# IP Source Tracker

**Last Updated: September 14, 2011**

The IP Source Tracker feature tracks information in the following ways:

- Gathers information about the traffic that is flowing to a host that is suspected of being under attack.
- Generates all the necessary information in an easy-to-use format to track the network entry point of a DoS attack.
- Tracks Multiple IPs at the same time.
- Tracks DoS attacks across the entire network.



## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

## Restrictions for IP Source Tracker

### Packets Can Be Dropped for Routers

IP source tracking is designed to track attacks against hosts. Packets can be dropped if the line card or port adapter CPU is overwhelmed. Therefore, when used to track an attack against a router, IP source tracking can drop control packets, such as Border Gateway Protocol (BGP) updates.

### Engine 0 and 1 Performances Affected on Cisco 12000 Series

There is no performance impact for packets destined to nontracked IP addresses on Engine 2 and Engine 4 line cards because the IP source tracker affects only tracked destinations. Engine 0 and Engine 1 performances are affected because on these engines all packets are switched by the CPU.

**Note** On Cisco 7500 series routers, there is no performance impact on destinations that are not tracked.

# Information About IP Source Tracker



## Identifying and Tracking Denial of Service Attacks

One of the many challenges faced by customers today is the tracking and blocking denial-of-service (DoS) attacks. Counteracting a DoS attack involves intrusion detection, source tracking, and blocking. This functionality addresses the need for source tracking.

To trace attacks, NetFlow and access control lists (ACLs) have been used. To block attacks, committed access rate (CAR) and ACLs have been used. Support for these features on the Cisco 12000 series Internet router has depended on the type of line card used. Support for these features on the Cisco 7500 series routers depends upon the type of port adapter used. There is, therefore, a need to develop a way to receive information that both traces the source of an attack and is supported on all line cards and port adapters.

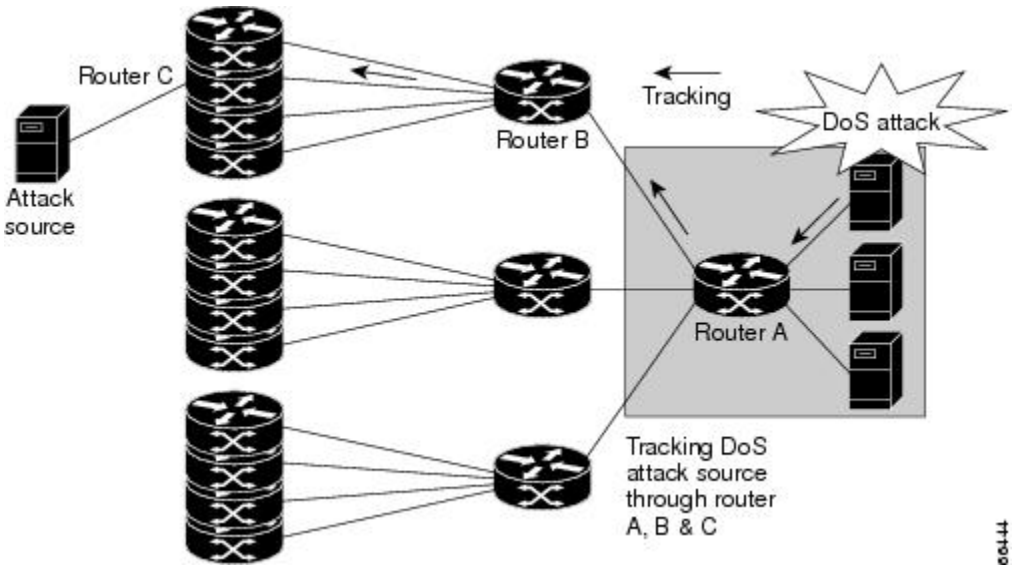
Normally, when you identify the host that is subject to a DoS attack, you must determine the network ingress point to effectively block the attack. This process starts at the router closest to the host.

For example, in the figure below, you would start at Router A and try to determine the next upstream router to examine. Traditionally, you would apply an output ACL to the interface connecting to the host to log packets that match the ACL. The logging information is dumped to the router console or system log. You then have to analyze this information, and possibly go through several ACLs in succession to identify the input interface for the attack. In this case the information points back to Router B.

You then repeat this process on Router B, which leads back to Router C, an ingress point into the network. At this point you can use ACLs or CAR to block the attack. This procedure can require applying several

ACLs that generate an excessive amount of output to analyze, making this procedure cumbersome and error prone.

***Figure 1 Source Tracking in a DoS Attack***




# Using IP Source Tracker

IP source tracker provides an easier, more scalable alternative to output ACLs for tracking DoS attacks, and it works as follows:

- After you identify the destination being attacked, enable tracking for the destination address on the whole router by entering the **ip source-track** command.
- Each line card creates a special Cisco Express Forwarding (CEF) entry for the destination address being tracked. For line cards or port adapters that use specialized Application-Specific Integrated Circuit (ASICs) for packet switching, the CEF entry is used to punt packets to the line card's or port adapter's CPU.
- Each line card CPU collects information about the traffic flow to the tracked destination.
- The data generated is periodically exported to the router. To display a summary of the flow information, enter the **show ip source-track summary** command. To display more detailed information for each input interface, enter the **show ip source-track** command.
- Statistics provide a breakdown of the traffic to each tracked IP address. This breakdown allows you to determine which upstream router to analyze next. You can shut down the IP source tracker on the current router by entering the **no ip source-track** command, and reopen it on the upstream router.
- Repeat Step 1 to Step 5 until you identify the source of the attack.
- Apply CAR or ACLs to limit or stop the attack.

- IP Source Tracker Hardware Support, page 3

## IP Source Tracker Hardware Support

IP source tracking is supported on all Engine 0, 1, 2, and 4 line cards in the Cisco 12000 series Internet router. It is also supported on all port adapters and RSPs that have CEF switching enabled on Cisco 7500 series routers.

# How to Configure IP Source Tracker



## Configuring IP Source Tracking

To configure IP source tracking for a host under attack, perform the following steps.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip source-track** *ip-address*
4. **ip source-track address-limit** *number*
5. **ip source-track syslog-interval** *number*
6. **ip source-track export-interval** *number*

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **ip source-track** *ip-address*<br><br>**Example:**<br>`Router(config)# ip source-track 100.10.0.1` | Enables IP source tracking for a specified host. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 4** | **ip source-track address-limit** *number*<br><br>**Example:**<br><br>`Router(config)# ip source-track address-limit 10` | (Optional) Limits the number of hosts that can be simultaneously tracked at any given time.<br><br>**Note** If this command is not enabled, there is no limit to the number of hosts that be can tracked. |
| **Step 5** | **ip source-track syslog-interval** *number*<br><br>**Example:**<br><br>`Router(config)# ip source-track syslog-interval 2` | (Optional) Sets the time interval, in minutes, used to generate syslog messages that indicate IP source tracking is enabled.<br><br>**Note** If this command is not enabled, system log messages are not generated. |
| **Step 6** | **ip source-track export-interval** *number*<br><br>**Example:**<br><br>`Router(config)# ip source-track export-interval 30` | (Optional) Sets the time interval, in seconds, used to export IP tracking statistics that are collected in the line cards to the gigabit route processor (GRP) and the port adapters to the route switch processor (RSP).<br><br>**Note** If this command is not enabled, traffic flow information is exported to the GRP and RSP every 30 seconds. |


- What to Do Next, page 5


## What to Do Next

After you have configured source tracking on your network device, you can verify your configuration and source tracking statistics, such as traffic flow. To complete this task, see the following section "Verifying IP Source Tracking, page 5."

# Verifying IP Source Tracking

To verify the status of source tracking, such as packet processing and traffic flow information, perform the following steps.

### SUMMARY STEPS

1. **enable**
2. **show ip source-track** [*ip-address*] [**summary** | **cache**
3. **show ip source-track export flows**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **show ip source-track** [*ip-address*] [**summary** \| **cache**<br><br>**Example:**<br>`Router# show ip source-track summary` | Displays traffic flow statistics for tracked IP host addresses |
| **Step 3** | **show ip source-track export flows**<br><br>**Example:**<br>`Router# show ip source-track export flows` | Displays the last 10 packet flows that were exported from the line card to the route processor.<br>**Note** This command can be issued only on distributed platforms, such as the GRP and the RSP. |

### Example

The following example, which is sample output from the **show ip source-track summary** command, shows how to verify that IP source tracking is enabled for one or more hosts:

```
Router# show ip source-track summary
Address          Bytes    Pkts    Bytes/s   Pkts/s
10.0.0.1          119G   1194M    443535      4432
192.168.1.1       119G   1194M    443535      4432
192.168.42.42     119G   1194M    443535      4432
```

The following example, which is sample output from the **show ip source-track summary** command, shows how to verify that no traffic has yet to be received for the destination hosts that are being tracked:

```
Router# show ip source-track summary
Address        Bytes   Pkts   Bytes/s   Pkts/s
10.0.0.1           0      0         0        0
192.168.1.1        0      0         0        0
192.168.42.42      0      0         0        0
```

The following example, which is sample output from the **show ip source-track**command, shows how to verify that IP source tracking is processing packets to the hosts and exporting statistics from the line card or port adapter to the GRP and RSP:

```
Router# show ip source-track
Address         SrcIF    Bytes   Pkts   Bytes/s   Pkts/s
10.0.0.1        PO0/0    119G   1194M    513009     5127
192.168.1.1     PO0/0    119G   1194M    513009     5127
```

192.168.42.42 PO0/0 119G 1194M 513009 5127

# Configuration Examples for IP Source Tracker



## Configuring IP Source Tracking Example

The following example shows how to configure IP source tracking on all line cards and port adapters in the router. In this example, each line card or port adapter collects traffic flow data to host address 100.10.0.1 for 2 minutes before creating an internal system log entry; packet and flow information recorded in the system log is exported for viewing to the route processor or switch processor every 60 seconds.

```
Router# configure interface
Router(config)# ip source-track 100.10.0.1
Router(config)# ip source-track syslog-interval 2
Router(config)# ip source-track export-interval 60
```

## Verifying Source Interface Statistics for All Tracked IP Addresses Example

The following example displays a summary of the traffic flow statistics that are collected on each source interface for tracked host addresses.

```
Router# show ip source-track
Address         SrcIF     Bytes    Pkts     Bytes/s     Pkts/s
10.0.0.1        PO2/0         0       0           0          0
192.168.9.9     PO1/2      131M    511M        1538          6
192.168.9.9     PO2/0      144G   3134M     6619923     143909
```

## Verifying a Flow Statistic Summary for All Tracked IP Addresses Example

The following example displays a summary of traffic flow statistics for all hosts that are being tracked; it shows that no traffic has yet been received.

```
Router# show ip source-track summary
Address              Bytes    Pkts     Bytes/s     Pkts/s
10.0.0.1                 0       0           0          0
100.10.1.1           131M    511M        1538          6
192.168.9.9          146G   3178M     6711866     145908
```

## Verifying Detailed Flow Statistics Collected by a Line Card Example

The following example displays traffic flow information that is collected on line card 0 for all tracked hosts.

```
Router# exec slot 0 show ip source-track cache
========= Line Card (Slot 0) =======
IP packet size distribution (7169M total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .000 .000 .000 0.00 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000
    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000
```

```
IP Flow Switching Cache, 278544 bytes
  1 active, 4095 inactive, 13291 added
  198735 ager polls, 0 flow alloc failures
  Active flows timeout in 0 minutes
  Inactive flows timeout in 15 seconds
  last clearing of statistics never
Protocol         Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
SrcIf          SrcIPaddress    DstIf          DstIPaddress    Pr TOS Flgs  Pkts
Port Msk AS                    Port Msk AS    NextHop              B/Pk  Active
PO0/0          101.1.1.0       Null           100.1.1.1       06 00  00      55K
0000 /0  0                     0000 /0  0     0.0.0.0                100    10.1
```

# Verifying Flow Statistics Exported from Line Cards and Port Adapters Example

The following example displays packet flow information that is exported from line cards and port adapters to the GRP and the RSP:

```
Router# show ip source-track export flows
SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
PO0/0         101.1.1.0       Null          100.1.1.1       06 0000 0000    88K
PO0/0         101.1.1.0       Null          100.1.1.3       06 0000 0000    88K
PO0/0         101.1.1.0       Null          100.1.1.2       06 0000 0000    88K
```

# Additional References

The following sections provide references related to IP Source Tracker.

### Related Documents

| Related Topic | Document Title |
|---|---|
| ACLs | *Cisco IOS Security Configuration Guide: Securing the Data Plane* , Release 12.4T |
| Dynamic ACLs | Configuring Lock-and-Key Security (Dynamic Access Lists) |
| DoS prevention | Configuring TCP Intercept (Preventing Denial-of-Service Attacks) |

### Standards

| Standards | Title |
|---|---|
| None | -- |

### MIBs

| MIBs | MIBs Link |
|---|---|
| None | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br>http://www.cisco.com/go/mibs |

### RFCs

| RFCs | Title |
|---|---|
| None | -- |

### Technical Assistance

| Description | Link |
|---|---|
| The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.<br>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.<br>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password. | http://www.cisco.com/techsupport |

# Feature Information for IP Source Tracker

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

*Table 1 Feature Information for IP Source Tracker*

| Feature Name | Releases | Feature Information |
|---|---|---|
| IP Source Tracker | 12.0(21)S 12.0(22)S 12.0(26)S 12.3(7)T 12.2(25)S | The IP Source Tracker feature allows information to be gathered about the traffic that is flowing to a host that is suspected of being under attack.<br>This feature was introduced in Release 12.0(21)S on the Cisco 12000 series.<br>This feature was implemented in Release 12.0(22)S on the Cisco 7500 series.<br>This feature was implemented in Release 12.0(26)S on the Cisco 12000 series IP Service Engine (ISE) line cards.<br>This feature was integrated into Cisco IOS Release 12.3(7)T.<br>This feature was integrated into Cisco IOS Release 12.2(25)S.<br>The following commands were introduced or modified: **ip source-track, ip source-track address-limit, ip source-track export-interval, ip source-track syslog-interval, show ip source-track, show ip source-track export flows.** |