolicyGroups
-----
3/1 -

Port  Security ACL                Sec ACL Type      QoS ACL Type
-----
3/1 -                          -                  -

Port  QoS Ingress ACL              QoS Egress ACL
-----
3/1 -                          -

Port  Critical Critical-Status Ip-Device-Tracking
-----
3/1 Disabled -              Enabled

Port  Session-ID
-----
3/1 -

Port  Posture Token URL-Redirect
-----
3/1 -
```

Enabling or Disabling IP Device Tracking on a Port with Web-Based Proxy Authentication

To enable or disable IP device tracking on a port with web-based proxy authentication, perform this task in privileged mode:

Task	Command
Enable or disable IP device tracking on a module or port with web-based proxy authentication. The default is enabled.	set port web-auth <i>mod/port</i> ip-device-tracking {disable enable}

This example shows how to enable IP device tracking on a port with web-based proxy authentication:

```
Console> (enable) set port web-auth 3/1 ip-device-tracking enable
```

```
Port 3/1 ip-device-tracking option is enabled.
Console> (enable)
```

This example shows how to view the current configuration of IP device tracking on a port with web-based proxy authentication:

```
Console> (enable) show port web-auth 3/1
Port  IP-Address      Vlan  Enabled  Web-Auth-State      Critical-Status
-----
 3/1  -                  1    enabled  -                   -

Port  IP-Address      Session-Timeout  Session-Timeleft  Radius-Rcvd-Timeout
-----
 3/1  -                -                -                  No

Port  IP-Address      Policy-Groups
-----
 3/1  -                -

Port  IP-Address      Ip-Device-Tracking
-----
 3/1  -                Enabled
```

Enabling or Disabling IP Device Tracking on a Port with EoU

To enable or disable IP device tracking on a port with EoU, perform this task in privileged mode:

Task	Command
Enable or disable IP device tracking on a module or port with EoU. The default is enabled.	set port eou <i>mod/port</i> ip-device-tracking {disable enable}

This example shows how to enable IP device tracking on a port with EoU:

```
Console> (enable) set port eou 3/1 ip-device-tracking enable
Port 3/1 ip-device-tracking option is enabled.
Console> (enable)
```

This example shows how to view the current configuration of IP device tracking on a port with EoU:

```
Console> (enable) show port eou 3/1
Port      EOU-State IP Address      MAC Address      Critical-Status
-----
 3/1      auto      -                -                -

Port      FSM State  Auth Type      SQ-Timeout      Session Timeout
-----
 3/1      -          -                -                -

Port      Posture    URL Redirect
-----
 3/1      -          -

Port      Termination action Session id
-----
 3/1      -          -

Port      PolicyGroups
-----
 3/1      -

Port      Critical Ip-Device-Tracking
-----
 3/1 disabled enabled
```