



## Configuring IP Services

---

This module describes how to configure optional IP services. For a complete description of the IP services commands in this chapter, refer to the *Cisco IOS IP Application Services Command Reference*. To locate documentation of other commands that appear in this module, use the master command list, or search online.

- [Finding Feature Information, page 1](#)
- [Information About IP Services, page 1](#)
- [How to Configure IP Services, page 2](#)
- [Configuration Examples for IP Services, page 9](#)
- [Additional References, page 9](#)
- [Feature Information for IP Services, page 10](#)

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and 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 module.

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](http://www.cisco.com/go/cfn). An account on Cisco.com is not required.

## Information About IP Services

### Cisco IP Accounting

Cisco IP accounting support provides basic IP accounting functions. By enabling IP accounting, users can see the number of bytes and packets switched through the software on a source and destination IP address basis. Only transit IP traffic is measured and only on an outbound basis; traffic generated by the software or terminating in the software is not included in the accounting statistics. To maintain accurate accounting totals, the software maintains two accounting databases: an active and a checkpointed database.

Cisco IP accounting support also provides information identifying IP traffic that fails IP access lists. Identifying IP source addresses that violate IP access lists alerts you to possible attempts to breach security. The data also indicates that you should verify IP access list configurations. To make this functionality available to users, you must enable IP accounting of access list violations using the **ip accounting access-violations** interface configuration command. Users can then display the number of bytes and packets from a single source that attempted to breach security against the access list for the source destination pair. By default, IP accounting displays the number of packets that have passed access lists and were routed.

## How to Configure IP Services

### Configuring IP Accounting

To configure IP accounting, perform this task for each interface.

#### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip accounting-threshold** *threshold*
4. **ip accounting-list** *ip-address wildcard*
5. **ip accounting-transits** *count*
6. **interface** *type number*
7. **ip accounting** [**access-violations**] [**output-packets**]
8. **ip accounting mac-address** {**input** | **output**}

#### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode.  <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>ip accounting-threshold</b> <i>threshold</i>  <b>Example:</b> Router(config)# ip accounting-threshold 500	(Optional) Sets the maximum number of accounting entries to be created.

	Command or Action	Purpose
<b>Step 4</b>	<b>ip accounting-list</b> <i>ip-address wildcard</i>  <b>Example:</b> <pre>Router(config)# ip accounting-list 192.31.0.0 0.0.255.255</pre>	(Optional) Filters accounting information for hosts.
<b>Step 5</b>	<b>ip accounting-transits</b> <i>count</i>  <b>Example:</b> <pre>Router(config)# ip accounting-transits 100</pre>	(Optional) Controls the number of transit records that will be stored in the IP accounting database.
<b>Step 6</b>	<b>interface</b> <i>type number</i>  <b>Example:</b> <pre>Router(config)# interface GigabitEthernet 1/0/0</pre>	Specifies the interface and enters interface configuration mode.
<b>Step 7</b>	<b>ip accounting</b> [ <b>access-violations</b> ] [ <b>output-packets</b> ]  <b>Example:</b> <pre>Router(config-if)# ip accounting access-violations</pre>	Configures basic IP accounting. <ul style="list-style-type: none"> <li>• Use the optional <b>access-violations</b> keyword to enable IP accounting with the ability to identify IP traffic that fails IP access lists.</li> <li>• Use the optional <b>output-packets</b> keyword to enable IP accounting based on the IP packets output on the interface.</li> </ul>
<b>Step 8</b>	<b>ip accounting mac-address</b> { <b>input</b>   <b>output</b> }  <b>Example:</b> <pre>Router(config-if)# ip accounting mac-address output</pre>	(Optional) Configures IP accounting based on the MAC address of received (input) or transmitted (output) packets.

## Monitoring and Maintaining the IP Network

You can display specific statistics such as the contents of IP routing tables, caches, databases and socket processes. The resulting information can be used to determine resource utilization and to solve network problems.

## SUMMARY STEPS

1. **clear ip traffic**
2. **clear ip accounting [checkpoint]**
3. **clear sockets *process-id***
4. **show ip accounting [checkpoint] [output-packets | access-violations]**
5. **show interface *type number* mac**
6. **show interface [*type number*] precedence**
7. **show ip redirects**
8. **show sockets *process-id* [detail] [events]**
9. **show udp [detail]**
10. **show ip traffic**

## DETAILED STEPS

---

### Step 1 **clear ip traffic**

To clear all IP traffic statistical counters on all interfaces, use the following command:

**Example:**

```
Router# clear ip traffic
```

### Step 2 **clear ip accounting [checkpoint]**

You can remove all contents of a particular cache, table, or database. Clearing a cache, table, or database can become necessary when the contents of the particular structure have become or are suspected to be invalid. To clear the active IP accounting database when IP accounting is enabled, use the following command:

**Example:**

```
Router# clear ip accounting
```

To clear the checkpointed IP accounting database when IP accounting is enabled, use the following command:

**Example:**

```
Router# clear ip accounting checkpoint
```

### Step 3 **clear sockets *process-id***

To close all IP sockets and clear the underlying transport connections and data structures for the specified process, use the following command:

**Example:**

```
Router# clear sockets 35
```

```
All sockets (TCP, UDP and SCTP) for this process will be cleared.
Do you want to proceed? [yes/no]: y
Cleared sockets for PID 35
```

### Step 4 **show ip accounting [checkpoint] [output-packets | access-violations]**

To display access list violations, use the **show ip accounting** command. To use this command, you must first enable IP accounting on a per-interface basis.

Use the **checkpoint** keyword to display the checkpointed database. Use the **output-packets** keyword to indicate that information pertaining to packets that passed access control and were routed should be displayed. Use the **access-violations** keyword to display the number of the access list failed by the last packet for the source and destination pair. The number of packets reveals how aggressive the attack is upon a specific destination. If you do not specify the **access-violations** keyword, the command defaults to displaying the number of packets that have passed access lists and were routed.

If neither the **output-packets** nor **access-violations** keyword is specified, **output-packets** is the default.

The following is sample output from the **show ip accounting** command:

**Example:**

```
Router# show ip accounting
```

Source	Destination	Packets	Bytes
172.16.19.40	192.168.67.20	7	306
172.16.13.55	192.168.67.20	67	2749
172.16.2.50	192.168.33.51	17	1111
172.16.2.50	172.31.2.1	5	319
172.16.2.50	172.31.1.2	463	30991
172.16.19.40	172.16.2.1	4	262
172.16.19.40	172.16.1.2	28	2552
172.16.20.2	172.16.6.100	39	2184
172.16.13.55	172.16.1.2	35	3020
172.16.19.40	192.168.33.51	1986	95091
172.16.2.50	192.168.67.20	233	14908
172.16.13.28	192.168.67.53	390	24817
172.16.13.55	192.168.33.51	214669	9806659
172.16.13.111	172.16.6.23	27739	1126607
172.16.13.44	192.168.33.51	35412	1523980
192.168.7.21	172.163.1.2	11	824
172.16.13.28	192.168.33.2	21	1762
172.16.2.166	192.168.7.130	797	141054
172.16.3.11	192.168.67.53	4	246
192.168.7.21	192.168.33.51	15696	695635
192.168.7.24	192.168.67.20	21	916
172.16.13.111	172.16.10.1	16	1137

accounting threshold exceeded for 7 packets and 433 bytes

The following is sample output from the **show ip accounting access-violations** command. The output pertains to packets that failed access lists and were not routed:

**Example:**

```
Router# show ip accounting access-violations
```

Source	Destination	Packets	Bytes	ACL
172.16.19.40	192.168.67.20	7	306	77
172.16.13.55	192.168.67.20	67	2749	185
172.16.2.50	192.168.33.51	17	1111	140
172.16.2.50	172.16.2.1	5	319	140
172.16.19.40	172.16.2.1	4	262	77

Accounting data age is 41

**Step 5** **show interface type number mac**

To display information for interfaces configured for MAC accounting, use the **show interface mac** command. The following is sample output from the **show interface mac** command:

**Example:**

```
Router# show interface ethernet 0/1 mac
```

```
Ethernet0/1
Input (511 free)
0007.f618.4449(228): 4 packets, 456 bytes, last: 2684ms ago
```

```
Total: 4 packets, 456 bytes
Output (511 free)
0007.f618.4449(228): 4 packets, 456 bytes, last: 2692ms ago
Total: 4 packets, 456 bytes
```

**Step 6** **show interface [type number] precedence**

To display information for interfaces configured for precedence accounting, use the **show interface precedence** command.

The following is sample output from the **show interface precedence** command. In this example, the total packet and byte counts are calculated for the interface that receives (input) or sends (output) IP packets and sorts the results based on IP precedence.

**Example:**

```
Router# show interface ethernet 0/1 precedence
```

```
Ethernet0/1
Input
Precedence 0: 4 packets, 456 bytes
Output
Precedence 0: 4 packets, 456 bytes
```

**Step 7** **show ip redirects**

To display the address of the default router and the address of hosts for which an ICMP redirect message has been received, use the **show ip redirects** command.

**Example:**

```
Router# show ip redirects
```

```
Default gateway is 172.16.80.29
```

Host	Gateway	Last Use	Total Uses	Interface
172.16.1.111	172.16.80.240	0:00	9	Ethernet0
172.16.1.4	172.16.80.240	0:00	4	Ethernet0

**Step 8** **show sockets process-id [detail] [events]**

To display the number of sockets currently open and their distribution with respect to the transport protocol process specified by the *process-id* argument, use the **show sockets** command. The following sample output from the **show sockets** command displays the total number of open sockets for the specified process:

**Example:**

```
Router# show sockets 35
```

```
Total open sockets - TCP:7, UDP:0, SCTP:0
```

The following sample output shows information about the same open processes with the **detail** keyword specified:

**Example:**

```
Router# show sockets 35 detail
```

```
FD LPort FPort Proto Type TransID
0 5000 0 TCP STREAM 0x6654DEBC
State: SS_ISBOUND
Options: SO_ACCEPTCONN

1 5001 0 TCP STREAM 0x6654E494
State: SS_ISBOUND
Options: SO_ACCEPTCONN

2 5002 0 TCP STREAM 0x656710B0
```

```

State: SS_ISBOUND
Options: SO_ACCEPTCONN

 3 5003 0 TCP STREAM 0x65671688
State: SS_ISBOUND
Options: SO_ACCEPTCONN

 4 5004 0 TCP STREAM 0x65671C60
State: SS_ISBOUND
Options: SO_ACCEPTCONN

 5 5005 0 TCP STREAM 0x65672238
State: SS_ISBOUND
Options: SO_ACCEPTCONN

 6 5006 0 TCP STREAM 0x64C7840C
State: SS_ISBOUND
Options: SO_ACCEPTCONN
    
```

Total open sockets - TCP:7, UDP:0, SCTP:0

The following example displays IP socket event information:

**Example:**

```

Router# show sockets 35 events

Events watched for this process: READ
FD Watched Present Select Present

0 --- --- R-- R--
    
```

**Step 9**

**show udp [detail]**

To display IP socket information about UDP processes, use the **show udp** command. The following example shows how to display detailed information about UDP sockets:

**Example:**

```

Router# show udp detail

Proto Remote Port Local Port In Out Stat TTY OutputIF
17 10.0.0.0 0 10.0.21.70 67 0 0 2211 0
Queues: output 0
input 0 (drops 0, max 50, highwater 0)
Proto Remote Port Local Port In Out Stat TTY OutputIF
17 10.0.0.0 0 10.0.21.70 2517 0 0 11 0
Queues: output 0
input 0 (drops 0, max 50, highwater 0)
Proto Remote Port Local Port In Out Stat TTY OutputIF
17 10.0.0.0 0 10.0.21.70 5000 0 0 211 0
Queues: output 0
input 0 (drops 0, max 50, highwater 0)
Proto Remote Port Local Port In Out Stat TTY OutputIF
17 10.0.0.0 0 10.0.21.70 5001 0 0 211 0
Queues: output 0
input 0 (drops 0, max 50, highwater 0)
Proto Remote Port Local Port In Out Stat TTY OutputIF
17 10.0.0.0 0 10.0.21.70 5002 0 0 211 0
Queues: output 0
input 0 (drops 0, max 50, highwater 0)
Proto Remote Port Local Port In Out Stat TTY OutputIF
17 10.0.0.0 0 10.0.21.70 5003 0 0 211 0
Queues: output 0
input 0 (drops 0, max 50, highwater 0)
Proto Remote Port Local Port In Out Stat TTY OutputIF
17 10.0.0.0 0 10.0.21.70 5004 0 0 211 0
    
```

```
Queues: output 0
        input 0 (drops 0, max 50, highwater 0)
```

### Step 10 show ip traffic

To display IP protocol statistics, use the **show ip traffic** command. The following example shows that the IP traffic statistics have been cleared by the **clear ip traffic** command:

#### Example:

```
Router# clear ip traffic
```

```
Router# show ip traffic
```

```
IP statistics:
Rcvd: 0 total, 0 local destination
      0 format errors, 0 checksum errors, 0 bad hop count
      0 unknown protocol, 0 not a gateway
      0 security failures, 0 bad options, 0 with options
Opts: 0 end, 0 nop, 0 basic security, 0 loose source route
      0 timestamp, 0 extended security, 0 record route
      0 stream ID, 0 strict source route, 0 alert, 0 cipso
      0 other
Frgs: 0 reassembled, 0 timeouts, 0 couldn't reassemble
      0 fragmented, 0 couldn't fragment
Bcast: 0 received, 0 sent
Mcast: 0 received, 0 sent
Sent: 0 generated, 0 forwarded
Drop: 0 encapsulation failed, 0 unresolved, 0 no adjacency
      0 no route, 0 unicast RPF, 0 forced drop

ICMP statistics:
Rcvd: 0 format errors, 0 checksum errors, 0 redirects, 0 unreachable
      0 echo, 0 echo reply, 0 mask requests, 0 mask replies, 0 quench
      0 parameter, 0 timestamp, 0 info request, 0 other
      0 irdp solicitations, 0 irdp advertisements
Sent: 0 redirects, 0 unreachable, 0 echo, 0 echo reply
      0 mask requests, 0 mask replies, 0 quench, 0 timestamp
      0 info reply, 0 time exceeded, 0 parameter problem
      0 irdp solicitations, 0 irdp advertisements

UDP statistics:
Rcvd: 0 total, 0 checksum errors, 0 no port
Sent: 0 total, 0 forwarded broadcasts

TCP statistics:
Rcvd: 0 total, 0 checksum errors, 0 no port
Sent: 0 total

Probe statistics:
Rcvd: 0 address requests, 0 address replies
      0 proxy name requests, 0 where-is requests, 0 other
Sent: 0 address requests, 0 address replies (0 proxy)
      0 proxy name replies, 0 where-is replies

EGP statistics:
Rcvd: 0 total, 0 format errors, 0 checksum errors, 0 no listener
Sent: 0 total

IGRP statistics:
Rcvd: 0 total, 0 checksum errors
Sent: 0 total

OSPF statistics:
Rcvd: 0 total, 0 checksum errors
      0 hello, 0 database desc, 0 link state req
      0 link state updates, 0 link state acks

Sent: 0 total
```



```

IP-IGRP2 statistics:
  Rcvd: 0 total
  Sent: 0 total

PIMv2 statistics: Sent/Received
  Total: 0/0, 0 checksum errors, 0 format errors
  Registers: 0/0, Register Stops: 0/0, Hellos: 0/0
  Join/Prunes: 0/0, Asserts: 0/0, grafts: 0/0
  Bootstraps: 0/0, Candidate_RP_Advertisements: 0/0

IGMP statistics: Sent/Received
  Total: 0/0, Format errors: 0/0, Checksum errors: 0/0
  Host Queries: 0/0, Host Reports: 0/0, Host Leaves: 0/0
  DVMRP: 0/0, PIM: 0/0

```

## Configuration Examples for IP Services

### Example: Configuring IP Accounting

The following example shows how to enable IP accounting based on the source and destination MAC address and based on IP precedence for received and transmitted packets:

```

Router# configure terminal
Router(config)# interface ethernet 0/5
Router(config-if)# ip accounting mac-address input
Router(config-if)# ip accounting mac-address output
Router(config-if)# ip accounting precedence input
Router(config-if)# ip accounting precedence output

```

The following example shows how to enable IP accounting with the ability to identify IP traffic that fails IP access lists and with the number of transit records that will be stored in the IP accounting database limited to 100:

```

Router# configure terminal
Router(config)# ip accounting-transits 100
Router(config)# interface ethernet 0/5
Router(config-if)# ip accounting output-packets
Router(config-if)# ip accounting access-violations

```

## Additional References

### Related Documents

Related Topic	Document Title
Cisco IOS commands	<a href="#">Cisco IOS Master Commands List, All Releases</a>
IP application services commands	<a href="#">Cisco IOS IP Application Services Command Reference</a>

**Standards and RFCs**

Standard	Title
RFC 1256	<a href="#">ICMP Router Discovery Messages</a>

**Technical Assistance**

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	<a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a>

## Feature Information for IP Services

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](http://www.cisco.com/go/cfn). An account on Cisco.com is not required.

**Table 1: Feature Information for IP Services**

Feature Name	Releases	Feature Information
IP Precedence Accounting	15.0(1)SY	<p>The IP Precedence Accounting feature provides accounting information for IP traffic based on the precedence of any interface. This feature calculates the total packet and byte counts for an interface that receives or sends IP packets and sorts the results based on the IP precedence. This feature is supported on all interfaces and subinterfaces and supports Cisco Express Forwarding, distributed Cisco Express Forwarding, flow, and optimum switching.</p> <p>The following commands were introduced by this feature: <b>ip accounting precedence</b>, <b>show interface precedence</b>.</p>

