



IP Source Tracker

Feature History

Release	Modification
12.0(21)S	This feature was introduced on the Cisco 12000 series.
12.0(22)S	This feature was implemented on the Cisco 7500 series.
12.0(26)S	This feature was implemented on Cisco 12000 Series IP Service Engine (ISE) line cards.

This feature module describes the IP Source Tracker feature and includes the following sections:

- [Feature Overview, page 1](#)
- [Supported Platforms, page 5](#)
- [Supported Standards, MIBs, and RFCs, page 5](#)
- [Configuration Tasks, page 6](#)
- [Monitoring and Maintaining IP Source Tracking, page 7](#)
- [Configuration Examples, page 8](#)
- [Command Reference, page 10](#)
- [Glossary, page 17](#)

Feature Overview

The IP Source Tracker feature allows you to gather information about the traffic flowing to a host that is suspected of being under attack. This feature also allows you to easily trace an attack back to its entry point into the network.



Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Copyright © 2003 Cisco Systems, Inc. All rights reserved.

Identifying and Tracking Denial of Service Attacks

One of the many challenges faced by ISPs today is tracking and blocking denial of service (DoS) attacks. Counteracting a DoS attack can be broken down into three areas: intrusion detection, source tracking, and blocking. This document discusses the need for source tracking.

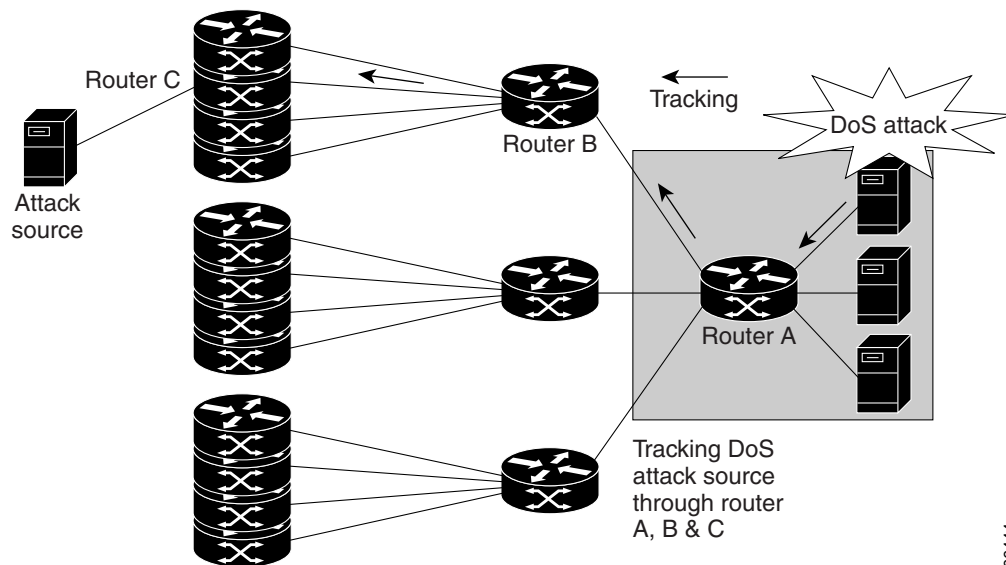
To trace attacks, NetFlow and access control lists (ACLs) have been used. To block attacks, committed access rate (CAR) and ACLs have been used. Support for these features on the Cisco 12000 series Internet router has depended on the type of line card used. Support for these features on the Cisco 7500 series routers depends upon the type of port adapter used. There is, therefore, a need to develop a way to receive information tracing the source of an attack that 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 [Figure 1](#), you would start at Router A and try to determine the next upstream router to examine. To do this, you would traditionally apply an output ACL to the interface connecting to the host in order to log packets matching the ACL. The logging information is dumped to the router console or syslog. 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 it cumbersome and error prone.

Figure 1 Source Tracking in a DoS Attack



66444

How the IP Source Tracker Works

The IP Source Tracker feature provides an easier, more scalable alternative to output ACLs for tracking DoS attacks. This feature is supported on all Engine 0, 1, 2, and 4 line cards in the Cisco 12000 series Internet router. In future releases, this feature will be supported on Engine 3. This feature is supported on all port adapters and Route Switch Processors (RSPs) that have Cisco Express Forwarding (CEF) switching enabled on Cisco 7500 series routers.

The IP Source Tracker works as follows:

-
- Step 1** After you identify the destination being attacked, enable tracking for the destination address on the whole router by entering the **ip source-track** command (see [“Configuration Tasks” section on page 6](#)).
 - Step 2** Each line card creates a special CEF entry for the destination address being tracked. For line cards or port adapters that use specialized ASICs to do packet switching, the CEF entry is used to punt packets to the line card’s or port adapter’s CPU.
 - Step 3** Each line card CPU collects information about the traffic flow to the tracked destination.
 - Step 4** 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.
 - Step 5** Statistics provide a breakdown of the traffic to each tracked IP address. This 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 re-open it on the upstream router.
 - Step 6** Repeat Step 1 to Step 5 until you identify the source of the attack.
 - Step 7** Apply CAR or ACLs to limit or stop the attack.
-

Benefits

Complete Network Coverage

Because the IP Source Tracker feature is supported on Engine 0, 1, 2, and 4 (in future releases, Engine 3) line cards on Cisco 12000 series routers and on all port adapters on Cisco 7500 series routers, it allows you to track DoS attacks across your entire network.

Complete Tracking Information Provided

The IP source tracker generates all the necessary information in an easy-to-use format to track the network entry point of a DoS attack.

Tracking an Unlimited Number of IPs Simultaneously

Using the IP source tracker, you can track multiple IPs at the same time. By default there is no limit. To limit the number of IPs that are simultaneously tracked, use the **ip source-track address-limit** command.

Restrictions

Support for Cisco 12000 Series Line Cards

Starting in IOS Release 12.0(21)S, the IP Source Tracker feature is supported on all Cisco 12000 Series line cards, except for ISE (Engine 3) line cards.

The IP Source Tracker is supported on ISE line cards in IOS Release 12.0(26)S and later releases.

Packets Can Be Dropped for Routers

The IP source tracker is designed to track attacks against hosts. Packets can be dropped if the line card or port adapter CPU is overwhelmed. Therefore, you should be aware that when used to track an attack against a router, the IP source tracker can drop control packets, such as BGP updates.

Engine 0 and 1 Performance Impacted 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 performance is impacted 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.

Related Features and Technologies

For related information, refer to other security features, such as:

- Authentication, authorization, and accounting (AAA) systems
- Crypto IP security encryption
- Firewall security features

Related Documents

- [Cisco Express Forwarding Overview](#)
- [Cisco IOS IP and IP Routing Configuration Guide](#)
- [Cisco IOS Release 12.0 Configuration Fundamentals Command Reference](#)
- [Cisco IOS Release 12.0 Configuration Fundamentals Configuration Guide](#)
- [Configuring Cisco Express Forwarding](#)

Supported Platforms

- Cisco 7500 series
- Cisco 12000 series

Determining Platform Support Through Feature Navigator

Cisco IOS software is packaged in feature sets that support specific platforms. To get updated information regarding platform support for this feature, access Feature Navigator. Feature Navigator dynamically updates the list of supported platforms as new platform support is added for the feature.

Feature Navigator is a web-based tool that enables you to quickly determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image.

To access Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions at the following URL:

<http://www.cisco.com/register>.

Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Feature Navigator home page at the following URL:

<http://www.cisco.com/go/fn>

Availability of Cisco IOS Software Images

Platform support for particular Cisco IOS software releases is dependent on the availability of the software images for those platforms. Software images for some platforms may be deferred, delayed, or changed without prior notice. For updated information about platform support and availability of software images for each Cisco IOS software release, refer to the online release notes or, if supported, Cisco Feature Navigator.

Supported Standards, MIBs, and RFCs

Standards

No new or modified standards are supported by this feature.

MIBs

No new or modified MIBs are supported by this feature.

To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

RFCs

No new or modified RFCs are supported by this feature.

Configuration Tasks

See the following sections for configuration tasks for the IP Source Tracker feature. Each task in the list is identified as either required or optional.

- [Enabling IP Source Tracking for a Host Under Attack](#) (required)
- [Limiting the Number of Hosts that Are Tracked](#) (optional)
- [Setting the Time Interval Used for Generating Syslog Messages](#) (required)
- [Setting the Time Interval Used for Exporting Statistics to the GRP or RSP](#) (optional)
- [Verifying IP Source Tracking](#) (required)

Enabling IP Source Tracking for a Host Under Attack

To enable IP source tracking, enter the following command in global configuration mode:

:

Command	Purpose
Router(config)# ip source-track <i>address</i>	Enables IP source tracking on all line cards and port adapters for the IP address of the host under attack.

Limiting the Number of Hosts that Are Tracked

To specify the limit for the number of hosts for which you can configure tracking, enter the following command in global configuration mode:

:

Command	Purpose
Router(config)# ip source-track address-limit <i>number</i>	Configures an administrative limit for the number of ip source-track commands that you can enter. By default, there is no limit.

Setting the Time Interval Used for Generating Syslog Messages

To set the time interval used to generate syslog messages, enter the following command in global configuration mode:

Command	Purpose
Router(config)# ip source-track syslog-interval <i>number</i>	Sets the number of minutes between syslog messages generated when the IP source tracker is enabled. The syslog messages serve only as a reminder to users that IP source tracking is enabled. The default is 0 (no syslog messages are generated).

Setting the Time Interval Used for Exporting Statistics to the GRP or RSP

To set the time interval used to export traffic flow information to the Gigabit Route Processor (GRP) or Route Switch Processor (RSP), enter the following command in global configuration mode:

Command	Purpose
Router(config)# ip source-track export-interval number	Sets the time interval (in seconds) used to export the IP tracking statistics collected in the line cards or port adapter to the GRP/RSP for viewing. The default is 30 seconds.

Verifying IP Source Tracking

- Step 1** Enter the **show ip source-track summary** command 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
```

If no traffic has yet been received for the hosts, the **show ip source-track summary** command displays the following:

```
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
```

- Step 2** Enter the **show ip source-track** command 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/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
```

Monitoring and Maintaining IP Source Tracking

Command	Purpose
Router# show ip source-track address	Displays the traffic flow statistics collected for the source interfaces of all hosts being tracked, or of a specified host.
Router# show ip source-track address summary	Displays more general traffic flow information collected for all hosts being tracked, or for a specified host.

Command	Purpose
Router# show ip source-track address cache	Displays detailed packet and flow information collected on line cards for all tracked IP addresses, or for a specified address (not displayed on the GRP/RSP).
Router# show ip source-track export flows	Displays packet and flow information exported from line cards to the GRP for all tracked IP addresses (displayed only on the GRP/RSP).

Configuration Examples

This section provides the following examples:

- [Configuring IP Source Tracking for an IP Address Example](#)
- [Displaying Source Interface Statistics for All Tracked IP Addresses Example](#)
- [Displaying a Flow Statistic Summary for All Tracked IP Addresses Example](#)
- [Displaying Detailed Flow Statistics Collected by a Line Card/Port Adapter Example](#)
- [Displaying Flow Statistics Exported from Line Cards/Port Adapters to the GRP/RSP Example](#)

Configuring IP Source Tracking for an IP Address Example

This example shows how to configure IP source tracking on all line cards/port adapters in the router, in order that each line card or port adapter collects traffic flow data to host address 100.10.0.1 for two minutes before creating an internal system log entry. Packet and flow information recorded in the system log is exported for viewing to the GRP/RSP 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
```

Displaying Source Interface Statistics for All Tracked IP Addresses Example

This example displays a summary of the traffic flow statistics 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
```

Displaying a Flow Statistic Summary for All Tracked IP Addresses Example

This example displays a summary of traffic flow statistics for all hosts being tracked and 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

```

Displaying Detailed Flow Statistics Collected by a Line Card/Port Adapter Example

This example displays the traffic flow information collected on line card/port adapter 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 aged 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

```

Displaying Flow Statistics Exported from Line Cards/Port Adapters to the GRP/RSP Example

This example displays the packet flow information exported from line cards/port adapters to the GRP/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

```

Command Reference

This section documents new commands. All other commands used with this feature are documented in the Cisco IOS Release 12.0 command reference publications.

- [ip source-track](#)
- [ip source-track address-limit](#)
- [ip source-track export-interval](#)
- [ip source-track syslog-interval](#)
- [show ip source-track](#)

ip source-track

To enable IP source tracking for a specified host, use the **ip source-track** command in global configuration mode. To disable IP source tracking, use the **no** form of this command.

ip source-track *address*

no ip source-track *address*

Syntax Description	<i>address</i>	IP address of the host enabled for IP source tracking.
--------------------	----------------	--

Defaults	No default behavior or values.
----------	--------------------------------

Command Modes	Global configuration
---------------	----------------------

Command History	Release	Modification
	12.0(21)S	This command was introduced.
	12.0(22)S	This command was implemented on the Cisco 7500 series routers.
	12.0(26)S	This command was implemented on Cisco 12000 Series ISE line cards.

Usage Guidelines	Use this command to enable IP source tracking for a specified destination address.
------------------	--

Examples	The following example configures IP source tracking for the host having the IP address 100.1.1.3:
----------	---

```
Router(config)# ip source-track 100.1.1.3
```

Related Commands	Command	Description
	ip source-track address-limit	Configures the maximum number of ip source-track commands that you can enter for hosts under attack.
	ip source-track export-interval	Sets the time interval used to export IP tracking statistics collected in the line cards/port adapters to the GRP/RSP.
	ip source-track syslog-interval	Sets the time interval used to generate syslog messages to remind users that IP source tracking is enabled.
	show ip source-track	Displays the traffic flow statistics collected for tracked IP host addresses.

ip source-track address-limit

To configure the maximum number of **ip source-track** commands that you can enter for hosts under attack, use the **ip source-track address-limit** command in global configuration mode. To cancel this administrative limit and return to the default, use the **no** form of this command.

ip source-track address-limit *number*

no ip source-track address-limit

Syntax Description	<i>number</i>	Maximum number of ip source-track commands for which you can specify hosts addresses.
---------------------------	---------------	--

Defaults None (unlimited number of hosts are tracked).

Command Modes Global configuration

Command History	Release	Modification
	12.0(21)S	This command was introduced.
	12.0(22)S	This command was implemented on the Cisco 7500 series routers.
	12.0(26)S	This command was implemented on Cisco 12000 Series ISE line cards.

Usage Guidelines Use this command to limit the number of destination addresses that you can configure for IP source tracking with the **ip source-track** command.

Examples The following example limits IP source tracking to 10 IP addresses:

```
Router (config)# ip source-track address-limit 10
```

Related Commands	Command	Description
	ip source-track	Enables IP source tracking for a specified host.
	ip source-track export-interval	Sets the time interval used to export IP tracking statistics collected in the line cards/port adapters to the GRP/RSP.
	ip source-track syslog-interval	Sets the time interval used to generate syslog messages to remind users that IP source tracking is enabled.
	show ip source-track	Displays the traffic flow statistics collected for tracked IP host addresses.

ip source-track export-interval

To set the time interval used to export IP tracking statistics collected in the line cards/port adapters to the GRP/RSP, use the **ip source-track export-interval** command in global configuration mode. To cancel this setting and return to the default interval, use the **no** form of this command.

ip source-track export-interval *number*

no ip source-track export-interval

Syntax Description	<i>number</i>	Number of seconds used by line cards or port adapters before exporting IP tracking information to the RSP/GRP.
---------------------------	---------------	--

Defaults	30 seconds.
-----------------	-------------

Command Modes	Global configuration
----------------------	----------------------

Command History	Release	Modification
	12.0(21)S	This command was introduced.
12.0(22)S	This command was implemented on the Cisco 7500 series routers.	
12.0(26)S	This command was implemented on Cisco 12000 Series ISE line cards.	

Usage Guidelines	Use this command to specify the frequency of IP tracking information to send to the GRP/RSP for viewing.
-------------------------	--

Examples	The following example sets the time interval used by line cards/port adapters to 30 seconds before exporting IP tracking information:
-----------------	---

```
Router(config)# ip source-track export-interval 30
```

Related Commands	Command	Description
		ip source-track
	ip source-track address-limit	Configures the maximum number of ip source-track commands that you can enter for hosts under attack.
	ip source-track syslog-interval	Sets the time interval used to generate syslog messages to remind users that IP source tracking is enabled.
	show ip source-track	Displays the traffic flow statistics collected for tracked IP host addresses.

ip source-track syslog-interval

To set the time interval used to generate syslog messages to remind users that IP source tracking is enabled, use the **ip source-track syslog-interval** command in global configuration mode. To cancel this setting and disable syslog generation, use the **no** form of this command.

ip source-track syslog-interval *number*

no ip source-track syslog-interval

Syntax Description

<i>number</i>	Number of minutes used to generate syslog messages.
---------------	---

Defaults

0 (no syslog messages are generated).

Command Modes

Global configuration

Command History

Release	Modification
12.0(21)S	This command was introduced.
12.0(22)S	This command was implemented on the Cisco 7500 series routers.
12.0(26)S	This command was implemented on Cisco 12000 Series ISE line cards.

Usage Guidelines

Use this command to enable the generation of reminder syslog messages.

Examples

The following example configures the router to generate a syslog message every two minutes after you enable IP source tracking with the **ip source-track** command:

```
Router(config)# ip source-track syslog-interval 2
```

Related Commands

Command	Description
ip source-track	Enables IP source tracking for a specified host.
ip source-track address-limit	Configures the maximum number of ip source-track commands that you can enter for hosts under attack.
ip source-track export-interval	Sets the time interval used to export IP tracking statistics collected in the line cards/port adapters to the GRP/RSP.
show ip source-track	Displays the traffic flow statistics collected for tracked IP host addresses.

show ip source-track

To display the traffic flow statistics collected for tracked IP host addresses, use the **show ip source-track** command in privileged EXEC mode.

```
show ip source-track {address} {summary | cache | export flows}
```

Syntax Description		
address		IP address of the tracked host for which traffic flow information is displayed.
summary		Displays a summary of the traffic flow information collected for a specified host address or for all configured hosts.
cache		Displays detailed packet and flow information collected on line cards/port adapters for all tracked IP addresses or for a specified address (not displayed on the GRP/RSP).
export flows		Displays the packet flow information exported from line cards/port adapters to the GRP/RSP for all tracked IP addresses or for a specified address (available only on the GRP/RSP).

Defaults No default behavior or values.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.0(21)S	This command was introduced.
	12.0(22)S	This command was implemented on the Cisco 7500 series routers.
	12.0(26)S	This command was implemented on Cisco 12000 Series ISE line cards.

Usage Guidelines Use this command to display a summary or details of the traffic flow and packet information collected for all host addresses (or a specific address) configured for IP source tracking.

Examples The following example displays a summary of traffic flow statistics for all host addresses being tracked:

```
Router# show ip source-track summary
Address          Bytes  Pkts  Bytes/s  Pkts/s
100.1.1.1        119G  1194M  443535   4432
100.1.1.2        119G  1194M  443510   4432
100.1.1.3        119G  1194M  443511   4432
```

Related Commands

Command	Description
<code>ip source-track</code>	Enables IP source tracking for a specified host.
<code>ip source-track address-limit</code>	Configures the maximum number of <code>ip source-track</code> commands that you can enter for hosts under attack.
<code>ip source-track export-interval</code>	Sets the time interval used to export IP tracking statistics collected in the line cards/port adapters to the GRP/RSP.
<code>ip source-track syslog-interval</code>	Sets the time interval used to generate syslog messages to remind users that IP source tracking is enabled.

Glossary

ASIC—Application-specific integrated circuit. Used to consolidate many chips into a single package to reduce board size and power consumption.

ACL—Access control list. List of packet filtering rules to provide security features.

CEF—Cisco Express Forwarding. A Layer 3 IP switching technology. CEF optimizes network performance and scalability for networks with large and dynamic traffic patterns, such as the Internet, on networks characterized by intensive Web-based applications, or interactive sessions.

DoS—Denial of Service. Denial of Service (DoS) attacks threaten a Service Provider's ability to ensure the high availability of network resources, such as Web servers. Usually launched by hackers from a bogus IP address, DoS attacks saturate a server or other network device with service requests. The network resource under attack then experiences a "traffic jam" of sorts that prevents customers from accessing it.

FIB—Forwarding information base. A table that contains a mirror image of the forwarding information in the IP routing table. When routing or topology changes occur in the network the route processor updates the IP routing table and CEF updates the FIB.

GRP—Gigabit route processor. The main system processor used in Cisco 12000 series routers.

GSR—Gigabit Switch Router. Former name of the Cisco 12000 series routers.

ISE—IP Services Engine. ISE line cards for Cisco 12000 series Internet Routers provide enhanced Layer 3 capabilities for high-speed customer aggregation, backbone connectivity, and peering solutions. These line cards are available in both concatenated and channelized versions.

LC—Line card. Any I/O card that can be inserted in a modular chassis.

PSA—Packet Switching ASIC. This is also known as Engine 2 on Cisco 12000 series routers.

RP—Route processor. Processor module in the Cisco 7000 family routers that contains the CPU, system software, and most of the memory components that are used in the router. Sometimes called a supervisory processor

RSP—Route switch processor. Processor module in the Cisco 7500 series routers that integrates the functions of the RP and the Switch Processor (SP).

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

Copyright © 2003 Cisco Systems, Inc. All rights reserved.

