show j - show o

show jumbo-frame reservation

要查看是否为所有接口启用巨帧，请使用 **show jumbo-frame reservation** 命令。

show jumbo-frame reservation

Command History

版本	修改
6.1	引入了此命令。

使用指南

只要将任何接口的 MTU 增加到 1500 以上，就会启用巨帧预留。当您将所有 MTU 恢复为 1500 或更低时，它会自动禁用。

示例

以下是启用巨帧支持时 **show jumbo-frame reservation** 命令的输出示例：

```
> show jumbo-frame-reservation
Jumbo Frame Support is currently enabled
```

show kernel

要显示 Linux brctl 实用程序提供的可用于调试的信息，请使用 **show kernel** 命令。

show kernel {**process** | **bridge** [**mac-address** *bridge_name*] | **cgroup-controller** [**cpu** | **cpuset** | **memory**] [**detail**] | **ifconfig** | **module**}

Syntax Description

bridge [**mac-address** *bridge_name*]	显示Linux tap网桥、其成员端口以及在每个端口获知的可用于调试的MAC地址（包括远程 MAC 地址）。可以使用 **mac-address** 关键字查看有关特定网桥的 MAC 地址详细信息。使用不带关键字的命令查看可用的网桥名称，例如 br0。
cgroup-controller [**cpu** | **cpuset** | **memory**] [**detail**]	显示 cgroup-controller 统计信息。 **cpu**、 **cpuset** 和 **memory** 关键字允许您根据要求过滤 cgroup-controller 统计信息。使用 detail 关键字可查看额外信息。
ifconfig	显示 tap 和网桥接口统计信息。
module	显示已安装并且正在运行的模块。
process	显示设备上运行的活动内核进程的当前状态。

Command History

版本	修改
6.1	引入了此命令。

使用指南

此命令显示内核中运行的各个进程的统计信息。

示例

以下示例显示 **show kernel process** 命令的输出：

```
> show kernel process
PID PPID PRI NI      VSIZE      RSS      WCHAN STAT  RUNTIME COMMAND
  1    0  16  0     991232      268 3725684979    S       78 init
  2    1  34 19          0        0 3725694381    S        0 ksoftirqd/0
  3    1  10 -5          0        0 3725736671    S        0 events/0
  4    1  20 -5          0        0 3725736671    S        0 khelper
  5    1  20 -5          0        0 3725736671    S        0 kthread
  7    5  10 -5          0        0 3725736671    S        0 kblockd/0
  8    5  20 -5          0        0 3726794334    S        0 kseriod
 66    5  20  0          0        0 3725811768    S        0 pdflush
 67    5  15  0          0        0 3725811768    S        0 pdflush
 68    1  15  0          0        0 3725824451    S        2 kswapd0
 69    5  20 -5          0        0 3725736671    S        0 aio/0
171    1  16  0     991232       80 3725684979    S        0 init
172  171  19  0     983040      268 3725684979    S        0 rcS
201  172  21  0    1351680      344 3725712932    S        0 lina_monitor
202  201  16  0 1017602048   899932 3725716348    S      212 lina
203  202  16  0 1017602048   899932          0    S        0 lina
```

```
204  203  15  0 1017602048   899932          0    S        0 lina
205  203  15  0 1017602048   899932 3725712932    S        6 lina
206  203  25  0 1017602048   899932          0    R 13069390 lina
>
```

下表对每个字段进行了说明。

表 *1: show kernel process* 字段

字段	Description
PID	进程 ID。
PPID	父进程 ID。
PRI	进程的优先级。
Nexus Dashboard Insights	友好值，用于优先级计算。值范围为 19（最友好）到 -19（对其他进程不友好）。
VSIZE	虚拟内存大小（以字节为单位）。
RSS	进程的驻留集大小（以千字节为单位）。
WCHAN	进程处于等待状态时所处的通道。
STAT	进程的状态： • R - 正在运行 • S - 在可中断等待状态下休眠 • D - 在不可中断磁盘休眠状态下等待 • Z - 僵停 • T - 跟踪或停止（基于信号） • P - 分页
运行时间	进程在用户模式和内核模式中已计划的节拍数。运行时是 utime 和 stime 的总和。
COMMAND	进程名。

以下示例显示 **show kernel module** 命令的输出：

```
> show kernel module

Module                  Size  Used by    Tainted: P
cpp_base              861808  2
kvm_intel              44104  8
kvm                   174304  1 kvm_intel
msrif                   4180  0
```

```
tscsync                 3852  0
```

以下示例显示 **show kernel ifconfig** 命令的输出：

```
> show kernel ifconfig

br0       Link encap:Ethernet  HWaddr 42:9E:B8:6C:1F:23
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:43 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1708 (1.6 KiB)  TX bytes:0 (0.0 B)

br1       Link encap:Ethernet  HWaddr 6A:03:EC:BA:89:26
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.255.255.255
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

tap0      Link encap:Ethernet  HWaddr 6A:0C:48:32:FE:F4
          inet addr:127.0.2.2  Bcast:127.255.255.255  Mask:255.0.0.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:148 errors:0 dropped:0 overruns:0 frame:0
          TX packets:186 errors:0 dropped:13 overruns:0 carrier:0
          collisions:0 txqueuelen:500
          RX bytes:10320 (10.0 KiB)  TX bytes:12452 (12.1 KiB)

tap1      Link encap:Ethernet  HWaddr 8E:E7:61:CF:E9:BD
          UP BROADCAST RUNNING PROMISC MULTICAST  MTU:1500  Metric:1
          RX packets:259 errors:0 dropped:0 overruns:0 frame:0
          TX packets:187 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:500
          RX bytes:19368 (18.9 KiB)  TX bytes:14638 (14.2 KiB)

tap2      Link encap:Ethernet  HWaddr 6A:03:EC:BA:89:26
          UP BROADCAST RUNNING PROMISC MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:500
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

tap3      Link encap:Ethernet  HWaddr 42:9E:B8:6C:1F:23
          UP BROADCAST RUNNING PROMISC MULTICAST  MTU:1500  Metric:1
          RX packets:187 errors:0 dropped:0 overruns:0 frame:0
          TX packets:256 errors:0 dropped:3 overruns:0 carrier:0
          collisions:0 txqueuelen:500
          RX bytes:14638 (14.2 KiB)  TX bytes:19202 (18.7 KiB)

tap4      Link encap:Ethernet  HWaddr 6A:5C:60:BC:9C:ED
          UP BROADCAST RUNNING PROMISC MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:500
```

```
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

以下示例显示 **show kernel bridge** 命令的输出：

```
> show kernel bridge

bridge name     bridge id               STP enabled     interfaces
br0             8000.000000040001       no              tap1
                                                        tap3
br1             8000.84b261b192bd       no              tap2
                                                        tap4
                                                        tap5
```

以下示例显示 **show kernel bridge mac-address** 命令的输出：

```
> show kernel bridge mac-address br1

port no    mac addr       is local?   ageing timer
 1    00:21:d8:cb:dc:f7    no          12.93
 3    00:22:bd:d8:7d:da    no          12.93
 2    26:d2:9f:51:a4:90    yes          0.00
 1    4e:a4:e0:73:1f:ab    yes          0.00
 3    52:04:38:3d:79:c0    yes          0.00
```

Related Commands

命令	Description
show module	显示有关设备中安装的模块的信息。

show lacp

要显示流量统计信息、系统标识符和邻居详细信息等 EtherChannel LACP 信息，请输入此命令。

show lacp {*channel_group_number* {**counters** | **internal** [**detail**] | **neighbor** [**detail**]} | **neighbor** [**detail**] | **sys-id**}

Syntax Description

channel_group_number	指定 EtherChannel 通道组编号（介于 1 到 48 之间）并且仅显示有关此通道组的信息。
counters	显示用于已发送和接收的 LACPDU 和标记数量的计数器。
detail	显示项目的其他详细信息。
internal	显示内部信息。
neighbor	显示邻居信息。
sys-id	Shows the LACP system ID.

Command History

版本	修改
6.1	引入了此命令。

示例

以下是 **show lacp sys-id** 命令的输出示例：

```
> show lacp sys-id
32768,001c.c4e5.cfee
```

以下是 **show lacp counters** 命令的输出示例：

```
> show lacp counters

              LACPDUs         Marker      Marker Response    LACPDUs
Port       Sent   Recv     Sent   Recv     Sent     Recv      Pkts Err
--------------------------------------------------------------------------
Channel group: 1
Gi3/1      736    728      0      0        0        0         0
Gi3/2      739    730      0      0        0        0         0
Gi3/3      739    732      0      0        0        0         0
```

以下是 **show lacp internal** 命令的输出示例：

```
> show lacp internal

Flags:  S - Device is requesting Slow LACPDUs
        F - Device is requesting Fast LACPDUs
```

```
        A - Device is in Active mode       P - Device is in Passive mode

Channel group 1
                            LACP port     Admin     Oper    Port        Port
Port      Flags   State     Priority      Key       Key     Number      State
-------------------------------------------------------------------------------
Gi3/1     SA      bndl      32768         0x1       0x1     0x302       0x3d
Gi3/2     SA      bndl      32768         0x1       0x1     0x303       0x3d
Gi3/3     SA      bndl      32768         0x1       0x1     0x304       0x3d
```

以下是 **show lacp neighbor** 命令的输出示例：

```
> show lacp neighbor

Flags:  S - Device is requesting Slow LACPDUs
        F - Device is requesting Fast LACPDUs
        A - Device is in Active mode       P - Device is in Passive mode

Channel group 1 neighbors

Partner's information:
          Partner Partner    LACP Partner  Partner   Partner  Partner     Partner
Port      Flags   State      Port Priority Admin Key Oper Key Port Number Port State
--------------------------------------------------------------------------------
Gi3/1     SA      bndl       32768         0x0       0x1      0x306       0x3d
Gi3/2     SA      bndl       32768         0x0       0x1      0x303       0x3d
Gi3/3     SA      bndl       32768         0x0       0x1      0x302       0x3d
```

Related Commands

命令	Description
show port-channel	在详细的单行摘要表单中显示EtherChannel信息。此命令还显示端口和端口信道信息。
show port-channel load-balance	显示端口通道负载均衡信息以及为给定的一组参数选择的散列结果和成员接口。

show lacp cluster

要显示 cLACP 系统 MAC 和 ID，请使用 **show lacp cluster** 命令

show lacp cluster {**system-mac** | **system-id**}

Syntax Description

system-mac	显示系统 ID 以及它是自动生成还是手动输入的。
system-id	显示系统 ID 和优先级。

Command History

版本	修改
6.1	引入了此命令。

示例

以下是 **show lacp cluster system-mac** 命令的输出示例：

```
> show lacp cluster system-mac
lacp cluster system MAC is automatically generated: a300.010a.010a.
```

以下是 **show lacp cluster system-id** 命令的输出示例：

```
> show lacp cluster system-id
5    ,a300.010a.010a
```

show last-upgrade status

要显示有关上次系统软件升级的状态的信息，请使用 **show last-upgrade status** 命令。

show last-upgrade status

Command History

版本	修改
6.7	引入了此命令。

示例

以下示例显示上次升级成功。在实际输出中，xy0 将替换为实际版本号。

```
> show last-upgrade status
Upgrade from 6.7.0 to x.y.0 was successful.
Time started: Tue Dec  3 23:50:31 UTC 2020
```

以下示例显示上次升级已取消。在实际输出中，xy0 将替换为实际版本号。

```
> show last-upgrade status
Upgrade from 6.7.0 to x.y.0 failed.
Time started: Tue Dec  3 23:50:31 UTC 2020
Cancel Upgrade was successful.
```

Related Commands

命令	Description
show upgrade	显示有关当前系统软件升级的信息。
upgrade	取消、恢复或重试系统软件升级。

show lisp eid

要查看 EID 表，请使用 **show lisp eid** 命令。

show lisp eid ［**site-id** *ID*］

Syntax Description

site-id *id*	仅查看特定站点的 EID。

Command History

版本	修改
6.1	引入了此命令。

使用指南

设备维护着一个将 EID 和站点 ID 相关联的 EID 表。

示例

以下是 **show lisp eid** 命令的输出示例：

```
> show lisp eid
LISP EID       Site ID
10.44.33.105        2
10.44.33.201        2
192.168.11.1        4
192.168.11.2        4
```

Related Commands

命令	Description
clear cluster info flow-mobility counters	清除流移动性计数器。
clear lisp eid	从 ASA EID 表中删除 EID。
show cluster info flow-mobility counters	显示流移动性计数器。
show conn	显示受 LISP 流移动性影响的流量。
show service-policy	显示服务策略。

show lldp

要显示接口的链路层发现协议 (LLDP) 状态，请使用 **show lldp** 命令。

注释 LLDP 仅受 Firepower 1100 支持

show lldp { **neighbors** | **statistics** | **status** } *interface_id*

Syntax Description

interface_id	指定接口 ID。
neighbors	显示是否已建立 LLDP 邻居关系。
statistics	显示 LLDP 统计信息。
status	显示是否已启用 LLDP。

Command History

版本	修改
7.1	引入了此命令。

使用指南

如果 LLDP 处于活动状态，则 **通过** 字段显示；如果 LLDP 已禁用或不起作用，则显示未知。

示例

以下是 **show lldp neighbors** 命令的输出示例：

```
> show lldp neighbors

------------------------------------------------------------------------------
LLDP neighbors:
------------------------------------------------------------------------------
Interface: lldp-Eth1_6, via: LLDP, RID: 1, Time: 0 day, 00:00:18
  Chassis:
    ChassisID: mac 8c:60:4f:58:c1:ac
    SysName: ruintpo
    SysDescr: Cisco Nexus Operating System (NX OS) Software 7.0(1)N1(1)
 TAC support: http://www.cisco.com /tac
 Copyright (c) 2002-2014, Cisco Systems, Inc. All rights reserved.
    MgmtIP: 10.225.126.91
    Capability: Bridge, on
  Port:
    PortID: local Eth1/37
    PortDescr: Ethernet1/37
    TTL: 30
------------------------------------------------------------------------------
```

以下是 **show lldp statistics** 命令的输出示例：

```
> show lldp statistics interface Ethernet 1/6
------------------------------------------------------------------------------
LLDP statistics:
------------------------------------------------------------------------------
Interface: lldp-Eth1_6
  Transmitted: 115
  Received: 116
  Discarded: 0
  Unrecognized: 0
  Ageout: 0
  Inserted: 0
  Deleted: 0
------------------------------------------------------------------------------
```

以下是 **show lldp status** 命令的输出示例：

```
> show lldp status interface Ethernet 1/6
------------------------------------------------------------------------------
LLDP interfaces:
------------------------------------------------------------------------------
Interface: lldp-Eth1_6, via: unknown, Time: 18795 days, 05:38:39
  Chassis:
    ChassisID: mac 42:8f:14:a8:2f:c5
    SysName: firepower
    SysDescr: Cisco Firepower 1150 Threat Defense 7.1.0 1558
    MgmtIP: 127.128.254.1
    MgmtIP: fd00:0:0:1::3
    Capability: Bridge, on
    Capability: Router, off
    Capability: Wlan , off
    Capability: Station, off
  Port:
    PortID: mac 34:12:78:56:01:03
    PortDescr: Ethernet1/6
    TTL: 120
------------------------------------------------------------------------------
```

Related Commands

命令	Description
show interface	显示接口统计信息。

show local-host

要显示本地主机的网络状态，请使用 **show local-host** 命令。

show local-host ［*hostname* | *ip_address*］［**detail**］［**all**］［**brief**］［**connection** {**sctp** | **tcp** | **udp** | **embryonic**} *start*［*-end*］］［**zone**］

Syntax Description

all	（已弃用） 包括连接到设备和从设备连接的本地主机。
brief	（可选）显示有关本地主机的简要信息。
connection {**sctp** | **tcp** | **udp** | **embryonic**} *start*[*-end*]	（已弃用） 根据连接的数量和类型应用过滤器：初期、TCP、UDP 或 SCTP。起始编号表示该类型的最小连接数。包括 -end 数字以指定范围，例如 10-100。这些过滤器可以单独使用也可以联合使用。
detail	（可选）显示本地主机信息的详细网络状态，包括有关活动 xlate 和网络连接的详细信息。
hostname | *ip_address*	（可选）指定本地主机名或 IPv4/IPv6 地址。
zone	（可选）指定每个区域或内联集的本地主机。

Command History

版本	修改
6.1	引入了此命令。
7.0	以下关键字已弃用： **all**、 **connection**。

使用指南

要显示本地主机的网络状态，请使用 **show local-host** 命令。对于任何将流量转发到 threat defense 设备或通过其转发流量的主机，将为其创建一个本地主机。

对于运行 7.0 及更高版本的系统，请考虑使用 **show conn address** 命令而不是此命令。

此命令可显示本地主机的转换和连接插槽。转换信息包括分配给主机的任何 PAT 端口块。

此命令还显示连接限制值。如果未设置连接限制，值将显示为 0 并且不应用限制。

发生 SYN 攻击（已配置 TCP 拦截）时， **show local-host** 命令输出将已拦截连接数包括在使用计数中。此字段通常仅显示完全开放的连接。

在 **show local-host** 命令输出中，为使用静态连接的主机配置了最大初期限制（TCP 拦截水印）时使用 **TCP embryonic count to host counter** 。此计数器显示从其他主机到该主机的初期连接总数。如果此总数超过配置的最大限制，将对到主机的新连接应用 TCP 拦截。

示例

以下是 **show local-host** 命令的输出示例：

```
> show local-host

Interface mgmt: 2 active, 2 maximum active, 0 denied
local host: <10.24.250.191>,
    SCTP flow count/limit = 0/unlimited
    TCP flow count/limit = 1/unlimited
    TCP embryonic count to host = 0
    TCP intercept watermark = unlimited
    UDP flow count/limit = 0/unlimited
local host: <10.44.64.65>,
    SCTP flow count/limit = 0/unlimited
    TCP flow count/limit = 1/unlimited
    TCP embryonic count to host = 1
    TCP intercept watermark = unlimited
    UDP flow count/limit = 5/unlimited
Interface inside: 0 active, 0 maximum active, 0 denied
Interface outside: 0 active, 0 maximum active, 0 denied
Interface any: 0 active, 0 maximum active, 0 denied
```

以下示例展示本地主机的网络状态：

```
> show local-host all

Interface outside: 1 active, 2 maximum active, 0 denied
local host: <11.0.0.4>,
SCTP flow count/limit = 0/unlimited
TCP flow count/limit = 0/unlimited
TCP embryonic count to host = 0
TCP intercept watermark = unlimited
UDP flow count/limit = 0/unlimited
Conn:
105 out 11.0.0.4 in 11.0.0.3 idle 0:01:42 bytes 4464
105 out 11.0.0.4 in 11.0.0.3 idle 0:01:44 bytes 4464
Interface inside: 1 active, 2 maximum active, 0 denied
local host: <17.3.8.2>,
SCTP flow count/limit = 0/unlimited
TCP flow count/limit = 0/unlimited
TCP embryonic count to host = 0
TCP intercept watermark = unlimited
UDP flow count/limit = 0/unlimited
Conn:
105 out 17.3.8.2 in 17.3.8.1 idle 0:01:42 bytes 4464
105 out 17.3.8.2 in 17.3.8.1 idle 0:01:44 bytes 4464
Interface NP Identity Ifc: 2 active, 4 maximum active, 0 denied
local host: <11.0.0.3>,
SCTP flow count/limit = 0/unlimited
TCP flow count/limit = 0/unlimited
TCP embryonic count to host = 0
TCP intercept watermark = unlimited
UDP flow count/limit = 0/unlimited
Conn:
105 out 11.0.0.4 in 11.0.0.3 idle 0:01:44 bytes 4464
105 out 11.0.0.4 in 11.0.0.3 idle 0:01:42 bytes 4464
local host: <17.3.8.1>,
SCTP flow count/limit = 0/unlimited
TCP flow count/limit = 0/unlimited
TCP embryonic count to host = 0
TCP intercept watermark = unlimited
UDP flow count/limit = 0/unlimited
Conn:
105 out 17.3.8.2 in 17.3.8.1 idle 0:01:44 bytes 4464
```

```
105 out 17.3.8.2 in 17.3.8.1 idle 0:01:42 bytes 4464
```

以下示例显示有关特定主机的信息，后跟该主机的详细信息。

```
> show local-host 10.1.1.91
Interface third: 0 active, 0 maximum active, 0 denied
Interface inside: 1 active, 1 maximum active, 0 denied
local host: <10.1.1.91>,
SCTP flow count/limit = 0/unlimited
TCP flow count/limit = 1/unlimited
TCP embryonic count to (from) host = 0 (0)
TCP intercept watermark = unlimited
UDP flow count/limit = 0/unlimited

Xlate:
PAT Global 192.150.49.1(1024) Local 10.1.1.91(4984)

Conn:
TCP out 192.150.49.10:21 in 10.1.1.91:4984 idle 0:00:07 bytes 75 flags UI Interface
outside: 1 active, 1 maximum active, 0 denied

> show local-host 10.1.1.91 detail
Interface third: 0 active, 0 maximum active, 0 denied
Interface inside: 1 active, 1 maximum active, 0 denied
local host: <10.1.1.91>,
SCTP flow count/limit = 0/unlimited
TCP flow count/limit = 1/unlimited
TCP embryonic count to (from) host = 0 (0)
TCP intercept watermark = unlimited
UDP flow count/limit = 0/unlimited

Xlate:
TCP PAT from inside:10.1.1.91/4984 to outside:192.150.49.1/1024 flags ri

Conn:
TCP outside:192.150.49.10/21 inside:10.1.1.91/4984 flags UI Interface outside: 1 active,
1 maximum active, 0 denied
```

以下示例展示具有至少 4 个 UDP 连接以及同时具有 1 到 10 个 TCP 连接的所有主机：

```
> show local-host connection udp 4 tcp 1-10
Interface mng: 0 active, 3 maximum active, 0 denied
Interface INSIDE: 4 active, 5 maximum active, 0 denied
local host: <10.1.1.11>,
       TCP flow count/limit = 1/unlimited TCP embryonic count to host = 0 TCP intercept
       watermark = unlimited UDP flow count/limit = 4/unlimited
Xlate:
       Global 192.168.1.24 Local 10.1.1.11 Conn: UDP out 192.168.1.10:80 in
       10.1.1.11:1730 idle 0:00:21 bytes 0 flags - UDP out 192.168.1.10:80 in
       10.1.1.11:1729 idle 0:00:22 bytes 0 flags - UDP out 192.168.1.10:80 in
       10.1.1.11:1728 idle 0:00:23 bytes 0 flags - UDP out 192.168.1.10:80 in
       10.1.1.11:1727 idle 0:00:24 bytes 0 flags - TCP out 192.168.1.10:22 in
       10.1.1.11:27337 idle 0:01:55 bytes 2641 flags UIO Interface OUTSIDE: 3 active, 5
       maximum active, 0 denied
```

Related Commands

命令	Description
clear local-host	释放通过 **show local-host** 命令显示的本地主机的网络连接。

show log-events-to-ramdisk

要显示将连接事件记录到 RAM 磁盘的状态，请使用 **show log-events-to-ramdisk** 命令。

show log-events-to-ramdisk

Command History

版本	修改
6.1	引入了此命令。

使用指南

此命令显示您是将连接事件记录到RAM磁盘还是固态驱动器(SSD)。并非所有硬件型号都支持RAM磁盘日志记录。使用 **configure log-events-to-ramdisk** 命令配置 RAM 磁盘日志记录。

示例

以下示例显示此硬件型号不支持将日志记录到 RAM 磁盘。

```
> show log-events-to-ramdisk
This command is not available on this platform.
```

Related Commands

命令	Description
configure log-events-to-ramdisk	启用或禁用将连接事件记录到 RAM 磁盘。

show logging

要显示缓冲区中的日志或其他日志记录设置，请使用 **show logging** 命令。

show logging [**message** [*syslog_id* | **all**] | **asdm** | **flow-export-syslogs** | **queue** | **setting** | **unified-client** [**statistics**]]

Syntax Description

all	（可选）显示所有系统日志消息 ID，以及它们是启用还是禁用。
asdm	（可选）此关键字不适用于 设备管理器。它与配置ASA 软件设备的ASDM 相关。
flow-export-syslogs	（可选。显示其信息也由 NetFlow 捕获的所有系统日志消息。
message [*syslog_id* | **all**]	（可选）如果不指定系统日志 ID 或全部，则此关键字显示非默认级别的消息。您还可以按 ID 显示消息，或查看有关所有系统日志消息的信息。
queue	（可选）显示系统日志消息队列。
setting	（可选）显示日志记录设置，而不显示日志记录缓冲区。
syslog_id	（可选）指定要显示的消息编号。
unified-client [**statistics**]	显示有关系统日志客户端状态的详细统计信息，包括 loggerD 服务状态、系统日志客户端注册信息、loggerD 心跳详细信息以及系统日志客户端控制/数据和错误统计信息，

Command History

版本	修改
6.1	引入了此命令。
6.3	添加了 **unified-client** [**statistics**] 关键字。

使用指南

如果启用日志记录到内部缓冲区，则不带任何关键字的 **show logging** 命令会显示当前消息缓冲区和当前设置。

show logging queue 命令允许您显示以下内容：

- 队列中的消息数量
- 队列中记录的最大消息数量
- 由于块内存无法处理而被丢弃的消息数量
- 用于陷阱和其他系统日志消息的单独队列

注释 零是可接受的已配置队列大小，表示允许最大队列大小。如果配置的队列大小为零， **show logging queue** 命令的输出将显示实际队列大小。

show logging flow-export-syslogs 命令显示以下系统日志是已启用还是已禁用。使用 Netflow 时，您可以选择禁用这些系统日志，因为它们是冗余的。

系统日志消息	Description
106015	TCP 流被拒绝，因为第一个数据包不是 SYN 数据包。
106023	被连接到接口的入口 ACL 或出口 ACL 拒绝的流。
106100	ACL 允许或拒绝的流。
302013 and 302014	TCP 连接和删除。
302015 and 302016	UDP 连接和删除。
302017 and 302018	GRE 连接和删除。
302020 and 302021	ICMP 连接和删除。
313001	发送到 threat defense 设备的 ICMP 数据包被拒绝。
313008	发送到 threat defense 设备的 ICMPv6 数据包被拒绝。
710003	连接到 threat defense 的尝试被拒绝。

示例

以下是 **show logging** 命令的输出示例：

```
> show logging
Syslog logging: enabled
    Facility: 20
    Timestamp logging: enabled
    Standby logging:disabled
    Debug-trace logging: disabled
    Console logging: level informational, 3962 messages logged
    Monitor logging: disabled
    Buffer logging: disabled
    Trap logging: level informational, facility 20, 20549 messages logged
        Logging to inside 10.2.5.3 tcp/50001 connected
    Permit-hostdown state
    History logging: disabled
    Device ID: disabled
    Mail logging: disabled
    ASDM logging: disabled
```

注释 系统日志记录的可能值包括已启用、已禁用、已禁用-屏蔽和已禁用-不屏蔽。

以下是配置了安全系统日志服务器后 **show logging** 命令的输出示例：

```
> show logging
Syslog logging: disabled
    Facility:
    Timestamp logging: disabled
    Deny Conn when Queue Full: disabled
    Console logging: level debugging, 135 messages logged
    Monitor logging: disabled
    Buffer logging: disabled
    Trap logging: list show _syslog, facility, 20, 21 messages logged
        Logging to inside 10.0.0.1 tcp/1500 SECURE
    History logging: disabled
    Device ID: disabled
    Mail logging: disabled
    ASDM logging disabled
```

以下是 **show logging queue** 命令的输出示例：

```
> show logging queue
Logging Queue length limit: 512 msg(s)
0 msg(s) discarded due to queue overflow
0 msg(s) discarded due to memory allocation failure
Current 0 msgs on queue, 0 msgs most on queue
```

以下是 **show logging message all** 命令的输出示例：

```
> show logging message all
syslog 111111: default-level alerts (enabled)
syslog 101001: default-level alerts (enabled)
syslog 101002: default-level alerts (enabled)
syslog 101003: default-level alerts (enabled)
syslog 101004: default-level alerts (enabled)
syslog 101005: default-level alerts (enabled)
syslog 102001: default-level alerts (enabled)
syslog 103001: default-level alerts (enabled)
syslog 103002: default-level alerts (enabled)
syslog 103003: default-level alerts (enabled)
syslog 103004: default-level alerts (enabled)
syslog 103005: default-level alerts (enabled)
syslog 103011: default-level alerts (enabled)
syslog 103012: default-level informational (enabled)
```

以下是 **show logging unified-client** 命令的输出示例：

```
> show logging unified-client
Log client details:
 Name : Lina
 Id : 1331
 Init time : Fri Sep 7 07:20:14 2018
 Status : Registered
```

以下是 **show logging unified-client statistics** 命令的输出示例：

```
> show logging unified-client statistics
Log client details:
  Name                                          : Lina
  Id                                            : 1331
  Init time                                     : Fri Sep  7 07:20:14 2018
  Status                                        : Registered

Loggerd service up/down statistics:
  Service status                                : Up
  Instance-id                                   : 4602
  Last service down time                        : Wed Sep 12 05:17:43 2018

Log client register/unregister statistics:
  Total register messages Tx                    : 1222
  Total unregister messages Tx                  : 0
  Last register message Tx time                 : Wed Sep 12 05:40:16 2018
  Total register-ack messages Rx                : 39
  Last register-ack Rx time                     : Wed Sep 12 05:40:17 2018
  Total configuration sent messages Tx          : 14
  Number of configuration pushes                : 38

Heartbeat statistics:
  Last heartbeat Tx time                        : Wed Sep 12 06:38:33 2018
  Last Tx seqnum                                : 10019
  Total heartbeat Tx                            : 9981

Loggerd heartbeat statistics:
  Last heartbeat Rx time                        : Wed Sep 12 06:38:36 2018
  Last hearbeat Rx seqnum                       : 701
  Total heartbeat Rx                            : 5977
  Miss count                                    : 1

Log client data messages details:
  Syslogs Tx for ngfw-management                : 6554
  Syslogs Rx for data ports                     : 0
  Syslogs Tx drops for ngfw-management          : 0

Log client Control/Data channel statistics:
  Total control messages Tx                     : 11757
  Total service messages Rx                     : 98
  Total notify messages Rx                      : 6020
  Total data messages Rx                        : 0

Log-client error statistics:
  Register messages Tx                          : 2373
  Register-ack messages Rx                      : 5921
  Configuration push Tx                         : 1
  Heartbeat Tx                                  : 0
  Control channel Rx                            : 0
  Data channel Rx                               : 0
  Syslogs Rx for data ports                     : 0
```

show mac-address-table

要显示 MAC 地址表，请使用 **show mac-address-table** 命令。

show mac-address-table [*interface_name* | **count** | **static**]

Syntax Description

count	（可选）列出动态和静态条目的总数。
interface_name	（可选）标识要查看其 MAC 地址表条目的接口名称。
static	（可选）仅列出静态条目。

Command Default

如果不指定接口，将显示所有接口 MAC 地址条目。

Command History

版本	修改
6.1	添加了此命令。
6.2	使用集成路由和桥接时，我们在路由防火墙模式下添加了支持。

示例

以下是 **show mac-address-table** 命令的输出示例：

```
> show mac-address-table
interface    mac address     type      Time Left
-----------------------------------------------------------
outside      0009.7cbe.2100  static    -
inside       0010.7cbe.6101  static    -
inside       0009.7cbe.5101  dynamic   10
```

以下是 **show mac-address-table count** 命令的输出示例：

```
> show mac-address-table count
Static     mac-address bridges (curr/max): 0/65535
Dynamic    mac-address bridges (curr/max): 103/65535
```

show mac-learn

要显示为每个接口启用还是禁用 MAC 学习，请使用 **show mac-learn** 命令。

show mac-learn

Command History

版本	修改
6.1	添加了此命令。
6.2	使用集成路由和桥接时，我们在路由防火墙模式下添加了支持。

使用指南

默认情况下，每个接口会自动获悉进入流量的MAC地址，并且系统会将对应的条目添加到MAC地址表中。您可以禁用每个接口的 MAC 学习。

示例

以下是 **show mac-learn** 命令的输出示例。

```
> show mac-learn
no mac-learn flood
interface                          mac learn
-------------------------------------------
 outside                             enabled
 inside1_2                           enabled
 inside1_3                           enabled
 inside1_4                           enabled
 inside1_5                           enabled
 inside1_6                           enabled
 inside1_7                           enabled
 inside1_8                           enabled
 diagnostic                          enabled
 inside                              enabled
```

show managers

要显示管理设备配置的当前管理器，请使用 **show managers** 命令。

show managers

Command History

版本	修改
6.1	引入了此命令。
7.2	对多个安装管理器加强支持。输出现在包括 管理中心 显示名称、标识符和管理类型（配置或分析）。

使用指南

使用 **show managers** 命令确定定义了哪个应用来管理设备配置。然后，您可以使用网络浏览器登录管理器。

使用 **configure manager add** 命令为设备配置远程管理器 管理中心时，输出会显示主机地址和注册状态。仅在注册处于待处理状态时，才会显示注册密钥和NAT ID。如果设备已注册到高可用性对，将会同时显示有关两个管理管理中心的信息。如果设备被配置为堆叠配置中的次要设备，将会同时显示有关管理管理中心和主设备的信息。

示例

以下示例显示已完成的远程管理器 管理中心 注册。

```
> show managers
Type                      : Manager
Host                      : 10.10.1.4
Display name              : 10.10.1.4
Identifier                : f7ffad78-bf16-11ec-a737-baa2f76ef602
Registration              : Completed
Management type           : Configuration
```

以下示例显示启用了本地管理器 设备管理器。

```
> show managers
Managed locally.
```

以下示例显示当前未配置管理器。必须先使用 configure manager add 或 configure manager local 启用一个，然后才能配置设备。

```
> show managers
No managers configured.
```

以下示例显示三个管理器：一个处于待处理状态，当前未在使用；一个是主配置管理器 (CDO)；一个是本地分析专用管理器。

```
> show managers
Type                        : Manager
Host                        : 1.2.3.4
Display name                : 1.2.3.4
Identifier                  : 1.2.3.4
Registration                : Pending

Type                        : Manager
Host                        : 10.10.1.4
Display name                : 10.10.1.4
Identifier                  : f7ffad78-bf16-11ec-a737-baa2f76ef602
Registration                : Completed
Management type             : Configuration

Type                        : Manager
Host                        : 10.10.2.7
Display name                : 10.10.2.7
Identifier                  : 6d3df56e-bf16-11ec-972b-b07a16ffdd03
Registration                : Completed
Management type             : Analytics
```

Related Commands

命令	Description
configure manager add	添加远程管理器 管理中心。
configure manager delete	删除当前管理器并进入无管理器模式。
configure manager local	启用本地管理器 设备管理器。

show memory

要显示可供操作系统使用的最大物理内存量和当前可用内存量的摘要，请使用 **show memory** 命令。

show memory [**api** | **app-cache** | **binsize** *size* | **caller-address** | **detail** | **region** | **system** | **top-usage** [*num*]]

Syntax Description

api	（可选）显示在系统中注册的 malloc 堆栈 API。 如果开启任意内存调试功能（即无延迟毒化器、内存记录器、内存跟踪器或内存分析器），其 API 将显示在输出中。
app-cache	（可选）按应用显示内存使用情况。
binsize *size*	（可选）显示有关为特定 bin 大小分配的数据块（内存块）的摘要信息。bin 大小来自 **show memory detail** 命令输出的“分段大小”列。
caller-address	显示与 **memory caller-address** 网络配置相关的信息。
detail	（可选）显示空闲和已分配的系统内存的详细视图。
region	显示流程映射。
system	显示设备的总内存、使用中内存和可用内存。
top-usage [*num*]	显示通过 **show memory detail** 命令分配的最大分片大小。您可以选择指定要列出的 bin 大小的数量，范围为 1-64。默认值为 10。

Command History

版本	修改
6.1	引入了此命令。
6.2.2	**show memory** 和 **show memory detail** 的输出已更改。

使用指南

show memory 命令让您显示可供操作系统使用的最大物理内存量和当前可用内存量的摘要。内存会根据需要进行分配。

还可以使用 SNMP 显示 **show memory** 命令的信息。

您可以使用带有 **show memory binsize** 命令的 **show memory detail** 输出来调试内存泄漏。

show memory detail 命令输出可分为三个部分：摘要、DMA 内存和 HEAP 内存。摘要显示内存的总体分配方式。未绑定到 DMA 或保留的内存被视为 HEAP 内存。可用内存值是 HEAP 中的未使用内存。使用中的已分配内存值是已分配的 HEAP 数量。HEAP 分配的细目随后显示在输出中。保留内存和 DMA 保留内存主要被 VPN 服务使用，也被不同的系统进程使用。

可用内存分为两部分：可用内存堆和可用内存系统。可用内存堆是glibc堆中的可用内存量。当glibc堆按需增长和缩减时，空闲堆内存的量并不指示系统中剩余的总内存。可用内存系统表示ASA可用的可用内存量。

保留内存 (DMA) 是为 DMA 池保留的内存量。内存开销是各种运行进程的 glibc 开销和进程开销。

在 **show memory detail** 命令输出中，已分配内存统计合计（字节）列中显示的值未反映实际值 (MEMPOOL_GLOBAL_SHARED POOL STATS)。

注释 MEMPOOL_GLOBAL_SHARED 在启动期间不会占用所有系统内存，但会在需要时向底层操作系统请求内存。同样，当释放大量内存时，它会将内存返还给系统。因此，MEMPOOL_GLOBAL_SHARED 的大小似乎根据需求增长和缩小。MEMPOOL_GLOBAL_SHARED 中保留了最少量的可用内存，以加快分配速度。

输出表明，先分配了大小为 49,152 的块，随后该块返回到空闲池，并分配了另一个大小为 131,072 的块。在这种情况下，您会认为可用内存减少了 131,072-49,152=81,920 字节，但实际上减少了 100,000 字节（请参阅 Free memory 行）。

```
> show memory detail
MEMPOOL_GLOBAL_SHARED POOL STATS:            MEMPOOL_GLOBAL_SHARED POOL STATS:
Non-mmapped bytes allocated =   1862270976   Non-mmapped bytes allocated =   1862270976
Number of free chunks       =           99   Number of free chunks       =          100
Number of mmapped regions   =            0   Number of mmapped regions   =            0
Mmapped bytes allocated     =            0   Mmapped bytes allocated     =            0
Max memory footprint        =   1862270976   Max memory footprint        =   1862270976
Keepcost                    =   1762019304   Keepcost                    =   1761869256
Max contiguous free mem     =   1762019304   Max contiguous free mem     =   1761869256
Allocated memory in use     =    100133944   Allocated memory in use     =    100233944
Free memory                 =   1762137032   Free memory                 =   1762037032
----- fragmented memory statistics -----     ----- fragmented memory statistics -----
 fragment size       count          total      fragment size       count          total
    (bytes)                       (bytes)         (bytes)                       (bytes)
---------------  ----------  -------------- ---------------  ----------  --------------
        32768             1          33176           32768             1          33176
                                                      49152             1          50048
   1762019304             1     1762019304*     1761869256             1     1761869256*
----- allocated memory statistics -----      ----- allocated memory statistics -----
 fragment size       count          total      fragment size       count          total
    (bytes)                       (bytes)         (bytes)                       (bytes)
---------------  ----------  -------------- ---------------  ----------  --------------
        49152            10         491520           49152             9         442368
        65536           125        8192000           65536           125        8192000
        98304             3         294912           98304             3         294912
       131072            18        2359296          131072            19        2490368
```

以下输出确认分配了大小为 150,000 而不是 131,072 的块：

```
> show memory binsize 131072
MEMPOOL_DMA pool bin stats:
MEMPOOL_GLOBAL_SHARED pool bin stats:
pc = 0x8eda524, size = 150000   , count = 1
pc = 0x8f08054, size = 163904   , count = 1
pc = 0x846e477, size = 139264   , count = 1
pc = 0x8068691, size = 393216   , count = 3
pc = 0x8eea09b, size = 131072   , count = 1
pc = 0x88ca830, size = 141212   , count = 1
pc = 0x9589e93, size = 593580   , count = 4
pc = 0x9589bd2, size = 616004   , count = 4
pc = 0x8f2e060, size = 327808   , count = 2
```

```
pc = 0x8068284, size = 182000   , count = 1

0x8eda524 <logger_buffer_init_int+148 at syslog/main.c:403>
```

按照设计， **show memory detail** 命令输出中显示的总字节数是近似值。这有两个原因：

- 对于每个分段大小，如果您需要获取所有分段的总和，将会影响性能，因为可能有大量分配对应单个分段大小，要获得准确值，需要查遍数千个数据块。
- 对于每个 binsize，您需要查遍双重链接的分配列表，并且可能有多个分配。在这种情况下，您不能长时间占用 CPU，需要定期暂停分配。在恢复分配之后，其他进程可能已分配或取消分配内存，内存状态可能已发生变化。因此，总字节数列提供近似值而不是实际值。

示例

以下是 **show memory** 命令的输出示例：

```
> show memory
Free memory:        2986716635 bytes (64%)
Used memory:        1646723072 bytes (36%)
-------------     ------------------
Total memory:       4633439707 bytes (100%)

Note: Free memory is the free system memory. Additional memory may
      be available from memory pools internal to the ASA process.
      Use 'show memory detail' to see this information, but use it
      with care since it may cause CPU hogs and packet loss under load.
>
```

以下示例显示如何显示系统级内存使用情况。

```
> show memory system
             total       used       free     shared    buffers     cached
Mem:       3982640    3014544     240200          0     159932     567964
-/+ buffers/cache:    3014544     968096
Swap:      3998716     137704    3861012
```

以下是 **show memory detail** 命令的输出示例：

```
> show memory detail

Heap Memory:
   Free Memory:
      Heapcache Pool:                      3804848 bytes (  0% )
      Global Shared Pool:                 67372768 bytes (  1% )
      System:                           2986716635 bytes ( 64% )
   Used Memory:
      Heapcache Pool:                    308670800 bytes (  7% )
      Global Shared Pool:                     6432 bytes (  0% )
      Reserved (Size of DMA Pool):       499122176 bytes ( 11% )
      Reserved for messaging:              2097152 bytes (  0% )
      System Overhead:                   765648896 bytes ( 17% )
-----------------------------------     ----------------
   Total Memory:                        4633439707 bytes ( 100% )
```

```
Warning:  The information reported here is computationally expensive to
          determine, and may result in CPU hogs and performance impact.

------------------------------------------------------------------------
MEMPOOL_MSGLYR POOL STATS:

Non-mmapped bytes allocated =      2097152
Number of free chunks       =            1
Number of mmapped regions   =            0
Mmapped bytes allocated     =            0
Max memory footprint        =      2097152
Keepcost                    =      2092768
Max contiguous free mem     =      2092768
Allocated memory in use     =         4288
Free memory                 =      2092864

----- fragmented memory statistics -----

(...Remaining output truncated...)
```

以下示例显示分配给 bin 大小为 8192 的数据块。

```
> show memory binsize 8192
MEMPOOL_HEAPCACHE_0 pool bin stats:
pc = 0x7efc3f80e508, size = 773406   , count = 92
pc = 0x7efc3e3c5013, size = 189152   , count = 23
pc = 0x7efc405df64f, size = 287036   , count = 32
pc = 0x7efc3f9ef622, size = 8128     , count = 1
pc = 0x7efc3f4fd5f5, size = 871744   , count = 106
pc = 0x7efc3f4fd8b7, size = 82240    , count = 10
pc = 0x7efc3f18c3e6, size = 20272    , count = 2
pc = 0x7efc3f557139, size = 8192     , count = 1
pc = 0x7efc3e3f1697, size = 8344     , count = 1
pc = 0x7efc3e0506f6, size = 8192     , count = 1
MEMPOOL_DMA pool bin stats:
pc = 0x7efc3e1cca68, size = 10240    , count = 1
MEMPOOL_GLOBAL_SHARED pool bin stats:
```

以下是**show memory api** 命令的输出示例。它显示内存跟踪器和延迟释放毒物内存功能处于活动状态。

```
> show memory api
Resource Manager (0) ->
Tracking (0) ->
Delayed-free-poisoner (0) ->
Core malloc package (0)
```

以下示例显示如何显示系统级内存使用情况。

```
> show memory system
             total       used       free     shared    buffers     cached
Mem:       3982640    3014544     240200          0     159932     567964
-/+ buffers/cache:    3014544     968096
Swap:      3998716     137704    3861012
```

Related Commands

命令	Description
show memory profile	显示 threat defense 内存使用情况（分析）的信息。

show memory all

要显示 lina 和 Snort 的可供操作系统使用的最大物理内存量和当前可用内存量的摘要，请使用 **show memory all** 命令。

show memory all

Command History

版本	修改
7.0	引入了此命令。

使用指南

show memory all 命令让您显示可供操作系统使用的最大物理内存量和当前可用内存量的摘要。内存会根据需要进行分配。

```
> show memory all
Data Path:
Free memory:        3161408675 bytes (72%)
Used memory:        1203826208 bytes (28%)
-------------     ------------------
Total memory:       4365234883 bytes (100%)
Inspection Engine:
Free memory:                  0 bytes ( 0%)
Used memory:                  0 bytes ( 0%)
-------------     ------------------
Total memory:                 0 bytes (100%)
System:
Free memory:                  0 bytes ( 0%)
Used memory:                  0 bytes ( 0%)
-------------     ------------------
Total memory:                 0 bytes (100%)
```

show memory delayed-free-poisoner

要显示 **memory delayed-free-poisoner** 队列使用情况摘要，请使用 **show memory delayed-free-poisoner** 命令。

show memory delayed-free-poisoner

Command History

版本	修改
6.1	引入了此命令。

使用指南

使用 **memory delayed-free-poisoner enable** 命令启用此功能。使用 **clear memory delayed-free-poisoner** 命令清除队列和统计信息。

示例

以下是 **show memory delayed-free-poisoner** 命令的输出示例：

```
> memory delayed-free-poisoner enable
> show memory delayed-free-poisoner
delayed-free-poisoner settings:
 delayed-free-poisoner threshold 100
 delayed-free-poisoner desired-fragment-size 102400
 delayed-free-poisoner desired-fragment-count 16
 delayed-free-poisoner watchdog-percent 50
delayed-free-poisoner statistics:
                  136064:  current memory in queue
                     500:  current queue length
                       0:  frees dequeued
                     280:  frees not queued for size
                       0:  frees not queued for locking
                       0:  successful validate runs
                       0:  aborted validate runs
                   never:  time of last validate
                       0:  threshold defragment operations
                       0:  size and/or count defragment operations
                       0:  watchdog-aborts
```

show memory logging

要显示内存使用情况日志记录，请使用 **show memory logging** 命令。

show memory logging ［**wrap** | **brief** | **include** ［选项］］

Syntax Description

brief	（可选）显示缩写的内存使用情况日志记录。
include *option*	（可选）仅包含输出中的指定字段。您可以按任意顺序指定字段的关键词，但它们始终以下列顺序显示。如果不包括选项，则输出与指定了**brief**而不是 **include**。 • **process** • **time** • **operator** (free/malloc/etc.) • **address** • **size** • **callers** 输出格式如下： process=[XXX] time=[XXX] oper=[XXX] address=0xXXXXXXXX size=XX @ XXXXXXXX XXXXXXX XXXXXXX XXXXXXX 最多显示4个主叫方地址。操作类型列于示例所示的输出（...的数量）中。
wrap	（可选）显示内存使用情况日志记录包装的数据，在您输入此命令后，这些数据将被清除，因此不会出现重复的数据，也不会保存这些数据。

Command History

版本	修改
6.1	引入了此命令。

使用指南

使用 **show memory logging** 命令查看内存日志信息。您必须先使用 **memory logging** 命令启用此日志记录。

示例

以下是 **show memory logging** 命令的输出示例。

```
> memory logging 1024
> show memory logging
```

```
Number of free                          203989
Number of calloc                        83703
Number of malloc                        120286
Number of realloc-new                   0
Number of realloc-free                  0
Number of realloc-null                  0
Number of realloc-same                  0
Number of calloc-fail                   0
Number of malloc-fail                   0
Number of realloc-fail                  0
Total operations 407978
Buffer size: 1024 (73816 x2 bytes)
process=[cli_xml_server] time=[19:23:42.030] oper=[malloc] addr=0x00007efc358373c0 size=72

@ 0x00007efc3f8e9404 0x00007efc3f80e508 0x00007efc3f4d3cea 0x00007efc3e037f0c
process=[cli_xml_server] time=[19:23:42.030] oper=[free] addr=0x00007efc358373c0 size=72
@ 0x00007efc3f80e9c0 0x00007efc3f4d3fb8 0x00007efc3e037fb0 0x00007efc3f4d537d
(...Remaining output truncated...)
```

以下是 **show memory logging brief** 命令的输出示例。

```
> show memory logging brief
Number of free                          223195
Number of calloc                        91624
Number of malloc                        131572
Number of realloc-new                   0
Number of realloc-free                  0
Number of realloc-null                  0
Number of realloc-same                  0
Number of calloc-fail                   0
Number of malloc-fail                   0
Number of realloc-fail                  0
Total operations 446391
Buffer size: 1024 (73816 x2 bytes)
```

Related Commands

命令	Description
memory logging	启用内存日志记录。

show memory profile

要显示有关 threat defense 设备内存使用情况（分析）的信息，请使用 **show memory profile** 命令。

show memory profile ［**status** | **peak** ［**detail** | **collated**］］

Syntax Description

collated	（可选）整理显示的内存信息。
detail	（可选）显示详细内存信息。
peak	（可选）显示峰值捕获缓冲区而不是“使用中”缓冲区。
status	（可选）显示内存分析和峰值捕获缓冲区的当前状态。

Command History

版本	修改
6.1	引入了此命令。

使用指南

使用 **show memory profile** 命令可对内存使用级别和内存泄漏进行故障排除。即使内存分析已停止，您仍然可以查看分析缓冲区内容。开始内存分析将自动清除该缓冲区。

注释 启用内存分析时， threat defense 设备的性能可能会临时下降。

示例

以下是 **show memory profile** 命令的输出示例：

```
> show memory profile
Range: start = 0x004018b4, end = 0x004169d0, increment = 00000004
Total = 0
```

show memory profile detail 命令的输出分为六个数据列和最左侧的一个信头列。与第一个数据列对应的内存桶的地址在信头列给定（十六进制数字）。数据本身是通过桶地址中的文本/代码保存的字节数。数据列中的句点 (.) 表示此内存桶处的文本未保留内存。行中的其他列对应于大于前一列增量的桶地址。例如，第一行中第一个数据列的地址桶为 0x001069e0。第一行中第二个数据列的地址桶为 0x001069e4，依此类推。通常信头列地址是下一个桶地址；即，前一行的最后一个数据列的地址加上增量。所有未使用的行都不会显示。若不显示多个连续的此类行，用信头列中的三个句点 (...) 指示。

以下是 **show memory profile peak detail** 命令的输出示例，其中显示了峰值捕获缓冲区和通过相应桶地址中的文本/代码保存的字节数：

```
> show memory profile peak detail
Range: start = 0x00100020, end = 0x00e006e0, increment = 00000004
```

```
Total = 48941152
...
0x001069e0 . 24462 . . . .
...
0x00106d88 . 1865870 . . . .
...
0x0010adf0 . 7788 . . . .
...
0x00113640 . . . . 433152 .
...
0x00116790 2480 . . . . .
(...output truncated...)
```

以下是 **show memory profile peak collated** 命令的输出示例：

```
> show memory profile peak collated
Range: start = 0x00100020, end = 0x00e006e0, increment = 00000004
Total = 48941152
24462 0x001069e4
1865870 0x00106d8c
7788 0x0010adf4
433152 0x00113650
2480 0x00116790
<More>
```

以下是 **show memory profile peak** 命令的输出示例，其中显示了峰值捕获缓冲区：

```
> show memory profile peak
Range: start = 0x004018b4, end = 0x004169d0, increment = 00000004
Total = 102400
```

以下是 **show memory profile status** 命令的输出示例，其中显示了内存分析和峰值捕获缓冲区的当前状态：

```
> show memory profile status
InUse profiling: ON
Peak profiling: OFF
Memory used by profile buffers: 11518860 bytes
Profile:
0x00100020-0x00bfc3a8(00000004)
```

Related Commands

命令	Description
memory profile enable	启用对内存使用（内存分析）的监控。
memory profile text	配置要分析的内存的程序文本范围。
clear memory profile	清除内存分析功能保留的缓冲区。

show memory tracking

要显示该工具跟踪的当前已分配内存，请使用 **show memory tracking** 命令。

show memory tracking [**address** | **detail** | **dump** *tracked_address*]

Syntax Description

address	（可选）按地址显示内存跟踪。
detail	（可选）显示内存跟踪状态。
dump *tracked_address*	（可选）显示指定内存跟踪地址 0-4294967295 的转储。

Command History

版本	修改
6.1	引入了此命令。

使用指南

使用 **show memory tracking** 命令以要显示该工具跟踪的当前已分配内存。您必须先使用 **memory tracking enable**，然后才能看到此信息。

示例

以下是 **show memory tracking** 命令的输出示例：

```
> show memory tracking
memory tracking by caller:
  bytes-threshold:        0
  allocates-by-threshold: 0
         65406 bytes from    49 allocates by 0x00007efc3f80e508
          3000 bytes from     1 allocates by 0x00007efc3f4e1278
           159 bytes from     1 allocates by 0x00007efc3fe9ee13
            17 bytes from     1 allocates by 0x00007efc3fe9ef4e
```

以下是 **show memory tracking address** 命令的输出示例：

```
> show memory tracking address
memory tracking by caller:
  bytes-threshold:        0
  allocates-by-threshold: 0
         58918 bytes from    49 allocates by 0x00007efc3f80e508
          3000 bytes from     1 allocates by 0x00007efc3f4e1278
           167 bytes from     1 allocates by 0x00007efc3fe9ee13
            17 bytes from     1 allocates by 0x00007efc3fe9ef4e
memory tracking address pool:
            32 byte region @ 0x00007efc358a06e0 allocated by 0x00007efc3f80e508
            96 byte region @ 0x00007efc351d0880 allocated by 0x00007efc3f80e508
           896 byte region @ 0x00007efc35f121c0 allocated by 0x00007efc3f80e508
          8192 byte region @ 0x00007efc35832e20 allocated by 0x00007efc3f80e508
            96 byte region @ 0x00007efc30483910 allocated by 0x00007efc3f80e508
            88 byte region @ 0x00007efc359e3960 allocated by 0x00007efc3f80e508
          1036 byte region @ 0x00007efc35f04680 allocated by 0x00007efc3f80e508
            76 byte region @ 0x00007efc36024890 allocated by 0x00007efc3f80e508
```

```
  24 byte region @ 0x00007efc35fd48a0 allocated by 0x00007efc3f80e508
  32 byte region @ 0x00007efc35f04ad0 allocated by 0x00007efc3f80e508
  34 byte region @ 0x00007efc35e54e00 allocated by 0x00007efc3f80e508
8192 byte region @ 0x00007efc35834e70 allocated by 0x00007efc3f80e508
  40 byte region @ 0x00007efc36005cc0 allocated by 0x00007efc3f80e508
  11 byte region @ 0x00007efc360061e0 allocated by 0x00007efc3f80e508
  76 byte region @ 0x00007efc357a6dd0 allocated by 0x00007efc3f80e508
1024 byte region @ 0x00007efc358574f0 allocated by 0x00007efc3f80e508
  88 byte region @ 0x00007efc365b7ef0 allocated by 0x00007efc3f80e508
  56 byte region @ 0x00007efc365b7f90 allocated by 0x00007efc3f80e508
 168 byte region @ 0x00007efc365b8210 allocated by 0x00007efc3f80e508
 112 byte region @ 0x00007efc365b8300 allocated by 0x00007efc3f80e508
 112 byte region @ 0x00007efc365b83c0 allocated by 0x00007efc3f80e508
  16 byte region @ 0x00007efc365b8560 allocated by 0x00007efc3f80e508
 167 byte region @ 0x00007efc365b85c0 allocated by 0x00007efc3fe9ee13
2048 byte region @ 0x00007efc357a8610 allocated by 0x00007efc3f80e508
  88 byte region @ 0x00007efc35728be0 allocated by 0x00007efc3f80e508
  88 byte region @ 0x00007efc357a8e60 allocated by 0x00007efc3f80e508
4112 byte region @ 0x00007efc35fe90c0 allocated by 0x00007efc3f80e508
  17 byte region @ 0x00007efc365b95a0 allocated by 0x00007efc3fe9ef4e
  72 byte region @ 0x00007efc365b9600 allocated by 0x00007efc3f80e508
  72 byte region @ 0x00007efc365b9690 allocated by 0x00007efc3f80e508
  72 byte region @ 0x00007efc365b9720 allocated by 0x00007efc3f80e508
  40 byte region @ 0x00007efc365b97b0 allocated by 0x00007efc3f80e508
  24 byte region @ 0x00007efc365b9820 allocated by 0x00007efc3f80e508
   2 byte region @ 0x00007efc365b9880 allocated by 0x00007efc3f80e508
  76 byte region @ 0x00007efc35ff9aa0 allocated by 0x00007efc3f80e508
 776 byte region @ 0x00007efc35f19df0 allocated by 0x00007efc3f80e508
 512 byte region @ 0x00007efc3585a0a0 allocated by 0x00007efc3f80e508
 936 byte region @ 0x00007efc357aaea0 allocated by 0x00007efc3f80e508
  24 byte region @ 0x00007efc357ab290 allocated by 0x00007efc3f80e508
 568 byte region @ 0x00007efc3592bc40 allocated by 0x00007efc3f80e508
 512 byte region @ 0x00007efc35e5c8a0 allocated by 0x00007efc3f80e508
  40 byte region @ 0x00007efc35f2cae0 allocated by 0x00007efc3f80e508
1665 byte region @ 0x00007efc359fcda0 allocated by 0x00007efc3f80e508
 168 byte region @ 0x00007efc34fccf60 allocated by 0x00007efc3f80e508
 112 byte region @ 0x00007efc35ffd0e0 allocated by 0x00007efc3f80e508
4112 byte region @ 0x00007efc356bd340 allocated by 0x00007efc3f80e508
8208 byte region @ 0x00007efc3643d3e0 allocated by 0x00007efc3f80e508
 386 byte region @ 0x00007efc359fd470 allocated by 0x00007efc3f80e508
  72 byte region @ 0x00007efc35e4d570 allocated by 0x00007efc3f80e508
8208 byte region @ 0x00007efc359fd840 allocated by 0x00007efc3f80e508
4112 byte region @ 0x00007efc3592ded0 allocated by 0x00007efc3f80e508
3000 byte region @ 0x00007efc357ee5c0 allocated by 0x00007efc3f4e1278
  32 byte region @ 0x00007efc351be6d0 allocated by 0x00007efc3f80e508
  16 byte region @ 0x00007efc359de790 allocated by 0x00007efc3f80e508
1036 byte region @ 0x00007efc3524f080 allocated by 0x00007efc3f80e508
 512 byte region @ 0x00007efc357ff290 allocated by 0x00007efc3f80e508
 360 byte region @ 0x00007efc357ef360 allocated by 0x00007efc3f80e508
  24 byte region @ 0x00007efc357ff4e0 allocated by 0x00007efc3f80e508
```

Related Commands

命令	Description
clear memory tracking	清除所有当前已收集的信息。
memory tracking	启用内存跟踪。

show memory webvpn

要生成 WebVPN 的内存使用情况统计信息，请使用 **show memory webvpn** 命令。

show memory webvpn ［**allobjects** | **blocks** | **dumpstate** *filename* | **pools** | **usedobjects**］
show memory webvpn profile ［**clear** | **dump** *filename* | **start** | **stop**］

Syntax Description

allobjects	显示池、块以及所有已使用和已释放对象的 WebVPN 内存消耗详细信息。
blocks	显示内存块的 WebVPN 内存消耗详细信息。
clear	清除 WebVPN 内存配置。
dump *filename*	将 WebVPN 内存配置文件放入指定的文件中。文件名应包括位置，可以是 disk0:、disk1:、flash:、ftp:、tftp:。
dumpstate *filename*	将 WebVPN 内存状态放入指定文件。文件名应包括位置，可以是 disk0:、disk1:、flash:、ftp:、tftp:。
pools	显示内存池的 WebVPN 内存消耗详细信息。
profile	获取 WebVPN 内存配置并将其放入文件。
start	开始收集 WebVPN 内存分析。
stop	停止获取 WebVPN 内存分析。
usedobjects	显示已使用对象的 WebVPN 内存消耗详细信息。

Command History

版本	修改
6.1	引入了此命令。

示例

以下是 **show memory webvpn allobjects** 命令的输出示例：

```
> show memory webvpn allobjects
Arena 0x36b14f8 of 4094744 bytes (61 blocks of size 66048), maximum 134195200
130100456 free bytes (97%; 1969 blocks, zone 0)
Arena is dynamically allocated, not contiguous
Features: GroupMgmt: SET, MemDebugLog: unset
Pool 0xd719a78 ("cp_entries" => "pool for class cpool entries") (next 0xd6d91d8)
Size: 66040 (1% of current, 0% of limit)
Object frame size: 32
Load related limits: 70/50/30
Callbacks: !init/!prep/!f2ca/!dstr/!dump
Blocks in use:
Block 0xd719ac0..0xd729cb8 (size 66040), pool "cp_entries"
Watermarks { 0xd7098f8 <= 0xd70bb60 <= 0xd719a60 } = 57088 ready
```

```
Block size 66040 not equal to arena block 66048 (realigned-to-8)
Used objects: 0
Top allocated count: 275
Objects dump:
0. Object 0xd70bb50: FREED (by "jvclass_pool_free")
```

show mfib

要显示组播转发信息库中的信息，请使用 **show mfib** 命令。

show mfib [*source_or_group* [*group*]] [**cluster** | **count** | **verbose**]
show mfib [**active** [*kbps*] | **cluster-stats** | **interface** | **status** | **summary**]
show mfib reserved [**active** [*kbps*] | **cluster** | **count** | **verbose**]

Syntax Description

[**active** [*kbps*]	（可选）显示活动组播源。您可以指定千位/秒，将显示限制为大于或等于此值的组播流。默认值为 4，范围为 0-4294967295。
cluster	（可选）显示MFIB日期和当前计时器值。如果同时指定源和组，则无法指定 **cluster** 。
cluster-stats	（可选）显示 MFIB 集群同步统计信息。
count	（可选）显示MFIB路由和数据包计数数据。此命令显示数据包丢弃统计信息。
interface	（可选）显示与 MFIB 流程相关的接口的数据包统计信息。
reserved	（可选）显示保留组的 MFIB 条目，范围为 224.0.0.0 到 224.0.0.225。
source_or_group [*group*]	（可选）源或组 IPv4、IPv6 或名称。如果同时指定两者，请先指定源。源地址为单播地址。
status	（可选）显示常规 MFIB 配置和运行状态。
summary	（可选）显示有关 MFIB 条目和接口数量的摘要信息。
verbose	显示有关转发条目和接口的详细信息

Command Default

如果没有可选参数，则显示所有组的信息。

Command History

版本	修改
6.1	引入了此命令。

示例

以下是 **show mfib** 命令的输出示例：

```
> show mfib 224.0.2.39
Entry Flags: C - Directly Connected, S - Signal, IA - Inherit A flag,
             AR - Activity Required, D - Drop
Forwarding counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts: Total/RPF failed/Other drops
Interface flags: A - Accept, F - Forward, NS - Negate Signalling
```

```
             IC - Internal Copy, NP - Not platform switched
             SP - Signal Present
Interface Counts: FS Pkt Count/PS Pkt Count
(*,224.0.1.39) Flags: S K
  Forwarding: 0/0/0/0, Other: 0/0/0
```

以下是 **show mfib verbose** 命令的输出示例：

```
> show mfib verbose
Entry Flags: C - Directly Connected, S - Signal, IA - Inherit A flag,
             AR - Activity Required, D - Drop
Forwarding counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts: Total/RPF failed/Other drops
Interface flags: A - Accept, F - Forward, NS - Negate Signalling
             IC - Internal Copy, NP - Not platform switched
             SP - Signal Present
Interface Counts: FS Pkt Count/PS Pkt Count
(*,224.0.1.39) Flags: S K
  Forwarding: 0/0/0/0, Other: 0/0/0
(*,224.0.1.40) Flags: S K
  Forwarding: 0/0/0/0, Other: 0/0/0
(*,224.0.0.0/8) Flags: K
  Forwarding: 0/0/0/0, Other: 0/0/0
```

以下是 **show mfib count** 命令的输出示例：

```
> show mfib count
MFIB global counters are :
* Packets [no input idb] : 0
* Packets [failed route lookup] : 0
* Packets [Failed idb lookup] : 0
* Packets [Mcast disabled on input I/F] : 0
```

以下是 **show mfib active** 命令的输出示例。输出显示速率 PPS 的正数或负数。当 RPF 数据包发生故障或路由器观察到具有传出接口 (OIF) 列表的 RPF 数据包时，命令显示负数。此类型的活动可能指示组播路由问题。

```
> show mfib active
Active IP Multicast Sources - sending >= 4 kbps

Group: 224.2.127.254, (sdr.cisco.com)
   Source: 192.168.28.69 (mbone.ipd.anl.gov)
     Rate: 1 pps/4 kbps(1sec), 4 kbps(last 1 secs), 4 kbps(life avg)

Group: 224.2.201.241, ACM 97
   Source: 192.168.52.160 (webcast3-e1.acm97.interop.net)
     Rate: 9 pps/93 kbps(1sec), 145 kbps(last 20 secs), 85 kbps(life avg)

Group: 224.2.207.215, ACM 97
   Source: 192.168.52.160 (webcast3-e1.acm97.interop.net)
     Rate: 3 pps/31 kbps(1sec), 63 kbps(last 19 secs), 65 kbps(life avg)
```

以下是 **show mfib interface** 命令的输出示例：

```
> show mfib interface
IP Multicast Forwarding (MFIB) status:
```

```
    Configuration Status: enabled
    Operational Status: running
MFIB interface       status    CEF-based output
                               [configured,available]
           Ethernet0   up    [        no,       no]
           Ethernet1   up    [        no,       no]
           Ethernet2   up    [        no,       no]
```

以下是 **show mfib status** 命令的输出示例：

```
> show mfib status
IP Multicast Forwarding (MFIB) status:
    Configuration Status: enabled
    Operational Status: running
```

以下是 **show mfib summary** 命令的输出示例：

```
> show mfib summary
IPv6 MFIB summary:

  54     total entries [1 (S,G), 7 (*,G), 46 (*,G/m)]

  17     total MFIB interfaces
```

以下是 **show mfib reserved** 命令的输出示例：

```
> show mfib reserved
Entry Flags: C - Directly Connected, S - Signal, IA - Inherit A flag,
             AR - Activity Required, D - Drop
Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts: Total/RPF failed/Other drops
Interface Flags: A - Accept, F - Forward, NS - Negate Signalling
             IC - Internal Copy, NP - Not platform switched
             SP - Signal Present
Interface Counts: FS Pkt Count/PS Pkt Count
(*,224.0.0.0/4) Flags: C K
   Forwarding: 0/0/0/0, Other: 0/0/0
(*,224.0.0.0/24) Flags: K
   Forwarding: 0/0/0/0, Other: 0/0/0
(*,224.0.0.1) Flags:
   Forwarding: 0/0/0/0, Other: 0/0/0
   outside Flags: IC
   dmz Flags: IC
   inside Flags: IC
```

Related Commands

命令	Description
clear mfib counters	清除 MFIB 路由器数据包计数器。
show mroute active	显示活动的组播流。
show mroute count	显示组播路由计数器。
show mroute summary	显示组播路由表摘要信息。

show mgcp

要显示媒体网关控制协议 (MGCP) 配置和会话信息，请使用 **show mgcp** 命令。

show mgcp {commands | **sessions**} [**detail**]

Syntax Description

commands	列出命令队列中 MGCP 命令的数量。
detail	（可选）在输出中列出每个命令或会话的附加信息。
sessions	列出现有 MGCP 会话的数量。

Command History

版本	修改
6.2.1	引入了此命令。

使用指南

要显示 MGCP 信息，必须检查 MGCP 流量。要检查 MGCP 流量，您需要在 管理中心中配置 FlexConfig。

示例

以下是 **show mgcp** 命令选项的示例：

```
> show mgcp commands
1 in use, 1 most used, 200 maximum allowed
CRCX, gateway IP: host-pc-2, transaction ID: 2052, idle: 0:00:07

> show mgcp commands detail
1 in use, 1 most used, 200 maximum allowed
CRCX, idle: 0:00:10
       Gateway IP | host-pc-2
       Transaction ID  2052
       Endpoint name | aaln/1
       Call ID | 9876543210abcdef
       Connection ID |
       Media IP | 192.168.5.7
       Media port | 6058

> show mgcp sessions
1 in use, 1 most used
Gateway IP host-pc-2, connection ID 6789af54c9, active 0:00:11

> show mgcp sessions detail
1 in use, 1 most used
Session active 0:00:14
       Gateway IP | host-pc-2
       Call ID | 9876543210abcdef
       Connection ID | 6789af54c9
       Endpoint name | aaln/1
       Media lcl port  6166
       Media rmt IP | 192.168.5.7
```

```
Media rmt port  6058
```

show mini-coredump status

要显示迷你核心转储生成的设置，请输入 **show mini-coredump status** 命令。

show mini-coredump status

Command History

版本	修改
7.0	引入了此命令。

使用指南

默认情况下，迷你核心转储生成处于启用状态。

由于其多线程性质，Snort 3 流程会转储巨大的核心文件。这些转储需要一段时间才能写入硬盘。在写入核心并启动新流程之前，Snort 的流量检查会中断。创建迷你核心转储可避免时间延迟。迷你核心转储具有有助于调试的堆栈和内存值的基本详细信息。

示例

以下示例显示迷你核心转储生成已禁用。

```
> show mini-coredump status
minicoredump feature status : Disabled
```

Related Commands

命令	Description
configure mini-coredump	启用或禁用迷你核心转储生成。

show mode

要显示系统的安全情景模式，请使用 **show mode** 命令。

show mode

Command History

版本	修改
6.1	引入了此命令。

使用指南

threat defense 设备仅支持单情景模式。不支持多情景模式。

示例

以下示例显示如何显示安全情景模式。

```
> show mode
Security context mode: single
```

show model

要显示设备的硬件型号，请使用 **show model** 命令。

show model

Command History

版本	修改
6.1	引入了此命令。

示例

以下示例显示了设备型号。

```
> show model
Cisco ASA5516-X Threat Defense
```

Related Commands

命令	Description
show serial-number	显示设备序列号。
show version	显示软件和其他设备版本信息。

show module

要显示有关 threat defense 设备上安装的模块的信息，请在用户 EXEC 模式下使用 **show module** 命令。

show module ［*ID* ［**details** | **recover** | **log console**］］ | **all**］

Syntax Description

all	（默认）显示所有模块的信息。这是默认值。
details	（可选）显示附加信息，包括模块的远程管理配置。
ID	指定模块 ID。使用不带参数的 show module 查看可用插槽号，通常为 0 和 1。
log console	（可选）显示模块的日志信息。此选项可能并非对每个模块都有效。
recover	（可选）显示用于恢复模块的设置。

Command Default

默认情况下，显示所有模块的信息。

Command History

版本	修改
6.1	引入了此命令。

使用指南

此命令显示有关 threat defense 设备中安装的模块的信息。 threat defense 本身也会以模块形式出现在显示中（在插槽 0 中）。设备是否支持其他模块因设备型号而异。

show module details 命令的输出会根据已安装的模块而有所不同。

对于允许配置软件模块的型号， **show module** 命令会列出所有可能的模块。状态消息指示是否已安装其中一个模块。

示例

以下示例输出适用于运行 threat defense 软件的 ASA 5516-X。对于此设备，插槽 1 未知是正常的，因为 threat defense 不支持任何软件模块。

```
> show module

Mod  Card Type                                    Model              Serial No.
---- ------------------------------------------- ------------------ -----------
   0 ASA 5516-X with FirePOWER services, 8GE, AC, ASA5516            JAD19390056I
   1 Unknown                                     N/A                JAD19390056I

Mod  MAC Address Range                 Hw Version   Fw Version   Sw Version
---- --------------------------------- ------------ ------------ ---------------
   0 84b2.61b1.92be to 84b2.61b1.92c6  1.0          1.1.3        97.1(0)60
   1 84b2.61b1.92bd to 84b2.61b1.92bd  N/A          N/A
```

```
Mod  SSM Application Name           Status           SSM Application Version
---- ------------------------------ ---------------- --------------------------
   1 Unknown                        No Image Present Not Applicable

Mod  Status             Data Plane Status     Compatibility
---- ------------------ --------------------- -------------
   0 Up Sys             Not Applicable
   1 Unresponsive       Not Applicable
```

下表说明了输出中列出的每个字段。

表 *2: show module* 输出字段

字段	Description
Mod	模块编号，0 或 1。
Card Type	卡类型。对于模块 0 中显示的设备，类型为平台型号。对于插槽 1，它将是额外的模块（如果有）。
Model	此模块的型号。
Serial No.	序列号。
MAC Address Range	此模块上接口的 MAC 地址范围。
Hw Version	硬件版本。
Fw Version	固件版本。
Sw Version	软件版本。这不是 threat defense 版本。相反，它是 ASA 软件版本，是 threat defense 软件的组件。使用 **show version** 命令查看 threat defense 版本。
SSM Application Name	在安全服务模块上运行的应用的名称。
SSM Application Version	在安全服务模块上运行的应用的版本。

字段	Description
Status	对于模块 0 中的设备，状态为 Up Sys。模块 1 中的模块的状态可以是以下状态之一： • Initializing（正在初始化）- 检测到模块，并且设备正在初始化控制通信。 • Up（开启）- 模块已完成设备初始化。 • Unresponsive（无响应）- 设备在与此模块通信时遇到错误。 • Reloading（正在重新加载）- 模块正在重新加载。 • Shutting Down（正在关闭）- 模块正在关闭。 • Down（关闭）- 模块已关闭。 • Recover（恢复）- 模块正在尝试下载恢复映像。 • No Image Present（不存在映像）- 模块软件尚未安装。
Data Plane Status	数据层面的当前状态。
Compatibility	模块相对于设备其余部分的兼容性。

show monitor-interface

要显示有关故障转移监控接口的信息，请使用 **show monitor-interface** 命令。

show monitor-interface

Command History

版本	修改
6.1	引入了此命令。

使用指南

由于一个接口上可配置多个 IPv6 地址，因此 **show monitor-interface** 命令只显示本地链路的地址。如果接口上配置了 IPv4 和 IPv6 地址，则两个地址都会出现在输出中。如果接口上未配置 IPv4 地址，则输出中的 IPv4 地址会显示为 0.0.0.0。如果接口上未配置 IPv6 地址，则输出中会直接省略地址。

监测的故障切转移口可以具有以下状态：

- (Waiting) 加上任何其他状态，例如 Unknown (Waiting) - 接口尚未从对等体设备上的相应接口收到 hello 数据包。
- Unknown - 初始状态。此状态也可能意味着状态无法确定。
- Normal - 接口正在接收流量。如果状态为正常（等待），请检查该接口是否配置了备 IP 地址，且两个接口之间是否连接。
- Testing - 接口上有 5 个轮询时间未收听到 Hello 消息。
- Link Down - 接口或 VLAN 通过管理方式关闭。
- No Link - 接口的物理链路关闭。
- Failed - 在接口上没有收到流量，但在对等体接口上收听到流量。

示例

以下是 **show monitor-interface** 命令的输出示例：

```
> show monitor-interface
 This host: Primary - Active
  Interface inside (192.168.1.13): Normal (Monitored)
  Interface outside (192.168.2.13): Normal (Monitored)
 Other host: Secondary - Standby Ready
  Interface inside (192.168.1.14): Normal (Monitored)
  Interface outside (192.168.2.14): Normal (Monitored)
```

show mrib client

要显示有关 MRIB 客户端连接的信息，请使用 **show mrib client** 命令。

show mrib client ［**filter**］［**name** *client_name*］

Syntax Description

filter	（可选）显示客户端过滤器。用于查看有关每个客户端拥有的MRIB标志以及每个客户端感兴趣的标志的信息。
name *client_name*	（可选）用作 MRIB 客户端的组播路由协议的名称，如 PIM 或 IGMP。

Command History

版本	修改
6.1	引入了此命令。

使用指南

filter 选项用于显示各 MRIB 客户端已注册的路由和接口级别标志更改。此命令选项还显示哪些标志由 MRIB 客户端所有。

示例

以下是使用 **filter** 关键字的 **show mrib client** 命令的输出示例：

```
> show mrib client filter
MFWD:0 (connection id 0)
interest filter:
entry attributes: S C IA D
interface attributes: F A IC NS DP SP
groups:
include 0.0.0.0/0
interfaces:
include All
ownership filter:
groups:
include 0.0.0.0/0
interfaces:
include All
igmp:77964 (connection id 1)
ownership filter:
interface attributes: II ID LI LD
groups:
include 0.0.0.0/0
interfaces:
include All
pim:49287 (connection id 5)
interest filter:
entry attributes: E
interface attributes: SP II ID LI LD
groups:
include 0.0.0.0/0
interfaces:
include All
ownership filter:
entry attributes: L S C IA D
```

```
interface attributes: F A IC NS DP
groups:
include 0.0.0.0/0
interfaces:
include All
```

Related Commands

命令	Description
show mrib route	显示 MRIB 表条目。

show mrib route

要显示 MRIB 表中的条目，请使用 **show mrib route** 命令。

show mrib route [[[*source* | *****] [*group*[/*prefix-length*]]] | **summary**]

Syntax Description

*****	（可选）显示共享树条目。
/*prefix-length*	（可选）MRIB 路由的前缀长度。是一个十进制值，表示构成前缀（地址的网络部分）的地址高位的连续位数。十进制值前面必须有斜线标记。
group	（可选）组的 IP 地址或名称。
source	（可选）路由源的 IP 地址或名称。
summary	显示 MRIB 表条目的摘要。

Command History

版本	修改
6.1	引入了此命令。

使用指南

MFIB 表维护从 MRIB 更新的条目和标志子集。标志根据组播数据包的转发规则集来确定转发和信令行为。

除了接口和标志的列表外，每个路由条目都显示各种计数器。字节数是转发的总字节数。数据包数是针对此条目接收的数据包数。 **show mfib count** 命令显示与路由无关的全局计数器。

示例

以下是 **show mrib route** 命令的输出示例：

```
> show mrib route
IP Multicast Routing Information Base
Entry flags: L - Domain-Local Source, E - External Source to the Domain,
    C - Directly-Connected Check, S - Signal, IA - Inherit Accept, D - Drop
Interface flags: F - Forward, A - Accept, IC - Internal Copy,
    NS - Negate Signal, DP - Don't Preserve, SP - Signal Present,
    II - Internal Interest, ID - Internal Disinterest, LI - Local Interest,
LD - Local Disinterest
(*,224.0.0.0/4) RPF nbr: 10.11.1.20 Flags: L C
   Decapstunnel0 Flags: NS

(*,224.0.0.0/24) Flags: D

(*,224.0.1.39) Flags: S

(*,224.0.1.40) Flags: S
   POS0/3/0/0 Flags: II LI

(*,238.1.1.1) RPF nbr: 10.11.1.20 Flags: C
   POS0/3/0/0 Flags: F NS LI
```

```
   Decapstunnel0 Flags: A

(*,239.1.1.1) RPF nbr: 10.11.1.20 Flags: C
   POS0/3/0/0 Flags: F NS
   Decapstunnel0 Flags: A
```

Related Commands

命令	Description
show mfib count	显示 MFIB 表的路由和数据包计数数据。

show mroute

要显示 IPv4 组播路由表，请使用 **show mroute** 命令。

show mroute [*group* [*source*] | **reserved**] [**active** [*rate*] | **count** | **pruned** | **summary**]

Syntax Description

active *rate*	（可选）仅显示活动组播源。活动源是正在以指定 *rate* 或更高速率发送的源。如果未指定 *rate* ，则活动源是正在以 4 kbps 或更高速率发送的源。
count	（可选）显示有关组和源的统计信息，包括数据包数、每秒数据包数，平均数据包大小和 bps。
group	（可选）组播组的 IP 地址或名称，如 DNS 主机表中所定义。
pruned	（可选）显示修剪的路由。
reserved	（可选）显示预留组。
source	（可选）源主机名或 IP 地址。
summary	（可选）在组播路由表中显示每个条目的单行缩写摘要。

Command History

版本	修改
6.1	引入了此命令。

使用指南

show mroute 命令显示组播路由表的内容。设备通过创建基于 PIM 协议消息、IGMP 报告和流量的 (S,G) 和 (*,G) 条目来填充组播路由表。星号 (*) 指所有源地址，“S”指单个源地址，“G”是目标组播组地址。在创建 (S, G) 条目时，软件使用在单播路由表中找到的到该目标组的最佳路径（通过 RPF）。

要查看运行配置中的 **mroute** 命令，请使用 **show running-config mroute** 命令。

示例

以下是 **show mroute** 命令的输出示例：

```
> show mroute

Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group,
       C - Connected, L - Local, I - Received Source Specific Host Report,
       P - Pruned, R - RP-bit set, F - Register flag, T - SPT-bit set,
       J - Join SPT
Timers: Uptime/Expires
Interface state: Interface, State

(*, 239.1.1.40), 08:07:24/never, RP 0.0.0.0, flags: DPC
  Incoming interface: Null
```

```
  RPF nbr: 0.0.0.0
  Outgoing interface list:
    inside, Null, 08:05:45/never
    tftp, Null, 08:07:24/never

(*, 239.2.2.1), 08:07:44/never, RP 140.0.0.70, flags: SCJ
  Incoming interface: outside
  RPF nbr: 140.0.0.70
  Outgoing interface list:
    inside, Forward, 08:07:44/never
```

show mroute 输出中显示以下字段：

- Flags - 提供有关条目的信息。
  - D - 密集。条目在密集模式下工作。
  - S - 稀疏。条目在稀疏模式下工作。
  - B - 双向组。指示组播组在双向模式下工作。
  - s - SSM 组。指示组播组在 IP 地址的 SSM 范围内。如果 SSM 范围更改，此标志将重置。
  - C - 已连接。组播组的成员出现在直接连接的接口上。
  - L - 本地。设备本身是组播组的成员。通过 igmp join-group 命令以本地方式加入组（对于已配置的组）。
  - I - 已接收源特定主机报告。指示通过 (S, G) 报告创建了 (S, G) 条目。此 (S, G) 报告可能通过 IGMP 创建。此标志仅在 DR 上设置。
  - P - 已修剪。路由已修剪。软件将保留此信息，以便下游成员加入源。
  - R - RP 位已设置。指示 (S, G) 条目指向 RP。
  - F - 注册标志。指示软件正在注册组播源。
  - T - SPT 未已设置。指示已在最短路径源树上收到数据包。
  - J - 联合 SPT。对于 (*, G) 条目，指示流量流下共享树的速率超过为组设置的 SPT 阈值。（默认 SPT 阈值设置为 0 kbps。）当设置 J - Join 最短路径树 (SPT) 标志后，在共享树收到的下一个 (S, G) 数据包将触发源方向上的 (S, G) 加入，从而使设备加入源树。

    对于 (S, G) 条目，指示由于超过了组的 SPT 阈值而创建了条目。当为 (S, G) 条目设置 J - Join SPT 标志后，设备监控源树上的流量速率，并在源树上的流量速率低于组的 SPT 阈值超过 1 分钟时尝试切换回此源的共享树。

注释 设备会测量共享树上的流量速率，并将测量出的速率与组的 SPT 阈值进行比较，每秒比较一次。如果流量速率超过 SPT 阈值，将在 (*, G) 条目上设置 J - Join SPT 标志，直到下一次测量流量速率。当下一个数据包到达共享树并且开始新的测量间隔时，清除该标志。

如果组使用默认 SPT 阈值 0 Kbps，将始终在 (*, G) 条目上设置 J - Join SPT 标志，并且不会清除。当使用默认 SPT 阈值时，如果收到来自新源的流量，设备会立即切换到最短路径源树。

- 计时器：正常运行时间/到期时间 - 正常运行时间针对接口指示条目在 IP 组播路由表中的时长（以小时、分钟和秒为单位）。到期时间针对接口指示从 IP 组播路由表中删除条目之前的时长（以小时、分钟和秒为单位）。
- 接口状态 - 指示传入或传出接口的状态。
  - 接口 - 传入或传出接口列表中列出的接口名称。
  - 状态 - 指示数据包在接口上被转发、修剪还是变空，具体取决于是否因访问列表或生存时间 (TTL) 阈值而存在限制。
- (*, 239.1.1.40) 和 (* , 239.2.2.1) - IP 组播路由表中的条目。条目包含源的 IP 地址，后面紧跟组播组的 IP 地址。用星号 (*) 代替源则表示所有源。
- RP - RP 的地址。对于在稀疏模式下运行的路由器和访问服务器，此地址始终为 224.0.0.0。
- 传入接口 - 来自源的组播数据包的预期接口。如果在此接口上未接收到数据包，系统会将其丢弃。
- RPF nbr - 上游路由器相对于源的 IP 地址。
- 传出接口 — 通过其转发数据包的接口。

Related Commands

命令	Description
show running-config mroute	显示已配置的组播路由。

show nameif

要查看接口的逻辑名称，请使用 **show nameif** 命令。

show nameif [*physical_interface*[**.***subinterface*] | **zone**]

Syntax Description

physical_interface	（可选）标识接口 ID，例如 **gigabitethernet0/1**。
subinterface	（可选）识别一个介于 1 到 4294967293 之间整数，用以指定逻辑子接口。
zone	（可选）显示区域和内联集名称。

Command Default

如果不指定接口，此命令将显示所有接口名称。

Command History

版本	修改
6.1	引入了此命令。

使用指南

使用此命令可显示分配给接口的名称。必须为接口命名才能在任何配置设置中使用它。它还显示接口的安全级别， threat defense始终为 0。

如果添加**zone**关键字，则“区域名称”列指示接口所属的内联集或流量区域。流量区域与安全区域不同，因此如果没有被动接口或内联集，即使接口属于路由或交换安全区域，该列也可能为空。使用设备管理器确定哪些安全区域包含每个接口。

示例

以下是 **show nameif** 命令的输出示例：

```
> show nameif
Interface                Name                    Security
GigabitEthernet1/1       outside                   0
GigabitEthernet1/2       inside1_2                 0
GigabitEthernet1/3       inside1_3                 0
GigabitEthernet1/4       inside1_4                 0
GigabitEthernet1/5       inside1_5                 0
GigabitEthernet1/6       inside1_6                 0
GigabitEthernet1/7       inside1_7                 0
GigabitEthernet1/8       inside1_8                 0
Management1/1            diagnostic                0
BVI1                     inside                    0
```

以下是显示区域成员身份的示例输出。在本示例中，2个接口位于内联集中，一个接口位于被动流量区域。

```
> show nameif zone
Interface                Name                    Zone Name           Security
GigabitEthernet0/0       passive                 passive-security-zone
                                                                       0
GigabitEthernet0/1       in                      is-154              0
```

```
GigabitEthernet0/2      out                    is-154              0
Management0/0           diagnostic                                 0
```

show nat

要显示 NAT 策略的统计信息，请使用 **show nat** 命令。

show nat [**interface** *name*] [*ip_addr* [*mask*] | {**object** | **object-group**} *name*] [**translated** [**interface** *name*] {*ip_addr* [*mask*] | {**object** | **object-group**} *name*}] [**detail**]

Syntax Description

detail	（可选）包括对象字段更详细的扩展。
interface *name*	（可选）指定源接口。
ip_addr [*mask*]	（可选）指定 IP 地址和子网掩码。
object *name*	（可选）指定网络对象或服务对象。
object-group *name*	（可选）指定网络对象组
translated	（可选）指定转换参数。

Command History

版本	修改
6.1	引入了此命令。

使用指南

使用 **show nat** 命令以显示 NAT 策略的运行时间表示。使用 **detail** 可选关键字以展开对象并查看对象值。使用其他选择器字段以限制 **show nat** 命令输出。

输出显示所有 NAT 命令，甚至是隐藏的命令。例如，如果将管理接口配置为使用数据接口作为网关，则会为隐藏的虚拟接口（例如，nlp_int_tap）创建隐藏的 NAT 规则，以启用管理接口和每个数据接口之间的通信。这些规则不会反映在 设备管理器中的 NAT 表中。您还将看到允许与数据接口建立管理连接的任何 HTTPS/SSH 管理访问规则的隐藏规则，这些规则会反映在 设备管理器的管理访问表中，但不会反映在 NAT 表中。从版本 7.0 开始，系统为自己创建的任何规则都列在第 0 部分中。

示例

以下是 **show nat** 命令的输出示例：

```
> show nat
   Manual NAT Policies (Section 1)
   1 (any) to (any) source dynamic S S' destination static D' D
       translate_hits = 0, untranslate_hits = 0

   Auto NAT Policies (Section 2)
   1 (inside) to (outside) source dynamic A 2.2.2.2
       translate_hits = 0, untranslate_hits = 0

   Manual NAT Policies (Section 3)
   1 (any) to (any) source dynamic C C' destination static B' B service R R'
       translate_hits = 0, untranslate_hits = 0
```

```
> show nat detail
   Manual NAT Policies (Section 1)
   1 (any) to (any) source dynamic S S' destination static D' D
       translate_hits = 0, untranslate_hits = 0
       Source - Real: 1.1.1.2/32, Mapped: 2.2.2.3/32
       Destination - Real: 10.10.10.0/24, Mapped: 20.20.20.0/24

   Auto NAT Policies (Section 2)
   1 (inside) to (outside) source dynamic A 2.2.2.2
       translate_hits = 0, untranslate_hits = 0
       Source - Real: 1.1.1.1/32, Mapped: 2.2.2.2/32

   Manual NAT Policies (Section 3)
   1 (any) to (any) source dynamic C C' destination static B' B service R R'
       translate_hits = 0, untranslate_hits = 0
       Source - Real: 11.11.11.10-11.11.11.11, Mapped: 192.168.10.10/32
       Destination - Real: 192.168.1.0/24, Mapped: 10.75.1.0/24
       Service - Real: tcp source eq 10 destination eq ftp-data , Mapped: tcp source eq
       100 destination eq 200
```

以下是 **show nat detail** 命令在 IPv6 与 IPv4 之间的输出示例：

```
> show nat detail
1 (in) to (outside) source dynamic inside_nw outside_map destination static inside_map any
translate_hits = 0, untranslate_hits = 0
Source - Origin: 2001::/96, Translated: 192.168.102.200-192.168.102.210
Destination - Origin: 2001::/96, Translated: 0.0.0.0/0
```

以下示例显示第 0 部分中系统定义的规则。

```
> show nat detail
Manual NAT Policies Implicit (Section 0)
1 (nlp_int_tap) to (inside) source static nlp_server_0_snmp_intf3 interface  service udp
snmp snmp
    translate_hits = 1, untranslate_hits = 1
    Source - Origin: 169.254.1.2/32, Translated: 10.1.1.122/24
    Service - Protocol: udp Real: snmp Mapped: snmp
2 (nlp_int_tap) to (inside) source dynamic nlp_client_0_intf3 interface
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 169.254.1.2/32, Translated: 10.1.1.122/24

Manual NAT Policies (Section 1)
1 (inside) to (any) source dynamic obj_man interface
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 10.3.3.3/32, Translated: 10.1.1.122/24
```

Related Commands

命令	Description
clear nat counters	清除 NAT 策略计数器。

show nat divert-table

要显示 NAT 转向表的统计信息，请使用 **show nat divert-table** 命令。

show nat divert-table ［**ipv6**］［**interface** *interface_name*］

Syntax Description

divert-table	显示 NAT 转移表。
ipv6	（可选）显示转移表中的 IPv6 条目。
interface *interface_name*	（可选）将输出限制为指定的源接口。

Command History

版本	修改
6.1	引入了此命令。

使用指南

使用 **show nat divert-table** 命令显示 NAT 代理 NAT 转移表的运行时表示。使用 **ipv6** 可选关键字以查看转移表中的 IPv6 条目。使用 **interface** 可选关键字以查看特定源接口的 NAT 转向表。

转向表显示所有NAT命令，甚至是隐藏的命令。例如，如果将管理接口配置为使用数据接口作为网关，则会为隐藏的虚拟接口（例如，nlp_int_tap）创建隐藏的 NAT 规则，以启用管理接口和每个数据接口之间的通信。这些规则不会反映在 设备管理器中的 NAT 表中。

示例

以下是 **show nat divert-table** 命令的输出示例：

```
> show nat divert-table
Divert Table
id=0xad1521b8, domain=twice-nat section=1 ignore=no
        type=none, hits=0, flags=0x9, protocol=0
        src ip/id=0.0.0.0, mask=0.0.0.0, port=0-0
        dst ip/id=10.86.119.255, mask=255.255.255.255, port=0-0
        input_ifc=outside, output_ifc=NP Identity Ifc
id=0xad1523a8, domain=twice-nat section=1 ignore=no
        type=none, hits=0, flags=0x9, protocol=0
        src ip/id=0.0.0.0, mask=0.0.0.0, port=0-0
        dst ip/id=10.86.116.0, mask=255.255.255.255, port=0-0
        input_ifc=outside, output_ifc=NP Identity Ifc
id=0xad1865c0, domain=twice-nat section=1 ignore=no
        type=none, hits=0, flags=0x9, protocol=0
        src ip/id=0.0.0.0, mask=0.0.0.0, port=0-0
        dst ip/id=192.168.255.255, mask=255.255.255.255, port=0-0
        input_ifc=amallio-wizard, output_ifc=NP Identity Ifc
id=0xad1867b0, domain=twice-nat section=1 ignore=no
        type=none, hits=0, flags=0x9, protocol=0
        src ip/id=0.0.0.0, mask=0.0.0.0, port=0-0
        dst ip/id=192.168.0.0, mask=255.255.255.255, port=0-0
        input_ifc=amallio-wizard, output_ifc=NP Identity Ifc
id=0xad257bf8, domain=twice-nat section=1 ignore=no
        type=none, hits=0, flags=0x9, protocol=0
        src ip/id=0.0.0.0, mask=0.0.0.0, port=0-0
```

```
        dst ip/id=172.27.48.255, mask=255.255.255.255, port=0-0
        input_ifc=folink, output_ifc=NP Identity Ifc
id=0xad257db8, domain=twice-nat section=1 ignore=no
        type=none, hits=0, flags=0x9, protocol=0
        src ip/id=0.0.0.0, mask=0.0.0.0, port=0-0
        dst ip/id=172.27.48.0, mask=255.255.255.255, port=0-0
        input_ifc=folink, output_ifc=NP Identity Ifc
```

以下是 **show nat divert ipv6** 命令的输出示例：

```
> show nat divert ipv6
Divert Table
id=0xcb9ea518, domain=divert-route
type=static, hits=0, flags=0x21, protocol=0
src ip/id=2001::/ffff:ffff:ffff:ffff:ffff:ffff::, port=0-0
dst ip/id=2001::/ffff:ffff:ffff:ffff:ffff:ffff::, port=0-0
input_ifc=in, output_ifc=outside
id=0xcf24d4b8, domain=divert-route
type=static, hits=0, flags=0x20, protocol=0
src ip/id=::/::, port=0-0
dst ip/id=2222::/ffff:ffff:ffff:ffff:ffff:ffff::, port=0-0
input_ifc=in, output_ifc=mgmt
```

Related Commands

命令	Description
clear nat counters	清除 NAT 策略计数器。
show nat	显示 NAT 策略的运行时间表示。

show nat pool

要显示 NAT 池使用情况的统计信息，请使用 **show nat pool** 命令。

show nat pool ［ **interface** *if-name* ［ **ip** *address* ］ | **ip** *address* | **detail** ］

show nat pool cluster ［ **summary** | **interface** *if-name* ［ **ip** *address* ］ | **ip** *address* ］

Syntax Description

cluster	（可选）启用群集技术后，将显示当前分配到所有者设备和备用设备的 PAT 地址。 (6.7+) 包括 **summary** 关键字，以查看集群中设备之间的端口块分布情况。
interface *if_name*	将显示限制为指定接口的池。您可以选择包含 **ip** 关键字以进一步限制视图。
ip 地址	将显示限制为 PAT 池中的指定 IP 地址。
detail	显示与集群内端口块的使用和分布相关的信息。仅当设备是集群成员时，才会显示此关键字。不能将其与集群关键字一起使用。

Command History

版本	修改
6.1	引入了此命令。
6.7	添加了以下关键字： **interface**、 **ip**、 **detail**、 **summary**。

使用指南

(Pre-6.7) 为每个映射的协议/IP 地址/端口范围创建 NAT 池，其中端口范围默认为 1-511、512-1023 和 1024-65535。如果将 PAT 池配置为使用平面范围的端口，则会看到更少、更大的范围。

(6.7+) 从 6.7 开始，端口范围默认为平面，您可以选择在池中包含保留的端口 1-1023。对于集群系统，PAT 池以 512 个端口为一组分布在集群成员之间。

每个 NAT 池在上次使用后存在至少 10 分钟。如果您使用 **clear xlate**清除转换，则 10 分钟抑制计时器将被取消。

示例

以下是 **show running-config object network** 命令显示的动态 PAT 规则创建的 NAT 池的输出示例。

```
> show running-config object network
object network myhost
 host 10.10.10.10
 nat (pppoe2,inside) dynamic 10.76.11.25

> show nat pool
TCP inside, address 10.76.11.25, range 1-511, allocated 0
TCP inside, address 10.76.11.25, range 512-1023, allocated 0
```

```
TCP inside, address 10.76.11.25, range 1024-65535, allocated 1
```

以下是**show nat pool**命令展示如何使用PAT池**flat**选项的输出示例。如果没有**include-reserve**关键字，则显示两个范围；低于1024的源端口映射到同一端口时使用较低的范围。

```
> show nat pool
ICMP PAT pool dynamic-pat, address 172.16.2.200, range 1-65535, allocated 2
TCP PAT pool dynamic-pat, address 172.16.2.200, range 1-1024, allocated 0
TCP PAT pool dynamic-pat, address 172.16.2.200, range 1024-65535, allocated 2
UDP PAT pool dynamic-pat, address 172.16.2.200, range 1-1024, allocated 0
UDP PAT pool dynamic-pat, address 172.16.2.200, range 1024-65535, allocated 2
```

以下是**show nat pool**命令的输出示例，显示了PAT池**flat include-reserve**选项的使用。

```
> show nat pool
ICMP PAT pool dynamic-pat, address 172.16.2.200, range 1-65535, allocated 2
TCP PAT pool dynamic-pat, address 172.16.2.200, range 1-65535, allocated 2
UDP PAT pool dynamic-pat, address 172.16.2.200, range 1-65535, allocated 2
```

(Pre-6.7) 以下是**show nat pool**命令的输出示例，其中显示了PAT池**extended flat include-reserve**选项的使用。重要的项目是括号内的地址。这些是用于扩展PAT的目标地址。

```
ICMP PAT pool dynamic-pat, address 172.16.2.200, range 1-65535, allocated 0
ICMP PAT pool dynamic-pat, address 172.16.2.200(172.16.2.99), range 1-65535,
allocated 2
TCP PAT pool dynamic-pat, address 172.16.2.200(172.16.2.100), range 1-65535,
allocated 1
UDP PAT pool dynamic-pat, address 172.16.2.200(172.16.2.100), range 1-65535,
allocated 1
TCP PAT pool dynamic-pat, address 172.16.2.200, range 1-65535, allocated 0
ICMP PAT pool dynamic-pat, address 172.16.2.200(172.16.2.100), range 1-65535,
allocated 1
TCP PAT pool dynamic-pat, address 172.16.2.200(172.16.2.99), range 1-65535,
allocated 2
UDP PAT pool dynamic-pat, address 172.16.2.200, range 1-65535, allocated 0
```

(6.7+)以下示例显示了端口块的分布情况（显示端口范围）及其在集群中的使用情况，包括拥有该块的设备和该块的备用设备。

```
> show nat pool cluster
IP outside_a:src_map_a 174.0.1.20
               [1536  -  2047], owner A, backup B
               [8192  -  8703], owner A, backup B
               [4089  -  4600], owner B, backup A
               [11243  -  11754], owner B, backup A
IP outside_a:src_map_a 174.0.1.21
               [1536  -  2047], owner A, backup B
               [8192  -  8703], owner A, backup B
               [4089  -  4600], owner B, backup A
               [11243  -  11754], owner B, backup A
IP outside_b:src_map_b 174.0.1.22
               [6656 - 7167], owner A, backup B
               [13312 - 13823], owner A, backup B
```

```
               [20480 - 20991], owner B, backup A
               [58368 - 58879], owner B, backup A
IP outside_b:src_map_b 174.0.1.23
               [46592 - 47103], owner A, backup B
               [52224 - 52735], owner A, backup B
               [62976 - 63487], owner B, backup A
```

(6.7+) 以下示例显示集群中的池分配摘要。

```
> show nat pool cluster summary
port-blocks count display order: total, unit-A, unit-B, unit-C, unit-D
IP outside_a:src_map_a, 174.0.1.20 (128 - 32/32/32/32)
IP outside_a:src_map_a, 174.0.1.21 (128 - 36/32/32/28)
IP outside_b:src_map_b, 174.0.1.22 (128 - 31/32/32/33)
```

(6.7+) 以下示例显示了集群中池的 PAT 池的详细使用情况。查看详细输出时，备份端口范围用星号表示。例如：范围 63464-62975，已分配 27 *

```
> show nat pool detail
TCP PAT pool outside_a, address 174.0.1.1
                 range 1536-2047, allocated 56
                 range 8192-8703, allocated 16
UDP PAT pool outside_a, address 174.0.1.1
                 range 1536-2047, allocated 12
                 range 8192-8703, allocated 25
 TCP PAT pool outside_b, address 174.0.2.1
                 range 47104-47615, allocated 39
                 range 62464-62975, allocated 9
UDP PAT pool outside_b, address 174.0.2.1
                 range 47104-47615, allocated 35
                 range 62464-62975, allocated 27
```

(6.7+) 以下示例显示如何将视图限制为特定设备上的特定接口。

```
> show nat pool interface outside_b ip 174.0.2.1
TCP PAT pool outside_b, address 174.0.2.1, range 1-511, allocated 0
TCP PAT pool outside_b, address 174.0.2.1, range 512-1023, allocated 12
TCP PAT pool outside_b, address 174.0.2.1, range 1024-65535, allocated 48
UDP PAT pool outside_b, address 174.0.2.1, range 1-511, allocated 6
UDP PAT pool outside_b, address 174.0.2.1, range 512-1023, allocated 8
UDP PAT pool outside_b, address 174.0.2.1, range 1024-65535, allocated 62
```

Related Commands

命令	Description
show nat	显示 NAT 策略统计信息。

show nat proxy-arp

要显示 NAT 代理 ARP 表，请使用 **show nat proxy-arp** 命令。

show nat proxy-arp ［**ipv6**］［**interface** *name*］

Syntax Description

ipv6	（可选）显示代理 ARP 表中的 IPv6 条目。
interface *name*	（可选）将输出限制为指定的源接口。

Command History

版本	修改
6.1	引入了此命令。

使用指南

使用 **show nat proxy-arp** 命令显示 NAT 代理 ARP 表的运行时间表示。

代理 ARP 表显示所有 NAT 命令，甚至是隐藏的命令。例如，如果将管理接口配置为使用数据接口作为网关，则会为隐藏的虚拟接口（例如，nlp_int_tap）创建隐藏的 NAT 规则，以启用管理接口和每个数据接口之间的通信。这些规则不会反映在 设备管理器中的 NAT 表中。

示例

以下是 **show nat proxy-arp** 命令的输出示例：

```
> show nat proxy-arp
Nat Proxy-arp Table
id=0x00007f4ce491a010, ip/id=0.0.0.0, mask=255.255.255.255 ifc=outside
        config:(inside1_8) to (outside) source dynamic any-ipv4 interface
id=0x00007f4cdc6138d0, ip/id=0.0.0.0, mask=255.255.255.255 ifc=outside
        config:(inside1_7) to (outside) source dynamic any-ipv4 interface
id=0x00007f4ce491d2e0, ip/id=0.0.0.0, mask=255.255.255.255 ifc=outside
        config:(inside1_6) to (outside) source dynamic any-ipv4 interface
id=0x00007f4cdc618a10, ip/id=0.0.0.0, mask=255.255.255.255 ifc=outside
        config:(inside1_5) to (outside) source dynamic any-ipv4 interface
id=0x00007f4d019c9e70, ip/id=0.0.0.0, mask=255.255.255.255 ifc=outside
        config:(inside1_4) to (outside) source dynamic any-ipv4 interface
id=0x00007f4cdc61b300, ip/id=0.0.0.0, mask=255.255.255.255 ifc=outside
        config:(inside1_3) to (outside) source dynamic any-ipv4 interface
id=0x00007f4ce49261f0, ip/id=0.0.0.0, mask=255.255.255.255 ifc=outside
        config:(inside1_2) to (outside) source dynamic any-ipv4 interface
```

Related Commands

命令	Description
clear nat counters	清除 NAT 策略计数器。
show nat	显示 NAT 策略的运行时间表示。

show network

要显示管理接口的属性，请使用 **show network** 命令。

show network

Command History

版本	修改
6.1	引入了此命令。
6.7	此命令现在显示管理和 管理中心 访问数据接口网络设置。

使用指南

使用此命令可查看使用 **configure network** 命令设置的管理接口属性。

如果将管理地址配置为使用数据接口作为网关，则网关显示为“数据接口”。

示例

以下是 **show network** 命令的输出示例。

```
> show network
===============[ System Information ]===============
Hostname                  : 5516X-4
DNS Servers               : 208.67.220.220,208.67.222.222
Management port           : 8305
IPv4 Default route
  Gateway                 : data-interfaces
IPv6 Default route
  Gateway                 : data-interfaces

======================[ br1 ]=======================
State                     : Enabled
Link                      : Up
Channels                  : Management & Events
Mode                      : Non-Autonegotiation
MDI/MDIX                  : Auto/MDIX
MTU                       : 1500
MAC Address               : 28:6F:7F:D3:CB:8D
----------------------[ IPv4 ]----------------------
Configuration             : Manual
Address                   : 10.99.10.4
Netmask                   : 255.255.255.0
Gateway                   : 10.99.10.1
----------------------[ IPv6 ]----------------------
Configuration             : Disabled

===============[ Proxy Information ]================
State                     : Disabled
Authentication            : Disabled

======[ System Information - Data Interfaces ]======
DNS Servers               :
Interfaces                : GigabitEthernet1/1

===============[ GigabitEthernet1/1 ]===============
```

```
State                     : Enabled
Link                      : Up
Name                      : outside
MTU                       : 1500
MAC Address               : 28:6F:7F:D3:CB:8F
----------------------[ IPv4 ]----------------------
Configuration             : Manual
Address                   : 10.89.5.29
Netmask                   : 255.255.255.192
Gateway                   : 10.89.5.1
----------------------[ IPv6 ]----------------------
Configuration             : Disabled
```

show network-dhcp-server

要在管理接口上显示 DHCP 服务器的状态，请使用 **show network-dhcp-server** 命令。

show network-dhcp-server

Command History

版本	修改
6.2	引入了此命令。

使用指南

使用此命令可查看管理接口的可选 DHCP 服务器的状态。要配置 DHCP 服务器，请使用 **configure network ipv4 dhcp-server-enable** 命令。

输出显示 DHCP 服务器是已启用还是已禁用。如果启用，它还会显示地址池。

示例

以下示例显示如何配置 DHCP 服务器并显示其状态。

```
> show network-dhcp-server
DHCP Server Disabled
> configure network ipv4 dhcp-server-enable 192.168.45.46 192.168.45.254
DHCP Server Enabled
> show network-dhcp-server
DHCP Server Enabled
192.168.45.46-192.168.45.254
```

Related Commands

命令	Description
configure network ipv4 dhcp-server-enable	配置管理接口上的 DHCP 服务器。
configure network ipv4 dhcp-server-disable	禁用管理接口上的 DHCP 服务器。

show network-static-routes

要显示管理接口配置的静态路由，请使用 **show network-static-routes** 命令。

show network-static-routes

Command History

版本	修改
6.1	引入了此命令。

使用指南

配置多个管理接口时，使用管理接口的静态路由。这些路由不包括默认网关。如果使用单个管理接口，通常不会有其他静态路由。

使用此命令显示的路由仅适用于管理接口。任何数据接口都不使用它们。它们不用于通过设备的流量。

示例

以下示例显示管理接口没有其他静态路由。默认网关是唯一的路由。

```
> show network-static-routes
No static routes currently configured.
```

以下示例显示一个静态路由。

```
> show network-static-routes
---------------[ IPv4 Static Routes ]---------------
Interface                 : br1
Destination               : 10.1.1.0
Gateway                   : 192.168.0.254
Netmask                   : 255.255.255.0
```

Related Commands

命令	Description
configure network static-routes	为管理接口配置静态路由。

show ntp

要显示当前的网络时间协议 (NTP) 服务器和配置，请使用 **show ntp** 命令。

show ntp

Command History

版本	修改
6.1	引入了此命令。

使用指南

此命令显示有关 NTP 服务器的基本信息。如果您需要更全面的信息，请使用 **system support ntp** 命令，包括此命令的输出以及标准 NTP 命令 **ntpq**（该命令记录在 NTP 协议中）的输出。

示例

以下示例显示如何显示 NTP 配置。

```
> show ntp
NTP Server                : 209.208.79.69
Status                    : Available
Offset                    : -1.614 (milliseconds)
Last Update               : 578 (seconds)

NTP Server                : 45.127.112.2  (clocka.ntpjs.org)
Status                    : Available
Offset                    : -1.355 (milliseconds)
Last Update               : 874 (seconds)

NTP Server                : 198.58.105.63  (ha81.smatwebdesign.com)
Status                    : Not Available
Offset                    : -4.942 (milliseconds)
Last Update               : 369 (seconds)

NTP Server                : 204.9.54.119  (ntp.your.org)
Status                    : Being Used
Offset                    : 0.312 (milliseconds)
Last Update               : 962 (seconds)
```

以下示例显示如何使用 **system support ntp** 命令获取其他信息。如果需要确认 NTP 同步，请使用此命令。

查找“Results of ‘ntpq -pn’ ”部分。例如，您可能会看到类似如下的内容：

```
> system support ntp
... output redacted ...
Results of 'ntpq -pn'
remote                    : +216.229.0.50
refid                     : 129.7.1.66
st                        : 2
t                         : u
when                      : 704
poll                      : 1024
reach                     : 377
```

```
delay                       : 90.455
offset                      : 2.954
jitter                      : 2.473
... remaining output redacted ...
```

在本例中，NTP 服务器地址前的 + 表示作为潜在候选者。此处的星号 * 表示当前的时间源对等体。

NTP 后台守护程序 (NTPD) 使用每个对等体中的八个示例的滑动窗口，并选出一个示例，然后根据时钟选择确定正确的报时器和错误的断续器。然后，NTPD 会确定往返距离（候补者的偏移不得超过往返延迟的一半）。如果连接延迟、丢包或服务器问题导致一个或全部候补者被拒绝，则同步中会出现较长的延迟。而且，该调整很长一段时间后才会完成：时钟偏移和振荡器错误必须通过时钟训练算法解决，这可能会需要数小时的时间。

注释 如果 refid 是 .LOCL.，则表明对等体是一个未经训练的本地时钟，也即它只使用其本地时钟来设置时间。如果所选的对等体是 .LOCL.，则 设备管理器 始终将 NTP 连接标为黄色（未同步）。如果还有更好的证书，NTP 通常不会选择 .LOCL. 证书，这就是应配置至少三个服务器的原因所在。

Related Commands

命令	Description
system support ntp	显示 NTP 的详细故障排除信息。

show object

要显示有关网络服务对象的信息（包括命中计数和 IP 地址），请使用 **show object** 命令。

show object [**id** *object_name* | **network-service** [**detail**]]

Syntax Description

id *name*	（可选）要查看的对象的名称。大小写很重要。例如，“object-name”与“Object-Name”不匹配。
network-service [**detail**]	（可选。）显示所有网络服务对象。包括细节关键字以查看与对象成员关联的缓存 IP 地址。

Command Default

如果没有参数，则显示所有对象。

Command History

版本	修改
7.1	引入了此命令。

示例

以下示例显示名为 Cisco 的网络服务对象的详细信息。app-id（应用 ID）是内部编号。hitcnt（命中计数）是显示的唯一相关指标。

```
> show object id Cisco
object network-service "Cisco" dynamic
 description Official website for Cisco.
 app-id 2655
 domain cisco.com (bid=0) ip (hitcnt=0)
```

Related Commands

命令	Description
clear object	清除网络服务对象命中计数。
show object-groups	显示网络服务对象组和命中计数。

show object-group

要显示对象组信息和相关命中计数（如果对象组为 network 或 network-service object-group 类型），请使用 **show object-group** 命令。使用不带参数的 命令可查看所有类型的对象组。

show object-group [**count** | **interface** | **network** | **security** | **service** | **id** *name*]

show object-group network-service [*group_name* [**network-service-member** *member_name* [**dns** *domain_name*]] [**detail**]

Syntax Description

count	（可选。）显示与对象组数量和这些组中的对象数量相关的统计信息，以及它们的使用方式。
detail	对于网络服务对象，显示与对象成员关联的缓存 IP 地址。
dns *domain_name*	（可选。）对于按名称和成员指定的网络服务对象，将信息限制为该成员的特定域。例如 example.com。
id *name*	（可选）按名称标识对象组。
interface	（可选）接口类型对象
network	（可选）网络类型对象。
network-service [*group_name*]	（可选。）网络服务对象。您可以指定对象名称以将信息限制为单个对象。
network-service-member *member_name*	（可选。）对于按名称指定的网络服务对象，将信息限制为该对象的特定成员。
security	（可选）安全类型对象
service	（可选）服务类型对象。

Command History

版本	修改
6.1	引入了此命令。
7.1	我们添加了 **network-service** 关键字及其关联的参数。
7.2	添加了 **count** 关键字。

示例

以下是 **show object-group** 命令的输出示例，显示关于名为“Anet”的网络对象组的信息：

```
> show object-group id Anet
```

```
Object-group network Anet (hitcnt=10)
   Description OBJ SEARCH ALG APPLIED
   network-object 1.1.1.0 255.255.255.0 (hitcnt=4)
   network-object 2.2.2.0 255.255.255.0 (hitcnt=6)
```

以下是 **show object-group** 命令的输出示例，显示关于服务组的信息：

```
> show object-group service
object-group service B-Serobj
   description its a service group
   service-object tcp eq bgp
```

以下示例显示了网络服务对象及其命中计数。网络服务组 ID (nsg-id)、应用 ID (app-id) 和出价等各种标识符是可以忽略的内部索引编号。

```
> show object-group network-service FMC_NSG_4294969442
object-group network-service FMC_NSG_4294969442 (nsg-id 512/1)
 network-service-member "Facebook" dynamic
  description Facebook is a social networking service.
  app-id 629
  domain connect.facebook.net (bid=214491) ip (hitcnt=0)
  domain facebook.com (bid=370809) ip (hitcnt=0)
  domain fbcdn.net (bid=490321) ip (hitcnt=0)
  domain fbcdn-photos-a.akamaihd.net (bid=548791) ip (hitcnt=0)
  domain fbcdn-photos-e-a.akamaihd.net (bid=681143) ip (hitcnt=0)
  domain fbcdn-photos-b-a.akamaihd.net (bid=840741) ip (hitcnt=0)
  domain fbstatic-a.akamaihd.net (bid=1014669) ip (hitcnt=0)
  domain fbexternal-a.akamaihd.net (bid=1098051) ip (hitcnt=0)
  domain fbcdn-profile-a.akamaihd.net (bid=1217875) ip (hitcnt=0)
  domain fbcdn-creative-a.akamaihd.net (bid=1379985) ip (hitcnt=0)
  domain channel.facebook.com (bid=1524617) ip (hitcnt=0)
  domain fbcdn-dragon-a.akamaihd.net (bid=1683343) ip (hitcnt=0)
  domain contentcache-a.akamaihd.net (bid=1782703) ip (hitcnt=0)
  domain facebook.net (bid=1868733) ip (hitcnt=0)
 network-service-member "Google+ Videos" dynamic
  description Video sharing among Google+ community.
  app-id 2881
  domain plus.google.com (bid=2068293) ip (hitcnt=0)
 network-service-member "Instagram" dynamic
  description Mobile phone photo sharing.
  app-id 1233
  domain instagram.com (bid=2176667) ip (hitcnt=0)
 network-service-member "LinkedIn" dynamic
  description Career oriented social networking.
  app-id 713
  domain linkedin.com (bid=2317259) ip (hitcnt=0)
>
```

以下示例显示了对象计数，以便您了解对象组的数量、组中包含的对象数量以及ACL、NAT等中使用的对象数量。此信息与对象组搜索功能的性能相关。

```
ciscoasa(config)# show object-group count

Object Group Name                     Group Count Dyn Count V4 CNT     V6 CNT     ACL CNT
    NAT CNT    OG in OG
network    i28Z-route                 68          0          68         0          0
      0          0
network    i28Z-VRF-BGP-PEERS         4           0          4          0          2
      0          0
network    EXCH-BGP-PEERS             4           0          4          0          2
```

```
      0          0
network    obgr_SUBNETS_NO_ACL         112          0           112          0          0
      0          0
network    obgr_SUBNETS_ACL_ASAMgmt    1            0           1            0          0
      0          0
network    obgr_CLIENTS_ACL_ASAMgmt    8            0           8            0          1
      0          0
network    obgr_SUBNETS_CGS_vMotion    1            0           1            0          0
      0          0
network    obgr_CLIENTS_CGS_vMotion    9            0           9            0          1
      0          0
network    obgr_SUBNETS_UPMCOD_CGS     17           0           17           0          0
      0          0
network    obgr_CLIENTS_UPMCOD_CGS     90           0           90           0          1
      0          0
network    obgr_CLIENTS_10.68.0.0_16   2            0           2            0          1
      0          0
network    obgr_CLIENTS_10.68.1.198_31 4            0           4            0          1
      0          0
network    obgr_CLIENTS_10.68.73.133   7            0           7            0          1
      0          0
network    asa_zabbix_proxies          4            0           4            0          1
      0          0

Total Summary
Object-group count                          14
Object-group object count                   331
Object-group Dynamic count                  0
Object-group IPv4 count                     331
Object-group IPv6 count                     0
Object-group Used in ACL                    9
Object-group Used in NAT                    0
Object-group Unused                         5
Object-group Internal                       0
Object-group Dummy                          0
Redundant object-group in Network           4
Redundant object-group in IfC               0
```

Related Commands

命令	Description
clear object-group	清除指定对象组的网络对象命中计数。
show access-list	显示所有访问列表、相关扩展访问列表条目以及命中计数。
show object	显示网络服务对象和命中计数。

show ospf

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

show ospf ［**vrf** *name* | **all**］ ［*pid* ［*area_id*］］

Syntax Description

area_id	（可选）与 OSPF 地址范围关联的区域的 ID。
pid	（可选）OSPF 流程的 ID。
［**vrf** *name*	**all**］	如果启用虚拟路由和转发 (VRF)（也称为虚拟路由器），则可以使用 **vrf** *name* 关键字将该命令限制为特定虚拟路由器。如果您希望 命令影响所有虚拟路由器，请包含 **all** 关键字。如果不包括这些与 VRF 相关的关键字，则 命令适用于全局 VRF 虚拟路由器。

Command History

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

示例

以下是 **show ospf** 命令的输出示例，展示如何显示关于特定 OSPF 路由流程的一般信息：

```
> show ospf 5
 Routing Process "ospf 5" with ID 127.0.0.1 and Domain ID 0.0.0.5
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
 Number of external LSA 0. Checksum Sum 0x     0
 Number of opaque AS LSA 0. Checksum Sum 0x     0
 Number of DCbitless external and opaque AS LSA 0
 Number of DoNotAge external and opaque AS LSA 0
 Number of areas in this router is 0. 0 normal 0 stub 0 nssa
 External flood list length 0
```

以下是 **show ospf** 命令的输出示例，展示如何显示关于所有 OSPF 路由流程的一般信息：

```
> show ospf
 Routing Process "ospf 5" with ID 127.0.0.1 and Domain ID 0.0.0.5
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
 Number of external LSA 0. Checksum Sum 0x     0
 Number of opaque AS LSA 0. Checksum Sum 0x     0
 Number of DCbitless external and opaque AS LSA 0
 Number of DoNotAge external and opaque AS LSA 0
```

```
Number of areas in this router is 0. 0 normal 0 stub 0 nssa
External flood list length 0

Routing Process "ospf 12" with ID 172.23.59.232 and Domain ID 0.0.0.12
Supports only single TOS(TOS0) routes
Supports opaque LSA
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
Number of external LSA 0. Checksum Sum 0x     0
Number of opaque AS LSA 0. Checksum Sum 0x     0
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 0. 0 normal 0 stub 0 nssa
External flood list length 0
```

show ospf border-routers

要向 ABR 和 ASBR 显示内部 OSPF 路由表条目，请使用 **show ospf border-routers** 命令。

show ospf border-routers ［**vrf** *name* | **all**］

Syntax Description

［**vrf** *name*	**all**］	如果启用虚拟路由和转发 (VRF)（也称为虚拟路由器），则可以使用 **vrf** *name* 关键字将该命令限制为特定虚拟路由器。如果您希望 命令影响所有虚拟路由器，请包含 **all** 关键字。如果不包括这些与 VRF 相关的关键字，则 命令适用于全局 VRF 虚拟路由器。

Command History

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

示例

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

```
> show ospf border-routers

OSPF Process 109 internal Routing Table

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

i 192.168.97.53 [10] via 192.168.1.53, fifth, ABR, Area 0, SPF 20
i 192.168.103.51 [10] via 192.168.96.51, outside, ASBR, Area 192.168.12.0, SPF 14
i 192.168.103.52 [10] via 192.168.96.51, outside, ABR/ASBR, Area 192.168.12.0, SPF 14
```

show ospf database

要显示 OSPF 拓扑数据库中包含的信息，请使用 **show ospf database** 命令。

show ospf ［**vrf** *name* | **all**］ ［*pid* ［*area_id*］］ **database** ［**router** | **network** | **summary** | **asbr-summary** | **external** | **nssa-external**］［*lsid*］［**internal**］［**self-originate** | **adv-router** *addr*］
show ospf ［*pid* ［*area_id*］］ **database database-summary**

Syntax Description

addr	（可选）路由器地址。
adv-router	（可选）通告的路由器。
area_id	（可选）与 OSPF 地址范围关联的区域的 ID。
asbr-summary	（可选）显示 ASBR 列表摘要。
database	显示数据库信息。
database-summary	（可选）显示完整的数据库摘要列表。
external	（可选）显示指定自主系统外部的路由。
internal	（可选）指定自主系统内部的路由。
lsid	（可选）LSA ID。
network	（可选）显示有关网络 LSA 的信息。
nssa-external	（可选）显示外部末节区域列表。
pid	（可选）OSPF 进程的 ID。
router	（可选）显示路由器。
self-originate	（可选）显示指定自主系统的信息。
summary	（可选）显示列表的摘要。
［**vrf** *name*	**all**］	如果启用虚拟路由和转发 (VRF)（也称为虚拟路由器），则可以使用 **vrf** *name* 关键字将该命令限制为特定虚拟路由器。如果您希望 命令影响所有虚拟路由器，请包含 **all** 关键字。如果不包括这些与 VRF 相关的关键字，则 命令适用于全局 VRF 虚拟路由器。

Command History

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

示例

以下是 **show ospf database** 命令的输出示例：

```
> show ospf database
OSPF Router with ID(192.168.1.11) (Process ID 1)

                Router Link States(Area 0)
Link ID   ADV Router   Age   Seq# Checksum Link count
192.168.1.8 192.168.1.8 1381 0x8000010D    0xEF60 2
192.168.1.11 192.168.1.11 1460 0x800002FE    0xEB3D 4
192.168.1.12 192.168.1.12 2027 0x80000090    0x875D 3
192.168.1.27 192.168.1.27 1323 0x800001D6    0x12CC 3

                Net Link States(Area 0)
Link ID ADV Router   Age   Seq# Checksum
172.16.1.27 192.168.1.27 1323 0x8000005B    0xA8EE
172.17.1.11 192.168.1.11 1461 0x8000005B    0x7AC

                Type-10 Opaque Link Area Link States (Area 0)
Link ID ADV Router   Age Seq# Checksum Opaque ID
10.0.0.0 192.168.1.11 1461 0x800002C8    0x8483   0
10.0.0.0 192.168.1.12 2027 0x80000080    0xF858   0
10.0.0.0 192.168.1.27 1323 0x800001BC    0x919B   0
10.0.0.1 192.168.1.11 1461 0x8000005E    0x5B43   1
```

以下是 **show ospf database asbr-summary** 命令的输出示例：

```
> show ospf database asbr-summary
OSPF Router with ID(192.168.239.66) (Process ID 300)
Summary ASB Link States(Area 0.0.0.0)
Routing Bit Set on this LSA
LS age: 1463
Options: (No TOS-capability)
LS Type: Summary Links(AS Boundary Router)
Link State ID: 172.16.245.1 (AS Boundary Router address)
Advertising Router: 172.16.241.5
LS Seq Number: 80000072
Checksum: 0x3548
Length: 28
Network Mask: 0.0.0.0
TOS: 0 Metric: 1
```

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

```
> show ospf database router
OSPF Router with id(192.168.239.66) (Process ID 300)
Router Link States(Area 0.0.0.0)
Routing Bit Set on this LSA
LS age: 1176
Options: (No TOS-capability)
LS Type: Router Links
Link State ID: 10.187.21.6
Advertising Router: 10.187.21.6
LS Seq Number: 80002CF6
Checksum: 0x73B7
Length: 120
AS Boundary Router
```

```
Number of Links: 8
Link connected to: another Router (point-to-point)
(link ID) Neighboring Router ID: 10.187.21.5
(Link Data) Router Interface address: 10.187.21.6
Number of TOS metrics: 0
TOS 0 Metrics: 2
```

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

```
> show ospf database network
OSPF Router with id(192.168.239.66) (Process ID 300)
Displaying Net Link States(Area 0.0.0.0)
LS age: 1367
Options: (No TOS-capability)
LS Type: Network Links
Link State ID: 10.187.1.3 (address of Designated Router)
Advertising Router: 192.168.239.66
LS Seq Number: 800000E7
Checksum: 0x1229
Length: 52
Network Mask: 255.255.255.0
Attached Router: 192.168.239.66
Attached Router: 10.187.241.5
Attached Router: 10.187.1.1
Attached Router: 10.187.54.5
Attached Router: 10.187.1.5
```

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

```
> show ospf database summary
OSPF Router with id(192.168.239.66) (Process ID 300)
Displaying Summary Net Link States(Area 0.0.0.0)
LS age: 1401
Options: (No TOS-capability)
LS Type: Summary Links(Network)
Link State ID: 10.187.240.0 (summary Network Number)
Advertising Router: 10.187.241.5
LS Seq Number: 80000072
Checksum: 0x84FF
Length: 28
Network Mask: 255.255.255.0 TOS: 0 Metric: 1
```

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

```
> show ospf database external
OSPF Router with id(192.168.239.66) (Autonomous system 300)

                  Displaying AS External Link States
LS age: 280
Options: (No TOS-capability)
LS Type: AS External Link
Link State ID: 172.16.0.0 (External Network Number)
Advertising Router: 10.187.70.6
LS Seq Number: 80000AFD
Checksum: 0xC3A
Length: 36
Network Mask: 255.255.0.0

      Metric Type: 2 (Larger than any link state path)
```

```
TOS: 0
Metric: 1
Forward Address: 0.0.0.0
External Route Tag: 0
```

show ospf events

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

show ospf ［**vrf** *name* | **all**］ ［*process_id*］ **events** ［*type*］

Syntax Description

process_id	（可选）指定本地分配的内部ID，可以是任何正整数。启用OSPF路由流程时，此 ID 是管理性分配的号码。
type	（可选）要查看的事件类型的列表。如果不指定一种或多种类型，则会看到所有事件。您可以过滤以下类型： • **generic**-通用事件。 • **interface**- 接口状态更改事件。 • **lsa**- LSA 到达和 LSA 生成事件。 • **neighbor**- 邻居状态更改事件。 • **reverse**- 以相反的顺序显示事件。 • **rib**- 路由器信息库更新、删除和重新分发事件。 • **spf**- SPF 计划和 SPF 运行事件。
［**vrf** *name*	**all**］	如果启用虚拟路由和转发 (VRF)（也称为虚拟路由器），则可以使用 **vrf** *name* 关键字将该命令限制为特定虚拟路由器。如果您希望 命令影响所有虚拟路由器，请包含 **all** 关键字。如果不包括这些与 VRF 相关的关键字，则 命令适用于全局 VRF 虚拟路由器。

Command History

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

示例

以下是 **show ospf events** 命令的输出示例：

```
> show ospf events

            OSPF Router with ID (192.168.77.1) (Process ID 5)

  1 Apr 27 16:33:23.556: RIB Redist, dest 0.0.0.0, mask 0.0.0.0, Up
  2 Apr 27 16:33:23.556: Rescanning RIB:  0x00x0
  3 Apr 27 16:33:23.556: Service Redist scan:  0x00x0
```

Related Commands

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

show ospf flood-list

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

show ospf flood-list ［**vrf** *name* | **all**］ *interface_name*

Syntax Description

interface_name	要显示邻居信息的接口的名称。
［**vrf** *name*	**all**］	如果启用虚拟路由和转发 (VRF)（也称为虚拟路由器），则可以使用 **vrf** *name* 关键字将该命令限制为特定虚拟路由器。如果您希望 命令影响所有虚拟路由器，请包含 **all** 关键字。如果不包括这些与 VRF 相关的关键字，则 命令适用于全局 VRF 虚拟路由器。

Command History

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

示例

以下是 **show ospf flood-list** 命令的输出示例：

```
> show ospf flood-list outside

  Interface outside, Queue length 20
  Link state flooding due in 12 msec

  Type  LS ID          ADV RTR          Seq NO       Age   Checksum
     5  10.2.195.0     192.168.0.163    0x80000009   0     0xFB61
     5  10.1.192.0     192.168.0.163    0x80000009   0     0x2938
     5  10.2.194.0     192.168.0.163    0x80000009   0     0x757
     5  10.1.193.0     192.168.0.163    0x80000009   0     0x1E42
     5  10.2.193.0     192.168.0.163    0x80000009   0     0x124D
     5  10.1.194.0     192.168.0.163    0x80000009   0     0x134C
```

show ospf interface

要显示 OSPF 相关接口信息，请使用 **show ospf interface** 命令。

show ospf interface ［**vrf** *name* | **all**］ ［*interface_name*］

Syntax Description

interface_name	（可选）要显示 OSPF 相关信息的接口的名称。
［**vrf** *name*	**all**］	如果启用虚拟路由和转发 (VRF)（也称为虚拟路由器），则可以使用 **vrf** *name* 关键字将该命令限制为特定虚拟路由器。如果您希望 命令影响所有虚拟路由器，请包含 **all** 关键字。如果不包括这些与 VRF 相关的关键字，则 命令适用于全局 VRF 虚拟路由器。

Command Default

当不指定接口名称时，则会显示所有接口的 OSPF 信息。

Command History

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

示例

以下是 **show ospf interface** 命令的输出示例：

```
> show ospf interface outside
out is up, line protocol is up
  Internet Address 10.0.3.4 mask 255.255.255.0, Area 0
  Process ID 2, Router ID 10.0.3.4, Network Type BROADCAST, Cost: 10
  Transmit Delay is 1 sec, State WAITING, Priority 1
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 10 msec, Dead 1, Wait 1, Retransmit 5
    Hello due in 5 msec
    Wait time before Designated router selection 0:00:11
  Index 1/1, flood queue length 0
  Next 0x00000000(0)/0x00000000(0)
  Last flood scan length is 0, maximum is 0
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
```

show ospf neighbor

要显示每个接口上的 OSPF 邻居信息，请使用 **show ospf neighbor** 命令。

show ospf neighbor ［**vrf** *name* | **all**］ ［**detail** | *interface_name* ［*nbr_router_id*］］

Syntax Description

detail	（可选）列出指定路由器的详细信息。
interface_name	（可选）要显示邻居信息的接口的名称。
nbr_router_id	（可选）邻居路由器的路由器 ID。
［**vrf** *name*	**all**］	如果启用虚拟路由和转发 (VRF)（也称为虚拟路由器），则可以使用 **vrf** *name* 关键字将该命令限制为特定虚拟路由器。如果您希望 命令影响所有虚拟路由器，请包含 **all** 关键字。如果不包括这些与 VRF 相关的关键字，则 命令适用于全局 VRF 虚拟路由器。

Command History

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

示例

以下是 **show ospf neighbor** 命令的输出示例。它基于每个接口展示如何显示 OSPF 邻居信息。

```
> show ospf neighbor outside

Neighbor 192.168.5.2, interface address 10.225.200.28
    In the area 0 via interface outside
    Neighbor priority is 1, State is FULL, 6 state changes
    DR is 10.225.200.28 BDR is 10.225.200.30
    Options is 0x42
    Dead timer due in 00:00:36
    Neighbor is up for 00:09:46
  Index 1/1, retransmission queue length 0, number of retransmission 1
    First 0x0(0)/0x0(0) Next 0x0(0)/0x0(0)
    Last retransmission scan length is 1, maximum is 1
    Last retransmission scan time is 0 msec, maximum is 0 msec
```

以下是 **show ospf neighbor detail** 命令的输出示例。它展示如何显示指定 OSPF 邻居的详细信息。

```
> show ospf neighbor detail

Neighbor 25.1.1.60, interface address 15.1.1.60
    In the area 0 via interface inside
```

```
Neighbor priority is 1, State is FULL, 46 state changes
DR is 15.1.1.62 BDR is 15.1.1.60
Options is 0x12 in Hello (E-bit, L-bit)
Options is 0x52 in DBD (E-bit, L-bit, O-bit)
LLS Options is 0x1 (LR), last OOB-Resync 00:03:07 ago
Dead timer due in 0:00:24
Neighbor is up for 01:42:15
Index 5/5, retransmission queue length 0, number of retransmission 0
First 0x0(0)/0x0(0) Next 0x0(0)/0x0(0)
Last retransmission scan length is 0, maximum is 0
Last retransmission scan time is 0 msec, maximum is 0 msec
```

show ospf nsf

要显示 OSPFv2 相关的 NSF 信息，请使用 **show ospf nsf** 命令。

show ospf nsf ［**vrf** *name* | **all**］

Syntax Description

［**vrf** *name*	**all**］	如果启用虚拟路由和转发 (VRF)（也称为虚拟路由器），则可以使用 **vrf** *name* 关键字将该命令限制为特定虚拟路由器。如果您希望 命令影响所有虚拟路由器，请包含 **all** 关键字。如果不包括这些与 VRF 相关的关键字，则 命令适用于全局 VRF 虚拟路由器。

Command History

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

示例

以下是 **show ospf nsf** 命令的输出示例：

```
> show ospf nsf
Routing Process "ospf 10"
Non-Stop Forwarding enabled
    Clustering is not configured in spanned etherchannel mode
IETF NSF helper support enabled
Cisco NSF helper support enabled
    OSPF restart state is
    Handle 1, Router ID 25.1.1.60, checkpoint Router ID 0.0.0.0
    Config wait timer interval 10, timer not running
    Dbase wait timer interval 120, timer not running
```

show ospf request-list

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

show ospf request-list ［**vrf** *name* | **all**］ *nbr_router_id interface_name*

Syntax Description

interface_name	要显示邻居信息的接口的名称。显示路由器从此接口请求的所有 LSA 的列表。
nbr_router_id	邻居路由器的路由器 ID。显示路由器从此邻居请求的所有 LSA 的列表。
［**vrf** *name*	**all**］	如果启用虚拟路由和转发 (VRF)（也称为虚拟路由器），则可以使用 **vrf** *name* 关键字将该命令限制为特定虚拟路由器。如果您希望 命令影响所有虚拟路由器，请包含 **all** 关键字。如果不包括这些与 VRF 相关的关键字，则 命令适用于全局 VRF 虚拟路由器。

Command History

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

示例

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

```
> show ospf request-list 192.168.1.12 inside

         OSPF Router with ID (192.168.1.11) (Process ID 1)

 Neighbor 192.168.1.12, interface inside address 172.16.1.12

 Type   LS ID          ADV RTR        Seq NO       Age   Checksum
    1   192.168.1.12   192.168.1.12   0x8000020D   8     0x6572
```

Related Commands

命令	Description
show ospf retransmission-list	显示等待重新发送的所有 LSA 的列表。

show ospf retransmission-list

要显示等待为特定邻居和接口重新发送的所有 LSA 的列表，请使用 **show ospf retransmission-list** 命令。

show ospf retransmission-list ［**vrf** *name* | **all**］ *nbr_router_id interface_name*

Syntax Description

interface_name	要显示邻居信息的接口的名称。
nbr_router_id	邻居路由器的路由器 ID。
［**vrf** *name*	**all**］	如果启用虚拟路由和转发 (VRF)（也称为虚拟路由器），则可以使用 **vrf** *name* 关键字将该命令限制为特定虚拟路由器。如果您希望 命令影响所有虚拟路由器，请包含 **all** 关键字。如果不包括这些与 VRF 相关的关键字，则 命令适用于全局 VRF 虚拟路由器。

Command History

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

示例

以下是外部接口上 192.168.1.11 邻居路由器的 **show ospf retransmission-list** 命令输出示例。

```
> show ospf retransmission-list 192.168.1.11 outside

         OSPF Router with ID (192.168.1.12) (Process ID 1)

  Neighbor 192.168.1.11, interface outside address 172.16.1.11

  Link state retransmission due in 3764 msec, Queue length 2
  Type   LS ID          ADV RTR        Seq NO       Age   Checksum
     1   192.168.1.12   192.168.1.12   0x80000210   0     0xB196
```

Related Commands

命令	Description
show ospf request-list	显示路由器请求的所有 LSA 的列表。

show ospf rib

要显示 OSPF 路由器信息库 (RIB)，请使用 **show ospf rib** 命令。

show ospf ［**vrf** *name* | **all**］ ［*process_id* ［*area_id*］］ **rib** ［*network_prefix* ［*network_mask*］］ | **detail** | **redistribution** ［*network_prefix* ［*network_mask*］］ | **detail**］］

Syntax Description

process_id	（可选）OSPF 流程的 ID。
area_id	（可选）与 OSPF 地址范围关联的区域的 ID。
network_prefix [*network_mask*]	（可选）要查看的路由的网络前缀和掩码（可选），例如： 10.100.10.1 10.100.10.0 255.255.255.0
detail	（可选）显示有关 RIB 的详细信息。
redistribution	（可选）显示重新分发信息。您还可以在重新分发 **detail** 关键字后指定网络前缀和掩码或关键字。
［**vrf** *name*	**all**］	如果启用虚拟路由和转发 (VRF)（也称为虚拟路由器），则可以使用 **vrf** *name* 关键字将该命令限制为特定虚拟路由器。如果您希望 命令影响所有虚拟路由器，请包含 **all** 关键字。如果不包括这些与 VRF 相关的关键字，则 命令适用于全局 VRF 虚拟路由器。

Command History

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

show ospf statistics

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

show ospf ［**vrf** *name* | **all**］ ［*process_id*］ **statistics** ［**detail**］

Syntax Description

detail	（可选）指定详细 SPF 信息，包括触发点。
process_id	（可选）指定本地分配的内部ID，可以是任何正整数。启用OSPF路由流程时，此 ID 是管理性分配的号码。
［**vrf** *name*	**all**］	如果启用虚拟路由和转发 (VRF)（也称为虚拟路由器），则可以使用 **vrf** *name* 关键字将该命令限制为特定虚拟路由器。如果您希望 命令影响所有虚拟路由器，请包含 **all** 关键字。如果不包括这些与 VRF 相关的关键字，则 命令适用于全局 VRF 虚拟路由器。

Command History

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

示例

以下是 **show ospf statistics** 命令的输出示例：

```
> show ospf 10 statistics 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 ospf summary-address

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

show ospf summary-address ［**vrf** *name* | **all**］

Syntax Description

［**vrf** *name* | **all**］	如果启用虚拟路由和转发 (VRF)（也称为虚拟路由器），则可以使用 **vrf** *name* 关键字将该命令限制为特定虚拟路由器。如果您希望 命令影响所有虚拟路由器，请包含 **all** 关键字。如果不包括这些与 VRF 相关的关键字，则 命令适用于全局 VRF 虚拟路由器。

Command History

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

示例

以下显示 **show ospf summary-address** 命令的输出示例。它展示如何在为 ID 为 5 的 OSPF 流程配置摘要地址之前显示所有摘要地址重分布信息的列表。

```
> show ospf 5 summary-address

OSPF Process 2, Summary-address

10.2.0.0/255.255.0.0 Metric -1, Type 0, Tag 0
10.2.0.0/255.255.0.0 Metric -1, Type 0, Tag 10
```

show ospf traffic

要显示已由特定 OSPF 实例处理（发送或接收）的不同类型数据包的列表，请使用 **show ospf traffic** 命令。

show ospf traffic ［**vrf** *name* | **all**］

Syntax Description

［**vrf** *name*	**all**］	如果启用虚拟路由和转发 (VRF)（也称为虚拟路由器），则可以使用 **vrf** *name* 关键字将该命令限制为特定虚拟路由器。如果您希望 命令影响所有虚拟路由器，请包含 **all** 关键字。如果不包括这些与 VRF 相关的关键字，则 命令适用于全局 VRF 虚拟路由器。

Command History

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

使用指南

通过此命令，您可以获取处理的不同类型 OSPF 数据包的快照而无需启用调试。如果配置了两个 OSPF 实例，则 **show ospf traffic** 命令会显示两个实例的统计信息及每个实例的流程 ID。您还可以通过使用 **show ospf** *process_id* **traffic** 命令显示单一实例的统计信息。

示例

以下显示 **show ospf traffic** 命令的输出示例。

```
> show ospf traffic

OSPF statistics (Process ID 70):

       Rcvd: 244 total, 0 checksum errors
             234 hello, 4 database desc, 1 link state req
             3 link state updates, 2 link state acks
       Sent: 485 total
             472 hello, 7 database desc, 1 link state req
             3 link state updates, 2 link state acks
```

Related Commands

命令	Description
show ospf virtual-links	显示 OSPF 虚拟链路的参数和当前状态。

show ospf virtual-links

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

show ospf virtual-links ［**vrf** *name* | **all**］

Syntax Description

［**vrf** *name*	**all**］	如果启用虚拟路由和转发 (VRF)（也称为虚拟路由器），则可以使用 **vrf** *name* 关键字将该命令限制为特定虚拟路由器。如果您希望 命令影响所有虚拟路由器，请包含 **all** 关键字。如果不包括这些与 VRF 相关的关键字，则 命令适用于全局 VRF 虚拟路由器。

Command History

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

示例

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

```
> show ospf virtual-links

Virtual Link to router 192.168.101.2 is up
Transit area 0.0.0.1, via interface Ethernet0, Cost of using 10
Transmit Delay is 1 sec, State POINT_TO_POINT
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 0:00:08
Adjacency State FULL
```

当地语言翻译版本说明

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