show i

show idb

要显示有关接口描述符块状态的信息（表示接口资源的内部数据结构），请使用 **show idb** 命令。

show idb

Command History

版本	修改
6.1	引入了此命令。

示例

以下是 **show idb** 命令的输出示例：

```
> show idb
Maximum number of Software IDBs 2252.  In use(total) 16. In use(active) 16

                    HWIDBs     SWIDBs
              Active 15         15
            Inactive 1          1
          Total IDBs 16         16
 Size each (bytes) 984        1512
        Total bytes 15744      24192

HWIDB#  1 0xdacf1420  Virtual0
HWIDB#  2 0xdac4da20  GigabitEthernet1/1
HWIDB#  3 0xdac5aa20  GigabitEthernet1/2
HWIDB#  4 0xdac651b0  GigabitEthernet1/3
HWIDB#  5 0xdac6f940  GigabitEthernet1/4
HWIDB#  6 0xdac7a0d0  GigabitEthernet1/5
HWIDB#  7 0xdac84860  GigabitEthernet1/6
HWIDB#  8 0xdac8eff0  GigabitEthernet1/7
HWIDB#  9 0xdac99780  GigabitEthernet1/8
HWIDB# 10 0xdacbda00  Internal-Control1/1
HWIDB# 11 0xdaca3f10  Internal-Data1/1
HWIDB# 12 0xdacb3260  Internal-Data1/2
HWIDB# 13 0xdacc81a0  Internal-Data1/3
HWIDB# 14 0xd409e4e0  Internal-Data1/4
HWIDB# 15 0xd409d090  Management1/1

SWIDB#  1 0xdacf1840 0x00000041 Virtual0 UP UP
SWIDB#  2 0xdac4de40 0x00000002 GigabitEthernet1/1 UP DOWN
SWIDB#  3 0xdac5ae40 0x00000003 GigabitEthernet1/2 UP DOWN
SWIDB#  4 0xdac655d0 0xffffffff GigabitEthernet1/3 DOWN DOWN
SWIDB#  5 0xdac6fd60 0xffffffff GigabitEthernet1/4 DOWN DOWN
SWIDB#  6 0xdac7a4f0 0xffffffff GigabitEthernet1/5 DOWN DOWN
SWIDB#  7 0xdac84c80 0xffffffff GigabitEthernet1/6 DOWN DOWN
SWIDB#  8 0xdac8f410 0xffffffff GigabitEthernet1/7 DOWN DOWN
SWIDB#  9 0xdac99ba0 0xffffffff GigabitEthernet1/8 DOWN DOWN
SWIDB# 10 0xdacbde20 0x0000003f Internal-Control1/1 UP UP
SWIDB# 11 0xdaca4330 0x00000043 Internal-Data1/1 UP UP
SWIDB# 12 0xdacb3680 0xffffffff Internal-Data1/2 UP UP
SWIDB# 13 0xdacc85c0 0x00000044 Internal-Data1/3 UP UP
SWIDB# 14 0xdacae210 0x00000045 Internal-Data1/4 UP UP
SWIDB# 15 0xd409d4b0 0x00000004 Management1/1 UP UP
```

下表对每个字段进行了说明。

表 *1: show idb stats* 字段

字段	说明
HWIDB	显示所有 HWIDB 的统计信息。为系统中的每个硬件端口创建 HWIDB。
SWIDB	显示所有 SWIDB 的统计信息。为系统中的每个主接口和子接口以及分配给情景的每个接口创建 SWIDB。 其他一些内部软件模块还会创建 IDB。
HWIDB#	指定硬件接口条目。IDB 序列号、地址和接口名称显示在每行中。
SWIDB#	指定软件接口条目。IDB 序列号、地址、对应的 vPif ID 和接口名称显示在每行中。
PEER IDB#	指定分配给情景的接口。IDB 序列号、地址、对应的 vPif ID 和接口名称显示在每行中。

Related Commands

命令	说明
show interface	显示接口的运行时间状态和统计信息。

show identity-subnet-filter

要显示从接收用户到 IP 和安全组标记 (SGT) 到 IP 映射中排除的子网，请使用 **show identity-subnet-filter** 命令。

show identity-subnet-filter

Command History

版本	修改
6.7	引入了此命令。

使用指南

show identity-subnet-filter 命令显示当前从用户到 IP 和安全组标记 (SGT) 到 IP 映射中排除的所有子网。

示例

如果当前未排除任何子网，则 **show identity-subnet-filter** 命令的输出示例如下：

```
> show identity-subnet-filter

Subnet filter file doesn't exist
```

如果当前排除了某些子网，则 **show identity-subnet-filter** 命令的输出示例如下：

```
> show identity-subnet-filter

Subnet filters are:
2001:db8::2/64
192.0.2.0/24
```

Related Commands

命令	说明
configure identity-subnet-filter	从用户到 IP 和 SGT 到 IP 映射中排除子网。

show igmp groups

要显示其接收器直接连接到 威胁防御 设备并且通过 IGMP 获知的组播组，请使用 **show igmp groups** 命令。

show igmp groups [[**reserved** | *group*] [*if_name*] [**detail**]] | **summary**]

Syntax Description

detail	（可选）提供源的详细说明。
group	（可选）IGMP 组的地址。包括此可选参数可限制只显示指定的组。
if_name	（可选）显示指定接口的组信息。
reserved	（可选）显示有关预留组的信息。
summary	（可选）显示组加入汇总信息。

Command History

版本	修改
6.1	引入了此命令。

使用指南

如果省略所有可选参数和关键字，则 **show igmp groups** 命令会按组地址、接口类型和接口号显示所有直接连接的组播组。

示例

以下是 **show igmp groups** 命令的输出示例：

```
> show igmp groups

IGMP Connected Group Membership
Group Address    Interface            Uptime    Expires   Last Reporter
224.1.1.1        inside               00:00:53  00:03:26  192.168.1.6
```

Related Commands

命令	说明
show igmp interface	显示接口的组播信息。

show igmp interface

要显示接口的组播信息，请使用 **show igmp interface** 命令。

show igmp interface ［*if_name*］

Syntax Description

if_name	（可选）显示选定接口的 IGMP 组信息。

Command History

版本	修改
6.1	引入了此命令。

使用指南

如果省略可选 *if_name* 参数，则 **show igmp interface** 命令会显示有关所有接口的信息。

示例

以下是 **show igmp interface** 命令的输出示例：

```
> show igmp interface inside

inside is up, line protocol is up
 Internet address is 192.168.37.6, subnet mask is 255.255.255.0
 IGMP is enabled on interface
 IGMP query interval is 60 seconds
 Inbound IGMP access group is not set
 Multicast routing is enabled on interface
 Multicast TTL threshold is 0
 Multicast designated router (DR) is 192.168.37.33
 No multicast groups joined
```

Related Commands

命令	说明
show igmp groups	显示其接收器直接连接到 威胁防御 设备并且通过 IGMP 获知的组播组。

show igmp traffic

要显示 IGMP 流量统计信息，请使用 **show igmp traffic** 命令。

show igmp traffic

Command History

版本	修改
6.1	引入了此命令。

示例

以下是 **show igmp traffic** 命令的输出示例：

```
> show igmp traffic

IGMP Traffic Counters
Elapsed time since counters cleared: 00:02:30
                              Received     Sent
Valid IGMP Packets               3           6
Queries                          2           6
Reports                          1           0
Leaves                           0           0
Mtrace packets                   0           0
DVMRP packets                    0           0
PIM packets                      0           0

Errors:
Malformed Packets                0
Martian source                   0
Bad Checksums                    0
```

Related Commands

命令	说明
clear igmp counters	清除所有 IGMP 统计信息计数器。
clear igmp traffic	清除 IGMP 流量计数器。

show inline-set

要查看有关设备上配置的内联集（仅 IPS 接口）的信息，请使用 **show inline-set** 命令。

show inline-set ［*inline-set-name* | **mac-address-table**］

Syntax Description

inline-set-name	（可选）显示有关指定内联集的信息。如果不包括名称，则显示所有内联集。
mac-address-table	（可选）显示内联集的 MAC 地址网桥表。

Command History

版本	修改
6.1	引入了此命令。

示例

以下是 **show inline-set** 命令的输出示例：

```
> show inline-set
Inline-set ips-inline
  Mtu is 1500 bytes
  Fail-open for snort down is on
  Fail-open for snort busy is off
  Tap mode is off
  Propagate-link-state option is off
  hardware-bypass mode is disabled
  Interface-Pair[1]:
    Interface: GigabitEthernet0/3 "inline-inside"
      Current-Status: UP
    Interface: GigabitEthernet0/4 "inline-outside"
      Current-Status: DOWN
    Bridge Group ID: 504
```

show interface

要查看接口统计信息，请使用 **show interface** 命令。

show interface [{*physical_interface* | **redundant***number*}[**.***subinterface*] | *interface_name* | **BVI** *ID* |] [**summary** | **stats** | **detail**]

Syntax Description

BVI *id*	（可选）显示指定网桥虚拟接口 (BVI) 的统计信息。输入 BVI 编号（1-250）。
detail	（可选）显示接口详细信息，包括添加接口的顺序、配置状态、真实状态和非对称路由统计信息（如果已启用）。 如果显示所有接口，则还会看到有关用于系统通信的内部接口的信息。用户无法配置内部接口，该信息只用于调试目的。
interface_name	（可选）按逻辑名称标识接口。
physical_interface	（可选）标识接口 ID，例如 **gigabitethernet0/1**。可用接口因设备型号而异。使用不带参数的 show interface 命令查看设备上可用的名称。
redundant*number*	（可选）标识冗余接口 ID，例如 **redundant1**。
stats	（默认）显示接口信息和统计信息。此关键字是默认值，而且是可选的。
summary	（可选）显示有关接口的摘要信息。
subinterface	（可选）识别一个介于 1 到 4294967293 之间整数，用以指定逻辑子接口。

Command Default

如果您不标识任何选项，则此命令显示除内部接口外的所有接口的基础统计。

Command History

版本	修改
6.1	引入了此命令。
6.2	添加了 **BVI** 关键字。
6.7	在数据接口上配置访问 管理中心 权限时，已将输出添加到 Internal-Data0/1 "nlp_int_tap" 接口的 **detail** 关键字中。

使用指南

为子接口显示的统计信息数是为物理接口显示的统计信息数的子集。

注释 硬件中传输或接收的字节数计数和流量统计信息计数不同。

在硬件计数中，数量直接从硬件检索，并反映第 2 层数据包大小。而在流量统计信息中，它反映第 3 层数据包大小。

计数差异因接口卡硬件的具体设计而有所不同。

例如，对于快速以太网卡，因为它包括以太网信头，所以第 2 层计数比流量计数大 14 字节。对于千兆位以太网卡，因为它包括以太网信头和 CRC，所以第 2 层计数比流量计数大 18 字节。

请参阅“示例”部分，了解显示输出的说明。

示例

以下是 **show interface** 命令的输出示例：

```
> show interface
Interface GigabitEthernet1/1 "outside", is down, line protocol is down
  Hardware is Accelerator rev01, BW 1000 Mbps, DLY 10 usec
        Auto-Duplex, Auto-Speed
        Input flow control is unsupported, output flow control is off
        MAC address e865.49b8.97f2, MTU 1500
        IP address unassigned
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 pause input, 0 resume input
        0 L2 decode drops
        0 packets output, 0 bytes, 0 underruns
        0 pause output, 0 resume output
        0 output errors, 0 collisions, 0 interface resets
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
        input queue (blocks free curr/low): hardware (2047/2047)
        output queue (blocks free curr/low): hardware (2047/2047)
  Traffic Statistics for "outside":
        0 packets input, 0 bytes
        0 packets output, 0 bytes
        0 packets dropped
      1 minute input rate 0 pkts/sec,  0 bytes/sec
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  0 bytes/sec
      5 minute output rate 0 pkts/sec,  0 bytes/sec
      5 minute drop rate, 0 pkts/sec
Interface GigabitEthernet1/2 "inside", is down, line protocol is down
  Hardware is Accelerator rev01, BW 1000 Mbps, DLY 10 usec
        Auto-Duplex, Auto-Speed
        Input flow control is unsupported, output flow control is off
        MAC address e865.49b8.97f3, MTU 1500
        IP address 192.168.45.1, subnet mask 255.255.255.0
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 pause input, 0 resume input
        0 L2 decode drops
        0 packets output, 0 bytes, 0 underruns
```

```
        0 pause output, 0 resume output
        0 output errors, 0 collisions, 0 interface resets
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
        input queue (blocks free curr/low): hardware (2047/2047)
        output queue (blocks free curr/low): hardware (2047/2047)
  Traffic Statistics for "inside":
        0 packets input, 0 bytes
        0 packets output, 0 bytes
        0 packets dropped
      1 minute input rate 0 pkts/sec,  0 bytes/sec
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  0 bytes/sec
      5 minute output rate 0 pkts/sec,  0 bytes/sec
      5 minute drop rate, 0 pkts/sec
Interface GigabitEthernet1/3 "", is administratively down, line protocol is down
  Hardware is Accelerator rev01, BW 1000 Mbps, DLY 10 usec
        Auto-Duplex, Auto-Speed
        Input flow control is unsupported, output flow control is off
        Available but not configured via nameif
        MAC address e865.49b8.97f4, MTU not set
        IP address unassigned
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 pause input, 0 resume input
        0 L2 decode drops
        0 packets output, 0 bytes, 0 underruns
        0 pause output, 0 resume output
        0 output errors, 0 collisions, 0 interface resets
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
        input queue (blocks free curr/low): hardware (2047/2047)
        output queue (blocks free curr/low): hardware (2047/2047)
Interface GigabitEthernet1/4 "", is administratively down, line protocol is down
  Hardware is Accelerator rev01, BW 1000 Mbps, DLY 10 usec
        Auto-Duplex, Auto-Speed
        Input flow control is unsupported, output flow control is off
        Available but not configured via nameif
        MAC address e865.49b8.97f5, MTU not set
        IP address unassigned
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 pause input, 0 resume input
        0 L2 decode drops
        0 packets output, 0 bytes, 0 underruns
        0 pause output, 0 resume output
        0 output errors, 0 collisions, 0 interface resets
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
        input queue (blocks free curr/low): hardware (2047/2047)
        output queue (blocks free curr/low): hardware (2047/2047)
Interface GigabitEthernet1/5 "", is administratively down, line protocol is down
  Hardware is Accelerator rev01, BW 1000 Mbps, DLY 10 usec
        Auto-Duplex, Auto-Speed
        Input flow control is unsupported, output flow control is off
        Available but not configured via nameif
        MAC address e865.49b8.97f6, MTU not set
        IP address unassigned
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
```

```
        0 pause input, 0 resume input
        0 L2 decode drops
        0 packets output, 0 bytes, 0 underruns
        0 pause output, 0 resume output
        0 output errors, 0 collisions, 0 interface resets
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
        input queue (blocks free curr/low): hardware (2047/2047)
        output queue (blocks free curr/low): hardware (2047/2047)
Interface GigabitEthernet1/6 "", is administratively down, line protocol is down
  Hardware is Accelerator rev01, BW 1000 Mbps, DLY 10 usec
        Auto-Duplex, Auto-Speed
        Input flow control is unsupported, output flow control is off
        Available but not configured via nameif
        MAC address e865.49b8.97f7, MTU not set
        IP address unassigned
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 pause input, 0 resume input
        0 L2 decode drops
        0 packets output, 0 bytes, 0 underruns
        0 pause output, 0 resume output
        0 output errors, 0 collisions, 0 interface resets
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
        input queue (blocks free curr/low): hardware (2047/2047)
        output queue (blocks free curr/low): hardware (2047/2047)
Interface GigabitEthernet1/7 "", is administratively down, line protocol is down
  Hardware is Accelerator rev01, BW 1000 Mbps, DLY 10 usec
        Auto-Duplex, Auto-Speed
        Input flow control is unsupported, output flow control is off
        Available but not configured via nameif
        MAC address e865.49b8.97f8, MTU not set
        IP address unassigned
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 pause input, 0 resume input
        0 L2 decode drops
        0 packets output, 0 bytes, 0 underruns
        0 pause output, 0 resume output
        0 output errors, 0 collisions, 0 interface resets
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
        input queue (blocks free curr/low): hardware (2047/2047)
        output queue (blocks free curr/low): hardware (2047/2047)
Interface GigabitEthernet1/8 "", is administratively down, line protocol is down
  Hardware is Accelerator rev01, BW 1000 Mbps, DLY 10 usec
        Auto-Duplex, Auto-Speed
        Input flow control is unsupported, output flow control is off
        Available but not configured via nameif
        MAC address e865.49b8.97f9, MTU not set
        IP address unassigned
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 pause input, 0 resume input
        0 L2 decode drops
        0 packets output, 0 bytes, 0 underruns
        0 pause output, 0 resume output
        0 output errors, 0 collisions, 0 interface resets
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
```

```
        input queue (blocks free curr/low): hardware (2047/2047)
        output queue (blocks free curr/low): hardware (2047/2047)
Interface Management1/1 "diagnostic", is up, line protocol is up
  Hardware is en_vtun rev00, BW 1000 Mbps, DLY 10 usec
        Auto-Duplex(Full-duplex), Auto-Speed(1000 Mbps)
        Input flow control is unsupported, output flow control is off
        MAC address e865.49b8.97f1, MTU 1500
        IP address unassigned
        14247681 packets input, 896591753 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 pause input, 0 resume input
        0 L2 decode drops
        0 packets output, 0 bytes, 0 underruns
        0 pause output, 0 resume output
        0 output errors, 0 collisions, 0 interface resets
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
        input queue (blocks free curr/low): hardware (0/0)
        output queue (blocks free curr/low): hardware (0/0)
  Traffic Statistics for "diagnostic":
        14247685 packets input, 697121911 bytes
        0 packets output, 0 bytes
        5054964 packets dropped
      1 minute input rate 2 pkts/sec,  131 bytes/sec
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 2 pkts/sec,  108 bytes/sec
      5 minute output rate 0 pkts/sec,  0 bytes/sec
      5 minute drop rate, 0 pkts/sec
        Management-only interface. Blocked 0 through-the-device packets
```

下表显示每个字段的说明。

表 *2: show interface* 字段

字段	说明
Interface ID	接口 ID。
“interface_name”	逻辑接口名称。如果不配置名称，则在硬件行之后会出现以下消息： `Available but not configured via nameif`
is *state*	管理状态，如下所示： • up - 接口没有关闭。 • administratively down - 人为地关闭接口。
Line protocol is state	线路状态，如下所示： • up - 工作电缆插入网络接口。 • down - 电缆不正确或未插入接口连接器。
VLAN identifier	对于子接口，是 VLAN ID。

字段	说明
Hardware	接口类型、最大带宽、延迟、复用和速度。在链路断开时，复用和速度显示配置的值。当链路连通时，这些字段显示配置的值，并在括号中包含实际设置。
Media-type	（并非始终显示）显示接口介质类型，例如 RJ-45 或 SFP。
message area	在某些情况下可能显示消息。请参阅以下示例： • 如果不配置名称，您会看到以下消息：Available but not configured via nameif • 如果接口是冗余接口的成员，您会看到以下消息：Active member of Redundant5
MAC address	接口 MAC 地址。
Site Specific MAC address	对于集群技术， 显示正在使用的站点特定 MAC 地址。
MTU	此接口上允许的最大数据包大小（以字节表示）。如果没有设置接口名称，此字段显示“MTU not set”（未设置 MTU）。
IP address	接口 IP 地址，静态或从 DHCP 服务器接收。
Subnet mask	IP 地址的子网掩码。
Packets input	此接口上接收的数据包数。
Bytes	此接口上接收的字节数。
No buffer	块分配的失败数。
Received:	
Broadcasts	接收的广播数。
Input errors	输入错误总数，包括如下所示的类型。其他与输入有关的错误也可能导致输入错误计数增加，并且一些数据报可能有多个错误；因此，这个总数可能超过以下类型列出的错误数。
Runts	由于小于最小数据包大小（64 字节）而丢弃的数据包数。超短帧通常是由冲突引起的。也可能是由接线不良和电子干扰引起的。
Giants	由于超出最大数据包大小而丢弃的数据包数。例如，大于 1518 字节的所有以太网数据包均被视为超长帧。

字段	说明
CRC	循环冗余检查错误数。当站发送帧时，会将 CRC 附加到帧尾。此 CRC 是使用算法基于帧中的数据生成的。如果在源和目的地之间更改了帧，系统会注意到 CRC 不匹配。CRC 数量过大通常是冲突或站传输错误数据引起的。
Frame	帧错误数。错误的帧包含长度不正确或帧校验和错误的数据包。此错误通常是冲突或以太网设备故障引起的。
Overrun	因输入速度超出接口处理数据的能力而导致接口无法将接收的数据传递至硬件缓冲区的次数。
Ignored	不使用此字段。值始终为 0。
Abort	不使用此字段。值始终为 0。
L2 decode drops	因未配置名称或接收具有无效 VLAN ID 的帧而丢弃的数据包。在冗余接口配置中的备用接口上，此计数器的数值可能因该接口没有配置名称而增加。
Packets output	在此接口上发送的数据包数。
Bytes	在此接口上发送的字节数。
Underruns	发射器运行速度比接口处理速度更快的次数
Output Errors	因超过已配置的最大冲突数而未传输的帧数。在网络流量巨大时，此计数器的数值只会增加。
Collisions	由于以太网冲突（单一和多个冲突）而重新传输的消息数。这通常发生在过度扩展的 LAN（以太网或收发器电缆太长、站之间超过两个中继器或层叠的多端口收发器太多）上。输出数据包仅对发生冲突的数据包计数一次。
Interface resets	接口已重置的次数。如果接口在三秒内无法传输，系统会重置接口以重启传输。在此时间间隔内，保持连接状态。接口环回或关闭时，也会出现接口重置。
Babbles	未使用。（“babble”意味着发射器在接口上的时间大于传输最大帧所花费的时间。）

字段	说明
Late collisions	因冲突发生在正常冲突时间范围之外而未传输的帧数。延迟冲突是在传输数据包中延迟检测到的冲突。通常，这些不应该发生。当两台以太网主机同时尝试通信时，它们应在数据包的早期阶段发生冲突且双方都退出，或者第二台主机应看到第一台正在通信和等待。 如果遇到延迟冲突，设备将迅速行动并尝试在以太网上发送数据包，而 威胁防御 设备已部分完成发送数据包。 威胁防御 设备不重新发送数据包，因为它可能已释放保留数据包第一部分的缓冲区。这不是真正的问题，因为网络协议设计为通过重新发送数据包来解决冲突。但是，延迟冲突指示您的网络中存在问题。常见问题是运行着大量重复的网络和以太网络，超出了指定范围。
Deferred	在传输之前由于链路上的活动而延迟的帧数。
input reset drops	当发生重置时，计算 RX 环中丢弃的数据包数。
output reset drops	当发生重置时，计算 RX 环中丢弃的数据包数。
Rate limit drops	将接口配置为非千兆位速度而尝试传输超过 10 Mbps 或 100 Mbps（具体取决于配置）时丢弃的数据包数。
Lost carrier	在传输期间载波信号丢失的次数。
No carrier	未使用。
Input queue (curr/max packets):	输入队列中数据包的当前数和最大数。
Hardware	硬件队列中的数据包数。
Software	软件队列中的数据包数。对千兆位以太网接口不可用。
Output queue (curr/max packets):	输出队列中数据包的当前数和最大数。
Hardware	硬件队列中的数据包数。
Software	软件队列中的数据包数。
input queue (blocks free curr/low)	当前/低条目指示接口的接收（输入）描述符环上当前可用和始终可用的最低插槽数。这些数值由主 CPU 更新，因此最低（直到接口统计信息清除或设备重新加载）水印不是十分准确。
output queue (blocks free curr/low)	当前/低条目指示接口的接收传输（输出）描述符环上当前可用和始终可用的最低插槽数。这些数值由主 CPU 更新，因此最低（直到接口统计信息清除或设备重新加载）水印不是十分准确。
Traffic Statistics:	接收、传输或丢弃的数据包数。

字段	说明
Packets input	The number of packets received and the number of bytes.
Packets output	传输的数据包数和字节数。
Packets dropped	丢弃的数据包数。通常，当加速安全路径(ASP)上丢弃数据包（例如，如果数据包由于访问列表拒绝而被丢弃）时，此计数器数值会增加。 有关接口上潜在丢弃的原因，请参阅 **show asp drop** 命令。
1 minute input rate	在过去一分钟内接收的数据包数（包/秒和字节/秒）。
1 minute output rate	在过去一分钟内传输的数据包数（包/秒和字节/秒）。
1 minute drop rate	在过去一分钟内丢弃的数据包数（包/秒）。
5 minute input rate	在过去 5 分钟内接收的数据包数（包/秒和字节/秒）。
5 minute output rate	在过去 5 分钟内传输的数据包数（包/秒和字节/秒）。
5 minute drop rate	在过去 5 分钟内丢弃的数据包数（包/秒）。
Redundancy Information:	对冗余接口，显示成员的物理接口。主用接口在接口ID后有“(Active)”。 如果您尚未指定成员，您会看到以下输出： `Members unassigned`
Last switchover	对冗余接口，显示上次主用接口故障切换到备用接口的时间。

注释 **show interface detail** 命令结果中的输入和输出速率可能与 管理中心 用户界面的接口模块中显示的输入和输出流量速率不同。

接口模块根据Snort性能监控的值显示流量速率。Snort性能监控和接口统计信息的采样间隔不同。这种采样间隔的差异会导致 管理中心 用户界面和 **show interface detail** 命令结果中的吞吐量值不同。

以下是**show interface detail**命令的输出示例。以下示例展示所有接口的详细接口统计信息，包括内部接口（如果针对您的平台存在）和非对称路由统计信息（如果已启用）：

```
> show interface detail
Interface GigabitEthernet0/0 "outside", is up, line protocol is up
  Hardware is i82546GB rev03, BW 1000 Mbps, DLY 1000 usec
        Auto-Duplex(Full-duplex), Auto-Speed(100 Mbps)
        MAC address 000b.fcf8.c44e, MTU 1500
        IP address 10.86.194.60, subnet mask 255.255.254.0
        1330214 packets input, 124580214 bytes, 0 no buffer
        Received 1216917 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
```

```
        9 L2 decode drops
        124863 packets output, 86956597 bytes, 0 underruns
        0 output errors, 0 collisions
        0 late collisions, 0 deferred
        input queue (curr/max packets): hardware (0/7)
        output queue (curr/max packets): hardware (0/13)
  Traffic Statistics for "outside":
        1330201 packets input, 99995120 bytes
        124863 packets output, 84651382 bytes
        525233 packets dropped
Queue Stats:
      RX[00]: 6599382 packets, 697116251 bytes, 0 overrun
              Blocks free curr/low: 512/432
      RX[01]: 924929 packets, 258924873 bytes, 0 overrun
              Blocks free curr/low: 512/483
      RX[02]: 832587 packets, 245912949 bytes, 0 overrun
              Blocks free curr/low: 512/479
      RX[03]: 1581947 packets, 327352778 bytes, 0 overrun
              Blocks free curr/low: 512/466
      RX[04]: 1248125 packets, 304273571 bytes, 0 overrun
              Blocks free curr/low: 512/491
      RX[05]: 1040026 packets, 420338105 bytes, 0 overrun
              Blocks free curr/low: 512/476
      RX[06]: 995323 packets, 343474141 bytes, 0 overrun
              Blocks free curr/low: 512/433
      RX[07]: 73018771 packets, 46411510982 bytes, 0 overrun
              Blocks free curr/low: 512/463
      RX[08]: 0 packets, 0 bytes, 0 overrun
              Blocks free curr/low: 512/512
      RX[09]: 0 packets, 0 bytes, 0 overrun
              Blocks free curr/low: 512/512
      RX[10]: 0 packets, 0 bytes, 0 overrun
              Blocks free curr/low: 512/512
 RX[11]: 0 packets, 0 bytes, 0 overrun
              Blocks free curr/low: 512/512
      RX[12]: 0 packets, 0 bytes, 0 overrun
              Blocks free curr/low: 512/512
      RX[13]: 0 packets, 0 bytes, 0 overrun
              Blocks free curr/low: 512/512
      RX[14]: 94177 packets, 17778198 bytes, 0 overrun
              Blocks free curr/low: 512/505
      RX[256]: 6 packets, 96 bytes, 0 overrun
              Blocks free curr/low: 512/512
      RX[257]: 180 packets, 3332 bytes, 0 overrun
              Blocks free curr/low: 512/512
      RX[258]: 0 packets, 0 bytes, 0 overrun
              Blocks free curr/low: 512/512
      RX[259]: 9 packets, 144 bytes, 0 overrun
              Blocks free curr/low: 512/512
      RX[260]: 0 packets, 0 bytes, 0 overrun
              Blocks free curr/low: 512/512
      RX[261]: 6 packets, 96 bytes, 0 overrun
              Blocks free curr/low: 512/512
      RX[262]: 0 packets, 0 bytes, 0 overrun
              Blocks free curr/low: 512/512
      RX[263]: 4 packets, 64 bytes, 0 overrun
              Blocks free curr/low: 512/512
      RX[288]: 0 packets, 0 bytes, 0 overrun
              Blocks free curr/low: 512/512
      RX[289]: 0 packets, 0 bytes, 0 overrun
              Blocks free curr/low: 512/512
      RX[290]: 0 packets, 0 bytes, 0 overrun
              Blocks free curr/low: 512/512
      RX[291]: 0 packets, 0 bytes, 0 overrun
```

```
                Blocks free curr/low: 512/512
              RX[292]: 0 packets, 0 bytes, 0 overrun
                Blocks free curr/low: 512/512
              RX[293]: 0 packets, 0 bytes, 0 overrun
                Blocks free curr/low: 512/512
              RX[294]: 0 packets, 0 bytes, 0 overrun
                Blocks free curr/low: 512/512
              RX[295]: 0 packets, 0 bytes, 0 overrun
                Blocks free curr/low: 512/512
              TX[00]: 3258599 packets, 860813811 bytes, 0 underruns
                Blocks free curr/low: 511/388
              TX[01]: 891279 packets, 238071978 bytes, 0 underruns
                Blocks free curr/low: 511/405
              TX[02]: 787368 packets, 233492817 bytes, 0 underruns
                Blocks free curr/low: 511/409
              TX[03]: 1407442 packets, 294192127 bytes, 0 underruns
                Blocks free curr/low: 511/423
              TX[04]: 1143794 packets, 266269203 bytes, 0 underruns
                Blocks free curr/low: 511/433
              TX[05]: 1813341 packets, 1343723097 bytes, 0 underruns
                Blocks free curr/low: 511/413
              TX[06]: 745612 packets, 178752603 bytes, 0 underruns
                Blocks free curr/low: 511/389
              TX[07]: 498701 packets, 140487728 bytes, 0 underruns
                Blocks free curr/low: 511/382
              TX[08]: 107232 packets, 66899140 bytes, 0 underruns
                Blocks free curr/low: 511/419
              TX[09]: 108350 packets, 68658558 bytes, 0 underruns
                Blocks free curr/low: 511/441
              TX[10]: 98761 packets, 64801332 bytes, 0 underruns
                Blocks free curr/low: 511/438
      [...]
              TX[254]: 0 packets, 0 bytes, 0 underruns
                Blocks free curr/low: 511/512
              TX[255]: 0 packets, 0 bytes, 0 underruns
                Blocks free curr/low: 511/512
              TX[256]: 123 packets, 3444 bytes, 0 underruns
                Blocks free curr/low: 511/512
              TX[257]: 270048 packets, 2420741524 bytes, 0 underruns
                Blocks free curr/low: 511/512
              TX[258]: 0 packets, 0 bytes, 0 underruns
                Blocks free curr/low: 511/512
              TX[259]: 9 packets, 576 bytes, 0 underruns
                Blocks free curr/low: 511/512
              TX[260]: 0 packets, 0 bytes, 0 underruns
                Blocks free curr/low: 511/512
              TX[261]: 6 packets, 384 bytes, 0 underruns
                Blocks free curr/low: 511/512
              TX[262]: 0 packets, 0 bytes, 0 underruns
                Blocks free curr/low: 511/512
              TX[263]: 4 packets, 256 bytes, 0 underruns
                Blocks free curr/low: 511/512
              TX[288]: 0 packets, 0 bytes, 0 underruns
                Blocks free curr/low: 511/512
              TX[289]: 0 packets, 0 bytes, 0 underruns
                Blocks free curr/low: 511/512
              TX[290]: 0 packets, 0 bytes, 0 underruns
                Blocks free curr/low: 511/512
              TX[291]: 0 packets, 0 bytes, 0 underruns
                Blocks free curr/low: 511/512
              TX[292]: 0 packets, 0 bytes, 0 underruns
                Blocks free curr/low: 511/512
              TX[293]: 0 packets, 0 bytes, 0 underruns
                Blocks free curr/low: 511/512
```

```
      TX[294]: 0 packets, 0 bytes, 0 underruns
              Blocks free curr/low: 511/512
      TX[295]: 0 packets, 0 bytes, 0 underruns
   Blocks free curr/low: 511/512
  Control Point Interface States:
        Interface number is 1
        Interface config status is active
        Interface state is active
Interface Internal-Data0/0 "", is up, line protocol is up
  Hardware is i82547GI rev00, BW 1000 Mbps, DLY 1000 usec
        (Full-duplex), (1000 Mbps)
        MAC address 0000.0001.0002, MTU not set
        IP address unassigned
        6 packets input, 1094 bytes, 0 no buffer
        Received 6 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 L2 decode drops, 0 demux drops
        0 packets output, 0 bytes, 0 underruns
        0 output errors, 0 collisions
        0 late collisions, 0 deferred
        input queue (curr/max packets): hardware (0/2) software (0/0)
        output queue (curr/max packets): hardware (0/0) software (0/0)
   Control Point Interface States:
        Interface number is unassigned
Interface Internal-Data0/1 "nlp_int_tap", is up, line protocol is up
  Hardware is en_vtun rev00, BW Unknown Speed-Capability, DLY 1000 usec
 (Full-duplex), (1000 Mbps)
 Input flow control is unsupported, output flow control is unsupported
 MAC address 0000.0100.0001, MTU 1500
 IP address 169.254.1.1, subnet mask 255.255.255.248
 37 packets input, 2822 bytes, 0 no buffer
 Received 0 broadcasts, 0 runts, 0 giants
 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
 0 pause input, 0 resume input
 0 L2 decode drops
 5 packets output, 370 bytes, 0 underruns
 0 pause output, 0 resume output
 0 output errors, 0 collisions, 0 interface resets
 0 late collisions, 0 deferred
 0 input reset drops, 0 output reset drops
 input queue (blocks free curr/low): hardware (0/0)
 output queue (blocks free curr/low): hardware (0/0)
  Traffic Statistics for "nlp_int_tap":
 37 packets input, 2304 bytes
 5 packets output, 300 bytes
 37 packets dropped
      1 minute input rate 0 pkts/sec,  0 bytes/sec
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  0 bytes/sec
      5 minute output rate 0 pkts/sec,  0 bytes/sec
      5 minute drop rate, 0 pkts/sec
  Control Point Interface States:
 Interface number is 14
 Interface config status is active
 Interface state is active
[...]
```

下表说明 **show interface detail** 命令显示的其他字段。

表 *3: show interface detail* 字段

字段	说明
Demux drops	（仅在内部数据接口上）因 威胁防御 设备无法多路复用来自其他接口的数据包而丢弃的数据包数。
内部数据接口	数据平面（系统支持 diagnostic-cli）上的接口是 Internal-Data0/0 和 Internal-Data0/1。 其中每个接口都有一个缓冲区。其中一个设备线程从缓冲区读取数据，并将数据包移动到 RX 环中。例如，在 4120 设备中，环总数为 23（从 00 到 22），其中 RX 环 16 和 17 为 OSPF 保留。同样，根据设备型号，某些环会保留给故障转移和 CCL 数据包。 这些环是数据包堆栈，可确保来自同一数据流的数据包顺序相同；具有相同 5 元组（基于源/目的 IP）的数据包将始终位于同一 RX 环上。
Control Point Interface States:	
Interface number	用于调试的编号，指示此接口创建的顺序，从 0 开始。
Interface config status	管理状态，如下所示： • active - 该接口没有关闭。 • not active - 接口被有意关闭。
Interface state	接口的实际状态。在大多数情况下，此状态与上述配置状态匹配。如果配置高可用性，则可能不匹配，因为 威胁防御 设备会根据需要打开或关闭接口。
Asymmetrical Routing Statistics:	
Received X1 packets	在此接口上接收的 ASR 数据包数。
Transmitted X2 packets	在此接口上发送的 ASR 数据包数。
Dropped X3 packets	在此接口上丢弃的ASR数据包数。当尝试转发数据包时，如果接口关闭，则可能丢弃数据包。

Related Commands

命令	说明
clear interface	清除 **show interface** 命令的计数器。
show interface ip brief	显示接口 IP 地址和状态。

show interface ip brief

要查看接口 IP 地址和状态，请使用 **show interface ip brief** 命令。

show interface [[*physical_interface*[**.***subinterface*] | *interface_name* | **BVI** *ID* |] **ip brief**

Syntax Description

BVI *id*	（可选）显示指定网桥虚拟接口 (BVI) 的统计信息。输入 BVI 编号（1-250）。
interface_name	（可选）标识接口 ID。
physical_interface	（可选）标识接口 ID，例如 **gigabitethernet0/1**。
subinterface	（可选）识别一个介于 1 到 4294967293 之间整数，用以指定逻辑子接口。

Command Default

如果不指定接口， 命令会显示所有接口，包括内部接口。

Command History

版本	修改
6.1	引入了此命令。
6.2	添加了 **BVI** 关键字。

示例

以下是 **show ip brief** 命令的输出示例：

```
> show interface ip brief
    Interface                  IP-Address      OK? Method  Status                Protocol
    Control0/0                 127.0.1.1       YES CONFIG  up                    up
    GigabitEthernet0/0         209.165.200.226 YES CONFIG  up                    up
    GigabitEthernet0/1         unassigned      YES unset   administratively down down
    GigabitEthernet0/2         10.1.1.50       YES manual  administratively down down
    GigabitEthernet0/3         192.168.2.6     YES DHCP    administratively down down
    Management0/0              209.165.201.3   YES CONFIG  up
```

以下示例显示大多数接口属于 BVI 时的寻址。成员接口与父 BVI 具有相同的地址。

```
> show interface ip brief
Interface                  IP-Address      OK? Method Status                Protocol
GigabitEthernet1/1         unassigned      YES DHCP   down                  down
GigabitEthernet1/2         192.168.1.1     YES unset  down                  down
GigabitEthernet1/3         192.168.1.1     YES unset  down                  down
GigabitEthernet1/4         192.168.1.1     YES unset  down                  down
GigabitEthernet1/5         192.168.1.1     YES unset  down                  down
GigabitEthernet1/6         192.168.1.1     YES unset  down                  down
GigabitEthernet1/7         192.168.1.1     YES unset  down                  down
GigabitEthernet1/8         192.168.1.1     YES unset  down                  down
Internal-Control1/1        127.0.1.1       YES unset  up                    up
Internal-Data1/1           unassigned      YES unset  up                    up
```

```
Internal-Data1/2           unassigned      YES unset  down                  down
Internal-Data1/3           unassigned      YES unset  up                    up
Internal-Data1/4           169.254.1.1     YES unset  up                    up
Management1/1              unassigned      YES unset  up                    up
BVI1                       192.168.1.1     YES manual up                    up
```

下表对输出字段进行了说明。

表 *4: show interface ip brief* 字段

字段	说明
接口	接口 ID。 如果显示所有接口，则还会看到有关用于系统通信的内部接口的信息。用户无法配置内部接口，该信息只用于调试目的。
IP-Address	接口 IP 地址。
OK?	此列没有使用并始终显示为“Yes”。
Method	接口接收 IP 地址的方法。值包括以下各项： • unset - 未配置 IP 地址。 • manual - 接口具有静态地址。 • CONFIG - 已从启动配置载入。 • DHCP — 从 DHCP 服务器接收。
Status	管理状态，如下所示： • up - 接口没有关闭。 • down - 接口未启动，也未有意关闭。 • administratively down - 人为地关闭接口。
Protocol	线路状态，如下所示： • up - 工作电缆插入网络接口。 • down - 电缆不正确或未插入接口连接器。

Related Commands

命令	说明
show interface	显示接口的运行时间状态和统计信息。

show inventory

要显示有关安装在网络设备中并指定了产品标识符 (PID)、版本标识符 (VID) 和序列号 (SN) 的思科产品的所有信息，请在用户 EXEC 模式或特权 EXEC 模式下使用 **show inventory** 命令。

show inventory ［*slot_id*］

Syntax Description

slot_id	（可选）指定模块 ID 或插槽号码 0-3。

Command Default

如果在显示项目的库存时不指定插槽，则会显示所有模块（包括电源）的库存信息。

Command History

版本	修改
6.1	引入了此命令。

使用指南

show inventory 命令检索和显示有关每个思科产品的库存信息，这些产品的形式为 UDI，是以下三个不同数据元素的组合：产品标识符 (PID)、版本标识符 (VID) 和序列号 (SN)。

PID 是可以用来订购产品的名称；过去称为“产品名称”或“部件号”。这是您订购精确替换部件时使用的标识符。

VID 是产品的版本。每当修订产品后，VID 即根据 Telcordia GR-209-CORE（管理产品更改通知的行业标准）的严格流程来递增。

SN 是供应商提供的唯一产品序列号。每个产品都具有工厂指定的唯一序列号，无法在实际应用中更改。序列号是用于标识各具体产品实例的方法。对于设备的不同组件，序列号的长度可以不同。

UDI 将每个产品作为一个实体。部分实体（如机箱）具有子实体（像插槽）。每个实体以逻辑排序呈现方式显示在思科实体分层排列的单独行上。

使用 **show inventory** 命令（不带选项）可显示安装在网络设备中并分配了 PID 的思科实体列表。

如果未对思科实体分配 PID，则不会检索或显示该实体。

由于 ASA 5500-X 系列的硬件限制，序列号可能不显示。对于这些型号中 PCI-E I/O (NIC) 选项卡的 UDI 显示，根据机箱类型有六种可能的输出，尽管只有两种不同类型的卡。这是因为根据指定的机箱使用了不同的 PCI-E 支架组件。以下示例展示每个 PCI-E I/O 卡组装的预期输出。例如，如果检测到 Silicom SFP NIC 卡，则 UDI 显示取决于安装该 UDI 的设备。VID 和 S/N 值为 N/A，因为没有这些值的电子存储。

对于 ASA 5512-X 或 5515-X 中的 6 端口 SFP 以太网 NIC 卡：

```
Name: "module1", DESCR: "ASA 5512-X/5515-X Interface Card 6-port GE SFP, SX/LX"
PID: ASA-IC-6GE-SFP-A    , VID: N/A, SN: N/A
```

对于 ASA 5525-X 中的 6 端口 SFP 以太网 NIC 卡：

```
Name: "module1", DESCR: "ASA 5525-X Interface Card 6-port GE SFP, SX/LX"
```

```
PID: ASA-IC-6GE-SFP-B    , VID: N/A, SN: N/A
```

对于 ASA 5545-X 或 5555-X 中的 6 端口 SFP 以太网 NIC 卡：

```
Name: "module1", DESCR: "ASA 5545-X/5555-X Interface Card 6-port GE SFP, SX/LX"
PID: ASA-IC-6GE-SFP-C    , VID: N/A, SN: N/A
```

对于 ASA 5512-X 或 5515-X 中的 6 端口铜缆以太网 NIC 卡：

```
Name: "module1", DESCR: "ASA 5512-X/5515-X Interface Card 6-port 10/100/1000, RJ-45"
PID: ASA-IC-6GE-CU-A    , VID: N/A, SN: N/A
```

对于 ASA 5525-X 中的 6 端口铜缆以太网 NIC 卡：

```
Name: "module1", DESCR: "ASA 5525-X Interface Card 6-port 10/100/1000, RJ-45"
PID: ASA-IC-6GE-CU-B    , VID: N/A, SN: N/A
```

对于 ASA 5545-X 或 5555-X 中的 6 端口铜缆以太网 NIC 卡：

```
Name: "module1", DESCR: "ASA 5545-X/5555-X Interface Card 6-port 10/100/1000, RJ-45"
PID: ASA-IC-6GE-CU-C    , VID: N/A, SN: N/A
```

示例

以下是没有任何关键字或参数的 **show inventory** 命令的输出示例。此示例输出显示 威胁防御 设备中安装的思科实体的列表，每个实体都分配了 PID。

```
> show inventory
Name: "Chassis", DESCR: "ASA 5508-X with FirePOWER services, 8GE, AC, DES"
PID: ASA5508           , VID: V01     , SN: JMX1923408S

Name: "Storage Device 1", DESCR: "ASA 5508-X SSD"
PID: ASA5508-SSD       , VID: N/A     , SN: MXA184205MC
```

下表介绍了显示屏中显示的字段。

表 *5: show inventory* 的字段说明

字段	说明
名称	分配给思科实体的物理名称（文本字符串）。例如，控制台、SSP 或简单组件号（端口或模块号，如“1”）取决于设备的物理组件的命名语法。相当于 RFC 2737 中的 entPhysicalName MIB 变量。
DESCR	用于描述对象的思科实体的物理说明。相当于 RFC 2737 中的 entPhysicalName MIB 变量。
PID	实体的产品标识符。相当于 RFC 2737 中的 entPhysicalModelName MIB 变量。

字段	说明
VID	实体的版本标识符。相当于 RFC 2737 中的 entPhysicalHardwareRev MIB 变量。
SN	实体的序列号。相当于 RFC 2737 中的 entPhysicalSerialNum MIB 变量。

show ip address

要查看接口 IP 地址，或在透明模式下查看管理 IP 地址，请使用 **show ip address** 命令。

show ip address [[*physical_interface*[**.***subinterface*] | *interface_name* |]

Syntax Description

interface_name	（可选）标识接口 ID。
physical_interface	（可选）标识接口 ID，例如 **gigabit**ethernet0/1。
subinterface	（可选）识别一个介于 1 到 4294967293 之间整数，用以指定逻辑子接口。

Command Default

如果不指定接口，则输出显示所有接口的 IP 地址。

Command History

版本	修改
6.1	引入了此命令。

使用指南

此命令显示主要 IP 地址（在显示屏幕中称为“System”，适用于配置高可用性时）以及当前 IP 地址。如果设备处于主用状态，则系统和当前 IP 地址匹配。如果设备处于备用状态，则当前 IP 地址显示备用地址。

IP 地址仅用于数据接口。此命令不会在诊断接口（与透明模式管理接口）上的管理接口上显示系统的 IP 地址。信息将包括诊断接口的 IP 地址信息（如果已配置）。要查看管理接口上有关的信息，请使用 **show network** 命令。

示例

以下是 **show ip address** 命令的输出示例：

```
> show ip address
System IP Addresses:
Interface               Name         IP address      Subnet mask       Method
GigabitEthernet0/0      mgmt         10.7.12.100     255.255.255.0     CONFIG
GigabitEthernet0/1      inside       10.1.1.100      255.255.255.0     CONFIG
GigabitEthernet0/2.40   outside      209.165.201.2   255.255.255.224   DHCP
GigabitEthernet0/3      dmz          209.165.200.225 255.255.255.224   manual
Current IP Addresses:
Interface               Name         IP address      Subnet mask       Method
GigabitEthernet0/0      mgmt         10.7.12.100     255.255.255.0     CONFIG
GigabitEthernet0/1      inside       10.1.1.100      255.255.255.0     CONFIG
GigabitEthernet0/2.40   outside      209.165.201.2   255.255.255.224   DHCP
GigabitEthernet0/3      dmz          209.165.200.225 255.255.255.224   manual
```

下表对每个字段进行了说明。

表 *6: show ip address* 字段

字段	说明
接口	接口 ID。
Name	接口名称。
IP address	接口 IP 地址。
Subnet mask	IP 地址子网掩码。
Method	接口接收 IP 地址的方法。值包括以下各项： • unset - 未配置 IP 地址。 • manual - 接口具有静态地址。 • CONFIG - 已从启动配置载入。 • DHCP — 从 DHCP 服务器接收。

Related Commands

命令	说明
show interface	显示接口的运行时间状态和统计信息。
show interface ip brief	显示接口 IP 地址和状态。

show ip address dhcp

要查看接口的 DHCP 租用或服务器的详细信息，请使用 **show ip address dhcp** 命令。

show ip address {*physical_interface*[**.***subinterface*] | *interface_name*} **dhcp server**
show ip address {*physical_interface*[**.***subinterface*] | *interface_name*} **dhcp lease** [**proxy** | **server**] [**summary**]

Syntax Description

interface_name	标识接口名称。
lease	显示有关 DHCP 租用的信息。
physical_interface	标识接口 ID，例如 **gigabitethernet0/1**。
proxy	显示 IPL 表中的代理条目。
server	显示 IPL 表中的服务器条目。
subinterface	识别一个介于 1 到 4294967293 之间整数，用以指定逻辑子接口。
summary	显示条目的汇总。

Command History

版本	修改
6.1	引入了此命令。

示例

以下是 **show ip address dhcp lease** 命令的输出示例：

```
> show ip address outside dhcp lease
Temp IP Addr:209.165.201.57 for peer on interface:outside
Temp sub net mask:255.255.255.224
   DHCP Lease server:209.165.200.225, state:3 Bound
   DHCP Transaction id:0x4123
   Lease:259200 secs, Renewal:129600 secs, Rebind:226800 secs
   Temp default-gateway addr:209.165.201.1
   Temp ip static route0: dest 10.9.0.0 router 10.7.12.255
   Next timer fires after:111797 secs
   Retry count:0, Client-ID:cisco-0000.0000.0000-outside
   Proxy: TRUE  Proxy Network: 10.1.1.1
   Hostname: device1
```

下表对每个字段进行了说明。

表 *7: show ip address dhcp lease* 字段

字段	说明
Temp IP Addr	分配给接口的 IP 地址。
Temp sub net mask	分配给接口的子网掩码。
DHCP Lease server	DHCP 服务器地址。
state	DHCP 租用的状态，如下所示： • Initial - 初始化状态，设备启动获取租用流程。当租用结束或租用协商失败时，也会显示此状态。 • Selecting - 设备正在等待检索来自一个或多个 DHCP 服务器的 DHCPOFFER 消息，从而可从中选择一个。 • Requesting - 设备正在等待接收所发送请求的目标服务器的回应。 • Purging - 设备正在删除租用，因为客户端已释放 IP 地址或出现其他错误。 • Bound - 设备具有有效租用且正在正常运行。 • Renewing - 设备正在尝试续订租用。它定期将 DHCPREQUEST 消息发送到当前 DHCP 服务器，然后等待回复。 • Rebinding - 设备无法对原始服务器的租用续约，现在发送 DHCPREQUEST 消息，直到收到任何服务器的回复或租用结束。 • Holddown - 设备已启动用于删除租用的流程。 • Releasing - 设备将释放消息发送到服务器，指示不再需要 IP 地址。
DHCP transaction id	客户端选择的随机号码，供客户端和服务器用来关联请求消息。
Lease	DHCP 服务器指定的时间长度，接口可在该时间段内使用此 IP 地址。
Renewal	接口自动尝试续订此租用之前的时间长度。
Rebind	威胁防御 设备尝试重新绑定 DHCP 服务器之前的时间长度。如果设备无法与原始 DHCP 服务器通信且租用时间已超过 87.5%，就会进行重新绑定。然后，设备尝试通过广播 DHCP 请求与任何可用的 DHCP 服务器联系。
Temp default-gateway addr	DHCP 服务器提供的默认网关地址。
Temp ip static route0	默认静态路由。
Next timer fires after	内部计时器触发之前的秒数。

字段	说明
Retry count	如果 威胁防御 设备正在尝试建立租用，则此字段显示设备已尝试发送 DHCP 消息的次数。例如，如果设备处于 Selecting（选择中）状态，则此值显示设备已发送发现消息的次数。如果设备处于 Requesting（请求中）状态，则此值显示设备已发送请求消息的次数。
Client-ID	在与服务器的所有通信中使用的客户端 ID。
Proxy	指定此接口是否为 VPN 客户端的代理 DHCP 客户端，值为 True 或 False。
Proxy Network	请求的网络。
Hostname	客户端主机名称。

以下是 **show ip address dhcp server** 命令的输出示例：

```
> show ip address outside dhcp server
   DHCP server: ANY (255.255.255.255)
    Leases:   0
    Offers:   0      Requests: 0     Acks: 0     Naks: 0
    Declines: 0      Releases: 0     Bad:  0

   DHCP server: 40.7.12.6
    Leases:   1
    Offers:   1      Requests: 17     Acks: 17     Naks: 0
    Declines: 0      Releases: 0     Bad:  0
    DNS0:   171.69.161.23,   DNS1:  171.69.161.24
    WINS0:  172.69.161.23,   WINS1: 172.69.161.23
    Subnet: 255.255.0.0   DNS Domain: cisco.com
```

下表对每个字段进行了说明。

***表 8: show ip address dhcp server* 字段**

字段	说明
DHCP server	向此接口提供租用的 DHCP 服务器的地址。顶部条目（“ANY”）是默认服务器并始终存在。
Leases	从服务器获取的租用数。对于一个接口，租用数通常是1。如果服务器为正在运行 VPN 代理的接口提供地址，会有数个租用。
Offers	服务器所提供的项的数量。
Requests	发送至服务器的请求数。
Acks	从服务器接收的确认数。
Naks	从服务器接收的否定确认数。
Declines	从服务器接收的拒绝数。

字段	说明
Releases	发送至服务器的释放数。
Bad	从服务器接收的错误数据包数。
DNS0	从 DHCP 服务器获取的主要 DNS 服务器地址。
DNS1	从 DHCP 服务器获取的辅助 DNS 服务器地址。
WINS0	从 DHCP 服务器获取的主要 WINS 服务器地址。
WINS1	从 DHCP 服务器获取的辅助 WINS 服务器地址。
Subnet	从 DHCP 服务器获取的子网地址。
DNS Domain	从 DHCP 服务器获取的域。

Related Commands

命令	说明
show interface ip brief	显示接口 IP 地址和状态。
show ip address	显示接口的 IP 地址。

show ip address pppoe

要查看有关 PPPoE 连接的详细信息，请使用 **show ip address pppoe** 命令。

show ip address {*physical_interface*[**.***subinterface*] | *interface_name* | } **pppoe**

Syntax Description

interface_name	标识接口名称。
physical_interface	标识接口 ID，例如 **gigabitethernet0/1**。
subinterface	识别一个介于 1 到 4294967293 之间整数，用以指定逻辑子接口。

Command History

版本	修改
6.1	引入了此命令。

Related Commands

命令	说明
show interface ip brief	显示接口 IP 地址和状态。
show ip address	显示接口的 IP 地址。

show ip audit count

要在将审核策略应用于接口时显示签名匹配数，请使用 **show ip audit count** 命令。

show ip audit count ［**global** | **interface** *interface_name*］

Syntax Description

global	（默认）显示所有接口的匹配数。
interface *interface_name*	（可选）显示指定接口的匹配数。

Command History

版本	修改
6.1	引入了此命令。

使用指南

通常不配置审核策略，但如果使用 FlexConfig 进行配置，则可以查看相关统计信息。

Related Commands

命令	说明
clear ip audit count	清除 IP 审核的统计信息。
show running-config ip audit name	显示 **ip audit name** 命令的配置。除 **name**外，您可以检查 **interface** 和 **signature** 配置。

show ip local pool

要显示 IPv4 地址池信息，请使用 **show ip local pool** 命令。

show ip local pool *pool_name*

Syntax Description

pool_name	IPv6 地址池的名称。

Command History

版本	修改
6.1	引入了此命令。

使用指南

使用此命令可查看 IPv4 地址池的内容。这些池用于远程访问 VPN 和集群技术。使用 **show ipv6 local pool** 以查看IPv6 地址池。

示例

以下是 **show ip local pool** 命令的输出示例：

```
> show ip local pool test-ipv4-pool
Begin           End             Mask            Free     Held     In use
10.100.10.10    10.100.10.254   255.255.255.0     245        0        0

Available Addresses:
10.100.10.10
10.100.10.11
10.100.10.12
10.100.10.13
10.100.10.14
10.100.10.15
10.100.10.16
... (remaining output redacted)...
```

show ip verify statistics

要显示因单播拟向转发 (RPF) 功能而丢弃的数据包数，请使用 **show ip verify statistics** 命令。

show ip verify statistics ［**interface** *interface_name*］

Syntax Description

interface *interface_name*	（可选）显示指定接口的统计信息。

Command Default

此命令显示所有接口的统计信息。

Command History

版本	修改
6.1	引入了此命令。

使用指南

ip verify reverse-path 功能通常未配置，但如果使用 FlexConfig 进行配置，则可以查看相关统计信息。

示例

以下是 **show ip verify statistics** 命令的输出示例：

```
> show ip verify statistics
interface outside: 2 unicast rpf drops
interface inside: 1 unicast rpf drops
interface intf2: 3 unicast rpf drops
```

Related Commands

命令	说明
clear ip verify statistics	清除单播 RPF 统计信息。
show running-config ip verify reverse-path	显示 **ip verify reverse-path** 配置。

show ipsec df-bit

要显示指定接口的 IPsec 数据包的 IPsec 不分片（DF 位）策略，请使用 **show ipsec df-bit** 命令。您还可以使用 **show crypto ipsec df-bit** 命令同义词。

show ipsec df-bit *interface*

Syntax Description

interface	指定接口名称。

Command History

版本	修改
6.1	引入了此命令。

使用指南

df-bit 设置确定系统如何处理封装信头中的不分片 (DF) 位。IP 信头中的 DF 位确定是否允许设备对数据包分段。根据此设置，系统在应用加密时会清除、设置或复制明文数据包的 DF 位设置，也可以将其复制到外 IPsec 信头。

示例

以下示例展示名为 inside 的接口的 IPsec DF 位策略：

```
> show ipsec df-bit inside
df-bit inside copy
```

Related Commands

命令	说明
show ipsec fragmentation	显示 IPsec 数据包的分段策略。

show ipsec fragmentation

要显示 IPsec 数据包的分段策略，请使用 **show ipsec fragmentation** 命令。您还可以使用 **show crypto ipsec fragmentation** 命令同义词。

show ipsec fragmentation *interface*

Syntax Description

interface	指定接口名称。

Command History

版本	修改
6.1	引入了此命令。

使用指南

为 VPN 加密数据包时，系统会将数据包长度与出站接口的 MTU 进行比较。如果加密数据包将超过 MTU，则必须对数据包进行分段。此命令显示系统是在数据包加密后（加密后）还是加密前（加密前）对数据包进行分片。在加密之前对数据包进行分片也称为预分片，这是默认的系统行为，因为它可以提高整体加密性能。

示例

以下示例显示名为 inside 的接口的 IPsec 分段策略：

```
> show ipsec fragmentation inside
fragmentation inside before-encryption
```

Related Commands

命令	说明
show ipsec df-bit	显示指定接口的 DF 位策略。

show ipsec policy

要显示为 OSPFv3 配置的 IPsec 安全套接字 API (SS API) 安全策略，请使用 **show ipsec policy** 命令。您还可以使用此命令的替代形式： **show crypto ipsec policy**。

show ipsec policy

Command History

版本	修改
6.1	引入了此命令。

示例

以下示例显示 OSPFv3 身份验证和加密策略。

```
> show ipsec policy
Crypto IPsec client security policy data

Policy name:      OSPFv3-1-256
Policy refcount:  1
Policy flags:     0x00000000
SA handles:       sess 268382208 (0xfff3000) / in 55017 (0xd6e9) / out 90369 (0x16101)
Inbound  ESP SPI:        256 (0x100)
Outbound ESP SPI:        256 (0x100)
Inbound  ESP Auth Key:   12345678901234567890123456789012345678901234567890
Outbound ESP Auth Key:   12345678901234567890123456789012345678901234567890
Inbound  ESP Cipher Key: 123456789012345678901234567890123456789012
Outbound ESP Cipher Key: 123456789012345678901234567890123456789012
Transform set:    esp-aes esp-sha-hmac
```

Related Commands

命令	说明
show crypto sockets	显示安全套接字信息。
show ipv6 ospf interface	显示有关 OSPFv3 接口的信息。

show ipsec sa

要显示 IPsec 安全关联 (SA) 列表，请使用 **show ipsec sa** 命令。您还可以使用此命令的替代形式：**show crypto ipsec sa**。

show ipsec sa [**assigned-address** *hostname_or_IP_address* | **entry** | **identity** | **inactive** | **map** *map-name* | **peer** *peer-addr* | **spi** *spi-num*] [**detail**]

Syntax Description

assigned-address *hostname_or_IP_address*	（可选）显示指定的主机名或 IP 地址的 IPsec SA。
detail	（可选）显示有关所显示内容的详细错误信息。
entry	（可选）显示按对等设备地址排序的 IPsec SA
identity	（可选）显示按身份排序的 IPsec SA，不包括 ESP。这是简洁形式。
inactive	（可选）显示无法传递流量的 IPsec SA。
map *map-name*	（可选）显示指定加密映射的 IPsec SA。
peer *peer-addr*	（可选）显示指定对等设备 IP 地址的 IPsec SA。
spi *spi-num*	（可选）显示 SPI 的 IPsec SA。

Command History

版本	修改
6.1	引入了此命令。

示例

以下示例显示 IPsec SA，包括分配的 IPv6 地址以及传输模式和 GRE 封装指示。

```
> show ipsec sa
interface: outside
    Crypto map tag: def, seq num: 1, local addr: 75.2.1.23

      local ident (addr/mask/prot/port): (75.2.1.23/255.255.255.255/47/0)
      remote ident (addr/mask/prot/port): (75.2.1.60/255.255.255.255/47/0)
      current_peer: 75.2.1.60, username: rashmi
      dynamic allocated peer ip: 65.2.1.100
      dynamic allocated peer ip(ipv6): 2001:1000::10

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 18, #pkts decrypt: 18, #pkts verify: 18
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #post-frag successes: 0, #post-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #TFC rcvd: 0, #TFC sent: 0
      #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
```

```
      #send errors: 0, #recv errors: 4

     local crypto endpt.: 75.2.1.23/4500, remote crypto endpt.: 75.2.1.60/64251
      path mtu 1342, ipsec overhead 62(44), override mtu 1280, media mtu 1500
      PMTU time remaining (sec): 0, DF policy: copy-df
      ICMP error validation: disabled, TFC packets: disabled
      current outbound spi: D9C00FC2
      current inbound spi : 4FCB6624

    inbound esp sas:
      spi: 0x4FCB6624 (1338730020)
         transform: esp-3des esp-sha-hmac no compression
         in use settings ={RA, Transport,  NAT-T-Encaps, GRE, IKEv2, }
         slot: 0, conn_id: 8192, crypto-map: def
         sa timing: remaining key lifetime (sec): 28387
         IV size: 8 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x0003FFFF 0xFFFFFFFF
    outbound esp sas:
      spi: 0xD9C00FC2 (3653242818)
         transform: esp-3des esp-sha-hmac no compression
         in use settings ={RA, Transport,  NAT-T-Encaps, GRE, IKEv2, }
         slot: 0, conn_id: 8192, crypto-map: def
         sa timing: remaining key lifetime (sec): 28387
         IV size: 8 bytes
        replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x00000001
```

以下示例显示 IPsec SA，包括用于将隧道标识为 OSPFv3 的使用中设置。

```
> show ipsec sa
interface: outside2
    Crypto map tag: def, local addr: 10.132.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (172.20.0.21/255.255.255.255/0/0)
      current_peer: 172.20.0.21
      dynamic allocated peer ip: 10.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1145, #pkts decrypt: 1145, #pkts verify: 1145
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 2, #pre-frag failures: 1, #fragments created: 10
      #PMTUs sent: 5, #PMTUs rcvd: 2, #decapstulated frags needing reassembly: 1
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 10.132.0.17, remote crypto endpt.: 172.20.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    inbound esp sas:
      spi: 0x1E8246FC (511854332)
         transform: esp-3des esp-md5-hmac
         in use settings ={L2L, Transport, Manual key (OSPFv3),}
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 548
         IV size: 8 bytes
         replay detection support: Y
```

```
outbound esp sas:
  spi: 0xDC15BF68 (3692412776)
     transform: esp-3des esp-md5-hmac
     in use settings ={L2L, Transport, Manual key (OSPFv3), }
     slot: 0, conn_id: 3, crypto-map: def
     sa timing: remaining key lifetime (sec): 548
     IV size: 8 bytes
     replay detection support: Y

Crypto map tag: def, local addr: 10.132.0.17

  local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
```

注释 如果 IPsec SA 策略表明在 IPsec 处理前进行碎片整理，则碎片整理统计信息为碎片整理前统计信息。如果 SA 策略表明在 IPsec 处理后进行碎片整理，则显示碎片整理后统计信息。

以下示例在全局配置模式下输入，显示名为 def 的加密映射的 IPsec SA。

```
> show ipsec sa map def
cryptomap: def
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1146, #pkts decrypt: 1146, #pkts verify: 1146
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    inbound esp sas:
      spi: 0x1E8246FC (511854332)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 480
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0xDC15BF68 (3692412776)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 480
         IV size: 8 bytes
         replay detection support: Y

    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
```

```
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73672, #pkts encrypt: 73672, #pkts digest: 73672
      #pkts decaps: 78824, #pkts decrypt: 78824, #pkts verify: 78824
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73672, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35

    inbound esp sas:
      spi: 0xB32CF0BD (3006066877)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 263
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0x3B6F6A35 (997157429)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 263
         IV size: 8 bytes
         replay detection support: Y
```

以下示例显示 **entry** 关键字的 IPsec SA。

```
> show ipsec sa entry
peer address: 10.132.0.21
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1147, #pkts decrypt: 1147, #pkts verify: 1147
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    inbound esp sas:
      spi: 0x1E8246FC (511854332)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 429
         IV size: 8 bytes
         replay detection support: Y
```

```
    outbound esp sas:
      spi: 0xDC15BF68 (3692412776)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 429
         IV size: 8 bytes
         replay detection support: Y
peer address: 10.135.1.8
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73723, #pkts encrypt: 73723, #pkts digest: 73723
      #pkts decaps: 78878, #pkts decrypt: 78878, #pkts verify: 78878
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73723, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35

    inbound esp sas:
      spi: 0xB32CF0BD (3006066877)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 212
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0x3B6F6A35 (997157429)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 212
         IV size: 8 bytes
         replay detection support: Y
```

以下示例显示带有 **entry detail** 关键字的 IPsec SA。

```
> show ipsec sa entry detail
peer address: 10.132.0.21
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1148, #pkts decrypt: 1148, #pkts verify: 1148
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
      #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
      #pkts invalid prot (rcv): 0, #pkts verify failed: 0
```

```
      #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
      #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
      #pkts replay failed (rcv): 0
      #pkts internal err (send): 0, #pkts internal err (rcv): 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    inbound esp sas:
      spi: 0x1E8246FC (511854332)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 322
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0xDC15BF68 (3692412776)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 322
         IV size: 8 bytes
         replay detection support: Y

peer address: 10.135.1.8
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73831, #pkts encrypt: 73831, #pkts digest: 73831
      #pkts decaps: 78989, #pkts decrypt: 78989, #pkts verify: 78989
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73831, #pkts comp failed: 0, #pkts decomp failed: 0
      #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
      #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
      #pkts invalid prot (rcv): 0, #pkts verify failed: 0
      #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
      #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
      #pkts replay failed (rcv): 0
      #pkts internal err (send): 0, #pkts internal err (rcv): 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35

    inbound esp sas:
      spi: 0xB32CF0BD (3006066877)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 104
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0x3B6F6A35 (997157429)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
```

```
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 104
         IV size: 8 bytes
         replay detection support: Y
>
```

以下示例显示带有 **identity** 关键字的 IPsec SA。

```
> show ipsec sa identity
interface: outside2
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1147, #pkts decrypt: 1147, #pkts verify: 1147
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73756, #pkts encrypt: 73756, #pkts digest: 73756
      #pkts decaps: 78911, #pkts decrypt: 78911, #pkts verify: 78911
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73756, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35
```

以下示例显示具有关键字 **identity** 和 **detail** 的 IPsec SA。

```
> show ipsec sa identity detail
interface: outside2
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1147, #pkts decrypt: 1147, #pkts verify: 1147
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
```

```
      #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
      #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
      #pkts invalid prot (rcv): 0, #pkts verify failed: 0
      #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
      #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
      #pkts replay failed (rcv): 0
      #pkts internal err (send): 0, #pkts internal err (rcv): 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73771, #pkts encrypt: 73771, #pkts digest: 73771
      #pkts decaps: 78926, #pkts decrypt: 78926, #pkts verify: 78926
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73771, #pkts comp failed: 0, #pkts decomp failed: 0
      #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
      #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
      #pkts invalid prot (rcv): 0, #pkts verify failed: 0
      #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
      #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
      #pkts replay failed (rcv): 0
      #pkts internal err (send): 0, #pkts internal err (rcv): 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35
```

以下示例展示基于分配 IPv6 地址的 IPSec SA：

```
> show ipsec sa assigned-address 2001:1000::10
assigned address: 2001:1000::10
    Crypto map tag: def, seq num: 1, local addr: 75.2.1.23

      local ident (addr/mask/prot/port): (75.2.1.23/255.255.255.255/47/0)
      remote ident (addr/mask/prot/port): (75.2.1.60/255.255.255.255/47/0)
      current_peer: 75.2.1.60, username: rashmi
      dynamic allocated peer ip: 65.2.1.100
      dynamic allocated peer ip(ipv6): 2001:1000::10

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 326, #pkts decrypt: 326, #pkts verify: 326
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #post-frag successes: 0, #post-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #TFC rcvd: 0, #TFC sent: 0
      #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
      #send errors: 0, #recv errors: 35

      local crypto endpt.: 75.2.1.23/4500, remote crypto endpt.: 75.2.1.60/64251
      path mtu 1342, ipsec overhead 62(44), override mtu 1280, media mtu 1500
      PMTU time remaining (sec): 0, DF policy: copy-df
```

```
  ICMP error validation: disabled, TFC packets: disabled
  current outbound spi: D9C00FC2
  current inbound spi : 4FCB6624

inbound esp sas:
  spi: 0x4FCB6624 (1338730020)
     transform: esp-3des esp-sha-hmac no compression
     in use settings ={RA, Transport,  NAT-T-Encaps, GRE, IKEv2, }
     slot: 0, conn_id: 8192, crypto-map: def
     sa timing: remaining key lifetime (sec): 28108
     IV size: 8 bytes
     replay detection support: Y
     Anti replay bitmap:
      0xFFFFFFFF 0xFFFFFFFF
outbound esp sas:
  spi: 0xD9C00FC2 (3653242818)
     transform: esp-3des esp-sha-hmac no compression
     in use settings ={RA, Transport,  NAT-T-Encaps, GRE, IKEv2, }
     slot: 0, conn_id: 8192, crypto-map: def
     sa timing: remaining key lifetime (sec): 28108
     IV size: 8 bytes
     replay detection support: Y
     Anti replay bitmap:
      0x00000000 0x00000001
```

Related Commands

命令	说明
clear isakmp sa	清除 IKE 运行时间 SA 数据库。
show running-config isakmp	显示所有活动的 ISAKMP 配置。

show ipsec sa summary

要显示 IPsec SA 摘要，请使用 **show ipsec sa summary**命令。

show ipsec sa summary

Command History

版本	修改
6.1	引入了此命令。

示例

以下示例按以下连接类型显示 IPsec SA 摘要：

- IPSec
- IPsec over UDP
- IPsec over NAT-T
- IPsec over TCP
- IPsec VPN 负载平衡

```
> show ipsec sa summary
Current IPsec SA's:           Peak IPsec SA's:
IPsec            :     2        Peak Concurrent SA  :    14
IPsec over UDP   :     2        Peak Concurrent L2L :     0
IPsec over NAT-T :     4        Peak Concurrent RA  :    14
IPsec over TCP   :     6
IPsec VPN LB     :     0
Total            :    14
```

Related Commands

命令	说明
clear ipsec sa	全部或基于特定参数删除 IPsec SA。
show ipsec sa	显示 IPsec SA 列表。
show ipsec stats	显示 IPsec 统计信息列表。

show ipsec stats

要显示 IPsec 统计信息列表，请使用 **show ipsec stats** 命令。

show ipsec stats

Command History

版本	修改
6.1	引入了此命令。

使用指南

下表说明了输出条目指示的内容。

输出（续）	说明（续）
IPsec Global Statistics	此部分显示 威胁防御 设备支持的 IPsec 隧道总数。
Active tunnels	当前连接的 IPsec 隧道数。
Previous tunnels	已连接的 IPsec 隧道数，包括主用隧道。
入站	此部分显示通过 IPsec 隧道接收的入站加密流量。
Bytes	接收的加密流量的字节数。
解压缩的字节	执行解压缩之后接收的加密流量的字节数（如果适用）。如果未启用压缩，此计数器应始终等于前一个计数器。
数据包	接收的加密 IPsec 数据包数。
已丢弃的数据包	已接收但由于错误而丢弃的加密 IPsec 数据包数。
重播故障	对接收的加密 IPsec 数据包检测到的反重播故障数。
身份验证	对接收的加密 IPsec 数据包执行的身份验证成功数。
身份验证失败	对接收的加密 IPsec 数据包检测到的身份验证失败数。
解密	对接收的加密 IPsec 数据包执行的解密成功数。
解密失败	对接收的加密 IPsec 数据包检测到的解密失败数。
需要重组地解封分段	包括要重组的 IP 分段的解密 IPsec 数据包数。
发送	此部分显示要通过 IPsec 流量传输的出站明文流量。
Bytes	要通过 IPsec 隧道加密并传输的明文流量字节数。
未压缩字节数	要通过IPsec隧道加密并传输的未压缩明文流量字节数。如果未启用压缩，此计数器应始终等于前一个计数器。

输出（续）	说明（续）
数据包	要通过 IPsec 隧道加密并传输的明文流量字节数据包。
已丢弃的数据包	要通过IPsec隧道加密并传输而由于错误已丢弃的明文数据包数。
身份验证	对要通过 IPsec 隧道传输的数据包执行的身份验证成功数。
身份验证失败	对要通过IPsec隧道传输的数据包检测到的身份验证失败数。
加密	对要通过 IPsec 隧道传输的数据包执行的加密成功数。
加密失败	对要通过 IPsec 隧道传输的数据包检测到的加密失败数。
分段成功	作为出站IPsec数据包转换的一部分执行的分段操作成功数。
预分段成功	作为出站 IPsec 数据包转换的一部分执行的预分段操作成功数。预分段发生在将明文数据包加密和封装为一个或多个 IPsec 数据包之前。
后分段成功	作为出站 IPsec 数据包转换的一部分执行的预分段操作成功数。后分段发生在明文数据包加密和封装为 IPsec 数据包之后，会导致多个 IP 分段。必须在解密之前重组这些分段。
分段失败	出站 IPsec 数据包转换时发生的分段失败数。
预分段失败	出站IPsec数据包转换时发生的预分段失败数。预分段发生在将明文数据包加密和封装为一个或多个 IPsec 数据包之前。
后分段失败	出站IPsec数据包转换时发生的后分段失败数。后分段发生在明文数据包加密和封装为 IPsec 数据包之后，会导致多个 IP 分段。必须在解密之前重组这些分段。
创建的分段	IPsec 转换过程中创建的分段数。
发送的PMTU	IPsec 系统发送的路径 MTU 消息数。IPsec 将 PMTU 消息发送至内部主机，此主机正在发送封装后由于太大而无法通过 IPsec 隧道传输的数据包。PMTU 消息用于请求主机降低其 MTU 和发送更小的数据包以通过 IPsec 隧道传输。
接收的 PMTU	IPsec 系统接收的路径 MTU 消息数。如果通过隧道发送的数据包太大而无法遍历下游网络元素，IPsec将接收来自该网络元素的路径 MTU 消息。当接收路径 MTU 消息时，IPsec 通常会降低其隧道 MTU。
协议失败	接收的错误 IPsec 数据包数。
遗漏 SA 失败	因指定 IPsec 安全关联不存在而请求的 IPsec 操作数。

输出（续）	说明（续）
系统容量失败	因 IPsec 系统容量不足以支持数据速率而无法完成的 IPsec 操作数。

示例

以下示例在全局配置模式下输入，显示 IPsec 统计信息：

```
> show ipsec stats

IPsec Global Statistics
-----------------------
Active tunnels: 2
Previous tunnels: 9
Inbound
    Bytes: 4933013
    Decompressed bytes: 4933013
    Packets: 80348
    Dropped packets: 0
    Replay failures: 0
    Authentications: 80348
    Authentication failures: 0
    Decryptions: 80348
    Decryption failures: 0
    Decapsulated fragments needing reassembly: 0
Outbound
    Bytes: 4441740
    Uncompressed bytes: 4441740
    Packets: 74029
    Dropped packets: 0
    Authentications: 74029
    Authentication failures: 0
    Encryptions: 74029
    Encryption failures: 0
    Fragmentation successes: 3
        Pre-fragmentation successes:2
        Post-fragmentation successes: 1
    Fragmentation failures: 2
        Pre-fragmentation failures:1
        Post-fragmentation failures: 1
    Fragments created: 10
    PMTUs sent: 1
    PMTUs recvd: 2
Protocol failures: 0
Missing SA failures: 0
System capacity failures: 0
```

在支持 IPsec 流分流的平台上，输出显示已分流的流的计数器，而常规计数器显示已分流和未分流的流的总数。

```
> show ipsec stats

IPsec Global Statistics
-----------------------
Active tunnels: 1
Previous tunnels: 1
Inbound
    Bytes: 93568
```

```
    Decompressed bytes: 0
    Packets: 86
    Dropped packets: 0
    Replay failures: 0
    Authentications: 0
    Authentication failures: 0
    Decryptions: 86
    Decryption failures: 0
    TFC Packets: 0
    Decapsulated fragments needing reassembly: 0
    Valid ICMP Errors rcvd: 0
    Invalid ICMP Errors rcvd: 0
Outbound
    Bytes: 93568
    Uncompressed bytes: 90472
    Packets: 86
    Dropped packets: 0
    Authentications: 0
    Authentication failures: 0
    Encryptions: 86
    Encryption failures: 0
    TFC Packets: 0
    Fragmentation successes: 0
        Pre-fragmentation successes: 0
        Post-fragmentation successes: 0
    Fragmentation failures: 0
        Pre-fragmentation failures: 0
        Post-fragmentation failures: 0
    Fragments created: 0
    PMTUs sent: 0
    PMTUs rcvd: 0
Offloaded Inbound
    Bytes: 93568
    Packets: 86
    Authentications: 0
    Decryptions: 86
Offloaded Outbound
    Bytes: 93568
    Packets: 86
    Authentications: 0
    Encryptions: 86
Protocol failures: 0
Missing SA failures: 0
System capacity failures: 0
Inbound SA delete requests: 0
Outbound SA delete requests: 0
Inbound SA destroy calls: 0
Outbound SA destroy calls: 0
```

Related Commands

命令	说明
clear ipsec sa	基于指定的参数清除 IPsec SA 或计数器。
show ipsec sa	根据指定参数显示 IPsec SA。
show ipsec sa summary	显示 IPsec SA 摘要。

show ipv6 access-list

此命令用于 威胁防御不支持的功能。IPv6 访问控制已集成到标准访问控制策略中。查看管理器中的策略，或使用以下命令：

- **show access-list**
- **show access-control-config**

show ipv6 dhcp

要显示 DHCPv6 信息，请使用 **show ipv6 dhcp** 命令。

show ipv6 dhcp ［**client** ［**pd**］ **statistics** | **interface** ［*interface_name* ［**statistics**］］ | **ha statistics** | **server statistics** | **pool** ［*pool_name*］］

Syntax Description

client ［**pd**］ **statistics**	显示DHCPv6客户端统计信息，并显示已发送和已接收的消息数量的输出结果。添加 **pd** 关键字以显示 DHCPv6 前缀委派客户端统计信息。
interface ［*interface_name* ［**statistics**］］	显示所有接口或指定接口的 DHCPv6 信息（可选）。如果接口配置用于DHCPv6无状态服务器配置，则此命令将列出该服务器正在使用的DHCPv6池。如果接口包含DHCPv6地址客户端或前缀委派客户端配置，则此命令将显示各个客户端的状态，以及从该服务器收到的值。 如果指定接口名称，则可以添加 **statistics** 以查看该接口的 DHCP 服务器或客户端的消息统计信息。
ha statistics	显示故障转移设备之间的事务处理统计信息，包括在DUID信息各个设备之间的同步次数。
server statistics	显示 DHCPv6 无状态服务器统计信息。
pool ［*pool_name*］	显示所有 DHCPv6 池或（可选）指定的池。

Command History

版本	修改
6.2.1	引入了此命令。

使用指南

如果不指定任何参数，此命令将显示 DHCPv6 客户端或服务器正在使用的设备 DUID。

示例

以下是 **show ipv6 dhcp** 命令的输出示例：

```
> show ipv6 dhcp
This device's DHCPv6 unique identifier(DUID): 00030001377E8FD91020
```

以下是 **show ipv6 dhcp pool** 命令的输出示例：

```
> show ipv6 dhcp pool
DHCPv6 pool: Sample-Pool
  Imported DNS server: 2004:abcd:abcd:abcd::2
  Imported DNS server: 2004:abcd:abcd:abcd::4
  Imported Domain name: relay.com
  Imported Domain name: server.com
  SIP server address: 2001::abcd:1
```

```
  SIP server domain name: sip.xyz.com
```

以下是 **show ipv6 dhcp interface** 命令的输出示例：

```
> show ipv6 dhcp interface
GigabitEthernet1/1 is in server mode
  Using pool: Sample-Pool

GigabitEthernet1/2 is in client mode
  Prefix State is OPEN
  Renew will be sent in 00:03:46
  Address State is OPEN
  Renew for address will be sent in 00:03:47
  List of known servers:
    Reachable via address: fe80::20c:29ff:fe96:1bf4
    DUID: 000100011D9D1712005056A07E06
    Preference: 0
    Configuration parameters:
      IA PD: IA ID 0x00030001, T1 250, T2 400
        Prefix: 2005:abcd:ab03::/48
                preferred lifetime 500, valid lifetime 600
                expires at Nov 26 2014 03:11 PM (577 seconds)
      IA NA: IA ID 0x00030001, T1 250, T2 400
        Address: 2004:abcd:abcd:abcd:abcd:abcd:abcd:f2cb/128
                preferred lifetime 500, valid lifetime 600
                expires at Nov 26 2014 03:11 PM (577 seconds)
      DNS server: 2004:abcd:abcd:abcd::2
      DNS server: 2004:abcd:abcd:abcd::4
      Domain name: relay.com
      Domain name: server.com
      Information refresh time: 0
  Prefix name: Sample-PD

Management1/1 is in client mode
  Prefix State is IDLE
  Address State is OPEN
  Renew for address will be sent in 11:26:44
  List of known servers:
    Reachable via address: fe80::4e00:82ff:fe6f:f6f9
    DUID: 000300014C00826FF6F8
    Preference: 0
    Configuration parameters:
      IA NA: IA ID 0x000a0001, T1 43200, T2 69120
        Address: 2308:2308:210:1812:2504:1234:abcd:8e5a/128
                preferred lifetime INFINITY, valid lifetime INFINITY
      Information refresh time: 0
```

以下是 **show ipv6 dhcp interface outside** 命令的输出示例：

```
> show ipv6 dhcp interface outside
GigabitEthernet1/2 is in client mode


 Prefix State is OPEN
 Renew will be sent in 00:02:05
 Address State is OPEN
 Renew for address will be sent in 00:02:06
 List of known servers:
   Reachable via address: fe80::20c:29ff:fe96:1bf4
   DUID: 000100011D9D1712005056A07E06
   Preference: 0
```

```
   Configuration parameters:
     IA PD: IA ID 0x00030001, T1 250, T2 400
       Prefix: 2005:abcd:ab03::/48
               preferred lifetime 500, valid lifetime 600
               expires at Nov 26 2014 03:11 PM (476 seconds)
     IA NA: IA ID 0x00030001, T1 250, T2 400
       Address: 2004:abcd:abcd:abcd:abcd:abcd:abcd:f2cb/128
               preferred lifetime 500, valid lifetime 600
               expires at Nov 26 2014 03:11 PM (476 seconds)
     DNS server: 2004:abcd:abcd:abcd::2
     DNS server: 2004:abcd:abcd:abcd::4
     Domain name: relay.com
     Domain name: server.com
     Information refresh time: 0
 Prefix name: Sample-PD
```

以下是 **show ipv6 dhcp interface outside statistics** 命令的输出示例：

```
> show ipv6 dhcp interface outside statistics
DHCPV6 Client PD statistics:

Protocol Exchange Statistics:


 Number of Solicit messages sent:              1
 Number of Advertise messages received:        1
 Number of Request messages sent:              1
 Number of Renew messages sent:                45
 Number of Rebind messages sent:               0
 Number of Reply messages received:            46
 Number of Release messages sent:              0
 Number of Reconfigure messages received:      0
 Number of Information-request messages sent:  0

Error and Failure Statistics:


 Number of Re-transmission messages sent:                 1
 Number of Message Validation errors in received messages: 0

DHCPV6 Client address statistics:

Protocol Exchange Statistics:


 Number of Solicit messages sent:              1
 Number of Advertise messages received:        1
 Number of Request messages sent:              1
 Number of Renew messages sent:                45
 Number of Rebind messages sent:               0
 Number of Reply messages received:            46
 Number of Release messages sent:              0
 Number of Reconfigure messages received:      0
 Number of Information-request messages sent:  0

Error and Failure Statistics:


 Number of Re-transmission messages sent:                 1
 Number of Message Validation errors in received messages: 0
```

以下是 **show ipv6 dhcp client statistics** 命令的输出示例：

```
> show ipv6 dhcp client statistics

Protocol Exchange Statistics:
  Total number of Solicit messages sent:              4
  Total number of Advertise messages received:        4
  Total number of Request messages sent:              4
  Total number of Renew messages sent:                92
  Total number of Rebind messages sent:               0
  Total number of Reply messages received:            96
  Total number of Release messages sent:              6
  Total number of Reconfigure messages received:      0
  Total number of Information-request messages sent:  0

Error and Failure Statistics:
  Total number of Re-transmission messages sent:                  8
  Total number of Message Validation errors in received messages: 0
```

以下是 **show ipv6 dhcp client pd statistics** 命令的输出示例：

```
> show ipv6 dhcp client pd statistics

Protocol Exchange Statistics:


 Total number of Solicit messages sent:              1
 Total number of Advertise messages received:        1
 Total number of Request messages sent:              1
 Total number of Renew messages sent:                92
 Total number of Rebind messages sent:               0
 Total number of Reply messages received:            93
 Total number of Release messages sent:              0
 Total number of Reconfigure messages received:      0
 Total number of Information-request messages sent:  0

Error and Failure Statistics:


 Total number of Re-transmission messages sent:                  1
 Total number of Message Validation errors in received messages: 0
```

以下是 **show ipv6 dhcp server statistics** 命令的输出示例：

```
> show ipv6 dhcp server statistics

Protocol Exchange Statistics:
  Total number of Solicit messages received:             0
  Total number of Advertise messages sent:               0
  Total number of Request messages received:             0
  Total number of Renew messages received:               0
  Total number of Rebind messages received:              0
  Total number of Reply messages sent:                   10
  Total number of Release messages received:             0
  Total number of Reconfigure messages sent:             0
  Total number of Information-request messages received: 10
  Total number of Relay-Forward messages received:       0
  Total number of Relay-Reply messages sent:             0

Error and Failure Statistics:
```

```
  Total number of Re-transmission messages sent:                  0
  Total number of Message Validation errors in received messages: 0
```

以下是 **show ipv6 dhcp ha statistics** 命令的输出示例：

```
> show ipv6 dhcp ha statistics

DHCPv6 HA global statistics:
  DUID sync messages sent:              1
  DUID sync messages received:          0

DHCPv6 HA error statistics:
  Send errors:                          0
```

以下是备用设备上 **show ipv6 dhcp ha statistics** 命令的输出示例：

```
> show ipv6 dhcp ha statistics

DHCPv6 HA global statistics:
  DUID sync messages sent:              0
  DUID sync messages received:          1

DHCPv6 HA error statistics:
  Send errors:                          0
```

Related Commands

命令	说明
clear ipv6 dhcp	清除 DHCPv6 统计信息。

show ipv6 dhcprelay binding

使用 **show ipv6 dhcprelay binding** 命令以显示中继代理创建的中继绑定条目。

show ipv6 dhcprelay binding

Command History

版本	修改
6.1	引入了此命令。

示例

以下是 **show ipv6 dhcprelay binding** 命令的输出示例：

```
> show ipv6 dhcprelay binding
1 in use, 2 most used

Client: fe80::204:23ff:febb:b094 (inside)
  DUID: 000100010f9a59d1000423bbb094, Timeout in 60 seconds

Above binding is created for client with link local address of fe80::204:23ff:febb:b094 on
the inside interface using DHCPv6 id of 000100010f9a59d1000423bbb094, and will timeout in
60 seconds.

There will be limit of 1000 bindings for each context.
```

Related Commands

命令	说明
show ipv6 dhcprelay statistics	显示 IPv6 DHCP 中继代理信息。

show ipv6 dhcprelay statistics

要显示 IPv6 DHCP 中继代理统计信息，请使用 **show ipv6 dhcprelay statistics** 命令。

show ipv6 dhcprelay statistics

Command History

版本	修改
6.1	引入了此命令。

示例

以下是 **show ipv6 dhcprelay statistics** 命令的输出示例：

```
> show ipv6 dhcprelay statistics
Relay Messages:
  SOLICIT                                    1
  ADVERTISE                                  2
  REQUEST                                    1
  CONFIRM                                    1
  RENEW                                    496
  REBIND                                     0
  REPLY                                    498
  RELEASE                                    0
  DECLINE                                    0
  RECONFIGURE                                0
  INFORMATION-REQUEST                        0
  RELAY-FORWARD                            499
  RELAY-REPLY                              500

Relay Errors:
  Malformed message:                         0
  Block allocation/duplication failures:     0
  Hop count limit exceeded:                  0
  Forward binding creation failures:         0
  Reply binding lookup failures:             0
  No output route:                           0
  Conflict relay server route:               0
  Failed to add server NP rule:              0
  Unit or context is not active:             0

Total Relay Bindings Created:              498
```

Related Commands

命令	说明
show ipv6 dhcprelay binding	显示中继代理创建的中继绑定条目。

show ipv6 general-prefix

要显示 IPv6 通用前缀，请使用 **show ipv6 general-prefix** 命令。

show ipv6 general-prefix

Command History

版本	修改
6.1	引入了此命令。

使用指南

使用 **show ipv6 general-prefix** 命令可查看有关 IPv6 通用前缀的信息。

示例

以下是 **show ipv6 general-prefix** 命令的输出示例：

```
> show ipv6 general-prefix
IPv6 Prefix my-prefix, acquired via 6to4
2002:B0B:B0B::/48
 Loopback42 (Address command)
Codes: A - Address, P - Prefix-Advertisement, O - Pool
       U - Per-user prefix, D - Default       N - Not advertised, C - Calendar

AD      fec0:0:0:a::/64 [LA] Valid lifetime 2592000, preferred lifetime 604800
```

show ipv6 icmp

要显示在所有接口上配置的 ICMPv6 访问规则，请使用 **show ipv6 icmp** 命令。

show ipv6 icmp

Command History

版本	修改
6.1	引入了此命令。

使用指南

ICMPv6 规则控制流向设备接口的 ICMPv6 流量。它们不控制通过设备的流量。您可以使用这些规则来控制哪些地址可以向接口发送 ICMPv6 命令（例如 ping），以及可以发送哪些类型的 ICMPv6 命令。使用 **show ipv6 icmp** 命令查看这些规则。

示例

以下是 **show ipv6 icmp** 命令的输出示例。

```
> show ipv6 icmp
ipv6 icmp permit any inside
```

show ipv6 interface

要显示为 IPv6 配置的接口的状态，请使用 **show ipv6 interface** 命令。

show ipv6 interface ［**brief**］［*if_name* ［**prefix**］］

Syntax Description

brief	显示每个接口的 IPv6 状态和配置的简短汇总。
if_name	（可选）内部或外部接口名称。仅显示指定接口的状态和配置。 如果显示所有接口，则还会看到有关用于系统通信的内部接口的信息。用户无法配置内部接口，该信息只用于调试目的。
prefix	（可选）从本地 IPv6 前缀池生成的前缀。前缀是 IPv6 地址的网络部分。

Command Default

显示所有 IPv6 接口。

Command History

版本	修改
6.1	引入了此命令。

使用指南

show ipv6 interface 命令的输出类似于 **show interface** 命令的输出，唯一不同之处是，前者显示的信息是IPv6特定信息。如果接口硬件可用，会将接口标记为up。如果接口可以提供双向通信，会将线路协议标记为 up。

当未指定接口名称时，会显示所有IPv6接口的信息。指定接口名称则会显示有关指定接口的信息。

示例

以下是 **show ipv6 interface** 命令的输出示例：

```
> show ipv6 interface outside
interface ethernet0 “outside” is up, line protocol is up
  IPv6 is enabled, link-local address is 2001:0DB8::/29 [TENTATIVE]
  Global unicast address(es):
    2000::2, subnet is 2000::/64
  Joined group address(es):
    FF02::1
    FF02::1:FF11:6770
  MTU is 1500 bytes
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
```

以下是使用 **brief** 关键字输入的 **show ipv6 interface** 命令的输出示例：

```
> show ipv6 interface brief
outside [up/up]
    unassigned
inside [up/up]
    fe80::20d:29ff:fe1d:69f0
    fec0::a:0:0:a0a:a70
vlan101 [up/up]
    fe80::20d:29ff:fe1d:69f0
    fec0::65:0:0:a0a:6570
dmz-ca [up/up]
    unassigned
```

以下是 **show ipv6 interface** 命令的输出示例。它显示已从地址生成前缀的接口的特征。

```
> show ipv6 interface inside prefix
IPv6 Prefix Advertisements inside
Codes: A - Address, P - Prefix-Advertisement, O - Pool
       U - Per-user prefix, D - Default       N - Not advertised, C - Calendar

AD      fec0:0:0:a::/64 [LA] Valid lifetime 2592000, preferred lifetime 604800
```

show ipv6 local pool

要显示 IPv6 地址池信息，请使用 **show ipv6 local pool** 命令。

show ipv6 local pool *pool_name*

Syntax Description

pool_name	IPv6 地址池的名称。

Command History

版本	修改
6.1	引入了此命令。

使用指南

使用此命令可查看 IPv6 地址池的内容。这些池用于 远程访问 VPN 和 集群技术。使用 **show ip local pool** 以查看IPv4 地址池。

示例

以下是 **show ipv6 local pool** 命令的输出示例：

```
> show ipv6 local pool test-ipv6-pool
IPv6 Pool test-ipv6-pool
Begin Address: 2001:db8::db8:800:200c:417a
End Address: 2001:db8::db8:800:200c:4188
Prefix Length: 64
Pool Size: 15
Number of used addresses: 0
Number of available addresses: 15

Available Addresses:
2001:db8::db8:800:200c:417a
2001:db8::db8:800:200c:417b
2001:db8::db8:800:200c:417c
2001:db8::db8:800:200c:417d
2001:db8::db8:800:200c:417e
2001:db8::db8:800:200c:417f
2001:db8::db8:800:200c:4180
2001:db8::db8:800:200c:4181
2001:db8::db8:800:200c:4182
2001:db8::db8:800:200c:4183
2001:db8::db8:800:200c:4184
2001:db8::db8:800:200c:4185
2001:db8::db8:800:200c:4186
2001:db8::db8:800:200c:4187
2001:db8::db8:800:200c:4188
```

show ipv6 mld traffic

要显示组播侦听程序发现 (MLD) 流量计数器信息，请使用 **show ipv6 mld traffic** 命令。

show ipv6 mld traffic

Command History

版本	修改
6.1	引入了此命令。

使用指南

show ipv6 mld traffic 命令允许您检查是否已接收和发送预计的 MLD 消息数。以下信息是由 **show ipv6 mld traffic** 命令提供信息：

- 清除计数器以后经过的时间 - 自清除计数器以来的时间量。
- 有效 MLD 数据包 - 接收和发送的有效 MLD 数据包数。
- 查询 - 接收和发送的有效查询数。
- 报告 - 接收和发送的有效报告数。
- 保留 - 接收和发送的有效保留数。
- Mtrace 数据包 - 接收和发送的组播跟踪数据包数。
- Errors（错误）- 错误类型和发生的错误数。

示例

以下是 **show ipv6 mld traffic** 命令的输出示例：

```
> show ipv6 mld traffic
show ipv6 mld traffic
MLD Traffic Counters
Elapsed time since counters cleared: 00:01:19
                   Received          Sent
Valid MLD Packets  1                 3
Queries            1                 0
Reports            0                 3
Leaves             0                 0
Mtrace packets     0                 0
Errors:
Malformed Packets  0
Martian source     0
Non link-local source 0
Hop limit is not equal to 1 0
```

Related Commands

命令	说明
clear ipv6 mld traffic	重置所有 MLD 流量计数器。

show ipv6 neighbor

要显示 IPv6 邻居发现缓存信息，请使用 **show ipv6 neighbor** 命令。

show ipv6 neighbor ［*if_name* | 地址］

Syntax Description

地址	（可选）仅显示提供的 IPv6 地址的邻居发现缓存信息。
if_name	（可选）显示所提供接口名称的缓存信息。 如果显示所有接口，则还会看到有关用于系统通信的内部接口的信息。用户无法配置内部接口，该信息只用于调试目的。

Command History

版本	修改
6.1	引入了此命令。

使用指南

以下信息是由 **show ipv6 neighbor** 命令提供信息：

- IPv6 地址 - 邻居或接口的 IPv6 地址。
- Age（时间）- 自确认地址可到达以来的时间（以分钟为单位）。连字符 (-) 指示静态条目。
- 链路层地址 - MAC 地址。如果地址未知，则显示连字符 (-)。
- 状态 - 邻居缓存条目的状态。

注释 连通性检测不会应用于 IPv6 邻居发现缓存中的静态条目；因此，对于动态和静态缓存条目，INCMP（未完成）和 REACH（可达）状态的说明不同。

以下是 IPv6 邻居发现缓存中动态条目的可能状态：

- INCMP -（未完成）正在对条目执行地址解析。邻居请求消息已发送至目标的请求节点组播地址，但是尚未收到对应的邻居通告消息。
- REACH -（可达）在最后 ReachableTime 毫秒内收到正面确认，指示邻居的转发路径运行正常。在 REACH 状态下，由于数据包已发送，设备不执行任何特殊操作。
- STALE-自设备收到表明转发路径运行正常的最后一个正面确认之后，已经历了超过 ReachableTime 毫秒。在 STALE 状态下，设备在数据包发送完成之前不执行任何操作。
- DELAY-自设备收到表明转发路径运行正常的最后一个正面确认之后，已经历了超过 ReachableTime 毫秒。数据包在最后 DELAY_FIRST_PROBE_TIME 秒内已发送。在进入 DELAY 状态的 DELAY_FIRST_PROBE_TIME 秒内，如果未收到确定性确认，则发送邻居请求消息并将状态更改为 PROBE。

- PROBE - 通过每 RetransTimer 毫秒后重新发送邻居请求消息，积极寻找连通性确认，直至收到可达性确认。
- ???? - 未知状态。

以下是 IPv6 邻居发现缓存中静态条目的可能状态：

- INCMP -（未完成）此条目的接口关闭。
- REACH -（可达）此条目的接口开启。

- Interface

  可从中访问地址的接口。

示例

以下是输入具有接口的 **show ipv6 neighbor** 命令时的输出示例：

```
> show ipv6 neighbor inside
IPv6 Address                              Age Link-layer Addr State Interface
2000:0:0:4::2                               0 0003.a0d6.141e  REACH inside
FE80::203:A0FF:FED6:141E                    0 0003.a0d6.141e  REACH inside
3001:1::45a                                 - 0002.7d1a.9472  REACH inside
```

以下是输入具有 IPv6 地址的 **show ipv6 neighbor** 命令时，该命令的输出示例：

```
> show ipv6 neighbor 2000:0:0:4::2
IPv6 Address                              Age Link-layer Addr State Interface
2000:0:0:4::2                               0 0003.a0d6.141e  REACH inside
```

Related Commands

命令	说明
clear ipv6 neighbors	删除 IPv6 邻居发现缓存中除静态条目以外的所有条目。

show ipv6 ospf

要显示有关 OSPFv3 路由流程的一般信息，请使用 **show ipv6 ospf** 命令。

show ipv6 ospf ［*process_id*］［*area_id*］

Syntax Description

area_id	（可选）仅显示有关指定区域的信息。
process_id	（可选）指定本地分配的内部ID，可以是任何正整数。启用OSPFv3路由流程时，此 ID 是管理性分配的号码。

Command History

版本	修改
6.1	引入了此命令。

示例

以下是 **show ipv6 ospf** 命令的输出示例：

```
> show ipv6 ospf
Routing Process “ospfv3 1” with ID 10.9.4.1
Event-log enabled, Maximum number of events: 1000, Mode: cyclic
It is an autonomous system boundary router
Redistributing External Routes from,
   ospf 2
Initial SPF schedule delay 5000 msecs
Minimum hold time between two consecutive SPFs 10000 msecs
Maximum wait time between two consecutive SPFs 10000 msecs
Minimum LSA interval 5 secs
Minimum LSA arrival 1000 msecs
```

Related Commands

命令	说明
show ipv6 ospf border-routers	显示区域边界路由器(ABR)和自主系统边界路由器(ASBR)的内部OSPFv3路由表条目。
show ipv6 ospf database	显示与特定路由器 OSPFv3 数据库相关的信息列表。

show ipv6 ospf border-routers

要显示区域边界路由器 (ABR) 和自治系统边界路由器 (ASBR) 的内部 OSPFv3 路由表条目，请使用 **show ipv6 ospf border-routers** 命令。

show ipv6 ospf ［*process_id*］ **border-routers**

Syntax Description

process_id	（可选）指定本地分配的内部ID，可以是任何正整数。启用OSPFv3路由流程时，此 ID 是管理性分配的号码。

Command History

版本	修改
6.1	引入了此命令。

使用指南

show ipv6 ospf border-routers 命令列出以下设置：

- 区域内路由
- 区域间路由
- IPv6 地址
- 接口类型
- 区域 ID
- SPF 编号

示例

以下是 **show ipv6 ospf border-routers** 命令的输出示例：

```
> show ipv6 ospf border-routers
OSPFv3 Process 1 internal Routing Table

Codes: i - Intra-area route, I - Inter-area route

i 172.16.4.4 [2] via FE80::205:5FFF:FED3:5808, FastEthernet0/0, ABR, Area 1, SPF 13
i 172.16.4.4 [1] via FE80::205:5FFF:FED3:5406, POS4/0, ABR, Area 0, SPF 8
i 172.16.3.3 [1] via FE80::205:5FFF:FED3:5808, FastEthernet0/0, ASBR, Area 1, SPF 3
```

Related Commands

命令	说明
show ipv6 ospf	显示 OSPFv3 路由流程中的所有 IPv6 设置。
show ipv6 ospf database	显示与特定路由器 OSPFv3 数据库相关的信息列表。

show ipv6 ospf database

要显示与特定路由器 OSPFv3 数据库相关的信息列表，请使用 **show ipv6 ospf database** 命令。

show ipv6 ospf ［*process_id*］［*area_id*］ **database** ［**external** | **inter-area prefix** | **inter-area-router** | **network** | **nssa-external** | **router** | **area** | **as** | **ref-lsa** | ［*destination-router-id*］［**prefix** *ipv6-prefix*］［*link-state-id*］］［**link** ［**interface** *interface-name*］［**adv-router** *router-id*］ | **self-originate**］［**internal**］［**database-summary**］

Syntax Description

adv-router *router-id*	（可选）显示通告路由器的所有 LSA。路由器 ID 必须是 RFC 2740 中记录的形式，其中地址以使用冒号分隔 16 位值的十六进制格式指定。
area	（可选）仅显示有关区域 LSA 的信息。
area_id	（可选）仅显示有关指定区域的信息。
as	（可选）过滤未知自主系统 (AS) LSA。
database-summary	（可选）显示数据库中每个区域的每种类型的 LSA 数以及总数。
destination-router-id	（可选）仅显示有关指定目标路由器的信息。
external	（可选）仅显示有关外部 LSA 的信息。
interface	（可选）显示有关依据接口情景过滤的 LSA 的信息。
interface-name	（可选）指定 LSA 接口名称。
internal	（可选）仅显示有关内部 LSA 的信息。
inter-area prefix	（可选）仅显示有关基于区域间前缀的 LSA 的信息。
inter-area router	（可选）仅显示有关基于区域间路由器 LSA 的 LSA 的信息。
link	（可选）显示有关链路 LSA 的信息。当后面有 **unknown** 关键字时， **link** 关键字会过滤链路范围 LSA。
link-state-id	（可选）指定用于区分 LSA 的整数。在网络和链路 LSA 中，链路状态 ID 与接口索引匹配。
network	（可选）显示有关网络 LSA 的信息。
nssa-external	（可选）仅显示有关末节区域 (NSSA) 外部 LSA 的信息。
prefix *ipv6-prefix*	（可选）显示邻居的本地链路 IPv6 地址。IPv6 前缀必须采用 RFC 2373 规定的格式，其中地址以十六进制的 16 位值指定，各个值之间用冒号分隔。
process_id	（可选）指定本地分配的内部 ID，可以是任何正整数。启用 OSPF 路由流程时，此 ID 是管理性分配的号码。

ref-lsa	（可选）进一步过滤前缀 LSA 类型。
router	（可选）显示有关路由器 LSA 的信息。
self-originate	（可选）仅显示来自本地路由器的自发 LSA。

Command History

版本	修改
6.1	引入了此命令。

使用指南

多种形式的命令提供有关不同 OSPFv3 LSA 的信息。

示例

以下是 **show ipv6 ospf database** 命令的输出示例：

```
> show ipv6 ospf database

            OSPFv3 Router with ID (172.16.4.4) (Process ID 1)

                Router Link States (Area 0)

ADV Router         Age         Seq#        Fragment ID   Link count  Bits
172.16.4.4         239         0x80000003  0             1           B
172.16.6.6         239         0x80000003  0             1           B

            Inter Area Prefix Link States (Area 0)

ADV Router         Age         Seq#        Prefix
172.16.4.4         249         0x80000001  FEC0:3344::/32
172.16.4.4         219         0x80000001  FEC0:3366::/32
172.16.6.6         247         0x80000001  FEC0:3366::/32
172.16.6.6         193         0x80000001  FEC0:3344::/32
172.16.6.6         82          0x80000001  FEC0::/32

            Inter Area Router Link States (Area 0)

ADV Router         Age         Seq#        Link ID    Dest RtrID
172.16.4.4         219         0x80000001  50529027   172.16.3.3
172.16.6.6         193         0x80000001  50529027   172.16.3.3

            Link (Type-8) Link States (Area 0)

ADV Router         Age         Seq#        Link ID    Interface
172.16.4.4         242         0x80000002  14         PO4/0
172.16.6.6         252         0x80000002  14         PO4/0

            Intra Area Prefix Link States (Area 0)

ADV Router         Age         Seq#        Link ID    Ref-lstype  Ref-LSID
172.16.4.4         242         0x80000002  0          0x2001      0
172.16.6.6         252         0x80000002  0          0x2001      0
```

Related Commands

命令	说明
show ipv6 ospf	显示 OSPFv3 路由流程中的所有 IPv6 设置。
show ipv6 ospf border-routers	显示区域边界路由器 (ABR) 和自主系统边界路由器 (ASBR) 的内部 OSPFv3 路由表条目。

show ipv6 ospf events

要显示 OSPFv3 内部事件信息，请使用 **show ipv6 ospf events** 命令。

show ipv6 ospf ［*process_id*］ **events** ［*type*］

Syntax Description

process_id	（可选）指定本地分配的内部ID，可以是任何正整数。启用OSPF路由流程时，此 ID 是管理性分配的号码。
type	（可选）要查看的事件类型的列表。如果不指定一种或多种类型，则会看到所有事件。您可以过滤以下类型： • **generic**-通用事件。 • **interface**- 接口状态更改事件。 • **lsa**- LSA 到达和 LSA 生成事件。 • **neighbor**- 邻居状态更改事件。 • **reverse**- 以相反的顺序显示事件。 • **rib**- 路由器信息库更新、删除和重新分发事件。 • **spf**- SPF 计划和 SPF 运行事件。

Command History

版本	修改
6.1	引入了此命令。

示例

以下是 **show ipv6 ospf events** 命令的输出示例：

```
> show ipv6 ospf events

OSPFv3 Router with ID (10.1.3.2) (Process ID 10)

   1 Jul 9  18:49:34.071: Timer Exp:  ospfv3_if_ack_delayed  0xda05fad8
   2 Jul 9  18:49:31.571: Rcv Unchanged Type-0x2001 LSA, LSID 0.0.0.0, Adv-Rtr 10.1.1.2,

Seq# 80000008, Age 1, Area 10
   3 Jul 9  18:48:13.241: Generate Changed Type-0x8 LSA, LSID 2.0.0.0, Seq# 80000004,
Age    0, Area 10
   4 Jul 9  18:48:13.241: Generate Changed Type-0x2001 LSA, LSID 0.0.0.0, Seq# 80000005,

Age 0, Area 10
   5 Jul 9  18:41:18.901: End of SPF, SPF time 0ms, next wait-interval 10000ms
   6 Jul 9  18:41:18.902: Starting External processing in area 10
   7 Jul 9  18:41:18.902: Starting External processing
   8 Jul 9  18:41:18.902: Starting Inter-Area SPF in area 10
```

```
   9 Jul 9  18:41:18.902: Generic:  post_spf_intra  0x0
  10 Jul 9  18:41:18.902: RIB Delete (All Paths), Prefix 2002::/64, type Intra
  11 Jul 9  18:41:18.902: RIB Update, Prefix 5005::/64, gw ::, via inside, type Intra
  12 Jul 9  18:41:18.902: Starting Intra-Area SPF in Area 10
  13 Jul 9  18:41:18.903: Starting SPF, wait-interval 5000ms
  14 Jul 9  18:41:16.403: Timer Exp:  ospfv3_if_ack_delayed  0xda05fad8
  15 Jul 9  18:41:13.903: Schedule SPF, Area 10, Change in LSA type PLSID 0.8.0.0,
Adv-Rtr   50.100.168.192
  16 Jul 9  18:41:13.903: Rcv Changed Type-0x2009 LSA, LSID 0.8.0.0, Adv-Rtr 10.1.2.3,
Seq# 80000003, Age 1, Area 10
```

Related Commands

命令	说明
show ipv6 ospf	显示 OSPFv3 路由流程中的所有 IPv6 设置。
show ipv6 ospf border-routers	显示区域边界路由器 (ABR) 和自主系统边界路由器 (ASBR) 的内部 OSPFv3 路由表条目。

show ipv6 ospf flood-list

要显示等待通过接口泛洪的 OSPFv3 LSA 列表，请使用 **show ipv6 ospf flood-list** 命令。

show ipv6 ospf ［*process_id*］［*area_id*］ **flood-list** *interface-type interface-number*

Syntax Description

area_id	（可选）仅显示有关指定区域的信息。
interface-number	指定泛洪 LSA 所在的接口号。
interface-type	指定泛洪 LSA 所在的接口类型。
process_id	（可选）指定本地分配的内部ID，可以是任何正整数。启用OSPFv3路由流程时，此 ID 是管理性分配的号码。

Command History

版本	修改
6.1	引入了此命令。

使用指南

使用此命令可显示 OSPFv3 数据包节奏信息。

示例

以下是 **show ipv6 ospf flood-list** 命令的输出示例：

```
> show ipv6 ospf flood-list

OSPFv3 Router with ID (172.16.6.6) (Process ID 1)

 Interface POS4/0, Queue length 1
 Link state retransmission due in 14 msec

 Type    LS ID           ADV RTR         Seq NO      Age    Checksum
 0x2001  0               172.16.6.6      0x80000031  0      0x1971

 Interface FastEthernet0/0, Queue length 0

 Interface ATM3/0, Queue length 0
```

Related Commands

命令	说明
show ipv6 ospf	显示 OSPFv3 路由流程中的所有 IPv6 设置。
show ipv6 ospf border-routers	显示区域边界路由器(ABR)和自主系统边界路由器(ASBR)的内部OSPFv3路由表条目。

show ipv6 ospf graceful-restart

要显示有关 OSPFv3 graceful-restart 的信息，请使用 **show ipv6 ospf graceful-restart** 命令。

show ipv6 ospf graceful-restart

Command History

版本	修改
6.1	引入了此命令。

示例

以下是 **show ipv6 ospf graceful-restart** 命令的输出示例：

```
> show ipv6 ospf graceful-restart
Routing Process "ospfv3 10"
  Graceful Restart enabled
    restart-interval limit: 240 sec
    Clustering is not configured in spanned etherchannel mode
  Graceful Restart helper support enabled
    Number of neighbors performing Graceful Restart is 0
```

Related Commands

命令	说明
show ipv6 ospf	显示 OSPFv3 路由流程中的所有 IPv6 设置。

show ipv6 ospf interface

要显示 OSPFv3 相关的接口信息，请使用 **show ipv6 ospf interface** 命令。

show ipv6 ospf ［*process_id*］［*area_id*］ **interface** ［*type-number*］［**brief**］

Syntax Description

area_id	（可选）仅显示有关指定区域的信息。
brief	（可选）显示路由器上 OSPFv3 接口、状态、地址和掩码以及区域的简要概述信息。
process_id	（可选）指定本地分配的内部 ID，可以是任何正整数。启用 OSPF 路由流程时，此 ID 是管理性分配的号码。
type-number	（可选）指定接口类型和号码。

Command History

版本	修改
6.1	引入了此命令。

使用指南

使用此命令可显示路由器上 OSPFv3 接口、状态、地址和掩码以及区域的概述信息。

示例

以下是 **show ipv6 ospf interface** 命令的输出示例：

```
> show ipv6 ospf interface
ATM3/0 is up, line protocol is up
  Link Local Address 2001:0DB1:205:5FFF:FED3:5808, Interface ID 13
  Area 1, Process ID 1, Instance ID 0, Router ID 172.16.3.3
  Network Type POINT_TO_POINT, Cost: 1
  Transmit Delay is 1 sec, State POINT_TO_POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:06
  Index 1/2/2, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 12, maximum is 12
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 172.16.4.4
  Suppress hello for 0 neighbor(s)
FastEthernet0/0 is up, line protocol is up
  Link Local Address 2001:0DB1:205:5FFF:FED3:5808, Interface ID 3
  Area 1, Process ID 1, Instance ID 0, Router ID 172.16.3.3
  Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State BDR, Priority 1
  Designated Router (ID) 172.16.6.6, local address 2001:0DB1:205:5FFF:FED3:6408
  Backup Designated router (ID) 172.16.3.3, local address 2001:0DB1:205:5FFF:FED3:5808
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:05
  Index 1/1/1, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
```

```
Last flood scan length is 12, maximum is 12
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1, Adjacent neighbor count is 1
  Adjacent with neighbor 172.16.6.6  (Designated Router)
Suppress hello for 0 neighbor(s)
```

Related Commands

命令	说明
show ipv6 ospf	显示 OSPFv3 路由流程中的所有 IPv6 设置。
show ipv6 ospf border-routers	显示区域边界路由器 (ABR) 和自主系统边界路由器 (ASBR) 的内部 OSPFv3 路由表条目。

show ipv6 ospf request-list

要显示路由器已请求的所有 LSA 的列表，请使用 **show ipv6 ospf request-list** 命令。

show ipv6 ospf ［*process_id*］［*area_id*］ **request-list** ［*neighbor*］［*interface*］［*interface-neighbor*］

Syntax Description

area_id	（可选）仅显示有关指定区域的信息。
interface	（可选）指定路由器从此接口请求的所有 LSA 的列表。
interface-neighbor	（可选）指定路由器在此接口上从此邻居请求的所有 LSA 的列表。
neighbor	（可选）指定路由器从此邻居请求的所有 LSA 的列表。
process_id	（可选）指定本地分配的内部ID，可以是任何正整数。启用OSPF路由流程时，此 ID 是管理性分配的号码。

Command History

版本	修改
6.1	引入了此命令。

示例

以下是 **show ipv6 ospf request-list** 命令的输出示例：

```
> show ipv6 ospf request-list

            OSPFv3 Router with ID (192.168.255.5) (Process ID 1)

 Neighbor 192.168.255.2, interface Ethernet0/0 address
FE80::A8BB:CCFF:FE00:6600

 Type    LS ID           ADV RTR         Seq NO      Age    Checksum
  1      0.0.0.0         192.168.255.3   0x800000C2  1      0x0014C5
  1      0.0.0.0         192.168.255.2   0x800000C8  0      0x000BCA
  1      0.0.0.0         192.168.255.1   0x800000C5  1      0x008CD1
  2      0.0.0.3         192.168.255.3   0x800000A9  774    0x0058C0
  2      0.0.0.2         192.168.255.3   0x800000B7  1      0x003A63
```

Related Commands

命令	说明
show ipv6 ospf	显示 OSPFv3 路由流程中的所有 IPv6 设置。
show ipv6 ospf border-routers	显示区域边界路由器(ABR)和自主系统边界路由器(ASBR)的内部OSPFv3路由表条目。

show ipv6 ospf retransmission-list

要显示等待重新发送的所有 LSA 的列表，请使用 **show ipv6 ospf retransmission-list** 命令。

show ipv6 ospf ［*process_id*］［*area_id*］ **retransmission-list** ［*neighbor*］［*interface*］［*interface-neighbor*］

Syntax Description

area_id	（可选）仅显示有关指定区域的信息。
interface	（可选）指定在此接口上等待重新发送的所有 LSA 的列表。
interface-neighbor	（可选）指定针对此接口等待从此邻居重新发送的所有 LSA 的列表。
neighbor	（可选）指定等待针对此邻居重新发送的所有 LSA 的列表。
process_id	（可选）指定本地分配的内部ID，可以是任何正整数。启用OSPF路由流程时，此 ID 是管理性分配的号码。

Command History

版本	修改
6.1	引入了此命令。

示例

以下是 **show ipv6 ospf retransmission-list** 命令的输出示例：

```
> show ipv6 ospf retransmission-list

       OSPFv3 Router with ID (192.168.255.2) (Process ID 1)

Neighbor 192.168.255.1, interface Ethernet0/0
Link state retransmission due in 3759 msec, Queue length 1

Type    LS ID           ADV RTR         Seq NO      Age    Checksum
0x2001  0               192.168.255.2   0x80000222  1      0x00AE52
```

Related Commands

命令	说明
show ipv6 ospf	显示 OSPFv3 路由流程中的所有 IPv6 设置。
show ipv6 ospf border-routers	显示区域边界路由器(ABR)和自主系统边界路由器(ASBR)的内部OSPFv3路由表条目。

show ipv6 ospf statistic

使用 **show ipv6 ospf statistic** 命令以显示各种 OSPFv3 统计信息，例如 SPF 的执行次数、原因和持续时间。

show ipv6 ospf ［*process_id*］ **statistic** ［**detail**］

Syntax Description

detail	（可选）指定详细 SPF 信息，包括触发点。
process_id	（可选）指定本地分配的内部ID，可以是任何正整数。启用OSPF路由流程时，此 ID 是管理性分配的号码。

Command History

版本	修改
6.1	引入了此命令。

示例

以下是 **show ipv6 ospf statistic** 命令的输出示例：

```
> show ipv6 ospf 10 statistic detail
Area 10: SPF algorithm executed 6 times

SPF 1 executed 04:36:56 ago, SPF type Full
  SPF calculation time (in msec):
  SPT    Prefix D-Int  Sum    D-Sum  Ext    D-Ext  Total
       0      0      0      0      0      0      0 0
  RIB manipulation time (in msec):
  RIB Update    RIB Delete
              0             0
  LSIDs processed R:1 N:0 Prefix:0 SN:0 SA:0 X7:0
  Change record R L
  LSAs changed 2
  Changed LSAs. Recorded is Advertising Router, LSID and LS type:
  49.100.168.192/0(R) 49.100.168.192/2(L)

SPF 2 executed 04:35:50 ago, SPF type Full
  SPF calculation time (in msec):
  SPT    Prefix D-Int  Sum    D-Sum  Ext    D-Ext  Total
       0      0      0      0      0      0      0 0
  RIB manipulation time (in msec):
  RIB Update    RIB Delete
              0             0
  LSIDs processed R:2 N:1 Prefix:0 SN:0 SA:0 X7:0
  Change record R N L
  LSAs changed 5
  Changed LSAs. Recorded is Advertising Router, LSID and LS type:
  50.100.168.192/0(R) 50.100.168.192/2(L) 49.100.168.192/0(R) 50.100.168.192/0(R)
  50.100.168.192/2(N)
```

show ipv6 ospf summary-prefix

要显示在 OSPFv3 流程下配置的所有汇总地址重新分发信息的列表，请使用 **show ipv6 ospf summary-prefix** 命令。

show ipv6 ospf ［*process_id*］ **summary-prefix**

Syntax Description

process_id	（可选）指定本地分配的内部ID，可以是任何正整数。启用OSPF路由流程时，此 ID 是管理性分配的号码。

Command History

版本	修改
6.1	引入了此命令。

示例

以下是 **show ipv6 ospf summary-prefix** 命令的输出示例：

```
> show ipv6 ospf summary-prefix

OSPFv3 Process 1, Summary-prefix

FEC0::/24 Metric 16777215, Type 0, Tag 0
```

Related Commands

命令	说明
show ipv6 ospf	显示 OSPFv3 路由流程中的所有 IPv6 设置。
show ipv6 ospf border-routers	显示区域边界路由器(ABR)和自主系统边界路由器(ASBR)的内部OSPFv3路由表条目。

show ipv6 ospf timers

要显示 OSPFv3 计时器信息，请使用 **show ipv6 ospf timers** 命令。

show ipv6 ospf ［*process_id*］ **timers** ［**lsa-group** | **rate-limit**］

Syntax Description

lsa-group	（可选）指定 OSPFv3 LSA 组信息。
process_id	（可选）指定本地分配的内部ID，可以是任何正整数。启用OSPF路由流程时，此 ID 是管理性分配的号码。
rate-limit	（可选）指定 OSPFv3 LSA 速率限制信息。

Command History

版本	修改
6.1	引入了此命令。

示例

以下是 **show ipv6 ospf timers lsa-group** 命令的输出示例：

```
> show ipv6 ospf timers lsa-group

OSPFv3 Router with ID (10.10.13.101) (Process ID 1)

Group size 5, Head 2, Search Index 4, Interval 240 sec
Next update due in 0:00:13
Current time 96532
Index 0 Timestamp 96546
Index 1 Timestamp 96788
Index 2 Timestamp 97048
Index 3 Timestamp 97293
Index 4 Timestamp 97548

Failure Head 0, Last 0 LSA group failure logged

            OSPFv3 Router with ID (10.10.10.102) (Process ID 5709)

Group size 5, Head 2, Search Index 4, Interval 240 sec
Next update due in 0:00:22
Current time 96532
Index 0 Timestamp 96555
Index 1 Timestamp 96801
Index 2 Timestamp 97041
Index 3 Timestamp 97287
Index 4 Timestamp 97546

Failure Head 0, Last 0 LSA group failure logged
```

show ipv6 ospf traffic

要显示当前可用接口的 OSPFv3 流量相关统计信息，请使用 **show ipv6 ospf traffic** 命令。

show ipv6 ospf ［*process_id*］ **traffic** ［*interface_name*］

Syntax Description

interface_name	（可选）指定接口名称。使用此选项将流量隔离至特定接口。
process_id	（可选）指定本地分配的内部ID，可以是任何正整数。启用OSPF路由流程时，此 ID 是管理性分配的号码。

Command History

版本	修改
6.1	引入了此命令。

示例

以下是 **show ipv6 ospf traffic** 命令的输出示例：

```
> show ipv6 ospf 10 traffic inside
Interface inside

Last clearing of interface traffic counters never

OSPFv3 packets received/sent
  Type          Packets               Bytes
  RX Invalid                      0 0
  RX Hello                     1232 53132
  RX DB des                      27 896
  RX LS req                       3 216
  RX LS upd                      28 2436
  RX LS ack                      14 1064
  RX Total                     1304 57744

  TX Failed                       0 0
  TX Hello                      753 32072
  TX DB des                      27 1056
  TX LS req                       2 92
  TX LS upd                       9 1128
  TX LS ack                      15 900
  TX Total                      806 35248
```

Related Commands

命令	说明
show ipv6 ospf	显示 OSPFv3 路由流程中的所有 IPv6 设置。
show ipv6 ospf border-routers	显示区域边界路由器(ABR)和自主系统边界路由器(ASBR)的内部OSPFv3路由表条目。

show ipv6 ospf virtual-links

要显示 OSPFv3 虚拟链路的参数和当前状态，请使用 **show ipv6 ospf virtual-links** 命令。

show ipv6 ospf virtual-links

Command History

版本	修改
6.1	引入了此命令。

示例

以下是 **show ipv6 ospf virtual-links** 命令的输出示例：

```
> show ipv6 ospf virtual-links

Virtual Link OSPF_VL0 to router 172.16.6.6 is up
  Interface ID 27, IPv6 address FEC0:6666:6666::
  Run as demand circuit
  DoNotAge LSA allowed.
  Transit area 2, via interface ATM3/0, Cost of using 1
  Transmit Delay is 1 sec, State POINT_TO_POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:06
```

Related Commands

命令	说明
show ipv6 ospf	显示 OSPFv3 路由流程中的所有 IPv6 设置。
show ipv6 ospf border-routers	显示区域边界路由器 (ABR) 和自主系统边界路由器 (ASBR) 的内部 OSPFv3 路由表条目。

show ipv6 prefix-list

要列出配置为匹配 IPv6 流量的前缀列表，请使用 **show ipv6 prefix-list** 命令。

show ipv6 prefix-list ［**detail** | **summary**］［*prefix_list_name* ［**seq** *sequence_number* | *network/length* ［**longer** | **first-match**］］］

Syntax Description

detail	显示有关前缀列表的详细信息。
summary	显示前缀列表摘要。
prefix_list_name	前缀列表的名称。
seq *sequence-number*	（可选）仅显示指定前缀列表中具有指定序列号的前缀列表条目。
network/length [**longer** | **first-match**]	（可选）显示使用此网络地址和前缀长度（以位为单位）的指定前缀列表中的所有条目。 您可以选择包含以下关键字之一： • **longer** 显示与给定 network/length 匹配或比其更具体的指定前缀列表的所有条目。 • **first-match** 显示与给定 network/length 匹配的指定前缀列表的第一个条目。

Command History

版本	修改
6.1	引入了此命令。

示例

以下是 **show ipv6 prefix-list** 命令的输出示例。

```
> show ipv6 prefix-list
ipv6 prefix-list test-ipv6-prefix: 1 entries
   seq 5 permit 2001:db8:0:cd30::/64
```

以下是汇总输出的示例。

```
> show ipv6 prefix-list summary
Prefix-list with the last deletion/insertion: test-ipv6-prefix
ipv6 prefix-list test-ipv6-prefix:   count: 1, range entries: 0,
sequences: 5 - 5, refcount: 2
```

以下是详细输出示例。

```
> show ipv6 prefix-list detail
Prefix-list with the last deletion/insertion: test-ipv6-prefix
ipv6 prefix-list test-ipv6-prefix:   count: 1, range entries: 0,
sequences: 5 - 5, refcount: 2
```

Related Commands

命令	说明
clear ipv6 prefix-list	重置 IPv6 前缀列表的命中计数。
show bgp prefix-list	显示在边界网关协议情景下有关前缀列表或前缀列表条目的信息。
show prefix-list	显示有关 IPv4 前缀列表的信息。

show ipv6 route

要显示 IPv6 路由表的内容，请使用 **show ipv6 route** 命令。

show ipv6 route ［**vrf** *name* | **all**］ ［**management-only**］［**failover**］［**cluster**］［**interface** *name*］［**ospf**］［**summary**］

Syntax Description

managment-only	显示 IPv6 管理路由表中的路由。
cluster	（可选）显示集群中的 IPv6 路由表序号、IPv6 重新收敛计时器状态和 IPv6 路由条目序号。
failover	（可选）显示 IPv6 路由表序号、IPv6 重新收敛计时器状态和 IPv6 路由条目序号。
interface *name*	（可选）显示 IPv6 接口特定的路由。
ospf	（可选）显示 OSPFv3 路由。
summary	（可选）显示 IPv6 路由汇总。
［**vrf** *name*	**all**］	如果启用虚拟路由和转发 (VRF)（也称为虚拟路由器），则可以使用 **vrf** *name* 关键字将视图限制为特定虚拟路由器。如果要查看所有虚拟路由器的路由表，请包含 **all** 关键字。如果不包括这些与 VRF 相关的关键字，则命令会显示全局 VRF 虚拟路由器的路由表。

Command History

版本	修改
6.1	引入了此命令。
6.6	添加了 ［**vrf** *name*	**all**］ 关键字。

使用指南

show ipv6 route 命令的输出类似于 **show route** 命令的输出，唯一不同之处是，前者显示的信息是 IPv6 特定信息。

以下信息出现在 IPv6 路由表中：

- 代码 - 指示派生路由的协议。值如下所示：
  - C - 连接
  - L - 本地
  - S - 静态
  - R - 派生的 RIP
  - B - 派生的 BGP

- I1 - ISIS L1 - 派生的集成 IS-IS 级别 1
- I2 - ISIS L2 - 派生的集成 IS-IS 级别 2
- IA - ISIS interarea - 派生的集成 ISIS interarea

- fe80::/10 - 指示远程网络的 IPv6 前缀。
- [0/0] - 中括号中的第一个数字是信息源的管理距离；第二个数字是路由的指标。
- via :: - 指定到远程网络的下一个路由器的地址。
- inside - 指定可到达所指定网络的下一个路由器所使用的接口。

示例

以下是 **show ipv6 route** 命令的输出示例：

```
> show ipv6 route

IPv6 Routing Table - 7 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
L   fe80::/10 [0/0]
     via ::, inside
     via ::, vlan101
L   fec0::a:0:0:a0a:a70/128 [0/0]
     via ::, inside
C   fec0:0:0:a::/64 [0/0]
     via ::, inside
L   fec0::65:0:0:a0a:6570/128 [0/0]
     via ::, vlan101
C   fec0:0:0:65::/64 [0/0]
     via ::, vlan101
L   ff00::/8 [0/0]
     via ::, inside
     via ::, vlan101
S   ::/0 [0/0]
     via fec0::65:0:0:a0a:6575, vlan101
```

以下是 **show ipv6 route failover** 命令的输出示例：

```
> show ipv6 route failover

IPv6 Routing Table - 6 entries
Codes: C - Connected, L - Local, S - Static
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
           ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
IPv6 Routing table seq num 0
IPv6 Reconvergence timer expired

O   2009::1/128 [110/10]
     via fe80::217:94ff:fe85:4401, inside seq 0
OE2  2011::/64 [110/20]
     via fe80::217:94ff:fe85:4401, inside seq 0
```

```
S   4001::1/128 [0/0]
     via 4001::2, inside seq 0
C   7001::1/128 [0/0]
     via ::, outside seq 0
L   fe80::/10 [0/0]
     via ::, inside seq 0
     via ::, outside seq 0
L   ff00::/8 [0/0]
     via ::, inside seq 0
     via ::, outside seq 0
```

以下是主设备上 s**how ipv6 route cluster** 命令的输出示例：

```
> show ipv6 route cluster

IPv6 Routing Table - 5 entries
Codes: C - Connected, L - Local, S - Static
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
            ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
IPv6 Routing table seq num 2
IPv6 Reconvergence timer expired

OE2  2001::/58 [110/20]
     via fe80::21f:9eff:fe2a:78ba, inside seq 2
...
```

以下是角色更改期间辅助设备上 **show ipv6 route cluster** 命令的输出示例：

```
> cluster master
INFO: Wait for existing master to quit. Use "show cluster info"
to check status. Use "cluster remove unit <name>" to force
master unit out of the cluster if for some reason it refuses
to quit within reasonable time
> show ipv6 route cluster

IPv6 Routing Table - 5 entries
Codes: C - Connected, L - Local, S - Static
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
            ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
IPv6 Routing table seq num 3
IPv6 Reconvergence timer expires in 61 secs

OE2  2001::/58 [110/20]
     via fe80::21f:9eff:fe2a:78ba, inside seq 2
...
```

以下示例显示名为 red 的虚拟路由器的路由。请注意，泄漏到其他虚拟路由器的静态路由使用密钥 SI 表示。

```
> show ipv6 route vrf red

Codes: C - Connected, L - Local, S - Static, SI - Static InterVRF
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
            ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2, B - BGP, V - VPN
            I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary

IPv6 Routing Table : red - 5 entries
L   2301::/128 [0/0]
     via ::, gig0
C   2301::/64 [0/0]
```

```
     via ::, gig0
SI  2304::/64 [1/0]
     via ::, gig3
L   fe80::/10 [0/0]
     via ::, gig0
L   ff00::/8 [0/0]
     via ::, gig0
```

Related Commands

命令	说明
show route	显示 IPv4 路由表。
show vrf	显示系统上的虚拟路由器。

show ipv6 routers

要显示从链路上的路由器接收的 IPv6 路由器通告信息，请使用 **show ipv6 routers** 命令。

show ipv6 routers ［*if_name*］

Syntax Description

if_name	（可选）要显示相关信息的内部或外部接口名称。

Command History

版本	修改
6.1	引入了此命令。

使用指南

当未指定接口名称时，会显示所有 IPv6 接口的信息。指定接口名称则会显示有关指定接口的信息。

示例

以下是输入时没有接口名称的 **show ipv6 routers** 命令的输出示例：

```
> show ipv6 routers
Router FE80::83B3:60A4 on outside, last update 3 min
  Hops 0, Lifetime 6000 sec, AddrFlag=0, OtherFlag=0
  Reachable time 0 msec, Retransmit time 0 msec
  Prefix 3FFE:C00:8007::800:207C:4E37/96 autoconfig
    Valid lifetime -1, preferred lifetime -1
Router FE80::290:27FF:FE8C:B709 on inside, last update 0 min
  Hops 64, Lifetime 1800 sec, AddrFlag=0, OtherFlag=0
  Reachable time 0 msec, Retransmit time 0 msec
```

Related Commands

命令	说明
ipv6 route	将静态条目添加至 IPv6 路由表。

show ipv6 traffic

要显示有关 IPv6 流量的统计信息，请使用 **show ipv6 traffic** 命令。

show ipv6 traffic

Command History

版本	修改
6.1	引入了此命令。

使用指南

使用 **clear ipv6 traffic** 命令清除流量计数器。

示例

以下是 **show ipv6 traffic** 命令的输出示例：

```
> show ipv6 traffic
IPv6 statistics:
  Rcvd:  545 total, 545 local destination
         0 source-routed, 0 truncated
         0 format errors, 0 hop count exceeded
         0 bad header, 0 unknown option, 0 bad source
         0 unknown protocol, 0 not a router
         218 fragments, 109 total reassembled
         0 reassembly timeouts, 0 reassembly failures
  Sent:  228 generated, 0 forwarded
         1 fragmented into 2 fragments, 0 failed
         0 encapsulation failed, 0 no route, 0 too big
  Mcast: 168 received, 70 sent

ICMP statistics:
  Rcvd: 116 input, 0 checksum errors, 0 too short
        0 unknown info type, 0 unknown error type
        unreach: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
        parameter: 0 error, 0 header, 0 option
        0 hopcount expired, 0 reassembly timeout,0 too big
        0 echo request, 0 echo reply
        0 group query, 0 group report, 0 group reduce
        0 router solicit, 60 router advert, 0 redirects
        31 neighbor solicit, 25 neighbor advert
  Sent: 85 output, 0 rate-limited
        unreach: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
        parameter: 0 error, 0 header, 0 option
        0 hopcount expired, 0 reassembly timeout,0 too big
        0 echo request, 0 echo reply
        0 group query, 0 group report, 0 group reduce
        0 router solicit, 18 router advert, 0 redirects
        33 neighbor solicit, 34 neighbor advert

UDP statistics:
  Rcvd: 109 input, 0 checksum errors, 0 length errors
        0 no port, 0 dropped
  Sent: 37 output

TCP statistics:
```

```
Rcvd: 85 input, 0 checksum errors
Sent: 103 output, 0 retransmitted
```

Related Commands

命令	说明
clear ipv6 traffic	清除 IPv6 流量计数器。

show isakmp sa

要显示 IKE 运行时间 SA 数据库，请使用 **show isakmp sa** 命令。

show isakmp sa ［**detail**］

Syntax Description

detail	显示关于 SA 数据库的详细输出。

Command History

版本	修改
6.1	引入了此命令。

示例

以下示例显示有关 SA 数据库的详细信息：

```
> show isakmp sa detail

IKE Peer   Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
1 209.165.200.225 User  Resp  No   AM_Active  3des    SHA   preshrd 86400

IKE Peer   Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
2 209.165.200.226 User  Resp  No   AM_ACTIVE  3des    SHA   preshrd 86400

IKE Peer   Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
3 209.165.200.227 User  Resp  No   AM_ACTIVE  3des    SHA   preshrd 86400

IKE Peer   Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
4 209.165.200.228 User  Resp  No   AM_ACTIVE  3des    SHA   preshrd 86400
```

Related Commands

命令	说明
clear isakmp sa	清除 IKE 运行时间 SA 数据库。
show running-config isakmp	显示所有活动的 ISAKMP 配置。

show isakmp stats

要显示运行时间统计信息，请使用 **show isakmp stats** 命令。

威胁防御

show isakmp stats

Command History

版本	修改
6.1	引入了此命令。

使用指南

每个计数器都映射到一个关联的 cikePhase1GW 计数器。有关每个计数器的详细信息，请参阅 CISCO-IPSEC-FLOW-MONITOR-MIB.my。

- 主用/备用隧道数 - cikePhase1GWActiveTunnels
- 先前隧道数 - cikePhase1GWPreviousTunnels
- 输入八位组 - cikePhase1GWInOctets
- 输入数据包数 - cikePhase1GWInPkts
- 输入丢弃数据包数 - cikePhase1GWInDropPkts
- 输入通知数 - cikePhase1GWInNotifys
- 输入 P2 交换数 - cikePhase1GWInP2Exchgs
- 输入 P2 交换无效次数 - cikePhase1GWInP2ExchgInvalids
- 输入 P2 交换拒绝次数 - cikePhase1GWInP2ExchgRejects
- 输入 P2 Sa 删除请求数 - cikePhase1GWInP2SaDelRequests
- 输出八位组 - cikePhase1GWOutOctets
- 输出数据包数 - cikePhase1GWOutPkts
- 输出丢弃数据包数 - cikePhase1GWOutDropPkts
- 输出通知数 - cikePhase1GWOutNotifys
- 输出 P2 交换数 - cikePhase1GWOutP2Exchgs
- 输出 P2 交换无效次数 - cikePhase1GWOutP2ExchgInvalids
- 输出 P2 交换拒绝次数 - cikePhase1GWOutP2ExchgRejects
- 输出 P2 Sa 删除请求数 - cikePhase1GWOutP2SaDelRequests
- 发起方隧道数 - cikePhase1GWInitTunnels
- 发起方失败次数 - cikePhase1GWInitTunnelFails

- 响应方失败次数 - cikePhase1GWRespTunnelFails
- 系统容量故障次数 - cikePhase1GWSysCapFails
- 验证失败次数 - cikePhase1GWAuthFails
- 解密失败次数 - cikePhase1GWDecryptFails
- 散列有效失败次数 - cikePhase1GWHashValidFails
- 无 Sa 故障次数 - cikePhase1GWNoSaFails

示例

以下示例显示 ISAKMP 统计信息：

```
> show isakmp stats
Global IKE Statistics
Active Tunnels: 132
Previous Tunnels: 132
In Octets: 195471
In Packets: 1854
In Drop Packets: 925
In Notifys: 0
In P2 Exchanges: 132
In P2 Exchange Invalids: 0
In P2 Exchange Rejects: 0
In P2 Sa Delete Requests: 0
Out Octets: 119029
Out Packets: 796
Out Drop Packets: 0
Out Notifys: 264
Out P2 Exchanges: 0
Out P2 Exchange Invalids: 0
Out P2 Exchange Rejects: 0
Out P2 Sa Delete Requests: 0
Initiator Tunnels: 0
Initiator Fails: 0
Responder Fails: 0
System Capacity Fails: 0
Auth Fails: 0
Decrypt Fails: 0
Hash Valid Fails: 0
No Sa Fails: 0
```

Related Commands

命令	说明
clear isakmp sa	清除 IKE 运行时间 SA 数据库。
show running-config isakmp	显示所有活动的 ISAKMP 配置。

show isis database

要显示 IS-IS 链路状态数据库，请使用 **show isis database** 命令。

show isis database ［{**detail** | **verbose**} ［**ip** ［**unicast**］ | **ipv6** ［**unicast**］］ ［**topology base**］］ ［**level-1** | **level-2**］

Syntax Description

level-1	（可选）显示级别 1 的 IS-IS 链路状态数据库。
level-2	（可选）显示级别 2 的 IS-IS 链路状态数据库。
ip	（可选）显示 IPv4 地址系列的 IS-IS 链路状态数据库
ipv6	（可选）显示 IPv6 地址系列的 IS-IS 链路状态数据库
detail	（可选）显示每个链路状态数据包 (LSP) 的内容。
verbose	（可选）显示有关中间 IS-IS 数据库的其他信息。
topology base	（可选）显示 MTR 拓扑。
unicast	（可选）显示单播地址系列。

Command History

版本	修改
6.3	引入了此命令。

使用指南

下表对此命令的输出进行了解释。

表 *9: IS-IS* 数据库输出中的字段

字段	说明
LSPID	链路状态数据包 (LSP) 标识符。前六个八位组构成发起 LSP 的路由器的系统 ID。 下一个八位组是伪节点 ID。当此字节为非零值时，LSP 描述来自系统的链路。当它为零时，LSP 是所谓的非伪节点 LSP。此机制类似于开放最短路径优先 (OSPF) 协议中的路由器链路状态通告 (LSA)。LSP 将描述始发路由器的状态。 对于每个 LAN，该 LAN 的指定路由器将创建并泛洪伪节点 LSP，描述连接到该 LAN 的所有系统。 最后一个八位组是 LSP 编号。如果数据超过单个 LSP 的容量，LSP 将被划分为多个 LSP 分段。每个分段将具有不同的 LSP 编号。星号 (*) 表示 LSP 是由发出此命令的系统发起的。
LSP Seq Num	LSP 的序列号，允许其他系统确定它们是否已收到来自源的最新信息。

字段	说明
LSP Checksum	整个 LSP 数据包的校验和。
LSP Holdtime	LSP 保持有效的时间（以秒为单位）。LSP 保持时间为 0 表示此 LSP 已清除，并正在从所有路由器的链路状态数据库 (LSDB) 中删除。该值表示被清除的 LSP 在被完全删除之前将在 LSDB 中保留多长时间。
ATT	附加位。此位表示路由器也是第 2 级路由器，可以到达其他区域。仅 1 级路由器和与其他 2 级路由器失去连接的 1-2 级路由器将使用“连接”位来查找最近的 2 级路由器。它们会将默认路由指向最近的 2 级路由器。
P	P 位。检测中间系统是否支持区域分区修复。Cisco 和其他供应商不支持区域分区修复。
OL-	超载位。确定 IS 是否拥塞。如果设置了过载位，则其他路由器在计算路由器时不会将此系统用作中转路由器。只有目的地直接连接到过载路由器的数据包才会发送到此路由器。
Area Address (Detail and Verbose output only.)	可从路由器访问的区域地址。对于 1 级 LSP，这些是在源路由器上手动配置的区域地址。对于 2 级 LSP，这些是此路由器所属区域的所有区域地址。
NLPID (Detail and Verbose output only.)	网络层协议标识符。
Hostname (Detail and Verbose output only.)	节点的主机名。
Router ID (Detail and Verbose output only.)	节点的流量工程路由器标识符。
IP Address (Detail and Verbose output only.)	接口的 IPv4 地址。
Metric (Detail and Verbose output only.)	源路由器与通告邻居之间的邻接开销的 IS-IS 度量，或从通告路由器到通告目的地（可以是 IP 地址、终端系统 (ES)、或无连接网络服务 [CLNS] 前缀）。
Affinity （仅限 Verbose 输出。）	被泛洪的链路属性标志。

字段	说明
Physical BW （仅限 Verbose 输出。）	链路带宽容量（以位/秒为单位）。
Reservable BW （仅限 Verbose 输出。）	此链路上的可预留带宽量。
BW Unreserved （仅限 Verbose 输出。）	可用于预留的带宽量。

示例

以下示例显示 IS-IS 数据库。

```
> show isis database

IS-IS Level-1 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
c1.00-00              0xea19d300     0x3d0d               674                     0/0/0
routerA.00-00     0x1b541556     0xa349               928                     0/0/0
c3.00-00              0x9257c979     0x9952               759                     0/0/0
c2.00-00             *0xef11e977     0x3188               489                     0/0/0
c2.01-00             *0xa8333f03     0xd6ea               829                     0/0/0
IS-IS Level-2 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
c1.00-00              0x63871f24      0xaba2               526                      0/0/0
routerA.00-00     0x0d540b55      0x81d7             472                     0/0/0
routerA.00-01     0xffffff01          0xe20b              677                     0/0/0
c3.00-00              0x002e5434      0xb20a             487                     0/0/0
c2.00-00             *0x74fd1227      0xbb0f             742                     0/0/0
c2.01-00             *0x7ee72c1a      0xb506             968                     0/0/0
```

以下示例显示 IS-IS 数据库的详细输出。详细输出显示每个 LSP 的内容。

```
> show isis database detail

IS-IS Level-1 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
c1.00-00              0xea19d301      0x3b0e               1189                    0/0/0
  Area Address: 49.0001
  NLPID:        0xcc
  Hostname: c1
  IP Address:   10.22.22.1
  Metric:         10 IP 10.22.22.0 255.255.255.0
  Metric:         10 IS c2.01
routerA.00-00      0x1b541556     0xa349               642                     0/0/0
  Area Address: 49.0001
  NLPID:        0xcc
  Hostname: routerA
  IP Address:   10.22.22.5
```

```
  Metric:         10 IP 10.22.22.0 255.255.255.0
  Metric:         10 IS c2.01
```

以下示例仅显示级别 2 LSP 的详细输出。区域地址 39.0001 是路由器所在区域的地址。

```
> show isis database 12 detail

IS-IS Level-2 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
c1.00-00              0x63871f25      0xa9a3               1076                     0/0/0
  Area Address: 49.0001
  NLPID:        0xcc
  Hostname: c1
  IP Address:   10.22.22.1
  Metric:         10 IS c2.01
routerA.00-00     0x0d540b56     0x7fd8                941                      0/0/0
  Area Address: 49.0001
  NLPID:        0xcc
  Hostname: routerA
  IP Address:   10.22.22.5
  Metric:         10 IS c2.01
  Metric:          0 IP-External 1.1.1.0 255.255.255.0
  Metric:          0 IP-External 2.1.1.0 255.255.255.0
  Metric:          0 IP-External 2.2.2.0 255.255.255.0
  Metric:          0 IP-External 3.1.1.0 255.255.255.0
```

以下示例显示了详细输出。

```
> show isis database verbose

IS-IS Level-1 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
c1.00-00             *0xea19d301   0x3b0e        644               0/0/0
  Area Address: 49.0001
  NLPID:        0xcc
  Hostname: c1
  IP Address:   22.22.22.1
  Metric:         10 IP 22.22.22.0 255.255.255.0
  Metric:         10 IS c2.01
routerA.00-00         0x1b541557   0xa14a        783               0/0/0
  Area Address: 49.0001
  NLPID:        0xcc
  Hostname: routerA
  IP Address:   22.22.22.5
  Metric:         10 IP 22.22.22.0 255.255.255.0
  Metric:         10 IS c2.01
```

Related Commands

命令	说明
clear isis	清除 IS-IS 数据结构。
show clns	显示 CLNS 特定信息。
show route isis	显示 IS-IS 路由。

show isis hostname

要显示 IS-IS 路由器的路由器名称到系统 ID 映射表条目，请使用 **show isis hostname** 命令。

show isis hostname

Command History

版本	修改
6.3	引入了此命令。

使用指南

在 IS-IS 路由域中，使用系统 ID 代表每个路由器。系统 ID 是为每个 IS-IS 路由器配置的网络实体名称 (NET) 的一部分。例如，NET 配置为 49.0001.0023.0003.000a.00 的路由器的系统 ID 为 0023.0003.000a。对于网络管理员而言，在路由器上进行维护以及故障排除期间，很难记住路由器名称与系统 ID 的映射。输入 **show isis hostname** 命令可显示路由器名称与系统 ID 映射表中的条目。

示例

以下示例显示动态主机映射表。动态主机映射表显示思科威胁防御、c2、c3 和名为 routerA 的本地路由器的路由器名称到系统 ID 的映射表条目。该表还显示，c3 是级别 1 路由器，其主机名由级别 1 (L1) 链路状态协议 (LSP) 通告。C2 是第 2 层路由器，其主机名由 L2 LSP 通告。思科威胁防御 的“级别”下显示的 * 符号表示这是系统的路由器名称到系统 ID 的映射信息。

```
> show isis hostname

Level  System ID       Dynamic Hostname  (c1)
     * 0050.0500.5005   ciscoASA
    1  0050.0500.5007   c3
    2  0050.0500.5006   routerA
    2  0050.0500.5008   c2
```

Related Commands

命令	说明
clear isis	清除 IS-IS 数据结构。
show clns	显示 CLNS 特定信息。
show route isis	显示 IS-IS 路由。

show isis lsp-log

要显示触发新链路状态数据包 (LSP) 的接口的第 1 级和第 2 级 IS-IS LSP 日志，请使用 **show isis lsp-log** 命令。

show isis lsp-log

Command History

版本	修改
6.3	引入了此命令。

使用指南

使用此命令以要显示触发新链路状态数据包 (LSP) 的接口的第 1 级和第 2 级 IS-IS LSP 日志。输出包括以下信息：

- 时间 - 自生成 LSP 以来经过的时间。
- 计数 - 此时发生的事件数。
- 接口 - 导致 LSP 重新生成的接口。
- 触发器 - 触发 LSP 泛洪的事件。LSP 的可能触发器如下：
  - AREASET - 活动区域集已更改。
  - ATTACHFLAG - 附加位更改状态。
  - CLEAR - 发出了某种形式的手动清除命令。
  - CONFIG - 任何配置更改。
  - DELADJ - 邻接关系关闭。
  - DIS - DIS 已更改或伪节点已更改。
  - ES - 终端系统邻接关系已更改。
  - HIPPITY — LSPDB 过载位已更改状态。
  - IF_DOWN - 需要新的 LSP。
  - IP_DEF_ORIG - 默认信息来源已更改。
  - IPDOWN - 直连 IP 前缀关闭。
  - IP_EXTERNAL - 重新分发的 IP 路由出现或消失。
  - IPIA - 区域间 IP 路由出现或消失。
  - IPUP - 直连 IP 前缀开启。
  - NEWADJ — 建立新的邻接关系。
  - REDIST — 已更改的 2 级 CLNS 路由已更改。

- RRR_INFO - RRR 带宽资源信息。

示例

以下是 **show isis lsp-log** 命令的输出示例：

```
> show isis lsp-log

  Level 1 LSP log
When       Count       Interface         Triggers
04:16:47     1         subint             CONFIG NEWADJ DIS
03:52:42     2         subint             NEWADJ DIS
03:52:12     1         subint             ATTACHFLAG
03:31:41     1         subint             IPUP
03:30:08     2         subint             CONFIG
03:29:38     1         subint             DELADJ
03:09:07     1         subint             DIS ES
02:34:37     2         subint             NEWADJ
02:34:07     1         subint             NEWADJ DIS

  Level 2 LSP log
When       Count       Interface         Triggers
03:09:27     1         subint             CONFIG NEWADJ
03:09:22     1         subint             NEWADJ
02:34:57     2         subint             DIS
02:34:50     1                                IPUP
02:34:27     1         subint             CONFIG DELADJ
02:13:57     1         subint             DELADJ
02:13:52     1         subint             NEWADJ
01:35:58     2         subint             IPIA
01:35:51     1                              AREASET IPIA
```

Related Commands

命令	说明
clear isis	清除 IS-IS 数据结构。
show clns	显示 CLNS 特定信息。
show route isis	显示 IS-IS 路由。

show isis neighbors

要显示有关 IS-IS 邻居的信息，请使用 **show isis neighbors** 命令：

show isis neighbors ［**detail**］

Syntax Description

detail	（可选）显示 IS-IS 邻居的更多详细信息。

Command History

版本	修改
6.3	引入了此命令。

使用指南

下表解释 IS-IS 邻居信息。

表 ***10: IS-IS*** 邻居信息

字段	说明
System Id	标识区域中的系统的六字节值。
Type	级别类型。指示 IS-IS 邻居是 1 级、1-2 级还是 2 级路由器。
Interface	从中获知系统的接口。
IP Address	邻居路由器的 IP 地址。
State	指示 IS-IS 邻居的状态是开启还是关闭。
Holdtime	链路状态数据包 (LSP) 保持时间。LSP 保持有效的时间（以秒为单位）。
Circuit Id	IS-IS 邻居路由器的端口位置，指示其如何连接到本地路由器。
Area Address(es)	可从路由器访问的区域地址。对于 1 级 LSP，这些是在源路由器上手动配置的区域地址。对于 2 级 LSP，这些是此路由器所属区域的所有区域地址。
SNPA	子网连接点。这是数据链路地址。
State Changed	状态更改的时间。
LAN Priority	LAN 的优先级。
Remote TID	邻居路由器拓扑 ID。
Local TID	本地路由器拓扑 ID。

示例

以下示例显示基本 IS-IS 邻居信息。

```
> show isis neighbors

System Id      Type Interface   IP Address      State Holdtime Circuit Id
routerA          L1    subint   10.22.22.5        UP    21           c2.01
routerA          L2    subint   10.22.22.5        UP    22           c2.01
c2               L1    subint   10.22.22.3        UP     9           c2.01
c2               L2    subint   10.22.22.3        UP     9           c2.01
```

以下示例显示了详细的 IS-IS 邻居信息。

```
> show isis neighbors detail

System Id      Type Interface   IP Address      State Holdtime Circuit Id
routerA          L1    subint   10.22.22.5        UP    23           c2.01
  Area Address(es): 49.0001
  SNPA:       0025.8407.f2b0
  State Changed: 00:03:03
  LAN Priority: 64
  Format: Phase V
  Remote TID: 0
  Local TID:  0
  Interface name: subint
routerA          L2    subint   10.22.22.5        UP    22         c2.01
  Area Address(es): 49.0001
  SNPA:       0025.8407.f2b0
  State Changed: 00:03:03
  LAN Priority: 64
  Format: Phase V
  Remote TID: 0
  Local TID:  0
  Interface name: subint
```

Related Commands

命令	说明
clear isis	清除 IS-IS 数据结构。
show clns	显示 CLNS 特定信息。
show route isis	显示 IS-IS 路由。

show isis rib

要显示存储在 IP 本地路由信息库 (RIB) 中的特定路由或主网络下所有路由的路径，请使用 **show isis rib** 命令。

show isis [***** | **ip** [**unicast**] | **ipv6** [**unicast**]] **rib** [**redistribution** [**level-1** | **level-2**]] [*network_ip* [*mask*]]

Syntax Description

*****	（可选）显示所有 IS-IS 地址系列。
ip	（可选）显示 IPv4 地址系列。
ipv6	（可选）显示 IPv6 地址系列。
level-1	（可选）显示 1 级重新分发 RIB。
level-2	（可选）显示第 2 级重新分发 RIB
network_ip [*mask*]	（可选）显示网络的 RIB 信息。
redistribution	（可选）显示 IS-IS IP 重新分发 RIB 信息
unicast	（可选）显示单播地址系列。

Command History

版本	修改
6.3	引入了此命令。

使用指南

使用此命令可验证 IP 全局 RIB 中存在的 IP 前缀更新是否也已在 IS-IS 本地 RIB 中更新。

示例

以下示例显示了存储在 IS-IS 本地 RIB 中的所有路由。

```
> show isis rib

IPv4 local RIB for IS-IS process

IPV4 unicast topology base (TID 0, TOPOID 0x2) = = = = = = = = = = = = = =

10.10.0.0 255.255.0.0
  [115/L2/10] via 10.22.22.5(subint), from 10.22.22.5, tag 0, LSP[12/524]


10.1.2.0 255.255.255.0
  [115/L2/10] via 10.22.22.5(subint), from 10.22.22.5, tag 0, LSP[12/524]


10.3.2.0 255.255.255.0
  [115/L2/10] via 10.22.22.5(subint), from 10.22.22.5, tag 0, LSP[13/149]
```

以下示例显示了主网络 10.0.0.0 下 IP 地址为 10.3.2.0 且存储在 IS-IS 本地 RIB 中的所有路由。

```
> show isis rib 10.3.2.0

IPv4 local RIB for IS-IS process

IPV4 unicast topology base (TID 0, TOPOID 0x2) = = = = = = = = = = = = =
Routes under majornet 10.0.0.0 255.0.0.0:

10.1.2.0 255.255.255.0
  [115/L2/10] via 10.22.22.5(subint), from 10.22.22.5, tag 0, LSP[12/524]


10.3.2.0 255.255.255.0
  [115/L2/10] via 10.22.22.5(subint), from 10.22.22.5, tag 0, LSP[13/149]
```

以下示例显示了在 IS-IS 本地 RIB 中存储的 IP 地址和掩码为 10.3.2.0 255.255.255.0 的网络下的所有路由。

```
> show isis rib 10.3.2.0 255.255.255.0

IPv4 local RIB for IS-IS process

IPV4 unicast topology base (TID 0, TOPOID 0x2) = = = = = = = = = = = = =

10.3.2.0 255.255.255.0
  [115/L2/10] via 10.22.22.5(subint), from 10.22.22.5, tag 0, LSP[13/149]
```

Related Commands

命令	说明
clear isis	清除 IS-IS 数据结构。
show clns	显示 CLNS 特定信息。
show route isis	显示 IS-IS 路由。

show isis spf-log

要显示路由器运行完整最短路径优先 (SPF) 计算的频率和原因，请使用 **show isis spf-log** 命令。

show isis ［***** | **ip** ［**unicast**］ | **ipv6** ［**unicast**］］ **spf-log**

Syntax Description

*****	（可选）显示所有 IS-IS 地址系列。
ip	（可选）显示 IPv4 地址系列。
ipv6	（可选）显示 IPv6 地址系列。
unicast	（可选）显示单播地址系列。

Command History

版本	修改
6.3	引入了此命令。

使用指南

此命令显示路由器运行完整最短路径优先 (SPF) 计算的频率和原因。下表对输出字段进行了解释。

字段	说明
When	多久前（小时：分钟：秒）进行了完整的 SPF 计算。记录最近 20 次发生的事件。
Duration	完成此SPF运行所需的毫秒数。已用时间是挂钟时间，而不是CPU时间。
Nodes	构成此 SPF 运行中计算的拓扑的路由器和伪节点 (LAN) 的数量。
Count	触发此SPF运行的事件数。当拓扑发生变化时，通常会在短时间内收到多个链路状态数据包 (LSP)。路由器在运行完整 SPF 之前会等待 5 秒，因此它可以包含所有新信息。此计数表示路由器在运行完整SPF之前等待5秒时发生的事件数（例如接收新的 LSP）。
First Trigger LSP	每当新 LSP 到达时触发完整的 SPF 计算，路由器就会存储 LSP ID。LSP ID 可以提供有关区域中路由不稳定来源的线索。如果多个 LSP 导致 SPF 运行，则仅记住最后接收的 LSP 的 LSP ID。
Triggers	触发完整 SPF 计算的所有原因的列表。有关触发器，请参阅下一个表。

下表解释了可能的触发器。

触发器	说明
ATTACHFLAG	此路由器现在已连接到第 2 级中枢，或者刚刚失去与第 2 级中枢的联系。
ADMINDIST	此路由器上为 IS-IS 流程配置了另一个管理距离。

触发器	说明
AREASET	此区域中的已获知区域地址集已更改。
BACKUPOVFL	IP 前缀消失。路由器知道有另一种方法可以到达该前缀，但尚未存储该备份路由。查找替代路由的唯一方法是通过完整的 SPF 运行。
DBCHANGED	**clear isis *** 命令在此路由器上发出。
IPBACKUP	IP 路由消失了，该路由不是通过 IS-IS 获知的，而是通过具有更好管理距离的另一个协议获知的。IS-IS 将运行完整的 SPF，为消失的 IP 前缀安装 IS-IS 路由。
IPQUERY	**clear ip route** 命令在此路由器上发出。
LSPEXPIRED	链路状态数据库 (LSDB) 中的某些 LSP 已过期。
LSPHEADER	LSP 信头中的 ATT/P/OL 位或 is-type 已更改。
NEWADJ	此路由器与另一台路由器建立了新的邻接关系。
NEWAREA	已在此路由器上配置新区域（通过网络实体标题 [NET]）。
NEWLEVEL	已在此路由器上配置新级别（通过 is-type）。
NEWLSP	拓扑中出现新的路由器或伪节点。
NEWMETRIC	在此路由器的接口上配置了新的度量。
NEWSYSID	已在此路由器上配置新的系统 ID（通过 NET）。
PERIODIC	通常，路由器每隔 15 分钟运行一次完整的 SPF 计算。
RTCLEARED	**clear clns route** 命令在此路由器上发出。
TLVCODE	TLV 代码不匹配，表示 LSP 的最新版本中包含不同的 TLV。
TLVCONTENT	TLV 内容已更改。这通常表示该区域中某处的邻接关系已建立或关闭。“第一个触发 LSP”列指示可能发生不稳定的位置。

示例

以下是 **show isis ipv6 spf-log** 命令的输出示例：

```
> show isis ipv6 spf-log

      TID 0 level 1 SPF log
  When   Duration  Nodes  Count     First trigger LSP   Triggers
00:15:46    3124     40      1          milles.00-00  TLVCODE
00:15:24    3216     41      5          milles.00-00  TLVCODE NEWLSP
00:15:19    3096     41      1          deurze.00-00  TLVCODE
00:14:54    3004     41      2          milles.00-00  ATTACHFLAG LSPHEADER
```

```
00:14:49    3384     41      1          milles.00-01  TLVCODE
00:14:23    2932     41      3          milles.00-00  TLVCODE
00:05:18    3140     41      1                        PERIODIC
00:03:54    3144     41      1          milles.01-00  TLVCODE
00:03:49    2908     41      1          milles.01-00  TLVCODE
00:03:28    3148     41      3           bakel.00-00  TLVCODE TLVCONTENT
00:03:15    3054     41      1          milles.00-00  TLVCODE
00:02:53    2958     41      1          mortel.00-00  TLVCODE
00:02:48    3632     41      2          milles.00-00  NEWADJ TLVCODE
00:02:23    2988     41      1          milles.00-01  TLVCODE
00:02:18    3016     41      1          gemert.00-00  TLVCODE
00:02:14    2932     41      1           bakel.00-00  TLVCONTENT
00:02:09    2988     41      2           bakel.00-00  TLVCONTENT
00:01:54    3228     41      1          milles.00-00  TLVCODE
00:01:38    3120     41      3            rips.03-00  TLVCONTENT
```

Related Commands

命令	说明
clear isis	清除 IS-IS 数据结构。
show clns	显示 CLNS 特定信息。
show route isis	显示 IS-IS 路由。

show isis topology

要显示所有区域中所有连接的路由器的列表，请使用 **show isis topology** 命令。

show isis ［***** | **ip** ［**unicast**］ | **ipv6** ［**unicast**］］ **topology** ［**level-1** | **level-2**］

Syntax Description

*****	（可选）显示所有 IS-IS 地址系列。
ip	（可选）显示 IPv4 地址系列。
ipv6	（可选）显示 IPv6 地址系列。
level-1	（可选）显示 1 级重新分发 RIB。
level-2	（可选）显示第 2 级重新分发 RIB
unicast	（可选）显示单播地址系列。

Command History

版本	修改
6.3	引入了此命令。

使用指南

使用 **show isis topology** 命令以验证所有区域中所有路由器的存在性及其连接性。在下表中对字段进行了说明。

字段	说明
System Id	标识区域中的系统的六字节值。
Metric	源路由器与通告邻居之间的邻接关系开销的 IS-IS 度量，或从通告路由器到通告目的地的开销度量（可以是 IP 地址、终端系统 [ES]、或 CLNS 前缀）。
Next-Hop	下一跳路由器的 IP 地址
Interface	从中获知系统的接口。
SNPA	子网连接点。这是数据链路地址。

示例

以下示例显示 **show isis topology** 命令的输出示例。

```
> show isis topology

IS-IS TID 0 paths to level-1 routers
System Id           Metric     Next-Hop            Interface   SNPA
cisco1                 --
```

```
routerA                 10       routerA                 subint  0025.8407.f2b0
c3                      10
c2                      10            c2                subint  c08c.60e6.986f

IS-IS TID 0 paths to level-2 routers
System Id            Metric     Next-Hop             Interface   SNPA
cisco1                  --
routerA                 10       routerA                 subint  0025.8407.f2b0
c3                      10
c2                      10            c2                subint  c08c.60e6.986f
```

Related Commands

命令	说明
clear isis	清除 IS-IS 数据结构。
show clns	显示 CLNS 特定信息。
show route isis	显示 IS-IS 路由。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。