



show i

- [show idb \(3 ページ\)](#)
- [show identity-subnet-filter \(5 ページ\)](#)
- [show igmp groups \(6 ページ\)](#)
- [show igmp interface \(7 ページ\)](#)
- [show igmp traffic \(8 ページ\)](#)
- [show inline-set \(9 ページ\)](#)
- [show interface \(10 ページ\)](#)
- [show interface ip brief \(23 ページ\)](#)
- [show inventory \(26 ページ\)](#)
- [show ip address \(29 ページ\)](#)
- [show ip address dhcp \(31 ページ\)](#)
- [show ip address pppoe \(35 ページ\)](#)
- [show ip audit count \(36 ページ\)](#)
- [show ip local pool \(37 ページ\)](#)
- [show ip verify statistics \(38 ページ\)](#)
- [show ipsec df-bit \(39 ページ\)](#)
- [show ipsec fragmentation \(40 ページ\)](#)
- [show ipsec policy \(41 ページ\)](#)
- [show ipsec sa \(42 ページ\)](#)
- [show ipsec sa summary \(51 ページ\)](#)
- [show ipsec stats \(52 ページ\)](#)
- [show ipv6 access-list \(58 ページ\)](#)
- [show ipv6 dhcp \(59 ページ\)](#)
- [show ipv6 dhcprelay binding \(64 ページ\)](#)
- [show ipv6 dhcprelay statistics \(65 ページ\)](#)
- [show ipv6 general-prefix \(66 ページ\)](#)
- [show ipv6 icmp \(67 ページ\)](#)
- [show ipv6 interface \(68 ページ\)](#)
- [show ipv6 local pool \(70 ページ\)](#)
- [show ipv6 mld traffic \(71 ページ\)](#)

- [show ipv6 neighbor \(73 ページ\)](#)
- [show ipv6 ospf \(76 ページ\)](#)
- [show ipv6 ospf border-routers \(77 ページ\)](#)
- [show ipv6 ospf database \(78 ページ\)](#)
- [show ipv6 ospf events \(81 ページ\)](#)
- [show ipv6 ospf flood-list \(83 ページ\)](#)
- [show ipv6 ospf graceful-restart \(85 ページ\)](#)
- [show ipv6 ospf interface \(86 ページ\)](#)
- [show ipv6 ospf request-list \(88 ページ\)](#)
- [show ipv6 ospf retransmission-list \(90 ページ\)](#)
- [show ipv6 ospf statistic \(91 ページ\)](#)
- [show ipv6 ospf summary-prefix \(92 ページ\)](#)
- [show ipv6 ospf timers \(93 ページ\)](#)
- [show ipv6 ospf traffic \(94 ページ\)](#)
- [show ipv6 ospf virtual-links \(96 ページ\)](#)
- [show ipv6 prefix-list \(97 ページ\)](#)
- [show ipv6 route \(99 ページ\)](#)
- [show ipv6 routers \(103 ページ\)](#)
- [show ipv6 traffic \(104 ページ\)](#)
- [show isakmp sa \(106 ページ\)](#)
- [show isakmp stats \(107 ページ\)](#)
- [show isis database \(109 ページ\)](#)
- [show isis hostname \(114 ページ\)](#)
- [show isis lsp-log \(115 ページ\)](#)
- [show isis neighbors \(117 ページ\)](#)
- [show isis rib \(119 ページ\)](#)
- [show isis spf-log \(121 ページ\)](#)
- [show isis topology \(124 ページ\)](#)

show idb

インターフェイスリソースを表す内部データ構造であるインターフェイス記述子ブロックのステータスに関する情報を表示するには、**show idb** コマンドを使用します。

show idb

コマンド履歴

リリース

変更内容

リリース	変更内容
6.1	このコマンドが導入されました。

例

次に、**show idb** コマンドの出力例を示します。

```
> 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-Controll1/1
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 0xdacbd20 0x0000003f Internal-Controll1/1 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
```

次の表で各フィールドについて説明します。

表 1: `show idb stats` の各フィールド

フィールド	説明
HWIDBs	すべての HWIDB の統計情報を表示します。HWIDB は、システム内の各ハードウェア ポートについて作成されます。
SWIDBs	すべての SWIDB の統計情報を表示します。SWIDB は、システム内の各メインおよびサブインターフェイスについて、およびコンテキストに割り当てられている各インターフェイスについて作成されます。 他の一部の内部ソフトウェア モジュールも IDB を作成します。
HWIDB#	ハードウェア インターフェイス エントリを示します。IDB シーケンス番号、アドレス、およびインターフェイス名が各行に表示されます。
SWIDB#	ソフトウェア インターフェイス エントリを示します。IDB シーケンス番号、アドレス、対応する vPif ID、およびインターフェイス名が各行に表示されます。
PEER IDB#	コンテキストに割り当てられているインターフェイスを示します。IDB シーケンス番号、アドレス、対応する vPif ID、コンテキスト ID、およびインターフェイス名が各行に表示されます。

関連コマンド

Command	説明
<code>show interface</code>	インターフェイスの実行時ステータスと統計情報を表示します。

show identity-subnet-filter

ユーザから IP へ、およびセキュリティグループタグ (SGT) から IP へのマッピングの受信時に除外されたサブネットを表示するには、**show identity-subnet-filter** コマンドを使用します。

show identity-subnet-filter

コマンド履歴	リリース	変更内容
	6.7	このコマンドが導入されました。

使用上のガイドライン **show identity-subnet-filter** コマンドは、ユーザから IP およびセキュリティグループタグ (SGT) から IP へのマッピングから現在除外されているすべてのサブネットを表示します。

例

次に、現在除外されているサブネットがない場合の **show identity-subnet-filter** コマンドの出力例を示します。

```
> show identity-subnet-filter

Subnet filter file doesn't exist
```

次に、一部のサブネットが現在除外されている場合の **show identity-subnet-filter** コマンドの出力例を示します。

```
> show identity-subnet-filter

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

関連コマンド	コマンド	説明
	configure identity-subnet-filter	ユーザから IP および SGT から IP のマッピングからサブネットを除外します。

show igmp groups

脅威に対する防御デバイスに直接接続されている受信者、およびIGMPを通じて学習された受信者を含むマルチキャストグループを表示するには、**show igmp groups** コマンドを使用します。

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

構文の説明	detail	(任意) ソースの詳細説明を出力します。
	group	(任意) IGMP グループのアドレス。このオプション引数を含めると、表示は指定されたグループに限定されます。
	if_name	(任意) 指定されたインターフェイスについてのグループ情報を表示します。
	reserved	(任意) 予約されたグループについての情報を表示します。
	summary	(任意) グループ加入の要約情報を表示します。

コマンド履歴	リリース	変更内容
	6.1	このコマンドが導入されました。

使用上のガイドライン オプションの引数およびキーワードをすべて省略すると、**show igmp groups** コマンドは、直接接続されたすべてのマルチキャストグループを、グループアドレス、インターフェイスタイプ、およびインターフェイス番号別に表示します。

例

次に、**show igmp groups** コマンドの出力例を示します。

```
> 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
```

関連コマンド	Command	説明
	show igmp interface	インターフェイスのマルチキャスト情報を表示します。

show igmp interface

インターフェイスのマルチキャスト情報を表示するには、**show igmp interface** コマンドを使用します。

show igmp interface [*if_name*]

構文の説明	<i>if_name</i>	(任意) 選択したインターフェイスについての IGMP グループ情報を表示します。
コマンド履歴	リリース	変更内容
	6.1	このコマンドが導入されました。
使用上のガイドライン	オプションの <i>if_name</i> 引数を省略すると、 show igmp interface コマンドはすべてのインターフェイスに関する情報を表示します。	

例

次に、**show igmp interface** コマンドの出力例を示します。

```
> 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
```

関連コマンド	Command	説明
	show igmp groups	脅威に対する防御 デバイスに直接接続されている受信者、および IGMP を通じて学習された受信者を含むマルチキャストグループを表示します。

show igmp traffic

IGMP トラフィック統計情報を表示するには、**show igmp traffic** コマンドを使用します。

show igmp traffic

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

例

次に、**show igmp traffic** コマンドの出力例を示します。

```
> 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
```

関連コマンド

Command	説明
clear igmp counters	すべての IGMP 統計カウンタをクリアします。
clear igmp traffic	IGMP トラフィック カウンタをクリアします。

show inline-set

デバイスで設定されているインラインセット（IPS 専用インターフェイス）に関する情報を表示するには、**show inline-set** コマンドを使用します。

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

構文の説明	<i>inline-set-name</i>	(任意) 指定されたインラインセットに関する情報を表示します。名前を含めない場合は、すべてのインラインセットが表示されます。
	mac-address-table	(任意) インラインセットの MAC アドレスブリッジを表示します。
コマンド履歴	リリース	変更内容
	6.1	このコマンドが導入されました。

例

次に、**show inline-set** コマンドの出力例を示します。

```
> 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

IP インターフェイスの統計情報を表示するには、**show interface** コマンドを使用します。

```
show interface [{physical_interface | redundantnumber} [.subinterface] | interface_name |
BVI id | ] [summary | stats | detail]
```

構文の説明

BVI id	(任意) 指定されたブリッジ仮想インターフェイス (BVI) の統計情報を表示します。BVI 番号 (1 ~ 250) を入力します。
detail	(任意) インターフェイスの詳細な情報を表示します。この情報には、インターフェイスが追加された順序、設定されている状態、実際の状態、非対称ルーティングの統計情報 (有効になっている場合) が含まれます。 すべてのインターフェイスを表示すると、システム通信に使用される内部インターフェイスに関する情報も表示されます。内部インターフェイスをユーザーが設定することはできません。情報はデバッグのみを目的としています。
interface_name	(任意) 論理名でインターフェイスを指定します。
physical_interface	(任意) インターフェイス ID (gigabitethernet0/1 など) を指定します。使用可能なインターフェイスは、デバイスモデルによって異なります。デバイスで使用可能な名前を表示するには、パラメータなしで show interface コマンドを使用します。
redundantnumber	(任意) 冗長インターフェイス ID (redundant1 など) を指定します。
stats	(デフォルト) インターフェイス情報および統計情報を表示します。このキーワードはデフォルトであるため、このキーワードはオプションです。
summary	(任意) いずれかのインターフェイスに関する情報を表示します。
サブインターフェイス	(任意) 論理サブインターフェイスを示す 1 ~ 4294967293 の整数を指定します。

コマンド デフォルト

いずれのオプションも識別しない場合、このコマンドは、内部インターフェイスを除くすべてのインターフェイスについての基本的な統計情報を表示します。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。
6.2	BVI キーワードが追加されました。

リリース	変更内容
6.7	データインターフェイスで Management Center アクセスを設定したときに、Internal-Data0/1 "nlp_int_tap"インターフェイスの detail キーワードに出力が追加されました。

使用上のガイドライン サブインターフェイスについて表示される統計情報の数は、物理インターフェイスについて表示される統計情報の数のサブセットです。



(注) Hardware カウントと Traffic Statistics カウントでは、送信または受信されるバイト数が異なります。

Hardware カウントでは、この量はハードウェアから直接取得され、レイヤ2パケットのサイズが反映されます。一方、Traffic Statistics では、レイヤ3パケットのサイズが反映されます。

カウントの差はインターフェイス カードハードウェアの設計に基づいて異なります。

たとえば、ファストイーサネットカードの場合、レイヤ2カウントはイーサネットヘッダーを含むため、トラフィックカウントよりも14バイト大きくなります。ギガビットイーサネットカードの場合、レイヤ2カウントはイーサネットヘッダーとCRCの両方を含むため、トラフィックカウントよりも18バイト大きくなります。

出力の説明については、「例」を参照してください。

例

次に、**show interface** コマンドの出力例を示します。

```
> 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

```

次の表は、各フィールドの説明を示しています。

表 2: *show interface* の各フィールド

フィールド	説明
インターフェイス ID	インターフェイス ID。

フィールド	説明
<code>"interface_name"</code>	論理インターフェイス名。名前を設定しない場合、Hardware 行の下に次のメッセージが表示されます。 Available but not configured via nameif
is state	管理ステータスは次のとおりです。 <ul style="list-style-type: none"> • up : インターフェイスはシャットダウンされません。 • administratively down : インターフェイスは意図的にシャットダウンされています。
Line protocol is state	回線ステータスは次のとおりです。 <ul style="list-style-type: none"> • up : 動作するケーブルがネットワーク インターフェイスに接続されています。 • down : ケーブルが正しくないか、インターフェイス コネクタに接続されていません。
VLAN 識別子	サブインターフェイスの場合、VLAN ID。
ハードウェア	インターフェイスのタイプ、最大帯域幅、遅延、デュプレックス方式、および速度。リンクがダウンしている場合は、デュプレックス方式と速度は設定値が表示されます。リンクが動作している場合、これらのフィールドには実際の設定がカッコで囲まれて設定値とともに表示されます。
Media-type	(常に表示されるわけではない) RJ-45 や SFP などのインターフェイス メディア タイプを表示します。
message area	一部の状況で、メッセージが表示される場合もあります。次の例を参照してください。 <ul style="list-style-type: none"> • 名前を設定しないと、次のメッセージが表示されます。「Available but not configured via nameif」 • インターフェイスが冗長インターフェイスのメンバの場合、次のメッセージが表示されます。「Active member of Redundant5」
MAC address	インターフェイスの MAC アドレス。
Site Specific MAC address	クラスタリングの場合に、使用中のサイト固有の MAC アドレスを表示します。
MTU	このインターフェイス上で許可されるパケットの最大サイズ (バイト単位)。インターフェイス名を設定しない場合、このフィールドには「MTU not set」と表示されます。

フィールド	説明
IP address	静的なインターフェイス IP アドレスか、DHCP サーバーから受信したインターフェイス IP アドレス。
サブネット マスク	IP アドレスのサブネット マスク。
Packets input	このインターフェイスで受信したパケットの数。
Bytes	このインターフェイスで受信したバイト数。
No buffer	ブロック割り当てからの失敗の数。
Received:	
Broadcasts	受信したブロードキャストの数。
Input errors	次に示すタイプを含めた入力エラーの総数。入力に関する他のエラーも入力エラーのカウントが増加する原因になります。また、一部のデータグラムは複数のエラーを含んでいることもあります。したがって、この合計数は、次に示すタイプについて表示されるエラーの数を超えることがあります。
Runts	最小のパケット サイズ (64 バイト) よりも小さいために廃棄されたパケットの数。ラントは通常、コリジョンによって発生します。不適切な配線や電気干渉によって発生することもあります。
Giants	最大パケット サイズを超えたため廃棄されるパケットの数。たとえば、1518 バイトよりも大きいイーサネット パケットはジャイアントと見なされます。
CRC	巡回冗長検査エラーの数。ステーションがフレームを送信すると、フレームの末尾に CRC を付加します。この CRC は、フレーム内のデータに基づくアルゴリズムから生成されます。送信元と宛先の間でフレームが変更された場合、システムは CRC が一致しないことを通知します。CRC の数値が高いことは、通常、コリジョンの結果であるか、ステーションが不良データを送信することが原因です。
Frame	フレーム エラーの数。不良フレームには、長さが正しくないパケットや、フレーム チェックサムが正しくないパケットがあります。このエラーは通常、コリジョンまたはイーサネット デバイスの誤動作が原因です。
Overrun	インターフェイスのデータ処理能力を入力レートを超えたため、ハードウェアバッファに受信したデータをインターフェイスが処理できなかった回数。
Ignored	このフィールドは使用されません。値は常に 0 です。

フィールド	説明
中断	このフィールドは使用されません。値は常に 0 です。
L2 decode drops	名前がまだ設定されていないか、無効な VLAN ID を持つフレームが受信されたためにドロップされたパケットの数。冗長インターフェイス構成のスタンバイインターフェイスでは、このインターフェイスに名前が設定されていないため、数が増加する可能性があります。
Packets output	このインターフェイスに送信されたパケットの数。
Bytes	このインターフェイスに送信されたバイトの数。
Underruns	インターフェイスが処理できる速度よりも速くトランスミッタが動作した回数。
Output Errors	設定されたコリジョンの最大数を越えたため送信されなかったフレームの数。このカウンタは、ネットワークトラフィックが多い場合にのみ増加します。
Collisions	イーサネットコリジョン（単一および複数のコリジョン）が原因で再送信されたメッセージの数。これは通常、過渡に延長した LAN で発生します（イーサネットケーブルまたはトランシーバケーブルが長すぎる、ステーション間のリピータが2つよりも多い、またはマルチポートトランシーバのカスケードが多すぎる場合）。衝突するパケットは、出力パケットによって1回だけカウントされます。
Interface resets	インターフェイスがリセットされた回数。インターフェイスで3秒間送信できなかった場合、システムはインターフェイスをリセットして送信を再開します。この間隔では、接続状態が維持されます。インターフェイスのリセットは、インターフェイスがループバックまたはシャットダウンする場合も発生します。
Babbles	未使用。（「バブル」は、トランスミッタが最長フレームの送信に要した時間よりも長くインターフェイスに留まっていたことを意味します）。

フィールド	説明
Late collisions	<p>通常のコリジョン ウィンドウの外側でコリジョンが発生したため、送信されなかったフレームの数。レイト コリジョンは、パケットの送信中に遅れて検出されるコリジョンです。これは通常発生しません。2つのイーサネットホストが同時に通信しようとした場合、早期にパケットが衝突して両者がバックオフするか、2番めのホストが1番めのホストの通信状態を確認して待機します。</p> <p>レイトコリジョンが発生すると、デバイスは割り込みを行ってイーサネット上にパケットを送信しようとしませんが、脅威に対する防御 デバイスはパケットの送信を部分的に完了しています。脅威に対する防御 デバイスは、パケットの最初の部分を保持するバッファを解放した可能性があるため、パケットを再送しません。このことはあまり問題になりません。その理由は、ネットワークングプロトコルはパケットを再送することでコリジョンを処理する設計になっているためです。ただし、レイト コリジョンはネットワークに問題が存在することを示しています。一般的な問題は、リピータで接続された大規模ネットワーク、および仕様の範囲を超えて動作しているイーサネットネットワークです。</p>
Deferred	リンク上のアクティビティが原因で送信前に保留されたフレームの数。
input reset drops	リセットが発生したときにRXリングでドロップしたパケットの数をカウントします。
output reset drops	リセットが発生したときにTXリングでドロップしたパケットの数をカウントします。
Rate limit drops	ギガビット以外の速度でインターフェイスを設定して、設定に応じて10 Mbps または 100 Mbps を超えて送信しようとした場合にドロップされたパケットの数。
Lost carrier	送信中に搬送波信号が消失した回数。
No carrier	未使用。
Input queue (curr/max packets):	入力キュー内のパケットの数（現行値と最大値）。
ハードウェア	ハードウェア キュー内のパケットの数。
Software	ソフトウェア キュー内のパケットの数。ギガビット イーサネット インターフェイスでは使用できません。
Output queue (curr/max packets):	出力キュー内のパケットの数（現行値と最大値）。

フィールド	説明
ハードウェア	ハードウェア キュー内のパケットの数。
Software	ソフトウェア キュー内のパケットの数。
input queue (blocks free curr/low)	curr/low エントリは、インターフェイスの受信（入力）記述子リング上の現在のスロットおよび使用可能な all-time-lowest スロットの番号を示します。これらは、メイン CPU によって更新されるため、all-time-lowest（インターフェイス統計情報が削除されるか、またはデバイスがリロードされるまで）の水準点はあまり正確ではありません。
output queue (blocks free curr/low)	curr/low エントリは、インターフェイスの送信（出力）記述子リング上の現在のスロットおよび使用可能な all-time-lowest スロットの番号を示します。これらは、メイン CPU によって更新されるため、all-time-lowest（インターフェイス統計情報が削除されるか、またはデバイスがリロードされるまで）の水準点はあまり正確ではありません。
Traffic Statistics:	受信、送信、またはドロップしたパケットの数。
Packets input	受信したパケットの数とバイトの数。
Packets output	送信したパケットの数とバイトの数。
Packets dropped	ドロップしたパケットの数。このカウンタは通常、高速セキュリティパス（ASP）上でドロップしたパケットについて増分します（たとえば、アクセスリスト拒否が原因でパケットをドロップした場合など）。 インターフェイス上でドロップが発生する原因については、 show asp drop コマンドを参照してください。
1 minute input rate	過去1分間に受信したパケットの数（パケット/秒およびバイト/秒）。
1 minute output rate	過去1分間に送信したパケットの数（パケット/秒およびバイト/秒）。
1 minute drop rate	過去1分間にドロップしたパケットの数（パケット/秒）。
5 minute input rate	過去5分間に受信したパケットの数（パケット/秒およびバイト/秒）。
5 minute output rate	過去5分間に送信したパケットの数（パケット/秒およびバイト/秒）。
5 minute drop rate	過去5分間にドロップしたパケットの数（パケット/秒）。

フィールド	説明
Redundancy Information:	冗長インターフェイスについて、メンバー物理インターフェイスを示します。アクティブインターフェイスの場合はインターフェイス ID の後に「(Active)」と表示されます。 メンバーをまだ割り当てていない場合、次の出力が表示されます。 Members unassigned
Last switchover	冗長インターフェイスの場合、アクティブインターフェイスがスタンバイインターフェイスにフェールオーバーした時刻を表示します。



(注) **show interface detail** コマンドの結果に示されている入力レートと出力レートが、Management Center ユーザーインターフェイスのインターフェイスモジュールに表示される入出力のトラフィックレートとは異なる場合があります。

このインターフェイスモジュールは、Snort パフォーマンスモニタリングからの値に従ってトラフィックレートを表示します。Snort パフォーマンスモニタリングとインターフェイス統計のサンプリング間隔は異なります。このサンプリング間隔の違いにより、Management Center ユーザーインターフェイスと **show interface detail** コマンドの結果のスループット値が異なります。

次に、**show interface detail** コマンドの出力例を示します。次に、すべてのインターフェイス（プラットフォームに存在する場合は内部インターフェイスを含む）についての詳細なインターフェイス統計情報および非対称ルーティング統計情報（有効にされている場合）を表示する例を示します。

```
> 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
  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
[...]
```

次の表で、**show interface detail** コマンドによって表示される追加フィールドについて説明します。

表 3: *show interface detail* の各フィールド

フィールド	説明
Demux drops	(内部データインターフェイスのみ) 他のインターフェイスからのパケットを脅威に対する防御デバイスで逆多重化できなかったためロップしたパケットの数。

フィールド	説明
Control Point Interface States:	
Interface number	デバッグに使用される0から始まる番号で、このインターフェイスが作成された順番を示します。
Interface config status	管理ステータスは次のとおりです。 <ul style="list-style-type: none"> • active : インターフェイスはシャットダウンされていません。 • not active : インターフェイスは意図的にシャットダウンされています。
インターフェイスの状態	インターフェイスの実際の状態。この状態は通常、上記の config status と一致します。高可用性を設定した場合、脅威に対する防御 デバイスは必要に応じてインターフェイスを動作状態またはダウン状態にするため、不一致が生じる可能性があります。
Asymmetrical Routing Statistics:	
Received X1 packets	このインターフェイスで受信した ASR パケットの数。
Transmitted X2 packets	このインターフェイスで送信した ASR パケットの数。
Dropped X3 packets	このインターフェイスでドロップした ASR パケットの数。パケットは、パケットを転送しようとしたときにインターフェイスがダウン状態の場合にドロップされることがあります。

関連コマンド

Command	説明
clear interface	show interface コマンドのカウンタをクリアします。
show interface ip brief	インターフェイスの IP アドレスとステータスを表示します。

show interface ip brief

インターフェイスの IP アドレスとステータスを表示するには、**show interface ip brief** コマンドを使用します。

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

構文の説明

BVI id	(任意) 指定されたブリッジ仮想インターフェイス (BVI) の統計情報を表示します。BVI 番号 (1 ~ 250) を入力します。
<i>interface_name</i>	(任意) インターフェイス名を指定します。
<i>physical_interface</i>	(任意) インターフェイス ID (gigabitethernet0/1 など) を指定します。
サブインターフェイス	(任意) 論理サブインターフェイスを示す 1 ~ 4294967293 の整数を指定します。

コマンドデフォルト

インターフェイスを指定しない場合、内部インターフェイスを含むすべてのインターフェイスが表示されます。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。
6.2	BVI キーワードが追加されました。

例

次に、**show ip brief** コマンドの出力例を示します。

```
> 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
```

次の例は、ほとんどのインターフェイスが **BVI** の一部である場合のアドレスを表示しています。メンバーインターフェイスには、親 **BVI** と同じアドレスが設定されています。

```
> 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-Controll1/1    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

```

次の表では、出力フィールドについて説明されています。

表 4: *show interface ip brief* の各フィールド

フィールド	説明
インターフェイス (Interface)	インターフェイス ID。 すべてのインターフェイスを表示すると、システム通信に使用される内部インターフェイスに関する情報も表示されます。内部インターフェイスをユーザーが設定することはできません。情報はデバッグのみを目的としています。
IP-Address	インターフェイスの IP アドレス。
OK?	この列は使用されておらず、常に「Yes」と表示されます。
Method	インターフェイスが IP アドレスを受信した方法。値は次のとおりです。 <ul style="list-style-type: none"> • unset : IP アドレスは設定されていません。 • manual : インターフェイスには静的アドレスが設定されています。 • CONFIG : スタートアップコンフィギュレーションからロードしました。 • DHCP : DHCP サーバーから受信しました。
Status	管理ステータスは次のとおりです。 <ul style="list-style-type: none"> • up : インターフェイスはシャットダウンされません。 • down : インターフェイスは起動しておらず、意図的にシャットダウンもされていません。 • administratively down : インターフェイスは意図的にシャットダウンされています。

フィールド	説明
Protocol	回線ステータスは次のとおりです。 <ul style="list-style-type: none">• up : 動作するケーブルがネットワーク インターフェイスに接続されています。• down : ケーブルが正しくないか、インターフェイス コネクタに接続されていません。

関連コマンド

Command	説明
show interface	インターフェイスの実行時ステータスと統計情報を表示します。

show inventory

製品 ID (PID)、バージョン ID (VID)、およびシリアル番号 (SN) が割り当てられているネットワークデバイスにインストールされているすべてのシスコ製品に関する情報を表示するには、**show inventory** コマンドを使用します。

show inventory [*slot_id*]

構文の説明	<i>slot_id</i>	(オプション) モジュール ID またはスロット番号 (0~3) を指定します。
コマンド デフォルト	項目のインベントリを表示するスロットを指定しない場合は、すべてのモジュール (電源モジュールを含む) のインベントリ情報が表示されます。	
コマンド履歴	リリース	変更内容
	6.1	このコマンドが導入されました。

使用上のガイドライン

show inventory コマンドは、各シスコ製品に関するインベントリ情報を UDI 形式で取得および表示します。UDI 形式とは、製品 ID (PID)、バージョン ID (VID)、およびシリアル番号 (SN) という 3 つの異なるデータ要素の組み合わせです。

PID は製品を発注するための名前です。従来は「製品名」または「部品番号」と呼ばれていました。これは、正しい交換部品を発注するために使用する ID です。

VID は製品のバージョンです。製品が変更されると、VID は、製品の変更通知を管理する業界ガイドラインである Telcordia GR-209-CORE から定めた厳格なプロセスに従って増分されます。

SN はベンダー固有の製品の通し番号です。それぞれの製品には工場ですべての独自のシリアル番号があり、現場では変更できません。シリアル番号は、製品の個々の固有のインスタンスを識別するための手段です。シリアル番号は、デバイスのさまざまなコンポーネントに応じてその長さが異なる場合があります。

UDI では各製品をエンティティと呼びます。シャーシなどの一部のエンティティには、スロットのようなサブエンティティがあります。各エンティティは、シスコエンティティごとに階層的に配置された論理的な表示順で別々の行に表示されます。

オプションを指定せずに **show inventory** コマンドを使用すると、ネットワークデバイスに取り付けられており、PID が割り当てられているシスコエンティティのリストが表示されます。

シスコエンティティに PID が割り当てられていない場合、そのエンティティは取得または表示されません。

ASA 5500-X シリーズのハードウェア上の制限により、シリアル番号が表示されない場合があります。これらのモデルの PCI-E I/O (NIC) オプションカードの UDI 表示では、カードタイ

プは2つのみですが、出力はシャーシタイプに応じて6通りになります。これは、指定されたシャーシに応じて異なる PCI-E ブラケット アセンブリが使用されるためです。次に、各 PCI-E I/O カード アセンブリについて予想される出力を示します。たとえば、Silicom SFP NIC カードが検出された場合、UDI 表示はこのカードが取り付けられているデバイスによって決定されます。VID および S/N の値は N/A です。これは、これらの値が電子的に格納されていないためです。

ASA 5512-X または 5515-X 内の 6 ポート SFP イーサネット NIC カードの場合：

```
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
```

ASA 5525-X 内の 6 ポート SFP イーサネット NIC カードの場合：

```
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
```

ASA 5545-X または 5555-X 内の 6 ポート SFP イーサネット NIC カードの場合：

```
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
```

ASA 5512-X または 5515-X 内の 6 ポート銅線イーサネット NIC カードの場合：

```
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
```

ASA 5525-X 内の 6 ポート銅線イーサネット NIC カードの場合：

```
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
```

ASA 5545-X または 5555-X 内の 6 ポート銅線イーサネット NIC カードの場合：

```
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
```

例

次に、キーワードや引数を指定していない **show inventory** コマンドの出力例を示します。この出力例には、それぞれに PID が割り当てられている脅威に対する防御デバイスに取り付けられているシスコ エンティティのリストが表示されます。

```
> 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

次の表で、この出力で表示されるフィールドについて説明します。

表 5: *show inventory* のフィールドの説明

フィールド	説明
名前	シスコ エンティティに割り当てられた物理名 (テキスト ストリング)。たとえば、コンソール、SSP、または「1」などの簡易コンポーネント番号 (ポートまたはモジュールの番号) など、デバイスの物理コンポーネント命名構文に応じて異なります。RFC 2737 の entPhysicalName MIB 変数に相当します。
DESCR	オブジェクトを特徴付けるシスコ エンティティの物理的な説明。RFC 2737 の entPhysicalDesc MIB 変数に相当します。
PID	エンティティ製品 ID。RFC 2737 の entPhysicalModelName MIB 変数に相当します。
VID	エンティティのバージョン番号。RFC 2737 の entPhysicalHardwareRev MIB 変数に相当します。
SN	エンティティのシリアル番号。RFC 2737 の entPhysicalSerialNum MIB 変数に相当します。

show ip address

インターフェイス IP アドレス（トランスペアレントモードの場合は管理 IP アドレス）を表示するには、**show ip address** コマンドを使用します。

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

構文の説明

<i>interface_name</i>	(任意) インターフェイス名を指定します。
<i>physical_interface</i>	(任意) gigabitethernet0/1 などのインターフェイス ID を指定します。
サブインターフェイス	(任意) 論理サブインターフェイスを示す 1 ~ 4294967293 の整数を指定します。

コマンド デフォルト

インターフェイスを指定しない場合、出力にはすべてのインターフェイス IP アドレスが表示されます。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、ハイ アベイラビリティを設定するときのためのプライマリ IP アドレス（表示では「System」と記載される）と現在の IP アドレスを表示します。ユニットがアクティブの場合、システム IP アドレスと現在の IP アドレスは一致します。ユニットがスタンバイの場合、現在の IP アドレスにはスタンバイ アドレスが表示されます。

IP アドレスはデータインターフェイス専用です。このコマンドは、診断インターフェイス上の管理インターフェイスのシステムの IP アドレスは表示しません（トランスペアレントモードの管理インターフェイスとは異なります）。情報には、診断インターフェイスの IP アドレス情報（設定されている場合）が含まれます。管理インターフェイスに関する情報を表示するには、**show network** コマンドを使用します。

例

次に、**show ip address** コマンドの出力例を示します。

```
> 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
```

次の表で各フィールドについて説明します。

表 6: *show ip address* の各フィールド

フィールド	説明
インターフェイス (Interface)	インターフェイス ID。
名前	インターフェイス名。
IP address	インターフェイスの IP アドレス。
サブネットマスク	IP アドレスのサブネット マスク。
Method	インターフェイスが IP アドレスを受信した方法。値は次のとおりです。 <ul style="list-style-type: none"> • unset : IP アドレスは設定されていません。 • manual : インターフェイスには静的アドレスが設定されています。 • CONFIG : スタートアップ コンフィギュレーションからロードしました。 • DHCP : DHCP サーバーから受信しました。

関連コマンド

Command	説明
show interface	インターフェイスの実行時ステータスと統計情報を表示します。
show interface ip brief	インターフェイスの IP アドレスとステータスを表示します。

show ip address dhcp

インターフェイスに対する DHCP リースまたはサーバーに関する詳細情報を表示するには、**show ip address dhcp** コマンドを使用します。

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

構文の説明

<i>interface_name</i>	インターフェイス名を指定します。
lease	DHCP リースに関する情報を表示します。
<i>physical_interface</i>	インターフェイス ID (gigabitethernet0/1 など) を指定します。
proxy	IPL テーブル内のプロキシ エントリを表示します。
server	IPL テーブル内のサーバー エントリを表示します。
サブインターフェイス	論理サブインターフェイスを示す 1 ~ 4294967293 の整数を指定します。
summary	エントリの要約を表示します。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

例

次に、**show ip address dhcp lease** コマンドの出力例を示します。

```
> 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
```

次の表で各フィールドについて説明します。

表 7: show ip address dhcp lease の各フィールド

フィールド	説明
Temp IP Addr	インターフェイスに割り当てられている IP アドレス。
Temp sub net mask	インターフェイスに割り当てられているサブネットマスク。
DHCP Lease server	DHCP サーバー アドレス。
state	<p>DHCP リースの状態で、次のとおりです。</p> <ul style="list-style-type: none"> • [Initial] : 初期化状態で、デバイスがリースを取得するプロセスを開始します。この状態は、リースが終了したか、リースのネゴシエーションに失敗したときにも表示されます。 • [Selecting] : デバイスは 1 つ以上の DHCP サーバーから DHCPOFFER メッセージを受信するために待機しているため、メッセージを選択できます。 • [Requesting] : デバイスは、要求を送信した送信先サーバーからの応答を待機しています。 • [Purging] : クライアントが IP アドレスを解放したか、他のエラーが発生したため、デバイスはリースを削除しています。 • [Bound] : デバイスは有効なリースを保持し、正常に動作しています。 • [Renewing] : デバイスはリースを更新しようとしています。DHCPREQUEST メッセージを現在の DHCP サーバーに定期的に送信し、応答を待機します。 • [Rebinding] : デバイスは元のサーバーのリースの更新に失敗したため、いずれかのサーバーから応答を受け取るか、リースが終了するまで DHCPREQUEST メッセージを送信します。 • [Holddown] : デバイスはリースを削除するプロセスを開始しました。 • [Releasing] : デバイスは IP アドレスが不要になったことを示すリリースメッセージをサーバーに送信します。
DHCP transaction id	クライアントによって選択され、要求メッセージを関連付けるためにクライアントとサーバーによって使用される乱数。
Lease	DHCP サーバーによって指定される、インターフェイスがこの IP アドレスを使用できる時間の長さ。
Renewal	インターフェイスがこのリースを自動的に更新しようとするまでの時間の長さ。

フィールド	説明
Rebind	脅威に対する防御 デバイスが DHCP サーバーに再バインドしようとするまでの時間の長さ。再バインドが発生するのは、デバイスが元の DHCP サーバーと通信できず、リース期間の 87.5% を経過した場合です。デバイスは、DHCP 要求をブロードキャストすることで、使用可能な任意の DHCP サーバーに接続を試みます。
Temp default-gateway addr	DHCP サーバーによって指定されるデフォルト ゲートウェイ アドレス。
Temp ip static route0	デフォルト スタティック ルート。
Next timer fires after	内部タイマーがトリガーするまでの秒数。
リトライ回数	脅威に対する防御 デバイスがリースを確立しようとしているとき、このフィールドは、そのデバイスが DHCP メッセージの送信を試行した回数を示します。たとえば、デバイスが Selecting 状態の場合、この値はデバイスが探索メッセージを送信した回数を示します。デバイスが Requesting 状態の場合、この値はデバイスが要求メッセージを送信した回数を示します。
Client-ID	サーバーとのすべての通信に使用したクライアント ID。
Proxy	このインターフェイスが VPN クライアント用のプロキシ DHCP クライアントかどうかを True または False で指定します。
Proxy Network	要求されたネットワーク。
Hostname	クライアントのホスト名。

次に、**show ip address dhcp server** コマンドの出力例を示します。

```
> 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
```

次の表で各フィールドについて説明します。

表 8: show ip address dhcp server の各フィールド

フィールド	説明
DHCP サーバー	このインターフェイスがリースを取得した DHCP サーバー アドレス。最上位エントリ（「ANY」）はデフォルト サーバーで常に存在します。
Leases	サーバーから取得したリースの数。インターフェイスの場合、リースの数は一般的に 1 です。VPN 用のプロキシを実行中のインターフェイスに対してサーバーがアドレスを提供している場合、リースは複数となります。
Offers	サーバーからのオファーの数。
Requests	サーバーに送信された要求の数。
Acks	サーバーから受信した確認応答の数。
Naks	サーバーから受信した否定応答の数。
Declines	サーバーから受信した拒否の数。
リリース	サーバーに送信されたリリースの数。
Bad	サーバーから受信した不良パケットの数。
DNS0	DHCP サーバーから取得したプライマリ DNS サーバー アドレス。
DNS1	DHCP サーバーから取得したセカンダリ DNS サーバー アドレス。
WINS0	DHCP サーバーから取得したプライマリ WINS サーバー アドレス。
WINS1	DHCP サーバーから取得したセカンダリ WINS サーバー アドレス。
Subnet	DHCP サーバーから取得したサブネットアドレス。
DNS ドメイン	DHCP サーバーから取得したドメイン。

関連コマンド

Command	説明
show interface ip brief	インターフェイスの IP アドレスとステータスを表示します。
show ip address	インターフェイスの IP アドレスを表示します。

show ip address pppoe

PPPoE 接続に関する詳細情報を表示するには、**show ip address pppoe** コマンドを使用します。

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

構文の説明	<i>interface_name</i>	インターフェイス名を指定します。
	<i>physical_interface</i>	インターフェイス ID (gigabitethernet0/1 など) を指定します。
	サブインターフェイス	論理サブインターフェイスを示す 1 ~ 4294967293 の整数を指定します。
コマンド履歴	リリース	変更内容
	6.1	このコマンドが導入されました。
関連コマンド	Command	説明
	show interface ip brief	インターフェイスの IP アドレスとステータスを表示します。
	show ip address	インターフェイスの IP アドレスを表示します。

show ip audit count

監査ポリシーをインターフェイスに適用するときシグニチャの一致数を表示するには、**show ip audit count** コマンドを使用します。

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

構文の説明

global (デフォルト) すべてのインターフェイスについて的一致数を表示します。

interface *interface_name* (任意) 指定したインターフェイスについて的一致数を表示します。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

使用上のガイドライン

監査ポリシーは通常は設定しませんが、FlexConfig を使用して設定すると、関連する統計情報を表示できます。

関連コマンド

Command	説明
clear ip audit count	IP 監査の統計情報をクリアします。
show running-config ip audit name	ip audit name コマンドの設定を表示します。 name に加えて、 interface と signature の設定を確認できます。

show ip local pool

IPv4 アドレスプール情報を表示するには、**show ip local pool** コマンドを使用します。

show ip local pool *pool_name*

構文の説明	<i>pool_name</i>	IPv6 アドレスプールの名前。
コマンド履歴	リリース	変更内容
	6.1	このコマンドが導入されました。
使用上のガイドライン	このコマンドを使用して、IPv4 アドレスプールの内容を表示します。これらのプールは、リモートアクセス VPN およびクラスタリングで使用されます。 show ipv6 local pool を使用して、IPv6 アドレスプールを表示します。	

例

次に、**show ip local pool** コマンドの出力例を示します。

```
> 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

ユニキャストリバースパスフォワードイング（RPF）機能のためにドロップされたパケットの数を表示するには、**show ip verify statistics** コマンドを使用します。

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

構文の説明

interface *interface_name* （任意）指定したインターフェイスの統計情報を表示します。

コマンドデフォルト

このコマンドは、すべてのインターフェイスの統計情報を表示します。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

使用上のガイドライン

ip verify reverse-path 機能は通常は設定しませんが、FlexConfig を使用して設定すると、関連する統計情報を表示できます。

例

次に、**show ip verify statistics** コマンドの出力例を示します。

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

関連コマンド

Command	説明
clear ip verify statistics	ユニキャスト RPF の統計情報をクリアします。
show running-config ip verify reverse-path	ip verify reverse-path の設定を表示します。

show ipsec df-bit

指定されたインターフェイスの IPsec パケットの IPsec do-not-fragment (DF ビット) ポリシーを表示するには、**show ipsec df-bit** コマンドを使用します。同じ意味を持つ **show crypto ipsec df-bit** コマンドも使用できます。

show ipsec df-bit *interface*

構文の説明

interface インターフェイス名を指定します。

コマンド履歴

リリース 変更内容

6.1 このコマンドが導入されました。

使用上のガイドライン

df ビットの設定によって、カプセル化されたヘッダーの do-not-fragment (DF) ビットのシステムによる処理方法が決まります。IP ヘッダー内の DF ビットにより、デバイスがパケットをフラグメント化できるかどうかが決まります。この設定に基づき、システムは暗号の適用時に外側の IPsec ヘッダーに対するクリアテキストパケットの DF ビットの設定をクリアするか、設定するか、コピーするかのいずれかを実行します。

例

次に、inside というインターフェイスの IPsec DF ビット ポリシーを表示する例を示します。

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

関連コマンド

Command	説明
show ipsec fragmentation	IPsec パケットのフラグメンテーション ポリシーを表示します。

show ipsec fragmentation

IPsec パケットのフラグメンテーションポリシーを表示するには、**show ipsec fragmentation** コマンドを使用します。同じ意味を持つ **show crypto ipsec fragmentation** コマンドも使用できます。

show ipsec fragmentation *interface*

構文の説明

interface インターフェイス名を指定します。

コマンド履歴

リリース 変更内容

6.1 このコマンドが導入されました。

使用上のガイドライン

VPN に対するパケットを暗号化する際、システムはパケット長をアウトバウンドインターフェイスの MTU と比較します。パケットの暗号化が MTU を超える場合は、パケットをフラグメント化する必要があります。このコマンドは、パケットを暗号化した後（**after-encryption**）、または暗号化する前（**before-encryption**）にシステムがパケットをフラグメント化するかどうかを表示します。暗号化前のパケットのフラグメント化は、事前フラグメント化とも呼ばれ、暗号化パフォーマンス全体を向上させるため、システムのデフォルト動作になっています。

例

次に、**inside** というインターフェイスの IPsec フラグメンテーションポリシーを表示する例を示します。

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

関連コマンド

Command	説明
show ipsec df-bit	指定したインターフェイスの DF ビット ポリシーを表示します。

show ipsec policy

OSPFv3 に設定されている IPsec セキュアソケット API (SS API) セキュリティポリシーを表示するには、**show ipsec policy** コマンドを使用します。このコマンドの代替形式である **show crypto ipsec policy** を使用することもできます。

show ipsec policy

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

例

次に、OSPFv3 認証と暗号方式ポリシーを表示する例を示します。

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

Policy name:      OSPFv3-1-256
Policy refcount:  1
Policy flags:     0x00000000
SA handles:       sess 268382208 (0xffff3000) / in 55017 (0xd6e9) / out 90369 (0x16101)
Inbound ESP SPI: 256 (0x100)
Outbound ESP SPI: 256 (0x100)
Inbound ESP Auth Key: 1234567890123456789012345678901234567890
Outbound ESP Auth Key: 1234567890123456789012345678901234567890
Inbound ESP Cipher Key: 12345678901234567890123456789012
Outbound ESP Cipher Key: 12345678901234567890123456789012
Transform set:    esp-aes esp-sha-hmac
```

関連コマンド

Command	説明
show crypto sockets	セキュアなソケット情報を表示します。
show ipv6 ospf interface	OSPFv3 インターフェイスに関する情報を表示します。

show ipsec sa

IPSec セキュリティアソシエーション (SA) のリストを表示するには、**show ipsec sa** コマンドを使用します。このコマンドの代替形式である **show crypto ipsec sa** を使用することもできます。

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

構文の説明

assigned-address <i>hostname_or_IP_address</i>	(オプション) 指定されたホスト名または IP アドレスの IPsec SA を表示します。
detail	(任意) 表示されているものに対する詳細なエラー情報を表示します。
entry	(オプション) IPsec SA をピアアドレスの順に表示します。
identity	(オプション) IPsec SA を ID の順に表示します。ESP は含まれません。これは簡略化された形式です。
inactive	(オプション) トラフィックを渡すことができない IPsec SA を表示します。
map <i>map-name</i>	(オプション) 指定されたクリプトマップの IPsec SA を表示します。
peer <i>peer-addr</i>	(オプション) 指定されたピア IP アドレスの IPsec SA を表示します。
spi <i>spi-num</i>	(オプション) SPI の IPsec SA を表示します。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

例

次に、IPsec SA を表示する例を示します。この表示には、割り当てられた IPv6 アドレス、およびトランスポートモードと GRE カプセル化が含まれます。

```
> 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

```

次に、IPsec SA を表示する例を示します。この表示には使用中の設定が含まれ、トンネルが OSPFv3 として示されます。

```

> 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) IPsec SA ポリシーに、フラグメンテーションは IPsec 処理の前に発生すると明記されている場合、フラグメンテーション統計情報は、フラグメンテーション前の統計情報です。SA ポリシーに、フラグメンテーションは IPsec 処理の後に発生すると明記されている場合、フラグメンテーション後の統計情報が表示されます。

次に、グローバル コンフィギュレーション モードで、def という名前のクリプトマップの IPsec SA を表示する例を示します。

```

> 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

```

次に、キーワード **entry** に関する IPsec SA の例を示します。

```

> 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

```

次に、キーワード **entry detail** を使用した IPsec SA の例を示します。

```

> 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
>

```

次に、キーワード **identity** を使用した IPsec SA の例を示します。

```

> 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

```

次に、キーワード **identity** および **detail** を使用した IPsec SA の例を示します。


```

> 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

```

次の例では、IPv6で割り当てられたアドレスに基づいてIPSec SAを表示しています。

```

> 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

```

関連コマンド

Command	説明
clear isakmp sa	IKE ランタイム SA データベースをクリアします。
show running-config isakmp	アクティブな ISAKMP コンフィギュレーションをすべて表示します。

show ipsec sa summary

IPsec SA の要約を表示するには、**show ipsec sa summary** コマンドを使用します。

show ipsec sa summary

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

例

次に、次の接続タイプ別に IPsec SA の要約を表示する例を示します。

- IPsec
- IPsec over UDP
- IPsec over NAT-T
- IPsec over TCP
- IPsec VPN ロード バランシング

```
> 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
```

関連コマンド

Command	説明
clear ipsec sa	IPsec SA を完全に削除するか、特定のパラメータに基づいて削除します。
show ipsec sa	IPsec SA のリストを表示します。
show ipsec stats	IPsec 統計情報のリストを表示します。

show ipsec stats

IPSec 統計情報のリストを表示するには、**show ipsec stats** コマンドを使用します。

show ipsec stats

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

使用上のガイドライン

次に、出力エントリが示す内容について説明した表を示します。

出力（続き）	説明（続き）
IPsec Global Statistics	このセクションは、脅威に対する防御 デバイスがサポートする IPsec トンネルの総数に関連しています。
Active tunnels	現在接続されている IPsec トンネルの数。
Previous tunnels	接続されたことがある IPsec トンネルの数（アクティブなトンネルを含む）。
着信	このセクションは、IPsec トンネルを介して受信した着信暗号トラフィックに関係します。
Bytes	受信した暗号トラフィックのバイト数。
Decompressed bytes	圧縮解除が実行された後に受信された暗号トラフィックのバイト数（該当する場合）。圧縮がイネーブルでない場合、このカウンタは常に上記のカウンタと等しくなるはずですが。
Packets	受信された IPsec 暗号化パケットの数。
Dropped packets	受信されたがエラーのためドロップされた IPsec 暗号化パケットの数。
Replay failures	受信された IPsec 暗号化パケットについて検出されたアンチリプレイの失敗数。
Authentications	受信された IPsec 暗号化パケットについて実行された認証の成功数。
Authentication failures	受信された IPsec 暗号化パケットについて検出された認証の失敗数。
Decryptions	受信された IPsec 暗号化パケットについて実行された復号化の成功数。

出力 (続き)	説明 (続き)
Decryption failures	受信された IPsec 暗号化パケットについて検出された復号の失敗数。
Decapsulated fragments needing reassembly	再構築が必要な IP フラグメントを含む復号 IPsec パケットの数。
発信	このセクションは、IPsec トラフィックを介して送信される発信クリアテキストトラフィックに関係します。
Bytes	IPsec トンネルを介して暗号化および送信されるクリアテキストトラフィックのバイト数。
Uncompressed bytes	IPsec トンネルを介して暗号化および送信される圧縮解除されたクリアテキストトラフィックのバイト数。圧縮がイネーブルでない場合、このカウンタは常に上記のカウンタと等しくなるはずですが。
Packets	IPsec トンネルを介して暗号化および送信されるクリアテキストパケットの数。
Dropped packets	IPsec トンネルを介して暗号化および送信されるが、エラーが原因でドロップされたクリアテキストパケットの数。
Authentications	IPsec トンネルを介して送信されるパケットについて実行された認証の成功数。
Authentication failures	IPsec トンネルを介して送信されるパケットについて検出された認証の失敗数。
Encryptions	IPsec トンネルを介して送信されるパケットについて実行された暗号化の成功数。
Encryption failures	IPsec トンネルを介して送信されるパケットについて検出された暗号化の失敗数。
Fragmentation successes	発信 IPsec パケットの変換の一部として実行されたフラグメンテーション操作の成功数。
Pre-fragmentation successes	発信 IPsec パケット変換の一部として実行された、成功した事前フラグメンテーション操作の数。事前フラグメンテーションは、クリアテキストパケットが暗号化され、1 つ以上の IPsec パケットとしてカプセル化される前に行われます。

出力（続き）	説明（続き）
Post-fragmentation successes	発信 IPsec パケット変換の一部として実行された、成功した事前フラグメンテーション操作の数。事後フラグメンテーションは、クリアテキストパケットが暗号化され、IPsec パケットとしてカプセル化されることによって複数の IP フラグメントが作成される前に行われます。これらのフラグメントは、復号化前に再構築する必要があります。
Fragmentation failures	発信 IPsec パケットの変換中に発生したフラグメンテーションの失敗数。
Pre-fragmentation failures	発信 IPsec パケットの変換中に発生したプリフラグメンテーションの失敗数。事前フラグメンテーションは、クリアテキストパケットが暗号化され、1つ以上の IPsec パケットとしてカプセル化される前に行われます。
Post-fragmentation failure	発信 IPsec パケットの変換中に発生したポストフラグメンテーションの失敗数。事後フラグメンテーションは、クリアテキストパケットが暗号化され、IPsec パケットとしてカプセル化されることによって複数の IP フラグメントが作成される前に行われます。これらのフラグメントは、復号化前に再構築する必要があります。
Fragments created	IPsec の変換の一部として作成されたフラグメントの数。
PMTUs sent	IPsec システムによって送信されたパス MTU メッセージの数。IPsec は、暗号化後に、IPsec トンネルを介して送信するには大きすぎるパケットを送信している内部ホストに対して PMTU メッセージを送信します。PMTU メッセージは、ホストの MTU を低くして、IPsec トンネルを介して送信するパケットのサイズを小さくすることをホストに求めるメッセージです。
PMTUs recvd	IPsec システムによって受信されたパス MTU メッセージの数。IPsec は、トンネルを介して送信するパケットが大きすぎてネットワーク要素を通過できない場合、ダウンストリームのネットワーク要素からパス MTU メッセージを受信します。パス MTU メッセージを受信すると、IPsec は通常、トンネル MTU を低くします。
Protocol failures	受信した不正な形式の IPsec パケットの数。
Missing SA failures	指定された IPsec セキュリティアソシエーションが存在しない、要求された IPsec の動作の数。

出力 (続き)	説明 (続き)
System capacity failures	IPsec システムの容量が十分でないためデータ レートをサポートできないことが原因で完了できないIPsec の動作の数。

例

次の例をグローバル コンフィギュレーション モードで入力すると、IPSec 統計情報が表示されます。

```
> 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
```

IPsec フローオフロードをサポートするプラットフォームでは、出力にはオフロードフローのカウンタが表示され、通常のカウンタにはオフロードフローと非オフロードフローの合計が表示されます。

```
> 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

```

関連コマンド

Command	説明
clear ipsec sa	指定されたパラメータに基づいて、IPsec SA またはカウンタをクリアします。
show ipsec sa	指定されたパラメータに基づいて IPsec SA を表示します。

Command	説明
show ipsec sa summary	IPsec SA の要約を表示します。

show ipv6 access-list

このコマンドは、脅威に対する防御ではサポートされていない機能用です。IPv6 アクセス制御は、標準アクセス コントロール ポリシーに統合されています。マネージャでポリシーを表示するか、次のコマンドを使用します。

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

show ipv6 dhcp

DHCPv6 情報を表示するには、**show ipv6 dhcp** コマンドを使用します。

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

構文の説明

client [pd] statistics	DHCPv6 クライアント統計情報を表示し、送受信されたメッセージ数の出力を表示します。DHCPv6 プレフィックス委任クライアントの統計情報を表示するには、 pd キーワードを追加します。
interface [<i>interface_name</i>] [statistics]	すべてのインターフェイスの DHCPv6 情報、または必要に応じて、指定したインターフェイスの DHCPv6 情報を表示します。インターフェイスが DHCPv6 ステートレスサーバー構成用に設定されている場合、このコマンドは、サーバーによって使用されている DHCPv6 プールをリストします。インターフェイスに DHCPv6 アドレス クライアントまたはプレフィックス委任クライアントの設定がある場合、このコマンドは各クライアントの状態とサーバーから受信した値を表示します。 インターフェイス名を指定すると、指定したインターフェイスの DHCPv6 サーバーまたはクライアントのメッセージ統計情報を表示するために statistics を追加できます。
ha statistics	DUID 情報がフェールオーバーユニット間で同期された回数を含め、フェールオーバー ユニット間のトランザクションの統計情報を表示します。
server statistics	DHCPv6 ステートレス サーバーの統計情報を表示します。
pool [pool_name]	すべての DHCPv6 プール、または必要に応じて、指定したプールを表示します。

コマンド履歴

リリース	変更内容
6.2.1	このコマンドが導入されました。

使用上のガイドライン

引数を指定しない場合、このコマンドは、DHCPv6 クライアントまたはサーバーによって使用されているデバイス DUID を表示します。

例

次に、**show ipv6 dhcp** コマンドの出力例を示します。

```
> show ipv6 dhcp
```

This device's DHCPv6 unique identifier(DUID): 00030001377E8FD91020

次に、**show ipv6 dhcp pool** コマンドの出力例を示します。

```
> 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
```

次に、**show ipv6 dhcp interface** コマンドの出力例を示します。

```
> 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
```

次に、**show ipv6 dhcp interface outside** コマンドの出力例を示します。

```
> 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
```

次に、**show ipv6 dhcp interface outside statistics** コマンドの出力例を示します。

```
> 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

```

次に、**show ipv6 dhcp client statistics** コマンドの出力例を示します。

```
> 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

```

次に、**show ipv6 dhcp client pd statistics** コマンドの出力例を示します。

```
> 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

```

次に、**show ipv6 dhcp server statistics** コマンドの出力例を示します。

```
> 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

```

次に、**show ipv6 dhcp ha statistics** コマンドの出力例を示します。

```

> 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

```

次に、スタンバイユニットでの **show ipv6 dhcp ha statistics** コマンドの出力例を示します。

```

> 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

```

関連コマンド

Command	説明
clear ipv6 dhcp	DHCPv6 統計情報をクリアします。

show ipv6 dhcprelay binding

リレーエージェントによって作成されたリレーバインディングエントリを表示するには、**show ipv6 dhcprelay binding** コマンドを使用します。

show ipv6 dhcprelay binding

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

例

次に、**show ipv6 dhcprelay binding** コマンドの出力例を示します。

```
> 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.
```

関連コマンド

Command	説明
show ipv6 dhcprelay statistics	IPv6 DHCP リレー エージェントの情報を表示します。

show ipv6 dhcprelay statistics

IPv6 DHCP リレーエージェントの統計情報を表示するには、**show ipv6 dhcprelay statistics** コマンドを使用します。

show ipv6 dhcprelay statistics

コマンド履歴	リリース	変更内容
	6.1	このコマンドが導入されました。

例

次に、**show ipv6 dhcprelay statistics** コマンドの出力例を示します。

```
> 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
```

関連コマンド	Command	説明
	show ipv6 dhcprelay binding	リレー エージェントによって作成されたリレー バインディング エントリを表示します。

show ipv6 general-prefix

IPv6 の汎用プレフィックスを表示するには、**show ipv6 general-prefix** コマンドを使用します。

show ipv6 general-prefix

コマンド履歴	リリース	変更内容
	6.1	このコマンドが導入されました。

使用上のガイドライン **show ipv6 general-prefix** コマンドを使用して、IPv6 汎用プレフィックスに関する情報を表示します。

例

次に、**show ipv6 general-prefix** コマンドの出力例を示します。

```
> 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

すべてのインターフェイス上に設定されている ICMPv6 アクセスルールを表示するには、**show ipv6 icmp** コマンドを使用します。

show ipv6 icmp

コマンド履歴	リリース	変更内容
	6.1	このコマンドが導入されました。

使用上のガイドライン ICMPv6 のルールは、デバイス インターフェイスへの ICMPv6 トラフィックを制御します。これらは、**through-the-box** トラフィックを制御しません。これらのルールを使用して、ICMPv6 コマンド (ping など) をインターフェイスに送信できるアドレスや、送信できる ICMPv6 コマンドのタイプを制御します。これらのルールを表示するには、**show ipv6 icmp** コマンドを使用します。

例

次に、**show ipv6 icmp** コマンドの出力例を示します。

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

show ipv6 interface

IPv6 用に設定されたインターフェイスのステータスを表示するには、**show ipv6 interface** コマンドを使用します。

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

構文の説明

brief	各インターフェイスの IPv6 ステータスおよびコンフィギュレーションの要約を表示します。
<i>if_name</i>	(任意) 内部または外部のインターフェイス名。指定されたインターフェイスのステータスおよびコンフィギュレーションのみが表示されます。 すべてのインターフェイスを表示すると、システム通信に使用される内部インターフェイスに関する情報も表示されます。内部インターフェイスをユーザーが設定することはできません。情報はデバッグのみを目的としています。
prefix	(任意) ローカルの IPv6 プレフィックス プールから生成されるプレフィックス。プレフィックスは、IPv6 アドレスのネットワーク部分です。

コマンド デフォルト

すべての IPv6 インターフェイスを表示します。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

使用上のガイドライン

show ipv6 interface コマンドは、IPv6 固有である点を除き、**show interface** コマンドと同様の出力を提供します。インターフェイスのハードウェアが使用できる場合、インターフェイスは **up** とマークされます。インターフェイスが双方向通信を提供できる場合、回線プロトコルは **up** とマークされます。

インターフェイス名が指定されていない場合は、すべての IPv6 インターフェイスの情報が表示されます。インターフェイス名を指定すると、指定されたインターフェイスに関する情報が表示されます。

例

次に、**show ipv6 interface** コマンドの出力例を示します。

```
> 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
```

次に、**brief** キーワードを使用して入力した場合の **show ipv6 interface** コマンドの出力例を示します。

```
> 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
```

次に、**show ipv6 interface** コマンドの出力例を示します。アドレスからプレフィックスを生成したインターフェイスの特性が表示されています。

```
> 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

IPv6 アドレスプール情報を表示するには、**show ipv6 local pool** コマンドを使用します。

show ipv6 local pool *pool_name*

構文の説明

pool_name IPv6 アドレスプールの名前。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

使用上のガイドライン

IPv6 アドレスプールの内容を表示するには、このコマンドを使用します。これらのプールは、リモートアクセス VPN およびクラスタリングで使用されます。IPv4 アドレスプールを表示するには、**show ip local pool** を使用します。

例

次に、**show ipv6 local pool** コマンドの出力例を示します。

```
> 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

マルチキャストリスナー検出 (MLD) トラフィックカウンタ情報を表示するには、**show ipv6 mld traffic** コマンドを使用します。

show ipv6 mld traffic

コマンド履歴	リリース	変更内容
	6.1	このコマンドが導入されました。

使用上のガイドライン **show ipv6 mld traffic** コマンドを使用すると、予期される数の MLD メッセージが受信および送信されたかどうかをチェックできます。**show ipv6 mld traffic** コマンドによって次の情報が提供されます。

- Elapsed time since counters cleared : カウンタがクリアされてからの経過時間。
- Valid MLD Packets : 送受信された有効な MLD パケットの数。
- Queries : 送受信された有効なクエリーの数。
- Reports : 送受信された有効なレポートの数。
- Leaves : 送受信された有効な脱退の数。
- Mtrace packets : 送受信されたマルチキャスト トレース パケットの数。
- Errors : 発生したエラーのタイプと数。

例

次に、**show ipv6 mld traffic** コマンドの出力例を示します。

```
> 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
```

関連コマンド

Command	説明
clear ipv6 mld traffic	すべての MLD トラフィック カウンタをリセットします。

show ipv6 neighbor

IPv6 ネイバー探索キャッシュ情報を表示するには、**show ipv6 neighbor** コマンドを使用します。

show ipv6 neighbor [*if_name* | *address*]

構文の説明	<p><i>address</i> (任意) 指定された IPv6 アドレスについてのみネイバー探索キャッシュ情報を表示します。</p>				
	<p><i>if_name</i> (オプション) 指定されたインターフェイス名のキャッシュ情報を表示します。</p> <p>すべてのインターフェイスを表示すると、システム通信に使用される内部インターフェイスに関する情報も表示されます。内部インターフェイスをユーザーが設定することはできません。情報はデバッグのみを目的としています。</p>				
コマンド履歴	<table border="1"> <thead> <tr> <th data-bbox="406 856 682 919">リリース</th> <th data-bbox="682 856 1536 919">変更内容</th> </tr> </thead> <tbody> <tr> <td data-bbox="406 919 682 980">6.1</td> <td data-bbox="682 919 1536 980">このコマンドが導入されました。</td> </tr> </tbody> </table>	リリース	変更内容	6.1	このコマンドが導入されました。
リリース	変更内容				
6.1	このコマンドが導入されました。				

使用上のガイドライン **show ipv6 neighbor** コマンドによって次の情報が提供されます。

- IPv6 Address : ネイバーまたはインターフェイスの IPv6 アドレス。
- Age : アドレスが到達可能と確認されてからの経過時間 (分単位)。ハイフン (-) はスタティック エントリを示します。
- Link-layer Addr : MAC アドレス。アドレスが不明の場合、ハイフン (-) が表示されます。
- State : ネイバー キャッシュ エントリの状態。



(注) 到達可能性検出は IPv6 ネイバー探索キャッシュのスタティック エントリに適用されないため、INCMP (不完全) 状態と REACH (到達可能) 状態の記述は、ダイナミック キャッシュ エントリとスタティック キャッシュ エントリで異なります。

次に、IPv6 ネイバー探索キャッシュのダイナミック エントリについて表示される可能性のある状態を示します。

- INCMP : (不完全) エントリに対してアドレス解決を実行中です。ネイバー送信要求メッセージがターゲットの送信要求ノード マルチキャスト アドレスに送信されましたが、対応するネイバー アドバタイズメント メッセージが受信されていません。
- REACH : (到達可能) ネイバーへの転送パスが正常に機能していることを示す肯定確認が、直近の ReachableTime ミリ秒以内に受信されました。REACH 状態になって

いる間は、パケットが送信されるときにデバイスは特別なアクションを実行しません。

- **STALE** : 転送パスが正しく機能していたことを示す確認が最後に受信されてから経過した時間が、**ReachableTime** ミリ秒を超えています。**STALE** 状態になっている間は、パケットが送信されるまでデバイスはアクションを実行しません。
- **DELAY** : 転送パスが正しく機能していたことを示す確認が最後に受信されてから経過した時間が、**ReachableTime** ミリ秒を超えています。パケットは直近の **DELAY_FIRST_PROBE_TIME** 秒以内に送信されました。**DELAY** 状態に入ってから、**DELAY_FIRST_PROBE_TIME** 秒以内に到達可能性確認を受信できない場合は、ネイバー送信要求メッセージが送信され、状態が **PROBE** に変更されます。
- **PROBE** : 到達可能性確認が受信されるまで、**RetransTimer** ミリ秒ごとに、ネイバー要求メッセージを再送信することで、到達可能性確認が積極的に求められます。
- **????** : 不明な状態。

次に、IPv6 ネイバー探索キャッシュのスタティック エントリについて表示される可能性のある状態を示します。

- **INCMP** : (不完全) このエントリのインターフェイスはダウンしています。
- **REACH** : (到達可能) このエントリのインターフェイスは動作しています。

• インターフェイス

アドレスに到達可能であったインターフェイス。

例

次に、インターフェイスを指定して入力した **show ipv6 neighbor** コマンドの出力例を示します。

```
> 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
```

次に、IPv6 アドレスを指定して入力した **show ipv6 neighbor** コマンドの出力例を示します。

```
> 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
```

関連コマンド

Command	説明
clear ipv6 neighbors	スタティック エントリを除く、IPv6 ネイバー探索キャッシュ内のすべてのエントリを削除します。

show ipv6 ospf

OSPFv3 ルーティングプロセスに関する一般情報を表示するには、**show ipv6 ospf** コマンドを使用します。

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

構文の説明	<i>area_id</i>	(オプション) 指定したエリアに関する情報だけを表示します。
	<i>process_id</i>	(オプション) ローカルで割り当てられ、任意の正の整数である内部 ID を指定します。この ID は、OSPFv3 ルーティングプロセスがイネーブルになっている場合に、管理上割り当てられる番号です。
コマンド履歴	リリース	変更内容
	6.1	このコマンドが導入されました。

例

次に、**show ipv6 ospf** コマンドの出力例を示します。

```
> 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 msec
Minimum hold time between two consecutive SPF's 10000 msec
Maximum wait time between two consecutive SPF's 10000 msec
Minimum LSA interval 5 secs
Minimum LSA arrival 1000 msec
```

関連コマンド

Command	説明
show ipv6 ospf border-routers	エリア境界ルータ (ABR) と自律システム境界ルータ (ASBR) に対する内部 OSPFv3 ルーティングテーブルエントリを表示します。
show ipv6 ospf database	特定のルータの OSPFv3 データベースに関する情報の一覧を表示します。

show ipv6 ospf border-routers

エリア境界ルータ（ABR）と自律システム境界ルータ（ASBR）に対する内部OSPFv3ルーティングテーブルエントリを表示するには、**show ipv6 ospf border-routers** コマンドを使用します。

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

構文の説明	<i>process_id</i>	(オプション) ローカルで割り当てられ、任意の正の整数である内部IDを指定します。このIDは、OSPFv3ルーティングプロセスがイネーブルになっている場合に、管理上割り当てられる番号です。
コマンド履歴	リリース	変更内容
	6.1	このコマンドが導入されました。

使用上のガイドライン **show ipv6 ospf border-routers** コマンドを使用すると、次の設定が一覧表示されます。

- エリア内ルート
- エリア間ルート
- IPv6 アドレス
- インターフェイス タイプ
- Area ID
- SPF 番号

例

次に、**show ipv6 ospf border-routers** コマンドの出力例を示します。

```
> 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
```

関連コマンド	Command	説明
	show ipv6 ospf	OSPFv3 ルーティング プロセスのすべての IPv6 設定を表示します。
	show ipv6 ospf database	特定のルータのOSPFv3データベースに関する情報の一覧を表示します。

show ipv6 ospf database

特定のルータの OSPFv3 データベースに関連した情報リストを表示するには、**show ipv6 ospf database** コマンドを入力します。

```
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]
```

構文の説明

adv-router <i>router-id</i>	(オプション) アドバタイズするルータのすべての LSA を表示します。ルータ ID は、RFC 2740 に記載された形式にする必要があり、16 ビット値をコロンで区切った 16 進数でアドレスを指定します。
area	(オプション) エリア LSA に関する情報だけを表示します。
<i>area_id</i>	(オプション) 指定したエリアに関する情報だけを表示します。
as	(オプション) 不明な自律システム (AS) LSA をフィルタリングします。
database-summary	(オプション) データベースと全体にある各エリアの各 LSA タイプの数を表示します。
<i>destination-router-id</i>	(オプション) 指定した宛先ルータに関する情報だけを表示します。
external	(任意) 外部 LSA の情報だけを表示します。
interface	(オプション) インターフェイス コンテキストでフィルタリングされた LSA に関する情報を表示します。
<i>interface-name</i>	(オプション) LSA のインターフェイス名を指定します。
internal	(オプション) 内部 LSA の情報だけを表示します。
inter-area prefix	(オプション) エリア間プレフィックスに基づいた LSA の情報だけを表示します。
inter-area router	(オプション) エリア間ルータ LSA 基づいた LSA の情報だけを表示します。
link	(オプション) リンク LSA に関する情報を表示します。 unknown キーワードの後に入力した場合、 link キーワードでリンクスコープ LSA がフィルタ処理されます。
<i>link-state-id</i>	(オプション) LSA を区別するために使用する整数を指定します。ネットワーク LSA およびリンク LSA では、リンクステート ID はインターフェイス インデックスに一致します。

network	(オプション) ネットワーク LSA に関する情報を表示します。
nssa-external	(オプション) Not-So-Stubby-Area (NSSA) の外部 LSA に関する情報だけを表示します。
prefix ipv6-prefix	(オプション) ネイバーのリンクローカル IPv6 アドレスを表示します。IPv6 プレフィックスは、RFC 2373 に記載された形式にする必要があり、16 ビット値をコロンで区切った 16 進数でアドレスを指定します。
process_id	(オプション) ローカルで割り当てられ、任意の正の整数である内部 ID を指定します。この ID は、OSPF ルーティングプロセスがイネーブルになっている場合に、管理上割り当てられる番号です。
ref-lsa	(オプション) プレフィックス LSA タイプをさらにフィルタリングします。
router	(オプション) ルータ LSA に関する情報を表示します。
self-originate	(オプション) ローカル ルータから自己生成 LSA だけを表示します。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、さまざまな形式で、異なる OSPFv3 LSA に関する情報を提供します。

例

次に、**show ipv6 ospf database** コマンドの出力例を示します。

```
> 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)
```

show ipv6 ospf database

```

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

```

関連コマンド

Command	説明
show ipv6 ospf	OSPFv3 ルーティングプロセスのすべての IPv6 設定を表示します。
show ipv6 ospf border-routers	エリア境界ルータ (ABR) と自律システム境界ルータ (ASBR) に対する内部 OSPFv3 ルーティングテーブルエントリを表示します。

show ipv6 ospf events

OSPFv3 内部イベントの情報を表示するには、**show ipv6 ospf events** コマンドを使用します。

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

構文の説明

<i>process_id</i>	(オプション) ローカルで割り当てられ、任意の正の整数である内部 ID を指定します。この ID は、OSPF ルーティングプロセスがイネーブルになっている場合に、管理上割り当てられる番号です。
<i>type</i>	(オプション) 表示するイベント タイプのリスト。タイプを 1 つ以上指定しないと、すべてのイベントが表示されます。次のタイプでフィルタリングできます。 <ul style="list-style-type: none"> • generic : 一般的なイベント。 • interface : インターフェイス状態変化イベント。 • lsa : LSA 到着イベントおよび LSA 生成イベント。 • neighbor : ネイバー状態変化イベント。 • reverse : 逆の順序でイベントを表示。 • rib : ルータ情報ベースの更新イベント、削除イベント、および再配布イベント。 • spf : SPF のスケジューリングイベントおよび SPF 実行イベント。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

例

次に、**show ipv6 ospf events** コマンドの出力例を示します。

```
> 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

```

関連コマンド

Command	説明
show ipv6 ospf	OSPFv3 ルーティングプロセスのすべての IPv6 設定を表示します。
show ipv6 ospf border-routers	エリア境界ルータ (ABR) と自律システム境界ルータ (ASBR) に対する内部 OSPFv3 ルーティングテーブルエントリを表示します。

show ipv6 ospf flood-list

いずれかのインターフェイスを介したフラッディングを待機している OSPFv3 LSA のリストを表示するには、**show ipv6 ospf flood-list** コマンドを使用します。

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

構文の説明	
<i>area_id</i>	(オプション) 指定したエリアに関する情報だけを表示します。
<i>interface-number</i>	(オプション) LSA がフラッディングされるインターフェイス番号を指定します。
<i>interface-type</i>	(オプション) LSA がフラッディングされるインターフェイスタイプを指定します。
<i>process_id</i>	(オプション) ローカルで割り当てられ、任意の正の整数である内部 ID を指定します。この ID は、OSPFv3 ルーティングプロセスがイネーブルになっている場合に、管理上割り当てられる番号です。

コマンド履歴	リリース	変更内容
	6.1	このコマンドが導入されました。

使用上のガイドライン OSPFv3 パケット ペーシング情報を表示するには、このコマンドを使用します。

例

次に、**show ipv6 ospf flood-list** コマンドの出力例を示します。

```
> 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
```

関連コマンド	Command	説明
	show ipv6 ospf	OSPFv3 ルーティング プロセスのすべての IPv6 設定を表示します。

Command	説明
show ipv6 ospf border-routers	エリア境界ルータ（ABR）と自律システム境界ルータ（ASBR）に対する内部 OSPFv3 ルーティング テーブル エントリを表示します。

show ipv6 ospf graceful-restart

OSPFv3 グレースフルリスタートに関する情報を表示するには、**show ipv6 ospf graceful-restart** コマンドを使用します。

show ipv6 ospf graceful-restart

コマンド履歴	リリース	変更内容
	6.1	このコマンドが導入されました。

例

次に、**show ipv6 ospf graceful-restart** コマンドの出力例を示します。

```
> 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
```

関連コマンド	Command	説明
	show ipv6 ospf	OSPFv3 ルーティング プロセスのすべての IPv6 設定を表示します。

show ipv6 ospf interface

OSPFv3 関連のインターフェイス情報を表示するには、**show ipv6 ospf interface** コマンドを入力します。

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

構文の説明

<i>area_id</i>	(オプション) 指定したエリアに関する情報だけを表示します。
brief	(オプション) OSPFv3 インターフェイス、状態、アドレスとマスク、およびルータのエリアに関する簡単な概要情報を表示します。
<i>process_id</i>	(オプション) ローカルで割り当てられ、任意の正の整数である内部 ID を指定します。この ID は、OSPF ルーティングプロセスがイネーブルになっている場合に、管理上割り当てられる番号です。
<i>type-number</i>	(オプション) インターフェイスのタイプおよび番号を指定します。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

使用上のガイドライン

OSPFv3 インターフェイス、状態、アドレスとマスク、およびルータのエリアに関する概要情報を表示するには、このコマンドを使用します。

例

次に、**show ipv6 ospf interface** コマンドの出力例を示します。

```
> 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)

```

関連コマンド

Command	説明
show ipv6 ospf	OSPFv3 ルーティング プロセスのすべての IPv6 設定を表示します。
show ipv6 ospf border-routers	エリア境界ルータ (ABR) と自律システム境界ルータ (ASBR) に対する内部 OSPFv3 ルーティング テーブル エントリを表示します。

show ipv6 ospf request-list

ルータが要求したすべての LSA のリストを表示するには、**show ipv6 ospf request-list** コマンドを使用します。

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

構文の説明

<i>area_id</i>	(オプション) 指定したエリアに関する情報だけを表示します。
<i>interface</i>	(オプション) このインターフェイスからルータにより要求されるすべての LSA のリストを指定します。
<i>interface-neighbor</i>	(オプション) このネイバーのインターフェイスのルータにより要求されるすべての LSA のリストを指定します。
<i>neighbor</i>	(オプション) このネイバーからルータにより要求されるすべての LSA のリストを指定します。
<i>process_id</i>	(オプション) ローカルで割り当てられ、任意の正の整数である内部 ID を指定します。この ID は、OSPF ルーティングプロセスがイネーブルになっている場合に、管理上割り当てられる番号です。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

例

次に、**show ipv6 ospf request-list** コマンドの出力例を示します。

```
> 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
```

関連コマンド

Command	説明
show ipv6 ospf	OSPFv3 ルーティング プロセスのすべての IPv6 設定を表示します。

Command	説明
show ipv6 ospf border-routers	エリア境界ルータ（ABR）と自律システム境界ルータ（ASBR）に対する内部 OSPFv3 ルーティング テーブル エントリを表示します。

show ipv6 ospf retransmission-list

再送信待ちになっているすべての LSA のリストを表示するには、**show ipv6 ospf retransmission-list** コマンドを使用します。

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

構文の説明	
<i>area_id</i>	(オプション) 指定したエリアに関する情報だけを表示します。
<i>interface</i>	(オプション) このインターフェイスで再送信を待機しているすべての LSA のリストを指定します。
<i>interface-neighbor</i>	(オプション) このネイバーからこのインターフェイスの再送信を待機しているすべての LSA のリストを表示します。
<i>neighbor</i>	(オプション) このネイバーの再送信を待機しているすべての LSA のリストを指定します。
<i>process_id</i>	(オプション) ローカルで割り当てられ、任意の正の整数である内部 ID を指定します。この ID は、OSPF ルーティングプロセスがイネーブルになっている場合に、管理上割り当てられる番号です。

コマンド履歴	リリース	変更内容
	6.1	このコマンドが導入されました。

例

次に、**show ipv6 ospf retransmission-list** コマンドの出力例を示します。

```
> 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
```

関連コマンド	Command	説明
	show ipv6 ospf	OSPFv3 ルーティングプロセスのすべての IPv6 設定を表示します。
	show ipv6 ospf border-routers	エリア境界ルータ (ABR) と自律システム境界ルータ (ASBR) に対する内部 OSPFv3 ルーティングテーブルエントリを表示します。

show ipv6 ospf statistic

さまざまな OSPFv3 統計（SPF が実行された回数、理由、期間など）を表示するには、**show ipv6 ospf statistic** コマンドを使用します。

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

構文の説明	detail	(オプション) トリガー ポイントを含む詳細な SPF 情報を指定します。
	<i>process_id</i>	(オプション) ローカルで割り当てられ、任意の正の整数である内部 ID を指定します。この ID は、OSPF ルーティングプロセスがイネーブルになっている場合に、管理上割り当てられる番号です。
コマンド履歴	リリース	変更内容
	6.1	このコマンドが導入されました。

例

次に、**show ipv6 ospf statistic** コマンドの出力例を示します。

```
> 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

OSPFv3 プロセスで設定されているサマリーアドレスのすべての再配布情報のリストを表示するには、**show ipv6 ospf summary-prefix** コマンドを使用します。

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

構文の説明	<i>process_id</i>	(オプション) ローカルで割り当てられ、任意の正の整数である内部 ID を指定します。この ID は、OSPF ルーティングプロセスがイネーブルになっている場合に、管理上割り当てられる番号です。
コマンド履歴	リリース	変更内容
	6.1	このコマンドが導入されました。

例

次に、**show ipv6 ospf summary-prefix** コマンドの出力例を示します。

```
> show ipv6 ospf summary-prefix
OSPFv3 Process 1, Summary-prefix
FE00::/24 Metric 16777215, Type 0, Tag 0
```

関連コマンド	Command	説明
	show ipv6 ospf	OSPFv3 ルーティングプロセスのすべての IPv6 設定を表示します。
	show ipv6 ospf border-routers	エリア境界ルータ (ABR) と自律システム境界ルータ (ASBR) に対する内部 OSPFv3 ルーティングテーブル エントリを表示します。

show ipv6 ospf timers

OSPFv3 タイマー情報を表示するには、**show ipv6 ospf timers** コマンドを使用します。

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

構文の説明	lsa-group	(オプション) OSPFv3 LSA グループ情報を指定します。
	process_id	(オプション) ローカルで割り当てられ、任意の正の整数である内部 ID を指定します。この ID は、OSPF ルーティングプロセスがイネーブルになっている場合に、管理上割り当てられる番号です。
	rate-limit	(オプション) OSPFv3 LSA のレート制限情報を指定します。
コマンド履歴	リリース	変更内容
	6.1	このコマンドが導入されました。

例

次に、**show ipv6 ospf timers lsa-group** コマンドの出力例を示します。

```
> 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

現在使用可能なインターフェイスの OSPFv3 トラフィック関連の統計情報を表示するには、**show ipv6 ospf traffic** コマンドを使用します。

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

構文の説明

interface_name	(任意) インターフェイスの名前を指定します。特定のインターフェイスにトラフィックを分離するには、このオプションを使用します。
process_id	(オプション) ローカルで割り当てられ、任意の正の整数である内部 ID を指定します。この ID は、OSPF ルーティングプロセスがイネーブルになっている場合に、管理上割り当てられる番号です。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

例

次に、**show ipv6 ospf traffic** コマンドの出力例を示します。

```
> 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
```

関連コマンド

Command	説明
show ipv6 ospf	OSPFv3 ルーティングプロセスのすべての IPv6 設定を表示します。

Command	説明
show ipv6 ospf border-routers	エリア境界ルータ（ABR）と自律システム境界ルータ（ASBR）に対する内部 OSPFv3 ルーティング テーブル エントリを表示します。

show ipv6 ospf virtual-links

OSPFv3 仮想リンクのパラメータと現在の状態を表示するには、**show ipv6 ospf virtual-links** コマンドを使用します。

show ipv6 ospf virtual-links

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

例

次に、**show ipv6 ospf virtual-links** コマンドの出力例を示します。

```
> 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
```

関連コマンド

Command	説明
show ipv6 ospf	OSPFv3 ルーティングプロセスのすべての IPv6 設定を表示します。
show ipv6 ospf border-routers	エリア境界ルータ (ABR) と自律システム境界ルータ (ASBR) に対する内部 OSPFv3 ルーティングテーブルエントリを表示します。

show ipv6 prefix-list

IPv6 トラフィックに一致するように設定されているプレフィックスリストを一覧表示するには、**show ipv6 prefix-list** コマンドを使用します。

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

構文の説明	detail	プレフィックスリストに関する詳細を表示します。
	summary	プレフィックスリストの概要を表示します。
	<i>prefix_list_name</i>	プレフィックスリストの名前。
	seq <i>sequence_number</i>	(オプション) 指定されたプレフィックスリストに指定されたシーケンス番号を持つプレフィックスリストのエントリだけを表示します。
	<i>network/length</i> [longer first-match]	(オプション) このネットワークアドレスおよびプレフィックス長(ビット単位)を使用する、指定されたプレフィックスリストのすべてのエントリを表示します。 必要に応じて、次のキーワードのいずれかを含めることができます。 <ul style="list-style-type: none"> • longer 指定された <i>network/length</i> と一致する、または指定された <i>network/length</i> よりも限定的な、指定されたプレフィックスリストのエントリすべてを表示します。 • first-match 指定された <i>network/length</i> と一致する、指定されたプレフィックスリストの最初のエントリを表示します。
コマンド履歴	リリース	変更内容
	6.1	このコマンドが導入されました。

例

次に、**show ipv6 prefix-list** コマンドの出力例を示します。

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

次に、要約された出力の例を示します。

```
> 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
```

次に、詳細な出力の例を示します。

```
> 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
```

関連コマンド

Command	説明
clear ipv6 prefix-list	IPv6 プレフィックスリストに対するヒットカウントをリセットします。
show bgp prefix-list	ボーダー ゲートウェイ プロトコルのコンテキストに含まれるプレフィックスリストまたはプレフィックスリストのエントリに関する情報を表示します。
show prefix-list	IPv4 プレフィックス リストに関する情報を表示します。

show ipv6 route

IPv6 ルーティングテーブルの内容を表示するには、**show ipv6 route** コマンドを使用します。

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

構文の説明

managment-only	IPv6 管理ルーティング テーブル内のルートを表示します。
cluster	(オプション) クラスタ内の IPv6 ルーティング テーブルのシーケンス番号、IPv6 再コンバージェンス タイマーのステータス、および IPv6 ルーティング エントリのシーケンス番号を表示します。
failover	(オプション) IPv6 ルーティング テーブルのシーケンス番号、IPv6 再コンバージェンス タイマーのステータス、および IPv6 ルーティング エントリのシーケンス番号を表示します。
interface name	(オプション) IPv6 インターフェイス固有のルートを表示します。
ospf	(オプション) OSPFv3 ルートを表示します。
summary	(オプション) IPv6 ルート集約を表示します。
[vrf name all]	Virtual Route Forwarding (VRF) (仮想ルータとも呼ばれる) を有効にすると、vrf name キーワードを使用してビューを特定の仮想ルータに制限できます。すべての仮想ルータのルーティングテーブルを表示するには、all キーワードを含めます。これらの VRF 関連キーワードのいずれも含まない場合、コマンドはグローバル VRF 仮想ルータのルーティングテーブルを表示します。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。
6.6	[vrf name all] キーワードが追加されました。

使用上のガイドライン

show ipv6 route コマンドの出力は、IPv6 に固有の情報である点を除いて、**show route** コマンドの出力と類似しています。

次に、IPv6 ルーティング テーブルに表示される情報を示します。

- Codes : ルートを生成したプロトコルを示します。表示される値は次のとおりです。
 - C : 接続済み
 - L : ローカル
 - S : スタティック

- R : RIP 生成
 - B : BGP 生成
 - I1 : ISIS L1 : 統合 IS-IS Level 1 生成
 - I2 : ISIS L2 : 統合 IS-IS Level 2 生成
 - IA : ISIS エリア間 : 統合 IS-IS エリア間生成
- fe80::/10 : リモート ネットワークの IPv6 プレフィックスを示します。
 - [0/0] : カッコ内の最初の数値は情報ソースのアドミニストレーティブディスタンスです。2 番目の数値はルートのメトリックです。
 - via :: : リモート ネットワークへの次のルータのアドレスを指定します。
 - inside : 指定されたネットワークへの次のルータに到達できるインターフェイスを指定します。

例

次に、**show ipv6 route** コマンドの出力例を示します。

```
> 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
```

次に、**show ipv6 route failover** コマンドの出力例を示します。

```
> 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

```

プライマリユニットでの **show ipv6 route cluster** コマンドの出力例を次に示します。

```

> 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
...

```

ロール変更時のセカンダリユニットにおける **show ipv6 route cluster** コマンドの出力例を次に示します。

```

> 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
...

```

次に、**red** という名前の仮想ルータのルートを表示する例を示します。他の仮想ルータにリークされたスタティックルートは、キー **SI** で示されることに注意してください。

```

> 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

```

関連コマンド

Command	説明
show route	IPv4 ルーティングテーブルを表示します。
show vrf	システムで定義されている仮想ルータを表示します。

show ipv6 routers

オンラインルータから受信したIPv6ルータアドバタイズメント情報を表示するには、**show ipv6 routers** コマンドを使用します。

show ipv6 routers [*if_name*]

構文の説明	<i>if_name</i>	(任意) 情報を表示する対象となる内部インターフェイスまたは外部インターフェイス名。
-------	----------------	--

コマンド履歴	リリース	変更内容
	6.1	このコマンドが導入されました。

使用上のガイドライン インターフェイス名が指定されていない場合は、すべてのIPv6インターフェイスの情報が表示されます。インターフェイス名を指定すると、指定されたインターフェイスに関する情報が表示されます。

例

次に、インターフェイス名を指定せずに入力した **show ipv6 routers** コマンドの出力例を示します。

```
> 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
```

関連コマンド	Command	説明
	ipv6 route	IPv6 ルーティング テーブルにスタティック エントリを追加します。

show ipv6 traffic

IPv6 トラフィックに関する統計情報を表示するには、**show ipv6 traffic** コマンドを使用します。

show ipv6 traffic

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

使用上のガイドライン

clear ipv6 traffic コマンドを使用して、トラフィックカウンタをクリアします。

例

次に、**show ipv6 traffic** コマンドの出力例を示します。

```
> 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
  unreachable: 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
        unreachable: 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
```

関連コマンド

Command	説明
clear ipv6 traffic	IPv6 トラフィック カウンタをクリアします。

show isakmp sa

IKE ランタイム SA データベースを表示するには、**show isakmp sa** コマンドを使用します。

show isakmp sa [detail]

構文の説明	detail	SA データベースに関する詳細出力を表示します。
コマンド履歴	リリース	変更内容
	6.1	このコマンドが導入されました。

例

次に、SA データベースに関する詳細情報を表示する例を示します。

> **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

```

関連コマンド	Command	説明
	clear isakmp sa	IKE ランタイム SA データベースをクリアします。
	show running-config isakmp	アクティブな ISAKMP コンフィギュレーションをすべて表示します。

show isakmp stats

ランタイム統計情報を表示するには、**show isakmp stats** コマンドを使用します。

Threat Defense

show isakmp stats

コマンド履歴	リリース	変更内容
	6.1	このコマンドが導入されました。

使用上のガイドライン

各カウンタは、関連する cikePhase1GW カウンタにマッピングします。これらのカウンタの詳細については、「[CISCO-IPSEC-FLOW-MONITOR-MIB.my](#)」を参照してください。

- Active/Standby Tunnels : cikePhase1GWActiveTunnels
- Previous Tunnels : cikePhase1GWPreviousTunnels
- In Octets : cikePhase1GWInOctets
- In Packets : cikePhase1GWInPkts
- In Drop Packets : cikePhase1GWInDropPkts
- In Notifys : cikePhase1GWInNotifys
- In P2 Exchanges : cikePhase1GWInP2Exchgs
- In P2 Exchange Invalids : cikePhase1GWInP2ExchgInvalids
- In P2 Exchange Rejects : cikePhase1GWInP2ExchgRejects
- In P2 Sa Delete Requests : cikePhase1GWInP2SaDelRequests
- Out Octets : cikePhase1GWOutOctets
- Out Packets : cikePhase1GWOutPkts
- Out Drop Packets : cikePhase1GWOutDropPkts
- Out Notifys : cikePhase1GWOutNotifys
- Out P2 Exchanges : cikePhase1GWOutP2Exchgs
- Out P2 Exchange Invalids : cikePhase1GWOutP2ExchgInvalids
- Out P2 Exchange Rejects : cikePhase1GWOutP2ExchgRejects
- Out P2 Sa Delete Requests : cikePhase1GWOutP2SaDelRequests
- Initiator Tunnels : cikePhase1GWInitTunnels
- Initiator Fails : cikePhase1GWInitTunnelFails

- Responder Fails : cikePhase1GWRespTunnelFails
- System Capacity Fails : cikePhase1GWSysCapFails
- Auth Fails : cikePhase1GWAauthFails
- Decrypt Fails : cikePhase1GWDecryptFails
- Hash Valid Fails : cikePhase1GWHashValidFails
- No Sa Fails : cikePhase1GWNoSaFails

例

次の例では ISAKMP 統計情報が表示されます。

```
> 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
```

関連コマンド

Command	説明
clear isakmp sa	IKE ランタイム SA データベースをクリアします。
show running-config isakmp	アクティブな ISAKMP コンフィギュレーションをすべて表示します。

show isis database

IS-IS リンクステートデータベースを表示するには、**show isis database** コマンドを使用します。

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

構文の説明

level-1	(任意) レベル 1 の IS-IS リンクステート データベースを示します。
level-2	(任意) レベル 2 の IS-IS リンクステート データベースを示します。
ip	(オプション) IPv4 アドレスファミリの IS-IS リンクステート データベースを表示します。
ipv6	(オプション) IPv6 アドレスファミリの IS-IS リンクステート データベースを表示します。
detail	(任意) 各リンクステートパケット (LSP) のコンテンツを表示します。
verbose	(オプション) IS-IS データベースに関する追加情報を表示します。
topology base	(オプション) MTR トポロジを表示します。
unicast	(オプション) ユニキャストアドレスファミリを表示します。

コマンド履歴

リリース	変更内容
6.3	このコマンドが導入されました。

使用上のガイドライン 次の表では、このコマンドの出力について説明されています。

表 9: IS-IS データベース出力のフィールド

フィールド	説明
LSPID	<p>リンクステートパケット (LSP) ID。最初の 6 オクテットは、LSP を生成したルータのシステム ID を形成します。</p> <p>次のオクテットは疑似ノード ID です。このバイトが非ゼロの場合、LSP はシステムからのリンクを記述します。ゼロの場合は、LSP は、いわゆる非疑似ノード LSP です。このメカニズムは、Open Shortest Path First (OSPF) プロトコルのルータ リンクステート アドバタイズメント (LSA) に類似しています。LSP は、送信元ルータの状態を記述します。</p> <p>各 LAN に対して、その LAN の指定ルータは疑似ノード LSP の作成およびフラッドを行い、その LAN に接続されたすべてのシステムを記述します。</p> <p>最後のオクテットは LSP 番号です。単一の LSP に収容可能な量を超えるデータがある場合は、LSP は複数の LSP フラグメントに分割されます。各フラグメントには、異なる LSP 番号が割り当てられます。アスタリスク (*) は、その LSP が、このコマンドの送信元のシステムによって生成されたことを示します。</p>
LSP Seq Num	他のシステムが発信元から最新情報を受信しているか判断できる、LSP のシーケンス番号。
LSP Checksum	LSP パケットのチェックサム。
LSP Holdtime	LSP が有効である時間 (秒単位)。LSP Holdtime がゼロである場合は、LSP がパージされて、すべてのルータのリンクステート データベース (LSDB) から削除されていることを示します。この値は、パージされた LSP が、完全に削除されるまでに LSDB 内に存在する時間を示します。
ATT	Attach ビット。このビットは、そのルータがレベル 2 ルータでもあるため、他のエリアに到達できることを示します。レベル 1 だけのルータ、および他のレベル 2 ルータとの接続を失ったレベル 1-2 ルータは、Attach ビットを使用して最も近いレベル 2 ルータを検出します。ルータは、最も近いレベル 2 ルータへのデフォルト ルートを示します。
P	P ビット。中継システムが修復可能なエリアパーティションであるかどうかを検出します。シスコおよび他のベンダーは、エリアパーティション修復をサポートしません。
OL	過負荷ビット。IS が混雑しているかどうかを判断します。過負荷ビットがセットされると、他のルータは、ルータを計算しているときに中継ルータとしてこのシステムを使用しません。過負荷になっているルータに直接接続された宛先のパケットだけが、このルータに送信されます。

フィールド	説明
Area Address (詳細および詳細出力のみ)。	ルータから到達可能なエリアアドレス。レベル1 LSP の場合は、送信元ルータ上で手動により設定されるエリアアドレスになります。レベル2 LSP の場合は、このルータが属するエリアのすべてのエリアアドレスになります。
NLPID (詳細および詳細出力のみ)。	ネットワーク層プロトコル ID。
Hostname (詳細および詳細出力のみ)。	ノードのホスト名。
ルータ ID (詳細および詳細出力のみ)。	ノードのトラフィック エンジニアリング ルータ ID。
IP Address (詳細および詳細出力のみ)。	インターフェイスの IPv4 アドレス。
メトリック (詳細および詳細出力のみ)。	発信元ルータとアドバタイズされるネイバー間の隣接のコストの IS-IS メトリック、またはアドバタイズするルータからアドバタイズされる宛先までにかかるコストのメトリック (IP アドレス、エンドシステム (ES)、またはコネクションレス型ネットワーク サービス (CLNS) のプレフィックスを指定できます)。
アフィニティ (詳細出力のみ)。	フラッドされているリンク属性フラグ。
Physical BW (詳細出力のみ)。	リンクの帯域幅容量 (ビット/秒)。
Reservable BW (詳細出力のみ)。	このリンクの予約可能帯域幅。
BW Unreserved (詳細出力のみ)。	予約可能帯域幅。

例

次の例は、IS-IS データベースを示しています。

```
> show isis database
```

```
IS-IS Level-1 Link State Database:
LSPID          LSP Seq Num  LSP Checksum  LSP Holdtime  ATT/P/OL
c1.00-00       0xeal9d300  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  0xfffff01   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
```

次に、IS-ISデータベースの詳細な出力例を示します。詳細出力には、各LSPの内容が表示されます。

```
> 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       0xeal9d301  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
```

次に、レベル2LSPのみの詳細な出力例を示します。エリアアドレス39.0001は、ルータが存在するエリアのアドレスです。

```
> 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

```

次に、詳細出力の例を示します。

> **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

```

関連コマンド

Command	説明
clear isis	IS-IS データ構造をクリアします。
show clns	CLNS 固有の情報を表示します。
show route isis	IS-IS ルートを表示します。

show isis hostname

IS-IS ルータの、ルータ名とシステム ID のマッピングテーブルエントリを表示するには、**show isis hostname** コマンドを使用します。

show isis hostname

コマンド履歴

リリース

変更内容

6.3

このコマンドが導入されました。

使用上のガイドライン

IS-IS ルーティングドメインでは、各ルータはシステム ID により表されます。システム ID は、IS-IS ルータごと構成されている Network Entity Title (NET) の一部です。たとえば、NET 49.0001.0023.0003.000a.00 が設定されているルータのシステム ID が 0023.0003.000a であるとなります。ネットワーク管理者にとって、ルータでのメンテナンスやトラブルシューティングの間、ルータ名とシステム ID の対応を覚えているのは難しいことです。**show isis hostname** コマンドを入力すると、ルータ名とシステム ID のマッピングテーブルに含まれるエントリが表示されます。

例

次の例では、ダイナミック ホスト マッピング テーブルを表示します。ダイナミック ホスト マッピング テーブルは、cisco 脅威に対する防御、c2、c3 および routerA という名前のローカルルータの、ルータ名とシステム ID のマッピング テーブルエントリを表示します。このテーブルは、c3 がレベル-1 ルータであり、そのホスト名がレベル-1 (L1) リンクステートプロトコル (LSP) によりアドバタイズされることも示します。c2 はレベル-2 ルータであり、そのホスト名は L2 LSP によりアドバタイズされます。cisco 脅威に対する防御のレベルの下に表示される * 記号は、これがシステムのルータ名とシステム ID のマッピング情報であることを示します。

```
> 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
```

関連コマンド

Command	説明
clear isis	IS-IS データ構造をクリアします。
show clns	CLNS 固有の情報を表示します。
show route isis	IS-IS ルートを表示します。

show isis lsp-log

新しい LSP をトリガーしたインターフェイスのレベル 1 およびレベル 2 の IS-IS リンクステートパケット (LSP) のログを表示するには、**show isis lsp-log** コマンドを使用します。

show isis lsp-log

コマンド履歴	リリース	変更内容
	6.3	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用して、新しい LSP をトリガーしたインターフェイスのレベル 1 およびレベル 2 の IS-IS リンクステートパケット (LSP) のログを表示します。出力には次の情報が含まれます。

- [When] : LSP が生成されてからの経過時間。
- [Count] : 現時点で発生しているイベントの数。
- [Interface] : LSP を再生成したインターフェイス。
- [Triggers] : LSP のフラッディングをトリガーしたイベント。次のような、LSP に可能なトリガー。
 - AREASET : アクティブ エリア セットが変更されました。
 - ATTACHFLAG : Attach ビットの状態が変更されました。
 - CLEAR : ある形式の手動の clear コマンドが送信されました。
 - CONFIG : 任意のコンフィギュレーションが変更されました。
 - DELADJ : 隣接関係がダウンしました。
 - DIS : DIS が変更されたか、または疑似ノードが変更されました。
 - ES : エンド システムの隣接関係が変更されました。
 - HIPPIITY : LSPDB 過負荷ビットの状態が変更されました。
 - IF_DOWN : 新しい LSP が必要です。
 - IP_DEF_ORIG : 元のデフォルト情報が変更されました。
 - IPDOWN : 直接接続されている IP プレフィックスがダウンしました。
 - IP_EXTERNAL : 再配布された IP ルートが現れたか、または失われました。
 - IPIA : エリア間 IP ルートが現れたか、または失われました。
 - IPUP : 直接接続されている IP プレフィックスが起動しました。
 - NEWADJ : 新しい隣接関係が現れました。

- REDIST : 再配信されたレベル-2 CLNS ルートが変更されました。
- RRR_INFO : RRR 帯域幅リソース情報。

例

次に、**show isis lsp-log** コマンドの出力例を示します。

> **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          subint         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          subint         AREASET IPIA

```

関連コマンド

Command	説明
clear isis	IS-IS データ構造をクリアします。
show clns	CLNS 固有の情報を表示します。
show route isis	IS-IS ルートを表示します。

show isis neighbors

IS-IS ネイバーに関する情報を表示するには、**show isis neighbors** コマンドを使用します。

show isis neighbors [detail]

構文の説明	detail	(任意) IS-IS ネイバーの詳細情報を表示します。
コマンド履歴	リリース	変更内容
	6.3	このコマンドが導入されました。

使用上のガイドライン 次の表で、IS-IS ネイバー情報について説明します。

表 10: IS-IS ネイバー情報

フィールド	説明
System Id	エリア内のシステムを識別する 6 バイト値。
タイプ	レベルのタイプ。IS-IS ネイバーがレベル 1、レベル-1-2、またはレベル 2 のルータのいずれであるかを示します。
インターフェイス	システムが学習されたインターフェイス。
IP Address	ネイバー ルータの IP アドレス。
状態	IS-IS ネイバーの状態がアップかダウンか示します。
Holdtime	リンクステート パケット (LSP) のホールド時間。LSP が有効である時間 (秒単位)。
Circuit Id	IS-IS 近接ルータがどのようにローカル ルータに接続されているかを示す、IS-IS 近接ルータのポート ロケーション。
Area Address(es)	ルータから到達可能なエリアアドレス。レベル 1 LSP の場合は、送信元ルータ上で手動により設定されるエリアアドレスになります。レベル 2 LSP の場合は、このルータが属するエリアのすべてのエリアアドレスになります。
SNPA	サブネットワーク ポイント オブ アタッチメント。これはデータ リンクアドレスです。
State Changed	状態変更の時刻。
LAN Priority	LAN のプライオリティ。

フィールド	説明
Remote TID	ネイバルルータトポロジ ID。
Local TID	ローカルルータトポロジ ID。

例

次の例は、基本的な IS-IS ネイバー情報を示しています。

> 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
```

次の例は、詳細な IS-IS ネイバー情報を示しています。

> 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
```

関連コマンド

Command	説明
clear isis	IS-IS データ構造をクリアします。
show clns	CLNS 固有の情報を表示します。
show route isis	IS-IS ルートを表示します。

show isis rib

特定のルートのパス、またはIPローカルルーティング情報ベース（RIB）に格納されているメジャーネットワーク下の全ルートのパスを表示するには、**show isis rib** コマンドを使用します。

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

構文の説明	
*	(オプション) すべての IS-IS アドレス ファミリを表示します。
ip	(オプション) IPv4 アドレス ファミリを表示します。
ipv6	(オプション) IPv6 アドレス ファミリを表示します。
level-1	(オプション) レベル 1 再配布 RIB を表示します。
level-2	(オプション) レベル 2 再配布 RIB を表示します。
<i>network_ip</i> [<i>mask</i>]	(オプション) ネットワークの RIB 情報を表示します。
redistribution	(オプション) IS-IS IP 再配布 RIB 情報を表示します。
unicast	(オプション) ユニキャストアドレス ファミリを表示します。

コマンド履歴	リリース	変更内容
	6.3	このコマンドが導入されました。

使用上のガイドライン このコマンドを使用して、IP グローバル RIB 内に存在する IP プレフィックスアップデートも IS-IS ローカル RIB 内で更新されたことを確認します。

例

次に、IS-IS ローカル RIB 内に格納されているすべてのルートを表示する例を示します。

```
> 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]
```

次に、IS-IS ローカル RIB 内に格納されている、IP アドレスが 10.3.2.0 のメジャーネットワーク 10.0.0.0 下の全ルータを表示する例を示します。

```
> 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]
```

次に、IS-IS ローカル RIB 内に格納されている、IP アドレスとマスクが 10.3.2.0 255.255.255.0 のネットワーク下の全ルータを表示する例を示します。

```
> 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]
```

関連コマンド

Command	説明
clear isis	IS-IS データ構造をクリアします。
show clns	CLNS 固有の情報を表示します。
show route isis	IS-IS ルートを表示します。

show isis spf-log

ルータがフル最短パス優先（SPF）計算を実行した頻度と理由を表示するには、**show isis spf-log** コマンドを使用します。

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

構文の説明	
*	(オプション) すべての IS-IS アドレス ファミリを表示します。
ip	(オプション) IPv4 アドレス ファミリを表示します。
ipv6	(オプション) IPv6 アドレス ファミリを表示します。
unicast	(オプション) ユニキャストアドレス ファミリを表示します。

コマンド履歴	リリース	変更内容
	6.3	このコマンドが導入されました。

使用上のガイドライン このコマンドは、ルータがフル最短パス優先（SPF）計算を実行した頻度と理由を表示します。次の表で、出力のフィールドについて説明します。

フィールド	説明
When	今からどれくらい前（時間：分：秒）にフル SPF 計算が発生したか。直近 20 回分の発生内容が記録されます。
持続時間	今回の SPF 実行を完了させるために必要なミリ秒数。経過時間は実経過時間であり、CPU 時間ではありません。
ノード	今回の SPF 実行で計算されるトポロジを生成するルータおよび疑似ノード（LAN）の数。
Count	今回の SPF 実行をトリガーしたイベントの数。トポロジが変更されると、複数のリンクステート パケット（LSP）が短時間で受信されます。ルータは、フル SPF を実行するまでに 5 秒待機し、すべての新しい情報を保持できるようにします。この数は、ルータがフル SPF を実行するまで 5 秒待機する間に発生した（新しい LSP の受信のような）イベントの数を意味します。
First Trigger LSP	新しい LSP の到着でフル SPF 計算がトリガーされると、常にルータは LSP ID を保存します。LSP ID は、エリア内でルーティングが不安定である原因の手掛かりを提供できます。複数の LSP が 1 つの SPF を実行すると、最後に受信された LSP の LSP ID だけが記憶されません。

フィールド	説明
Triggers	フル SPF 計算をトリガーしたすべての理由のリスト。トリガーに関する次の表を参照してください。

次の表では、考えられるトリガーについて説明しています。

Trigger	説明
ATTACHFLAG	このルータは、レベル 2 バックボーンに接続されているか、または、レベル 2 バックボーンとの接続を失ったばかりです。
ADMINDIST	このルータの IS-IS プロセスに、別のアドミニストレーティブディスタンスが設定されました。
AREASET	このエリアの学習されたエリアアドレスの設定が変更されました。
BACKUPOVFL	IP プレフィックスが失われました。ルータはそのプレフィックスに到達するために別の方法があることを知っていますが、そのバックアップルートは保存していません。別のルートを見つける唯一の方法は、フル SPF の実行です。
DBCHANGED	このルータで、 clear isis * コマンドが発行されました。
IPBACKUP	IP ルートが失われましたが、これは IS-IS を介してではなく、優れたアドミニストレーティブディスタンスを持つ別のプロトコルを介して学習されました。IS-IS はフル SPF を実行し、失われた IP プレフィックスまでの IS-IS ルートをインストールします。
IPQUERY	このルータで、 clear ip route コマンドが発行されました。
LSPEXPIRED	リンクステートデータベース (LSDB) 内のいくつかの LSP の期限が切れました。
LSPHEADER	LSP ヘッダー内の ATT/P/OL ビットまたは IS タイプが変更されました。
NEWADJ	このルータが、別のルータとの新しい隣接関係を作成しました。
NEWAREA	このルータに、新しいエリアが (Network Entity Title [NET] を介して) 設定されました。
NEWLEVEL	このルータに、(IS タイプを介して) 新しいレベルが設定されました。
NEWLSP	トポロジ内に新しいルータまたは疑似ノードが現れました。
NEWMETRIC	このルータのインターフェイスに、新しいメトリックが設定されました。

Trigger	説明
NEWSYSID	このルータに、（NET を介して）新しいシステム ID が設定されました。
PERIODIC	ルータは通常、15 秒ごとの間隔でフル SPF 計算を実行します。
RTCLEARED	このルータで、 clear clns route コマンドが発行されました。
TLVCODE	TLV コードの不一致であり、最新バージョンの LSP に異なる TLV が含まれていることを示します。
TLVCONTENT	TLV のコンテンツが変更されました。これは通常、エリア内で隣接関係がアップまたはダウンしたことを示します。「First trigger LSP」カラムは、不安定な状態が発生した可能性のある場所を示します。

例

次に、**show isis ipv6 spf-log** コマンドの出力例を示します。

```
> 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

```

関連コマンド

Command	説明
clear isis	IS-IS データ構造をクリアします。
show clns	CLNS 固有の情報を表示します。
show route isis	IS-IS ルートを表示します。

show isis topology

すべてのエリア内の接続された全ルータのリストを表示するには、**show isis topology** コマンドを使用します。

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

構文の説明

*	(オプション) すべての IS-IS アドレス ファミリを表示します。
ip	(オプション) IPv4 アドレス ファミリを表示します。
ipv6	(オプション) IPv6 アドレス ファミリを表示します。
level-1	(オプション) レベル 1 再配布 RIB を表示します。
level-2	(オプション) レベル 2 再配布 RIB を表示します。
unicast	(オプション) ユニキャスト アドレス ファミリを表示します。

コマンド履歴

リリース	変更内容
6.3	このコマンドが導入されました。

使用上のガイドライン

show isis topology コマンドを使用すると、すべてのエリア内の全ルータの存在およびルータ間の接続状態を確認できます。次の表でフィールドを説明します。

フィールド	説明
System Id	エリア内のシステムを識別する 6 バイト値。
メトリック	送信側ルータとアドバタイズされたネイバー間の隣接関係のコスト用の IS-IS メトリック、またはアドバタイズ元のルータからアドバタイズ対象の宛先 (IP アドレス、エンドシステム [ES]、または CLNS プレフィックス) に到達するコスト用のメトリック。
Next-Hop	ネクスト ホップ ルータのアドレス。
インターフェイス	システムが学習されたインターフェイス。
SNPA	サブネットワーク ポイント オブ アタッチメント。これはデータ リンク アドレスです。

例

次に、**show isis topology** コマンドの出力例を示します。

```
> 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

関連コマンド

Command	説明
clear isis	IS-IS データ構造をクリアします。
show clns	CLNS 固有の情報を表示します。
show route isis	IS-IS ルートを表示します。

翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。