
# Global Configuration

**Revised: February 25, 2015,**

## Introduction

This chapter explains how to perform global configuration tasks, including IP routing and clock and time zone settings.

# IP Routing Configuration



## Configuring the IP Routing Table



For handling IP packets on the out-of-band MNG port, the Cisco SCE platform maintains a static routing table. When a packet is sent, the system checks the routing table for proper routing, and forwards the packet accordingly. In cases where the Cisco SCE platform cannot determine where to route a packet, it sends the packet to the default gateway.

The Cisco SCE platform supports the configuration of the default gateway as the default next hop router, as well as the configuration of the routing table to provide different next hop routers for different subnets (for maximum configuration of 100 subnets).

The following sections illustrate how to use CLI commands to configure various parameters.

The following commands are relevant to IP routing tables:

- **ip default-gateway**
- **ip route prefix mask next-hop**
- **no ip route all**
- **no ip route prefix mask**
- **show ip route**
- **show ip route prefix**
- **show ip route prefix mask**

### How to Configure the Default Gateway

#### Options

The following option is available:

- ip-address—the IP address of the default gateway.

From the SCE(config)# prompt, type:

| Command | Purpose |
|---|---|
| **ip default-gateway** *ip-address* | Configures the default gateway. |

#### Configuring the Default Gateway: Example

The following example shows how to set the default gateway IP of the Cisco SCE platform to 10.1.1.1.

```
SCE(config)#ip default-gateway 10.1.1.1
```

## How to Add an Entry to the IP Routing Table

### Options

The following options are available:

- **prefix—**IP address of the routing entry, in dotted notation.
- **mask—**The relevant subnet mask, in dotted notation
- **next-hop—**The IP address of the next hop in the route, in dotted notation.

  Must be within the MNG interface subnet.

From the SCE(config)# prompt, type:

| Command | Purpose |
|---|---|
| **ip route** *prefix mask next-hop* | Adds the specified IP routing entry to the routing table. |

### How to Add an Entry to the IP Routing Table: Example

The following example shows how to set the router 10.1.1.250 as the next hop to subnet 10.2.0.0.

```
SCE(config)#ip route 10.2.0.0 255.255.0.0 10.1.1.250
```

## How to Display the IP Routing Table

- How to Display the Entire IP Routing Table, page 6-3
- How to Display the IP Routing Table for a Specified Subnet, page 6-4

### How to Display the Entire IP Routing Table

From the SCE# prompt, type:

| Command | Purpose |
|---|---|
| **show ip route** | Displays the entire routing table and the destination of last resort (default-gateway). |

### Displaying the Entire IP Routing Table: Example

This example shows how to display the routing table.

```
SCE#show ip route
gateway of last resort is        10.1.1.1
|    prefix       |     mask         |    next hop     |
|-----------------|------------------|-----------------|
|        10.2.0.0 |     255.255.0.0  |      10.1.1.250 |
|        10.3.0.0 |     255.255.0.0  |      10.1.1.253 |
|        198.0.0.0 |       255.0.0.0 |      10.1.1.251 |
|        10.1.60.0 |   255.255.255.0 |      10.1.1.5   |
```

### How to Display the IP Routing Table for a Specified Subnet

#### Options

The following options are available:

- **prefix—**IP address of the routing entry, in dotted notation.
- **mask—**The relevant subnet mask, in dotted notation

From the SCE# prompt, type:

| Command | Purpose |
|---|---|
| **show ip route** *prefix mask* | Displays the routing table for the specified subnet (prefix/mask). |

#### Displaying the IP Routing Table for a Specified Subnet: Example

This example shows how to display the routing table for a specified subnet.

```
SCE#show ip route 10.1.60.0 255.255.255.0
|    prefix       |     mask        |    next hop     |
|-----------------|-----------------|-----------------|
|       10.1.60.0 |   255.255.255.0 |        10.1.1.5 |
sce#
```

# IP Advertising



IP advertising is the act of periodically sending ping requests to a configured address at configured intervals. This maintains the Cisco SCE platform IP/MAC addresses in the memory of adaptive network elements, such as switches, even during a long period of inactivity.

The following commands are relevant to IP advertising:

- **[no] ip advertising**
- **ip advertising destination**
- **ip advertising interval**
- **default ip advertising destination**
- **default ip advertising interval**
- **show ip advertising**
- **show ip advertising destination**
- **show ip advertising interval**

## Configuring IP Advertising

To configure IP advertising, you must first enable IP advertising. You may then specify a destination address to which the ping request is to be sent and/or the frequency of the ping requests (interval). If no destination or interval is explicitly configured, the default values are assumed.

#### Options

The following options are available in the IP advertising commands:

- **interval—**The time interval between pings in seconds.

  default interval = 300 seconds
- **destination—**The IP address of the destination for the ping requests

  default destination = 127.0.0.1

### How to Enable IP Advertising

From the SCE(config)# prompt, type:

| Command | Purpose |
|---|---|
| **ip advertising** | Enables IP advertising. |

### How to Configure the IP Advertising Destination

From the SCE(config)# prompt, type:

| Command | Purpose |
|---|---|
| **ip advertising destination** *destination* | Configures the destination for the IP advertising pings. |

### How to Configure the IP Advertising Interval

From the SCE(config)# prompt, type:

| Command | Purpose |
|---|---|
| **ip advertising interval** *interval* | Configures the frequency of the IP advertising pings. |

#### Configuring IP Advertising: Example

The following example shows how to configure IP advertising, specifying 10.1.1.1 as the destination and an interval of 240 seconds.

```
SCE(config)#ip advertising destination 10.1.1.1
SCE(config)#ip advertising interval 240
```

## How to Display the Current IP Advertising Configuration

From the SCE# prompt, type:

| Command | Purpose |
|---|---|
| **show ip advertising** | Displays the status of IP advertising (enabled or disabled), the configured destination, and the configured interval. |

# Configuring Time Clocks and Time Zone



The Cisco SCE platform has three types of time settings, which can be configured: the clock, the calendar, and the time zone. It is important to synchronize the clock and calendar to the local time, and to set the time zone properly. The Cisco SCE platform does not track Daylight Saving Time automatically, so you must update the time zone when the time changes bi-annually.

The Cisco SCE platform has the following two time sources:

- A real-time clock, called the calendar, that continuously keeps track of the time, even when the Cisco SCE platform is not powered up. When the Cisco SCE platform reboots, the calendar time is used to set the system clock. The calendar is not used for time tracking during system operation.
- A system clock, which creates all the time stamps during normal operation. This clock clears if the system shuts down. During a system boot, the clock is initialized to show the time indicated by the calendar.

It does not matter which clock you set first, as long as you use the clock and calendar read commands to ensure they are synchronized.

The time zone settings are important because they allow the system to communicate properly with other systems in other time zones. The system is configured based on Coordinated Universal Time (UTC), which is standard in the industry for coordination with other manufacturers' hardware and software. For example, Pacific Standard Time would be written as PST-10, meaning that the name of the time zone is PST, which is 10 hours behind Universal Time.

When setting and showing the time, the time is always typed or displayed according to the local time zone configured.

## Displaying the System Time

From the SCE(config)# prompt, type:

| Command | Purpose |
|---|---|
| **show clock** | Displays system time. |

### Displaying the System Time: Example

The following example shows the current system clock.

```
SCE#show clock
12:50:03  UTC  MON  November 13 2001
sce#
```

# Displaying the Calendar Time

From the SCE(config)# prompt, type:

| Command | Purpose |
|---|---|
| **show calendar** | Displays calendar time. |

## Displaying the Calendar Time: Example

The following example shows the current system calendar.

```
SCE#show calendar
12:50:03  UTC  MON  May 11 2007
sce#
```

# Setting the System Clock

## Options

The following option is available:

- **time-date** the time and date you want to set, in the following format:

  hh:mm:ss day month year

From the SCE# prompt, type:

| Command | Purpose |
|---|---|
| **clock set** *time-date* | Sets the system clock to the specified time and date. |

## Setting the System Clock: Example

The following example shows how to set the clock to 20 minutes past 10 AM, May 13, 2007, updates the calendar and then displays the time.

```
SCE#clock set 10:20:00 13 may 2007
SCE#clock update-calendar
SCE#show clock
10:21:10  UTC  THU  May  13  2007
```

# Setting the Calendar

The calendar is a system clock that continues functioning even when the system shuts down.

## Options

The following option is available:

- **time-date** —the time and date you want to set, in the following format:

  hh:mm:ss day month year

**Step 1** From the SCE# prompt, type **calendar set** *time-date* and press **Enter**.

Sets the system calendar to the specified time and date.

The time specified in this command is relative to the configured time zone.

**Step 2** From the SCE# prompt, type **clock read-calendar** and press **Enter**.

Synchronizes the system clock with the calendar time you just set .

## Setting the Calendar: Example

The following example shows that the calendar is set to 10:20 AM, May 13, 2007. The clock is then synchronized with the calendar setting.

```
SCE#calendar set 10:20:00 13 may 20017
SCE#clock read-calendar
SCE#show calendar
10:21:06  UTC  THU  May  13  2007
```

# Setting the Time Zone

## Options

The following options are available:

- **zone—**The name of the time zone to be displayed.

  default = GMT

- **hours—**The hours offset from UTC. This must be an integer in the range –23 to 23.

  default = 0

- **minutes—**The minutes offset from UTC. This must be an integer in the range of 0 to 59. Use this parameter to specify an additional offset in minutes when the offset is not measured in whole hours.

  default = 0

From the SCE(config)# prompt, type:

| Command | Purpose |
|---|---|
| **clock timezone** *zone hours minutes* | Sets the timezone to the specified timezone name with the configured offset in hours and minutes. |

### Setting the Time Zone: Example

The following example shows how to set the time zone to Pacific Standard Time with an offset of 10 hours behind UTC.

```
SCE(config)#clock timezone PST -10
SCE(config)#
```

## Removing the Current Time Zone Setting

From the SCE(config)# prompt, type:

| Command | Purpose |
|---|---|
| **no clock timezone** | Removes the timezone configuration and resets the timezone to the default value (UTC). |

## Configuring Daylight Saving Time

The Cisco SCE platform can be configured to automatically switch to daylight saving time on a specified date, and also to switch back to standard time. In addition, the time zone code can be configured to vary with daylight saving time if required. (For instance, in the eastern United States, standard time is designated EST, and daylight saving time is designated EDT).



### Options

The transition times into and out of daylight saving time may be configured in one of two ways, depending on how the dates for the beginning and end of daylight saving time are determined for the particular location:

- recurring—If daylight saving time always begins and ends on the same day every year, (as in the United States), the **clock summer-time recurring** command is used. The beginning and ending days for daylight saving time can be configured once, and the system will automatically perform the switch every year.
- not recurring—If the start and end of daylight saving time is different every year, (as in Israel), the **clock summer-time** command is used. In this case, the transitions must be configured every year for that particular year. (Note that "year" is not necessarily a calendar year. If the transition days are determined in the fall, the transitions for that fall and the next spring may be configured.)

The day on which the transition takes place may be defined in several ways:

- Specific date—For example, March 29, 2004. A specific date, including the year, is defined for a not recurring configuration.
- First/last occurrence of a day of the week in a specified month—For example, the last Sunday in March. This is used for a recurring configuration.
- Day of the week in a specific week in a specified month—For example, Sunday of the fourth week of March. (This would be different from the last Sunday of the month whenever there were five Sundays in the month). This is used for a recurring configuration.

The following options are available:

- **zone—**The time zone code for daylight saving time
- **week** (recurring only)— the week of the month on which daylight saving begins (week1) and ends (week2)
- **day** (recurring only)—The day of the week on which daylight savings begin (day1) and ends (day2)
- **date** (non-recurring only)—The date of the month on which daylight saving begins (date1) and ends (date2)
- **month—**The month in which daylight saving begins (month1) and ends (month2)
- **year** (non-recurring only)—The year in which daylight saving begins (year1) and ends (year2)
- **offset—**The difference in minutes between standard time and daylight saving time.

  Default = 60 minutes

## Guidelines

General guidelines for configuring daylight saving time transitions:

- Specify the time zone code for daylight saving time.
- recurring—Specify a day of the month (week#|first|last/day of the week/month).
- not recurring—Specify a date (month/day of the month/year).
- Define two days:
  - Day1 = beginning of daylight saving time.
  - Day2 = end of daylight saving time.
- In the Southern hemisphere, month2 must be before month1, as daylight saving time begins in the fall and ends in the spring.
- Specify the exact time that the transition should occur (24 hour clock).
  - Time of transition into daylight saving time—According to local standard time.
  - Time of transition out of daylight saving time—According to local daylight savings time.
- For the **clock summer-time recurring** command, the default values are the United States transition rules:
  - Daylight saving time begins: 2:00 (AM) on the second Sunday of March.
  - Daylight saving time ends: 2:00 (AM) on the first Sunday of November.

## How to Define Recurring Daylight Saving Time Transitions

From the SCE(config)# prompt, type:

| Command | Purpose |
|---|---|
| **clock summer-time** *zone* **recurring** *[week1 day1 month1 time1 week2 day2 month2 time2* [*offset* ]] | Configures daylight saving time to start and stop on the specified days every year. |

#### Defining Recurring Daylight Saving Time Transitions: Example

The following example shows how to configure recurring daylight saving time for a time zone designated "DST" as follows:

- Daylight saving time begins—0:00 on the last Sunday of March.
- Daylight saving time ends—23:59 on the Saturday of fourth week of November.
- Offset = 1 hour (default.

```
SCE(config)# clock summer-time DST recurring last Sunday March 00:00  4 Saturday November
23:59
```

## How to Define Non-Recurring Daylight Saving Time Transitions

From the SCE(config)# prompt, type:

| Command | Purpose |
|---|---|
| **clock summer-time** *zone* [*date1 month1 year1 time1 date2 month2 year2 time2* [*offset* ]] | Defines non-recurring daylight saving time transitions. |

#### Defining Non-Recurring Daylight Saving Time Transitions: Example

The following example shows how to configure non-recurring daylight saving time for a time zone designated "DST" as follows:

- Daylight saving time begins—0:00 on April 16, 2004.
- Daylight saving time ends—23:59 October 23, 2004.
- Offset = 1 hour (default)

```
SCE(config)# clock summer-time DST April 16 2004 00:00 October 23 2004 23:59
```

## How to Cancel the Daylight Saving Time Configuration

From the SCE(config)# prompt, type:

| Command | Purpose |
|---|---|
| **no clock summer-time** | Removes all daylight saving configuration. |

## How to Display the Current Daylight Saving Time Configuration

From the SCE# prompt, type:

| Command | Purpose |
|---|---|
| **show timezone** | Displays the current time zone and daylight saving time configuration. |

# Configuring SNTP



The Simple Network Timing Protocol (SNTP) is a simple solution to the problem of synchronizing the clocks in the various elements of the network. SNTP provides access to a time source via the network. The system clock and calendar are then set in accordance with this external source.

There are two options for the SNTP client. These functions are independent, and the system employ either one or both.

- Multicast SNTP client—Listens to SNTP broadcasts and updates the system clock accordingly.
- Unicast SNTP client—Sends a periodic request to a configured SNTP server, and updates the system clock according to the server response.

**Note** It is recommended that an IP access control list be configured to prevent access from unauthorized SNTP or NTP multicast servers (see "Configuring Access Control Lists (ACLs)" section on page 5-32).

The following commands are relevant to SNTP configuration:

- **[no] sntp broadcast client**
- **[no] sntp server address**
- **no sntp server all**
- **sntp update-interval**
- **show sntp**

## How to Enable the SNTP Multicast Client

From the SCE(config)# prompt, type:

| Command | Purpose |
|---|---|
| **sntp broadcast client** | Enables the SNTP multicast client. It will accept time updates from any broadcast server. |

# How to Disable the SNTP Multicast Client

From the SCE(config)# prompt, type:

| Command | Purpose |
|---|---|
| **no sntp broadcast client** | Disables the SNTP multicast client. It will not accept any broadcast time updates. |

# How to Enable the SNTP Unicast Client

## Options

The following option is available:

- **ip-address—**The IP address of the SNTP unicast server.

From the SCE(config)# prompt, type:

| Command | Purpose |
|---|---|
| **sntp server ip-address** | Defines the SNTP unicast server so that SNTP client is able to query that server. |

## Enabling SNTP Unicast Client: Example

The following example shows how to enable an SNTP server at IP address 128.182.58.100.

```
SCE(config)# sntp server 128.182.58.100
```

# Disabling the SNTP Unicast Client

## How to Disable the SNTP Unicast Client and Remove All Servers

From the SCE(config)# prompt, type:

| Command | Purpose |
|---|---|
| **no sntp server all** | Removes all SNTP unicast servers, preventing unicast SNTP query. |

## How to Remove One SNTP Server

### Options

The following option is available:

- **ip-address—**The IP address of the SNTP unicast server.

From the SCE(config)# prompt, type:

s

| Command | Purpose |
|---|---|
| **no sntp server** *ip-address* | Removes the specified SNTP unicast server. |

# How to Define the SNTP Unicast Update Interval

## Options

The following option is available:

- **interval—**The time in seconds between updates (64 through 1024)

  default interval = 64 seconds

From the SCE(config)# prompt, type;

| Command | Purpose |
|---|---|
| **sntp update-interval** *interval* | Configures the SNTP unicast client to query the server at the defined intervals. |

### Example

The following example shows how to set the SNTP update interval for 100 seconds.

```
SCE(config)# sntp update-interval 100
```

# How to Display SNTP Information

From the SCE> prompt, type:

| Command | Purpose |
|---|---|
| **show sntp** | Displays the configuration of both the SNTP unicast client and the SNTP multicast client. |

### Example

This example illustrates how to use this command.

```
SCE# show sntp
SNTP broadcast client: disabled
last update time: not available
SNTP unicast client: enabled
SNTP unicast server: 128.182.58.100
last update time: Feb 10 2002, 14:06:41
update interval: 100 seconds
```

# Domain Name Server (DNS) Settings



When a name of a host is given as a parameter to a CLI command that expects a host name or an IP address, the system translates the name to an IP address according to the following:

1. If the name is in a dotted decimal notation (that is, in the format x.x.x.x), it is directly translated to an IP address it represents.
2. If the name does not contain the dot character (.), the system looks it up in the IP Host table. If the name is found on the table, it is mapped to the corresponding IP address. The IP host table can be configured using the command **ip host.**
3. If the name does not contain the dot (.) character, and the domain name function is enabled (See the **ip domain-lookup** command), and a default domain name is specified (See the **ip domain-name** command), the default domain name is appended to the given name to form a fully qualified host name. This, in turn, is used to perform a DNS query translating the name to an IP address.
4. Otherwise, if the domain name function is enabled, the name is considered to be fully qualified, and is used to perform a DNS query translating the name to an IP address.

The following commands are relevant to DNS settings:

- **ip name-server**
- **ip domain-name**
- **no ip domain-name**
- **ip domain-lookup**
- **show hosts**

# Configuring DNS Lookup

## How to Enable DNS Lookup

From the SCE(config)# prompt, type:

| Command | Purpose |
|---|---|
| **ip domain-lookup** | Enables DNS lookup. |

## How to Disable DNS Lookup

From the SCE(config)# prompt, type:

| Command | Purpose |
|---|---|
| **no ip domain-lookup** | Disables DNS lookup. |

# Configuring Name Servers



## Options

The following options are available:

- **server-ip-address—**The IP address of the domain name server. You can define more than one DNS server (server-ip-address1, server-ip-address2, server-ip-address3)

## How to Define Domain Name Servers

Use this command to specify the address of one or more name servers to use for name and address resolution.

From the SCE(config)# prompt, type:

| Command | Purpose |
|---|---|
| **ip name-server** *server-address1 [server-address2 [server-address3]]* | Defines the servers at the specified addresses as domain name servers. |

#### Defining Domain Name Servers: Example

The following example shows how to configure the two name server (DNS) IP addresses.

```
SCE(config)#ip name-server 10.1.1.60 10.1.1.61
```

## How to Remove a Domain Name Server

From the SCE(config)# prompt, type:

| Command | Purpose |
|---|---|
| **no ip name-server** *server-address1 [server-address2 [server-address3]]* | Removes the specified server from the DNS list. |

#### Removing a Domain Name Server: Example

The following example shows how to remove name server (DNS) IP addresses.

```
SCE(config)#no ip name-server 10.1.1.60 10.1.1.61
```

### How to Remove All Domain Name Servers

From the SCE(config)# prompt, type:

| Command | Purpose |
|---|---|
| **no ip name-server** | Removes all configured DNS servers. |

## How to Add a Host to the Host Table

### Options

The following options are available:

- **hostname—**The name of the host.
- **ip-address—**The IP address of the host

From the SCE(config)# prompt, type:

| Command | Purpose |
|---|---|
| **ip host** *hostname ip-address* | Adds the specified host to the host table. |

### Adding Hosts to Removing them from the Host Table: Example

The following example shows how to add a host to the host table.

```
SCE(config)#ip host PC85 10.1.1.61
```

The following example shows how to remove a hostname together with all its IP mappings.

```
SCE(config)#no ip host PC85
```

## How to Display Current DNS Settings

From the SCE# prompt, type:

| Command | Purpose |
|---|---|
| **show hosts** | Displays current DNS settings. |

### Displaying Current DNS Settings: Example

The following example shows how to display current DNS information.

```
SCE#show hosts
Default domain is Cisco.com
Name/address lookup uses domain service
Name servers are 10.1.1.60, 10.1.1.61
Host                 Address
----                 -------
PC85                 10.1.1.61
sce#
```

# Configuring Cisco Discovery Protocol

*Cisco Discovery Protocol (CDP)* is a device discovery protocol that runs on Cisco manufactured equipment, and is now supported on the Cisco SCE 8000 platform.



## Cisco Discovery Protocol

CDP is primarily used to obtain protocol addresses of neighboring devices and discover the platform of those devices. It is media- and protocol-independent, and runs on all equipment manufactured by Cisco, including routers, bridges, access servers, and switches.

CDP runs on all media that support Subnetwork Access Protocol (SNAP), including LAN, Frame Relay, and ATM physical media. CDP runs over the data link layer only. Therefore, two systems that support different network-layer protocols can learn about each other.

Each device configured for CDP sends periodic messages, known as advertisements, to a multicast address. Each device advertises at least one address where it can receive SNMP messages. The advertisements also contain time-to-live, or holdtime, information, which indicates the length of time a receiving device should hold CDP information before discarding it. Each device also listens to the periodic CDP messages sent by others in order to learn about neighboring devices and determine when their interfaces to the media go up or down.

CDP Version-2 (CDPv2) is the most recent release of the protocol and provides more intelligent device tracking features. These features include a reporting mechanism that allows for more rapid error tracking, thereby reducing costly downtime. Reported error messages can be sent to the console or to a logging server, and include instances of native VLAN IDs (IEEE 802.1Q) on connecting ports that do not match, and port duplex states between connecting devices that do not match.

Type-Length-Value fields (TLVs) are blocks of information embedded in CDP advertisements. Table 6-1 summarizes the TLV definitions for CDP advertisements.

***Table 6-1 Type-Length-Value Definitions for CDPv2***

| TLV | Definition |
|---|---|
| Device-ID TLV | Identifies the device name in the form of a character string. |
| Address TLV | Contains a list of network addresses of both receiving and sending devices. |
| Port-ID TLV | Identifies the port on which the CDP packet is sent. |
| Capabilities TLV | Describes the functional capability for the device in the form of a device type, for example, a switch. |
| Version TLV | Contains information about the software release version on which the device is running. |
| Platform TLV | Describes the hardware platform name of the device, for example, Cisco 4500. |

*Table 6-1 Type-Length-Value Definitions for CDPv2 (continued)*

| TLV | Definition |
|---|---|
| IP Network Prefix TLV | Contains a list of network prefixes to which the sending device can forward IP packets. This information is in the form of the interface protocol and port number, for example, Eth 1/0. |
| VTP Management Domain TLV | Advertises the system's configured VTP management domain name-string. Used by network operators to verify VTP domain configuration in adjacent network nodes. |
| Native VLAN TLV | Indicates, per interface, the assumed VLAN for untagged packets on the interface. CDP learns the native VLAN for an interface. This feature is implemented only for interfaces that support the IEEE 802.1Q protocol. |
| Full/Half Duplex TLV | Indicates status (duplex configuration) of CDP broadcast interface. Used by network operators to diagnose connectivity problems between adjacent network elements. |

# Cisco Discovery Protocol on the Cisco SCE 8000 Platform

Because the Cisco SCE 8000 platform functions differently from a router or a switch, there are several unique features of CDP as supported on this device.

## CDP Operational Modes on the Cisco SCE 8000

With a typical Cisco device, CDP is either enabled or disabled. When enabled, CDP packets are received and transmitted. When disabled, CDP packets are discarded and no packets are transmitted.

The Cisco SCE 8000 is not a typical Cisco device. It is usually installed as a bump-in-the-wire device, and transparently forwards packets from one interface to the corresponding interface. This behavior conflicts with typical Cisco CDP packet processing; a typical Cisco device never forwards CDP packets from one interface to another interface. To accommodate this behavior, the Cisco SCE 8000 extends the enabled state with three different CDP modes:

- **Standard mode**: Standard CDP operation. CDP packets are received and processed, as well as generated.

  In this mode CDP functions as it does on a typical Cisco device. This mode should be used in most cases, even though it is not the default mode.

- **Bypass mode** (default): CDP packets are received and transmitted unchanged. Received packets are not processed. No packets are generated.

  In this mode, "bump-in-the-wire" behavior is applied to CDP packets. This is the backward-compatible mode, equivalent to not having CDP support.

- **Monitor mode**: CDP packets are received, processed, and transmitted unchanged. CDP packets are analyzed and CDP neighbor information is available. No packets are generated.

  In this mode "bump-in-the-wire" behavior is applied to CDP packets. This mode may be confusing to operators and network management tools, because it is contrary to the concept of CDP as a physical link protocol.

Table 6-2 summarizes the CDP state and modes behavior in the Cisco SCE 8000.

**Note** When CDP is either not running or disabled at the interface level, CDP packets are discarded and CDP packets are not generated, regardless of the CDP mode.

*Table 6-2 CDP Modes in the Cisco SCE 8000*

| CDP Mode | "cdp run" AND "cdp enable" | "no cdp run" OR "no cdp enable" |
|---|---|---|
| **Standard** | Received CDP packets processed<br>CDP packets generated | Received CDP packets discarded<br>CDP packets not generated |
| **Bypass (Default)** | Received CDP packets bypassed (not processed)<br>CDP packets not generated | Received CDP packets discarded<br>CDP packets not generated |
| **Monitor** | Received CDP packets processed and bypassed<br>CDP packets not generated | Received CDP packets discarded<br>CDP packets not generated |

## CDP Limitations on the Cisco SCE 8000

CDP as currently supported on the Cisco SCE 8000 has the following limitations:

- CDP is supported on traffic interfaces only (including cascade ports).
- CDP is currently managed by CLI only. There is currently no SNMP support for CDP on the Cisco SCE 8000.
- CDP always sends version 2 CDP packets. However it may receive v1 or v2 packets

# Configuring CDP on the Cisco SCE 8000 Platform

To configure CDP, perform the tasks in the following sections:

- Enabling CDP Globally, page 6-22
- Setting CDP Mode, page 6-23
- Enabling CDP on a Specific Traffic Interface, page 6-23
- Setting the Hold Time, page 6-24
- Setting the Timer, page 6-24

## Enabling CDP Globally

By default, CDP is enabled on the Cisco SCE 8000. If you prefer not to use the CDP device discovery capability, use the following command to disable it.

From the SCE(config)# prompt, type:

| Command | Purpose |
|---|---|
| **no cdp run** | Disables CDP. |

To reenable CDP after disabling it, use the following command.

From the SCE(config)# prompt, type:

| Command | Purpose |
|---|---|
| **cdp run** | Enables CDP. |

**Note** By default, when you enable CDP, it is set to bypass mode. To change the mode, see "Setting CDP Mode" section on page 6-23.

## Setting CDP Mode

The Cisco SCE 8000 is usually installed as a bump-in-the-wire device, and therefore forwards packets (including CDP packets) from one interface to the corresponding interface, whereas a typical Cisco device never forwards CDP packets from one interface to another interface. Therefore, the Cisco SCE 8000 extends the enabled state with the following three CDP modes:

- standard—function as a typical CDP device
- monitor—monitor the CDP packets
- bypass—bypass the CDP packets

(See "CDP Operational Modes on the Cisco SCE 8000" section on page 6-21 for a description of the different CDP modes.)

**Caution** In cascade topologies, both Cisco SCE 8000 platforms must be configured to the same CDP mode.

By default, the CDP mode is set to bypass.

To reset the CDP mode to the default mode (bypass) use the **default cdp mode** command.

To change the CDP mode, use the following command in global configuration mode.

From the SCE(config)# prompt, type:

| Command | Purpose |
|---|---|
| **cdp mode (standard \| monitor \| bypass)** | Changes the CDP mode. |

## Enabling CDP on a Specific Traffic Interface

By default, CDP is enabled on all traffic interfaces (see "CDP Limitations on the Cisco SCE 8000" section on page 6-22).

To disable CDP on a specific interface, use the **no cdp enable** command in the appropriate interface configuration mode.

To reenable CDP on a specific interface after disabling it, use the following command in the appropriate interface configuration mode. CDP must be enabled globally on the Cisco SCE 8000 platform (**cdp run** command) in order to enable a specific interface.

From the SCE(config if)# prompt, type:

| Command | Purpose |
|---|---|
| **cdp enable** | Enables CDP on a specific interface. |

**Tip** For consistent CDP operation, it is recommended that both ports of any one traffic link be either enabled or disabled.

## Setting the Hold Time

Use this command to set the mount of time the receiving device should hold a CDP packet from your router before discarding it. Use either the **no** or the **default** form of the command to restore the holdtime to the default value.

### Options

The following option is available:

- **seconds**— Hold time value to be sent in the CDP update packets in seconds.

  default = 180 seconds

From the SCE(config)# prompt, type:

| Command | Purpose |
|---|---|
| **cdp holdtime** *seconds* | Sets hold time. |

## Setting the Timer

Use this command to configure how often the Cisco SCE 8000 platform sends CDP updates. Use either the **no** or the **default** form of the command to restore the timer to the default value.

### Options

The following option is available:

- **seconds**— How often the Cisco SCE 8000 platform sends CDP updates, in seconds.

  default = 60 seconds

From the SCE(config)# prompt, type:

| Command | Purpose |
|---|---|
| **cdp timer** *seconds* | Sets the timer. |

# Monitoring and Maintaining CDP

To monitor and maintain CDP on the Cisco SCE 8000, use one or more of the following commands. The **clear** commands are in privileged EXEC mode. The **show** commands are in viewer mode.

| Command | Purpose |
|---|---|
| **clear cdp counters** | Resets CDP traffic counters to zero |
| **clear cdp table** | Clears the table that contains CDP information about neighbors |
| **show cdp** | Displays the following information:<br>• Interval between transmissions of CDP advertisements (transmission timer)<br>• Number of seconds the CDP advertisement is valid for a given port (hold time)<br>• Version of the advertisement<br>• CDP mode |
| **show cdp entry {*\|***device-name[*]* **[protocol \| version]}** | Displays protocol and version information about a specific neighboring device discovered using CDP.<br>• Use "*" to display all devices.<br>• Use *device-name** to display all devices beginning with device-name.<br>• Use the **protocol** keyword to display only protocol information<br>• Use the **version** keyword to display only version information. |

| Command | Purpose |
|---|---|
| **show cdp neighbors** [*type number*] [**detail**] | Displays the following information:<br>• Type of device that was discovered<br>• Name of the device<br>• Number and type of the local interface (port)<br>• Number of seconds the CDP advertisement is valid for the port<br>• Device type<br>• Device product number<br>• Port ID<br>If you use the **detail** keyword, the following additional information is displayed:<br>• Entry address(es)<br>• [Network protocol] address<br>• Version<br>• Advertisement version<br>• Native VLAN ID<br>• Duplex mode<br>• VTP domain name associated with neighbor devices. |
| **show cdp traffic** | Displays the following information:<br>• Total CDP packets output<br>• Total CDP packets input<br>• Number of CDP advertisements with bad headers<br>• Number of times the checksum operation failed<br>• Number of times CDP failed to send advertisements<br>• Number of times the local device did not have enough memory to store the CDP advertisements<br>• Number of invalid CDP advertisements<br>• Number of times fragments of CDP advertisement were received<br>• CDP version 1 advertisements output<br>• CDP version 1 advertisements input<br>• CDP version 2 advertisements output<br>• CDP version 2 advertisements input |

# CDP Configuration Examples

## Example: Setting the CDP Mode

The following example illustrates how to configure CDP mode to ‘standard’.

**Caution** In cascade topologies, both Cisco SCE 8000 platforms must be configured to the same CDP mode.

The **show** command verifies that the CDP configuration has been correctly updated.

```
sce(config)# cdp mode standard
sce(config)# do show cdp
Global CDP information:
        Sending CDP packets every 60 seconds
        Sending a holdtime value of 180 seconds
        Sending CDPv2 advertisements is enabled
        standard mode - CDP packets are received and processed. CDP packets are generated.
```

## Example: Monitoring and Maintaining CDP

The following example shows a typical series of steps for viewing information about CDP neighbors.

Table 6-3 describes the significant fields shown in the output of the **show cdp neighbors** command.

```
sce> show cdp
Global CDP information:
        Sending CDP packets every 60 seconds
        Sending a holdtime value of 180 seconds
        Sending CDPv2 advertisements is enabled
        standard mode - CDP packets are received and processed. CDP packets are generated.
sce> show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
Lab-Router       Ten 3/0/0          169         R S I     CISCO7604 Ten 3/1
Lab-Router       Ten 3/1/0          169         R S I     CISCO7604 Ten 3/2
Lab-Router       Ten 3/2/0          169         R S I     CISCO7604 Ten 3/3
Lab-Router       Ten 3/3/0          169         R S I     CISCO7604 Ten 3/4
sce>
```

***Table 6-3 show cdp neighbors Field Description***

| Field | Definition |
|---|---|
| Device ID | The name of the neighbor device and either the MAC address or the serial number of this device. |
| Local Intrfce | The protocol being used by the connectivity media. |
| Holdtme | The remaining amount of time (in seconds) the current device will hold the CDP advertisement from a sending router before discarding it. |

*Table 6-3 show cdp neighbors Field Description (continued)*

| Field | Definition |
|---|---|
| Capability (Capability Codes) | Capability (type of routing device) of the listed neighboring device.<br>The capability types that can be discovered are:<br>R—Router<br>T—Transparent bridge<br>B—Source-routing bridge<br>S—Switch<br>H—Host<br>I— device is using IGMP<br>r—Repeater<br>**Note** The capability of the Cisco SCE 8000 is 'r' (Repeater), since it is installed as a bump-in-the-wire device. |
| Platform | The product number of the device. |
| Port ID | The protocol and port number of the device. |

# Enabling the CLI Interface Warning Banner

A warning banner is a message displayed when the user connects to the Cisco SCE using either Telnet or the console connection. It serves as a security warning for unauthorized users trying to connect to Cisco SCE platform. It can also provide device details, as well as information about the service and application.

By default the banner is disabled. You do not have to shutdown the Cisco SCE platform in order to enable or disable the banner.

From the SCE(config)# prompt, type:

| Command | Purpose |
|---|---|
| **banner login "***banner-text"* | Enables the display of the specified text as the warning banner when the CLI interface is accessed.<br>Banner text should be enclosed in quotation marks or other delimiting characters. |

# OS Fingerprinting and NAT Detection

OS fingerprinting is the process of determining the identity of a remote host operating system by analyzing packets from that host. It detects the operating system used by the subscriber and whether the subscriber is present in a NAT environment by analyzing subscriber traffic. NAT detection is based on whether the same subscriber is connecting using multiple operating systems.

An encrypted fingerprint file that has the list of OS signatures is packaged with each SCOS release. Signature files are updated as needed, and the updated signature files are available on cisco.com.

The detected OS type is reported using the following mechanisms:

- RDRs—The subscriber OS type is reported in the Real-time Subscriber Usage RDR (SUR). These RDRs can be stored by the CM and interpreted using Insight.
- CLI—The subscriber OS type is available through OS fingerprinting and party info commands.
- VSA—Over mobile interfaces, the OS type is sent as a VSA in CCR-U over Gx.
- SCA BB Console—The OS type is available through an API that displays the OS type on the SCA BB console as part of the status of a subscriber.

## Restrictions and Limitations

Due to the nature of the Cisco SCE platform, there are certain limitations to the scope of the OS fingerprinting and NAT detection feature:

- OS information is available only for logged-in and active subscribers.
- OS fingerprinting is not done continuously for any subscriber. If a subscriber changes OS or moves to a NAT environment during the time when they are not sampled, OS type or NAT environment cannot be detected.
- OS fingerprinting depends mainly on the parameters in the TCP-SYN packets. The signature database is built based on the default settings used by various operating systems. If the subscriber changes default parameters, such as TCP window size, through registries, it may lead to misclassification of the OS.
- The OS type will not be detected in any of the following situations:
  - If the subscriber connects to the internet using an http-proxy, or if there is a proxy or gateway that changes L3/L4 packets of the subscriber.
  - If the subscriber has only one flow.
  - If the subscriber has only UDP flows
- In case of multiple IP or IP range subscribers, OS fingerprinting is done only for a limited number IP addresses (default is 5).
- NAT detection is based on whether the same subscriber is connecting using multiple operating systems. Therefore, if all the users behind a NAT use the same OS, it is not possible to detect the NAT.
- When a subscriber runs multiple operating systems using vmware, it may be detected as a NAT even though the subscriber is not in NAT environment.

# Configuring OS Fingerprinting

By default, the OS fingerprinting feature is disabled. When OS fingerprinting is enabled, you can also configure the following OS fingerprinting parameters:

- Sampling window—How long flows from a subscriber are fingerprinted
- Sampling interval—Interval between OS fingerprinting sampling windows

  OS fingerprinting is done for "sampling window" seconds every "sampling interval" minutes.
- NAT detection window—Time period within which detecting multiple operating systems for the same subscriber or IP address triggers NAT identification
- OS flush time–Time interval after which OS information is flushed from the system
- Signature file—Name of OS fingerprint signature file
- Scan port—Port used for opening OS fingerprinting flows
- GX reporting—Enable sending subscriber OS information in Gx messages

## SUMMARY STEPS

1. **enable**
2. **configure**
3. interface linecard 0
4. os-fingerprinting
5. (Optional) **os-fingerprinting sampling window** *window* **interval** *interval*
6. (Optional) **os-fingerprinting NAT-detection-window** *time*
7. (Optional) **os-fingerprinting os-flush-time** *time*
8. (Optional) **os-fingerprinting signature-file** *filename*
9. (Optional) **os-fingerprinting scan-port** *port#*
10. (Optional) **os-fingerprinting gx-report**

## DETAILED STEPS

| | Command | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`SCE> enable` | Enables privileged EXEC mode. Enter your password when prompted. |
| **Step 2** | **configure**<br><br>**Example:**<br>`SCE# configure` | Enters global configuration mode. |
| **Step 3** | **interface linecard**<br><br>**Example:**<br>`SCE(config)# interface linecard 0` | Enters interface linecard configuration mode. |

| | Command | Purpose |
|---|---|---|
| **Step 4** | **os**-fingerprinting<br><br>**Example:**<br>`SCE(config if)# os-fingerprinting` | Enables OS fingerprinting and loads the *default.fp* signature file. |
| **Step 5** | **os-fingerprinting sampling window** *window* **interval** *interval*<br><br>**Example:**<br>`SCE(config if)# os-fingerprinting sampling window 60 interval 5` | (Optional) Configures the following:<br>• Length of the OS sampling window, in seconds (10-300)<br>• Interval between sampling windows, in minutes (10-1440) |
| **Step 6** | **os-fingerprinting NAT-detection-window** *time*<br><br>**Example:**<br>`SCE(config if)# os-fingerprinting NAT-detection-window 600` | (Optional) Enables NAT detection and configures the time period, in seconds, within which detecting multiple operating systems for one subscriber will trigger NAT identification. (10-300) |
| **Step 7** | **os-fingerprinting os-flush-time** *time*<br><br>**Example:**<br>`SCE(config if)# os-fingerprinting os-flush-time 3` | (Optional) Enables flushing the OS fingerprinting information and configures the time interval, in days, after which OS fingerprinting information is flushed from the system. (1-5) |
| **Step 8** | **os-fingerprinting signature-file** *filename*<br><br>**Example:**<br>`SCE(config if)# os-fingerprinting signature-file new-signature-file` | (Optional) Specifies the signature file used for OS fingerprinting. |
| **Step 9** | **os-fingerprinting scan-port** *port#*<br><br>**Example:**<br>`SCE(config if)# os-fingerprinting scan-port 50` | (Optional) Configures the port used for opening OS fingerprinting flows. The port numbers can be in the range of 0 - 65535. However, the following port numbers are blocked, and cannot be used for OS fingerprinting:<br>20, 21, 194, 554, 651, 654, 1720, 1755, 2000, 2948, 2949, 4374, 5060, 5061.<br>For more information on this command, see the *Cisco SCE 8000 CLI Command Reference, Release 3.7.x*. |
| **Step 10** | **os**-fingerprinting gx-report<br><br>**Example:**<br>`SCE(config if)# os-fingerprinting gx-report` | (Optional) Enables sending subscriber OS information in Gx messages. |

# Monitoring OS Fingerprinting

To monitor OS fingerprinting, use one or more of the following commands.

These commands are in viewer mode.

| Command | Purpose |
|---|---|
| **show** os-fingerprinting config | Displays the current OS fingerprinting configuration.The following information is displayed:<br>• State of OS fingerprinting (enabled or disabled)<br>• Sampling period<br>• Sampling interval<br>• NAT detection window<br>• OS flush time<br>• OS fingerprinting port<br>• Signature file |
| **show** os-finger-printing signature-file | Displays the unencrypted contents of the signature file. |
| **show interface linecard** *slot-number* **subscriber name** *name* **[os-info]** | Displays information about a specified subscriber, including detected OS. To display only the OS fingerprinting information, use the **os-info** option**.** |
| **show os-finger-printing subscriber-name** *name* | Displays the OS fingerprinting information for the specified subscriber. This command displays the same information as the **show interface linecard** *slot-number* **subscriber name** *name* command with the **os-info** option. |

# Using the Bursty Traffic Convergence

During the peak hours, file sharing applications, such as P2P Bittorrent and other similar types of traffic, could go beyond the configured PIR level in the aggregative global controller mode. This is due to the bursty traffic nature of those applications. So, in order to have better convergence **bursty traffic convergence** enhancement is provided. The following steps are required to enable this **bursty traffic convergence** support to a particular AGC.

**Step 1** Choose AGC mode in Cisco SCABB.

**Step 2** It is recommended to create both upstream and downstream dedicated unique service AGC like P2P service AGC and apply SCABB policy.

**Step 3** Configure the new cli “bursty-traffic-convergence” for such unique service AGC like P2P directional AGC in both directions.

```
aggregative-global-controller network-side <agc-index> bursty-traffic-convergence
aggregative-global-controller subscriber-side <agc-index> bursty-traffic-convergence
```

**Step 4** Verify whether the bursty convergence is enabled in the running configuration.

**Step 5** Verify whether the traffic is mapped to a unique service AGC such as P2P service dedicated AGC.

**Step 6** Verify whether the corresponding traffic, such as P2P traffic, is mapped to the above AGC and is controlled in the configured PIR using insight graph reports.

---

The following steps are required to enable this **bursty traffic convergence** support to a particular GC.

---

**Step 1** Choose GC mode in Cisco SCABB.

**Step 2** It is recommended to create both upstream and downstream dedicated unique services GC, such as P2P service GC, and apply the SCABB policy.

**Step 3** Configure the new cli "bursty-traffic-convergence" for such unique service GC, like P2P directional GC, in both directions.

The enable/disable configuration cli command to be carried in each Ten Gig/One Gig interface port is given below:

```
global-controller <gc-id from scabb> bursty-traffic-convergence <flag >
```

flag -> 0 disable

flag -> 1 enable

The show command to be carried in each Ten Gig/ One Gig interface port is given below:

```
Show interface <TenGig/One Gig> global-controller < gc-id from scabb >
bursty-traffic-convergence
```

**Example:**

For downstream:

```
SCE8000(config)#>int TenGigabitEthernet 3/0/0
SCE8000(config)#>do sh running-config | I "DS GBWC P2P"
global-controller 1 name "DS GBWC P2P"
```

Attach the bursty cli to the above GC as shown below:

```
SCE8000(config)#>global-controller 1 bursty-traffic-convergence 1
```

Similarly for upstream:

```
SCE8000(config)#>int TenGigabitEthernet 3/1/0
SCE8000(config)#>do sh running-config | include "US GBWC P2P"
global-controller 1 name "US GBWC P2P"
```

Attach the bursty cli to above GC as shown below:

```
SCE8000(config)#>global-controller 1 bursty-traffic-convergence 1
```

**Step 4** Verify whether the bursty convergence is enabled in the running configuration.

**Step 5** Verify whether the traffic is mapped to a unique service GC such as P2P service dedicated GC.

**Step 6** Verify whether the corresponding traffic, such as P2P traffic, is mapped to the above GC and is controlled in the configured PIR using insight graph reports.

For more information on **bursty traffic convergence** CLI, see *CLI Command Reference* chapter of the *Cisco SCE 8000 CLI Command Reference, Release 5.1.0.*

---

## Restrictions and Known Limitations in Bursty Traffic Convergence

- Bursty traffic convergence is found to be effective for controlled environment traffic.
- For controlling bursty traffic such as P2P Bittorrent in AGC and GC mode, it is recommended to have a unique service under dedicated AGC and GC that needs bursty traffic convergence.

# DNS Assisted Classification/Sampling

DNS Assisted Classification supports existing Traffic-classification techniques to achieve more granular classification of encrypted subscriber traffic using the DNS traffic.

## Configuring DNS Assisted Classification

By default DNS Assisted Classification is disabled. Once we enable it, the following parameters can be configured:

- DNS sampling time - Sampling time frame for DNS packets
- Maximum DNS packets - Maximum DNS packets to be sampled within the sampling period
- DNS refresh time - Time in days to flush old DNS-assistance entries

### SUMMARY STEPS

1. **enable**
2. **configure**
3. interface linecard 0
4. Disable DNS bypass flow-filter rules and enable DNS classification on first packet via Service configuration
5. dns-flow sampling
6. (Optional) **dns-flow sampling** sample-time <*input in seconds*>
7. (Optional) **dns-flow sampling** max-dns-packets <*input as integer*>
8. (Optional) **dns-flow refresh-time** <*input is days*>
9. **do copy running-config startup-config**

### DETAILED STEPS

| | Command | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`SCE8000> enable` | Enables privileged EXEC mode. Enter your password when prompted. |
| **Step 2** | **configure**<br><br>**Example:**<br>`SCE8000# configure` | Enters global configuration mode. |
| **Step 3** | **interface linecard**<br><br>**Example:**<br>`SCE8000(config)# interface linecard 0` | Enters interface linecard configuration mode. |

| | Command | Purpose |
|---|---|---|
| **Step 4** | Disable DNS Bypass flow-filter rules and enable DNS First packet classification | By default, Flow-filter rules are configured to bypass dns traffic, for the DNS Assisted Classification to take effect, we need to configure the Service Configuration policy to allow SCE to process the dns traffic<br>For more information on configure policy to process DNS traffic, see Cisco Service Control Application for Broadband User Guide |
| **Step 5** | **dns-flow sampling**<br>**Example:**<br>`SCE8000(config if)# dns-flow sampling` | Enables sampling of DNS packets |
| **Step 6** | **dns-flow sampling** sample-time <*input in seconds*><br>**Example:**<br>`SCE8000(config if)# dns-flow sampling sample-time 25` | (Optional) Configures the length of the DNS sampling window, in seconds (1-1000) |
| **Step 7** | **dns-flow sampling** max-dns-packets <*input as integer*><br>**Example:**<br>`SCE8000(config if)# dns-flow sampling max-dns-packets 2000` | (Optional) Configures the Maximum number of DNS Packets to be processed per sample-time per traffic processor |
| **Step 8** | **dns-flow refresh-time** <*input is days*><br>**Example:**<br>`SCE8000(config if)# dns-flow refresh-time 2` | (Optional) Configures the Time Interval, in days, after which DNS Entries that exceed the interval are flushed from each of the traffic processor of the system. (1-1000). |
| **Step 9** | **do copy running-config startup-config** | Copies the current configured settings to the startup configuration. |

For more information on dns classification related CLI, see “CLI Command Reference” chapter in Cisco SCE 8000 CLI Command Reference, Release 5.1.x.