IP Device Tracking

IP Device Tracking on routers

IP Device Tracking (IPDT) is a feature used in Cisco routers and switches to monitor IPv4 devices connected on LAN ports by associating their MAC and IP addresses.

Key functionalities:

- Sends unicast Address Resolution Protocol (ARP) probes at a default interval of 30 seconds to maintain the tracking table
- Supports integration with security features like IP ARP Inspection and DHCP Snooping.Extracts device identity (MAC and IP address) from network traffic.
- Tracks the presence, location, and movement of end-nodes in the network.
- Stores this information in a binding table for use by other security features.

Table 1: Feature History Table

Feature name	Release information	Feature description
IP Device Tracking on routers	Release 17.18.1a	Enables IP Device Tracking with SISF support on LAN ports for IPv4 device monitoring and enhanced security integration.

Switch Integrated Security Features (SISF) based device tracking

The Switch Integrated Security Features (SISF)-based device tracking feature actively monitors the presence, location, and movement of end-nodes within the network as part of the First-Hop Security (FHS) suite. The feature enables the router to snoop incoming traffic, extract device identities (MAC and IP addresses), and store them in a binding table. Many features, including IEEE 802.1X, web authentication, Cisco TrustSec, and LISP, rely on the accuracy of this information to function correctly.

For more information on SISF, see the Chapter: Configuring Switch Integrated Security Features in the Security Configuration Guide

Guidelines and limitations

Many features, including Cisco TrustSec, IEEE 802.1X, LISP, and web authentication, rely on accurate IPDT database information for proper operation.

- LAN port limitation: SISF-based device tracking is configured on LAN ports only. VLAN targets are not supported
- The IPDT feature supports only IPv4 hosts; IPv6 hosts are not supported.
- The PDT feature supports up to 1,000 entries in the IPDT database.
- DHCPv4 host entries appear as ARP-based entries in the IPDT database. If DHCP snooping is enabled on the router, DHCPv4 host entries entries are tagged with a DHCP label in the database.
- A pre-configured default policy exists on the router. You only need to enable it on the interface target to activate basic IPDT functionality.
- For advanced configurations, you may create and apply custom IPDT policies on interfaces.

Guidelines and limitations for programmatically enabling SISF-based device tracking

- Different device tracking clients can exist simultaneously. Multiple programmatic policies may be created to accommodate these clients.
- The settings of each policy depend on the specific device tracking client that generates it.
- Policies are system-defined and may have different attributes.
- Policy attributes are configurable within the device tracking configuration mode (**config-device-tracking**).

Options to enable SISF-based device tracking

SISF-based device tracking is disabled by default and can be enabled either manually or programmatically.

- Manual enablement: Create a custom policy with configurable settings and attach it to a specific interface target.
- Programmatic enablement: Apply the default device tracking policy to an interface target.

Create and attach a custom device tracking policy

To enable and configure a custom device tracking policy for managing device tracking attributes and attaching the policy to a specific interface target.

Procedure

Step 1 Enter the global configuration mode.

Example:

```
Router#configure terminal
```

Step 2 Use the **device-tracking policy <policy_name>** command to create a custom device tracking policy.

Example:

```
Router(config)#device-tracking policy my_policy
```

Step 3 (Optional) Configure policy attributes.

- **data-glean**: Enables binding recovery by data traffic source address gleaning.
- **destination-glean**: Enables binding recovery by data traffic destination address gleaning.
- **prefix-glean**: Glean prefixes in RA and DHCP-PD traffic.
- **default**: Set a command to its default.
- **device-role**: Sets the role of the device attached to the port.
- **limit**: Specifies a limit.
- **medium-type-wireless**: Forces medium type to wireless.
- **no**: Negates a command or sets its default.
- **protocol** : Sets the protocol to glean (default all).
- **security-level**: Specifies the security level.
- **tracking**: Overrides default tracking behavior.
- **trusted-port**: Sets up a trusted port.

Step 4 Exit device-tracking configuration mode.

Example:

```
Router(config-device-tracking)#end
```

Step 5 Use the **interface interface-id** command to specify an interface.

Example:

```
Router(config)#interface gigabitethernet 1/1/4
```

Step 6 Use the **device-tracking attach-policy <policy_name>** command to attach the device tracking policy.

Example:

```
Router(config-if)#device-tracking attach-policy example_policy
```

SISF-based device-tracking policies can only be disabled if they are custom policies.

Step 7 Exit configuration mode.

Example:

```
Router(config-if)#end
```

Apply the default device tracking policy to an interface target

This task enables SISF-based device tracking programmatically by applying the default device tracking policy to an interface target.

Before you begin

Confirm the interface target to which the policy will be applied.

Procedure

Step 1 Enter the global configuration mode.

Example:

```
Rouetr#configure terminal
```

Step 2 Use the **interface type number** command to specify an interface target.

Example:

```
Device(config)#interface gigabitethernet 1/1/4
```

Step 3 Use the **device-tracking** command to enable SISF-based device tracking.

Example:

```
Router(config-if)#device-tracking
```

Step 4 Exit device-tracking configuration mode.

Example:

```
Router(config-device-tracking)#end
```

Step 5 Use the **interface interface-id** command to specify an interface.

Example:

```
Router(config)#interface gigabitethernet 1/1/4
```

Step 6 Use the **device-tracking attach-policy attach-policy** command to attach the device tracking policy.

Example:

```
Router(config-if)#device-tracking attach-policy attach-policy
```

Step 7 Exit configuration mode.

Example:

```
Router(config-if)#end
```

Configuration and verification examples

Configuration examples

Displays the device-tracking configuration:

```
Router#configure terminal
Router(config)#device-tracking policy my_policy
Router(config-device-tracking)#tracking enable
```

Displays the attaching of device-tracking policy:

```
Router#configure terminal
Router(config)#int gi0/1/2
Router(config-if)#device-tracking attach-policy my_policy
Router(config-if)#end
```

Verification examples

Displays the device-tracking policies:

```
Router#show device-tracking policies
Target               Type  Policy               Feature        Target range
Gi0/1/2              PORT  my_policy            Device-tracking vlan all
```

Displays all the configured attributes of the chosen device-tracking policy:

```
Router#show device-tracking policy my_policy

Device-tracking policy my_policy configuration:
  security-level guard
  device-role node
  gleaning from Neighbor Discovery
  gleaning from DHCP6
  gleaning from ARP
  gleaning from DHCP4
  NOT gleaning from protocol unkn
  tracking enable
Policy my_policy is applied on the following targets:
Target               Type  Policy               Feature        Target range
Gi0/1/2              PORT  my_policy            Device-tracking vlan all
```

Displays the database and counters of the device-tracking policy:

```
Router#show device-tracking database

Binding Table has 1 entries, 1 dynamic (limit 100000)
Codes: L - Local, S - Static, ND - Neighbor Discovery, ARP - Address Resolution Protocol,
DH4 - IPv4 DHCP, DH6 - IPv6 DHCP, PKT - Other Packet, API - API created
Preflevel flags (prlvl):
0001:MAC and LLA match     0002:Orig trunk           0004:Orig access
0008:Orig trusted trunk    0010:Orig trusted access  0020:DHCP assigned
0040:Cga authenticated     0080:Cert authenticated   0100:Statically assigned
    Network Layer Address                  Link Layer Address     Interface  vlan
prlvl      age        state      Time left
ARP 20.1.1.20                              bc4a.56ff.e786         Gi0/1/2    20
0005       111s       REACHABLE  196 s

Router#show device-tracking counters int gi0/1/2

Received messages on Gi0/1/2:
Protocol        Protocol message
```

```
NDP
DHCPv6
ARP             REQ[1] REP[2]
DHCPv4
ACD&DAD

Received Broadcast/Multicast messages on Gi0/1/2:
Protocol        Protocol message
NDP
DHCPv6
ARP             REQ[1] REP[2]
DHCPv4

Bridged messages from Gi0/1/2:
Protocol        Protocol message
NDP
DHCPv6
ARP             REP[1]
DHCPv4
ACD&DAD

Broadcast/Multicast converted to unicast messages from Gi0/1/2:
Protocol        Protocol message
NDP
DHCPv6
ARP
DHCPv4
ACD&DAD

Probe message on Gi0/1/2:
Type            Protocol message
PROBE_SEND
PROBE_REPLY

Limited Broadcast to Local message on Gi0/1/2:
Type            Protocol message
NDP
DHCPv6
ARP
DHCPv4

Dropped messages on Gi0/1/2:
Feature             Protocol Msg [Total dropped]

Faults on Gi0/1/2:
```