目 录

1 连接数限制

1.1 连接数限制配置命令

1.1.1 connection-limit

connection-limit 命令用来创建连接数限制策略，并进入连接数限制策略视图。如果指定的连接数限制策略已经存在，则直接进入连接数限制策略视图。

undo connection-limit 命令用来删除连接数限制策略。

【命令】

connection-limit { **ipv6-policy** | **policy** } *policy-id*

undo connection-limit { **ipv6-policy** | **policy** } *policy-id*

【缺省情况】

不存在连接数限制策略。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

ipv6-policy：指定 IPv6 连接数限制策略。

policy：指定 IPv4 连接数限制策略。

policy-id：连接数限制策略编号（IPv4、IPv6 连接数限制策略的编号空间各自独立），取值范围为 1～32。

【举例】

创建编号为 1 的 IPv4 连接数限制策略，并进入 IPv4 连接数限制策略视图。

```
<Sysname> system-view
[Sysname] connection-limit policy 1
[Sysname-connlmt-policy-1]
```

创建编号为 12 的 IPv6 连接数限制策略，并进入 IPv6 连接数限制策略视图。

```
<Sysname> system-view
[Sysname] connection-limit ipv6-policy 12
[Sysname-connlmt-ipv6-policy-12]
```

【相关命令】

- **connection-limit apply**
- **connection-limit apply global**
- **display connection-limit**

- **limit**

1.1.2 connection-limit apply

connection-limit apply 命令用来在接口上应用连接数限制策略。

undo connection-limit apply 命令用来在接口上取消应用的连接数限制策略。

【命令】

connection-limit apply { **ipv6-policy** | **policy** } *policy-id*

undo connection-limit apply { **ipv6-policy** | **policy** }

【缺省情况】

接口上未应用连接数限制策略。

【视图】

接口视图

【缺省用户角色】

network-admin

context-admin

【参数】

ipv6-policy：指定 IPv6 连接数限制策略。

policy：指定 IPv4 连接数限制策略。

policy-id：连接数限制策略编号，取值范围为 1～32。

【使用指导】

同一个接口上同时只能应用一个 IPv4 连接数限制策略和一个 IPv6 连接数限制策略，后配置的 IPv4 或 IPv6 连接数限制策略会覆盖已配置的对应类型的策略。

【相关命令】

- **connection-limit**
- **limit**

1.1.3 connection-limit apply global

connection-limit apply global 命令用来在全局应用连接数限制策略。

undo connection-limit apply global 命令用来在全局取消应用的连接数限制策略。

【命令】

connection-limit apply global { **ipv6-policy** | **policy** } *policy-id*

undo connection-limit apply global { **ipv6-policy** | **policy** }

【缺省情况】

全局未应用连接数限制策略。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

ipv6-policy：指定 IPv6 连接数限制策略。

policy：指定 IPv4 连接数限制策略。

policy-id：连接数限制策略编号，取值范围为 1～32。

【使用指导】

全局最多只能应用一个 IPv4 连接数限制策略和一个 IPv6 连接数限制策略，后配置的 IPv4 或 IPv6 连接数限制策略会覆盖已配置的对应类型的策略。

【举例】

在全局应用编号为 1 的 IPv4 连接数限制策略。

```
<Sysname> system-view
[Sysname] connection-limit apply global policy 1
```

在全局应用编号为 12 的 IPv6 连接数限制策略。

```
<Sysname> system-view
[Sysname] connection-limit apply global ipv6-policy 12
```

【相关命令】

- **connection-limit**
- **limit**

1.1.4 description

description 命令用来配置连接数限制策略的描述信息。

undo description 命令用来恢复缺省情况。

【命令】

description *text*

undo description

【缺省情况】

未配置描述信息。

【视图】

IPv4 连接数限制策略视图

IPv6 连接数限制策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

text：表示连接数限制策略的描述信息，为 1～127 个字符的字符串，区分大小写。

【使用指导】

使用 **description** 命令时，如果当前连接数限制策略没有描述信息，则为其添加描述信息，否则修改其现有的描述信息。

【举例】

配置编号为 1 的 IPv4 连接数限制策略的描述信息为 CenterToA。

```
<Sysname> system-view
[Sysname] connection-limit policy 1
[Sysname-connlmt-policy-1] description CenterToA
```

【相关命令】

- **display connection-limit**

1.1.5 display connection-limit

display connection-limit 命令用来显示连接数限制策略的配置信息。

【命令】

display connection-limit { **ipv6-policy** | **policy** } { *policy-id* | **all** }

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

context-admin

context-operator

【参数】

ipv6-policy：显示 IPv6 连接数限制策略。

policy：显示 IPv4 连接数限制策略。

policy-id：连接数限制策略编号，取值范围为 1～32。

all：显示所有指定类型的连接数限制策略。

【举例】

显示所有 IPv4 连接数限制策略的配置信息。

```
<Sysname> display connection-limit policy all
3 policies in total:
 Policy  Rule     Stat Type  HiThres  LoThres  Rate   PermitNew     ACL
------------------------------------------------------------------------------
      0     1  Src-Dst-Port     2000     1800    10          No   3000
           12       Src-Dst      500       45     0         Yes   3001
          255            --  1000000   980000     0          No   2001

      1     2      Dst-Port      800       70     0         Yes   3010
            3       Src-Dst      100       90     0          No   3000
```

```
          10  Src-Dst-Port       50       45     0          No   3003
          11           Src      200      200     0          No   3004
         200           --    500000   498000     0          No   2002

     28    4          Port     1500     1400     0          No   3100
           5           Dst     3000      280     0          No   3101
          21       Src-Dst      200      180     0          No   3102
          25      Src-Port       50       35     0          No   3200

Description list:
 Policy      Description
--------------------------------------------------------------------------------
      1      IPv4Description1
     28      Description for IPv4 28
```

显示编号为 1 的 IPv4 连接数策略的配置信息。

```
<Sysname> display connection-limit policy 1
IPv4 connection limit policy 1 has been applied 5 times, and has 5 limit rules.
Description: IPv4Description1
Limit rule list:
 Policy  Rule     Stat Type  HiThres  LoThres     Rate   PermitNew   ACL
--------------------------------------------------------------------------------
      1     2      Dst-Port      800       70        0         Yes   3010
            3       Src-Dst      100       90        0          No   3000
           10  Src-Dst-Port       50       45        0          No   3003
           11           Src      200      200        0          No   3004
          200           --    500000   498000        0          No   2002
 Application list:
     GigabitEthernet1/0/1
     GigabitEthernet1/0/2
     Vlan-interface2
     Global
```

显示所有 IPv6 连接数限制策略的配置信息。

```
<Sysname> display connection-limit ipv6-policy all
2 policies in total:
 Policy  Rule     Stat Type  HiThres  LoThres  Rate   PermitNew   ACL
--------------------------------------------------------------------------------
      3     1       Src-Dst     1000      800    10         Yes   3010
            2           Dst      500      450     0         Yes   3001

      4     2  Src-Dst-Port      800      700     0          No   3010
            3           Src      100       90     0          No   3020
          200            --   100000    89000     0          No   2005

Description list:
 Policy      Description
--------------------------------------------------------------------------------
      3      IPv6Description3
      4      Description for IPv6 4
```

显示编号为 3 的 IPv6 连接数限制策略的配置信息。

```
<Sysname> display connection-limit ipv6-policy 3
IPv6 connection limit policy 3 has been applied 3 times, and has 2 limit rules.
Description: IPv6Description3
Limit rule list:
Policy  Rule     Stat Type  HiThres  LoThres  Rate   PermitNew   ACL
------------------------------------------------------------------------------
     3     1       Src-Dst     1000      800     0         Yes   3010
           2           Dst      500      450     0          No   3001
Application list:
    GigabitEthernet1/0/1
    Vlan-interface2
```

表1-1 display connection-limit 命令显示信息描述表

字段	描述
Limit rule list	连接数限制策略信息列表
Policy	连接数限制策略编号
Rule	连接数限制规则编号
Stat Type	统计方式，有如下取值： • Src-Dst-Port：按源 IP－目的 IP－服务的组合进行统计和限制 • Src-Dst：按源 IP－目的 IP 的组合进行统计和限制 • Src-Port：按源 IP－服务的组合进行统计和限制 • Dst-Port：按目的 IP－服务的组合进行统计和限制 • Src：按源 IP 进行统计和限制 • Dst：按目的 IP 进行统计和限制 • Port：按服务进行统计和限制 • Dslite：按 DS-Lite 隧道的 B4 设备进行统计和限制 • --：不按照具体的 IP 地址、服务进行统计和限制，与本规则引用的 ACL 相匹配的所有连接将整体受到指定的阈值限制
HiThres	连接数上限
LoThres	连接数下限
Rate	每秒新建连接速率值
ACL	规则引用的ACL编号或ACL名称
PermitNew	连接数或者新建速率超过设定的上限时，允许用户继续新建连接
Application list	连接数限制策略应用列表，包括接口名称和Global，其中Global表示该连接数限制策略应用在全局
Description	连接数限制策略描述信息
Description list	连接数限制策略描述信息列表

【相关命令】

- **connection-limit**
- **connection-limit apply**
- **connection-limit apply global**
- **limit**

1.1.6 display connection-limit ipv6-stat-nodes

display connection-limit ipv6-stat-nodes 命令用来显示连接数限制在全局或接口的IPv6 统计节点列表。

【命令】

（独立运行模式）

display connection-limit ipv6-stat-nodes { **global** | **interface** *interface-type interface-number* } [**slot** *slot-number* [**cpu** *cpu-number*]] [{ **deny-new** | **permit-new** } | **destination** *destination-ip* | **service-port** *port-number* | **source** *source-ip*] * [**count**]

（IRF 模式）

display connection-limit ipv6-stat-nodes { **global** | **interface** *interface-type interface-number* } [**chassis** *chassis-number* **slot** *slot-number* [**cpu** *cpu-number*]] [{ **deny-new** | **permit-new** } | **destination** *destination-ip* | **service-port** *port-number* | **source** *source-ip*] * [**count**]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

context-admin

context-operator

【参数】

global：显示全局的 IPv6 统计节点列表。

interface *interface-type interface-number*：显示指定接口的 IPv6 统计节点列表，*interface-type interface-number* 表示接口类型和接口编号。

slot *slot-number*：显示指定单板上全局或全局接口的 IPv6 统计节点列表，*slot-number* 表示单板所在的槽位号。该参数仅在显示全局统计节点列表，或上述指定的接口为全局类型的接口（例如 VLAN 接口、Tunnel 接口）时可见。（独立运行模式）

chassis *chassis-number* **slot** *slot-number*：显示指定成员设备的指定单板上全局或全局接口的 IPv6 统计节点列表，*chassis-number* 表示设备在 IRF 中的成员编号，*slot-number* 表示单板所在的槽位号。该参数仅在指定显示全局统计节点列表，或上述指定的接口为全局类型的接口（例如 VLAN 接口、Tunnel 接口）时可见。（IRF 模式）

cpu *cpu-number*：显示指定 CPU 上全局或全局接口的 IPv6 统计节点列表，*cpu-number* 表示 CPU 的编号。只有指定的 **slot** 支持多 CPU 时，才能配置该参数。

deny-new：显示禁止创建新连接的 IPv6 统计节点列表。

permit-new：显示允许创建新连接的 IPv6 统计节点列表。

destination *destination-ip*：显示指定目的 IP 地址的 IPv6 统计节点列表。

service-port *port-number*：显示指定服务端口号的 IPv6 统计节点列表。

source *source-ip*：显示指定源 IP 地址的 IPv6 统计节点列表。

count：显示 IPv6 统计节点的个数。如果配置本参数，将仅显示符合条件的（由 count 前面的参数决定）IPv6 统计节点的数量，而不显示 IPv6 统计节点的具体内容。如果不指定本参数，则显示符合条件的 IPv6 统计节点的具体内容。

【使用指导】

一个统计节点标识了连接数限制进行统计和限制的一个对象（一个连接或一类连接），包括该连接的报文特征（源/目的 IP 地址、服务端口号、传输层协议类型等）、对该连接所应用的连接限制策略、当前连接数目以及当前是否允许创建新的连接。

如果指定 **source**、**destination**、**service-port**、**deny-new**、**permit-new** 中的一个或多个参数，则表示将按照多个条件来显示统计节点列表，比如指定了 **source** 和 **destination**，则显示同时符合指定源 IP 地址和目的 IP 地址的统计节点列表。

如果不指定 **source**、**destination**、**service-port**、**deny-new**、**permit-new** 中任何一个参数，则表示显示所有的统计节点列表。

修改或删除连接数限制策略后，由该策略产生且已经生效的连接数限制统计节点不会受到影响。这些节点将在所统计的连接都断开后自动删除。

【举例】

显示全局接口 Vlan-interface10 在 2 号单板的 0 号 CPU 上的所有 IPv6 连接数限制统计节点列表。（独立运行模式）

```
<Sysname> display connection-limit ipv6-stat-nodes interface vlan-interface 10 slot 2 cpu
0
CPU 0 on slot 2:
 Src IP address          : 112::2
     VPN instance        : --
 Dst IP address          : Any
     VPN instance        : --
 DS-Lite tunnel peer     : --
 Service                 : udp/300
 Limit rule ID           : 0(ACL: 3571)
 Sessions threshold Hi/Lo: 3000/2900
 Sessions count          : 2002
 Sessions limit rate     : 0
 New session flag        : Permit
```

显示接口 GigabitEthernet1/1/0/2 在 1 号成员设备的 1 号单板的 0 号 CPU 上的所有 IPv6 连接数限制统计节点列表。（IRF 模式）

```
<Sysname> display connection-limit ipv6-stat-nodes interface gigabitethernet 1/1/0/2
chassis 1 slot 1 cpu 0
CPU 0 on slot 1 in chassis 1:
```

```
Src IP address          : 5::1
    VPN instance        : Vpn1
Dst IP address          : Any
    VPN instance        : --
DS-Lite tunnel peer     : --
Service                 : All
Limit rule ID           : 21(ACL: 2988)
Sessions threshold Hi/Lo: 2000/1500
Sessions count          : 1988
Sessions limit rate     : 0
New session flag        : Deny
```

显示全局接口 Vlan-interface10 在 2 号单板的 0 号 CPU 上的 IPv6 连接数限制统计节点个数。（独立运行模式）

```
<Sysname> display connection-limit ipv6-stat-nodes interface vlan-interface 10 slot 2 cpu 0 count
CPU 0 on slot 2:
       Current limit statistic nodes count is 1.
```

显示 1 号成员设备的 2 号单板的 0 号 CPU 上的 IPv6 连接数限制统计节点个数。（IRF 模式）

```
<Sysname> display connection-limit ipv6-stat-nodes global chassis 1 slot 2 cpu 0 count
CPU 0 on slot 2 in chassis 1:
       Current limit statistic nodes count is 0.
```

表1-2 display connection-limit stat-nodes 命令显示信息描述表

字段	描述
Src IP address	源IP地址
Dst IP address	目的IP地址
VPN instance	该地址所属的MPLS L3VPN的VPN实例名称，“--”表示属于公网
DS-Lite tunnel peer	DS Lite隧道对端的IP地址，“--”表示不属于任何DS Lite Tunnel
Service	协议名及服务端口号。如果不是知名协议则显示为“unknown(xx)”，xx为协议编号，此时不显示服务端口号。其中，对于ICMP协议，括弧内的数字为ICMP的type和code字段组合表示的十六进制数所对应的十进制数
Limit rule ID	匹配的规则编号，括号里为匹配的ACL编号
Sessions threshold Hi/Lo	连接数限制的上限值及下限值
Sessions count	当前连接计数
Sessions limit rate	每秒新建连接的最大数目
New session flag	是否允许创建新连接，Permit表示允许创建，Deny表示不允许创建 说明 当连接数增长到上限值（max-amount）时，New session flag 仍显示为 Permit，但此时不允许创建新连接。只有连接数超过上限值，New session flag 才会显示为 Deny

【相关命令】

- **connection-limit apply global ipv6-policy**

- **connection-limit apply ipv6-policy**
- **connection-limit ipv6-policy**
- **limit**

1.1.7 display connection-limit statistics

display connection-limit statistics 命令用来显示连接数限制在全局或接口的统计信息。

【命令】

（独立运行模式）

display connection-limit statistics { **global** | **interface** *interface-type interface-number* } [**slot** *slot-number* [**cpu** *cpu-number*]]

（IRF 模式）

display connection-limit statistics { **global** | **interface** *interface-type interface-number* } [**chassis** *chassis-number* **slot** *slot-number* [**cpu** *cpu-number*]]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

context-admin

context-operator

【参数】

global：显示全局的连接数限制统计信息。

interface *interface-type interface-number*：显示指定接口的连接数限制统计信息，*interface-type interface-number* 表示接口类型和接口编号。

slot *slot-number*：显示指定单板上全局或全局接口的连接数限制统计信息，*slot-number* 表示单板所在的槽位号。该参数仅在指定显示全局的连接数限制统计信息，或上述指定的接口为全局类型的接口（例如 VLAN 接口、Tunnel 接口）时可见。（独立运行模式）

chassis *chassis-number* **slot** *slot-number*：显示指定成员设备的指定单板上全局或全局接口的连接数限制统计信息，*chassis-number* 表示设备在 IRF 中的成员编号，*slot-number* 表示单板所在的槽位号。该参数仅在指定显示全局的连接数限制统计信息，或上述指定的接口为全局类型的接口（例如 VLAN 接口、Tunnel 接口）时可见。（IRF 模式）

cpu *cpu-number*：显示指定 CPU 上全局或全局接口的连接数限制统计信息，*cpu-number* 表示 CPU 的编号。只有指定的 **slot** 支持多 CPU 时，才能配置该参数。

【举例】

显示 2 号单板的 0 号 CPU 上的全局的连接数限制统计信息。（独立运行模式）

```
<Sysname> display connection-limit statistics global slot 2 cpu 0
Connection limit statistics (Global, CPU 0 on slot 2):
    Dropped IPv4 packets:   74213
```

```
    Dropped IPv6 packets:   58174
```

显示全局接口 Vlan-interface10 在 2 号成员设备的 1 号单板的 0 号 CPU 上的连接数限制统计信息。

（IRF 模式）

```
<Sysname> display connection-limit statistics interface vlan-interface 10 chassis 2 slot 1
cpu 0
Connection limit statistics (Vlan-interface10, CPU 0 on slot 1 in chassis 2):
    Dropped IPv4 packets:   12345
    Dropped IPv6 packets:   55239
```

表1-3 display connection-limit statistics 命令显示信息描述表

字段	描述
Dropped IPv4 packet	匹配全局或接口IPv4连接数限制策略，因连接数超过指定上限而被丢弃的报文个数
Dropped IPv6 packet	匹配全局或接口IPv6连接数限制策略，因连接数超过指定上限而被丢弃的报文个数

【相关命令】

- **connection-limit**
- **connection-limit apply**
- **connection-limit apply global**
- **limit**

1.1.8 display connection-limit stat-nodes

display connection-limit stat-nodes 命令用来显示连接数限制在全局或接口的 IPv4 统计节点列表。

【命令】

（独立运行模式）

display connection-limit stat-nodes { **global** | **interface** *interface-type interface-number* } [**slot** *slot-number* [**cpu** *cpu-number*]] [{ **deny-new** | **permit-new** } | **destination** *destination-ip* | **service-port** *port-number* | **source** *source-ip*] * [**count**]

display connection-limit stat-nodes { **global** | **interface** *interface-type interface-number* } [**slot** *slot-number* [**cpu** *cpu-number*]] **dslite-peer** *b4-address* [**count**]

（IRF 模式）

display connection-limit stat-nodes { **global** | **interface** *interface-type interface-number* } [**chassis** *chassis-number* **slot** *slot-number* [**cpu** *cpu-number*]] [{ **deny-new** | **permit-new** } | **destination** *destination-ip* | **service-port** *port-number* | **source** *source-ip*] * [**count**]

display connection-limit stat-nodes { **global** | **interface** *interface-type interface-number* } [**chassis** *chassis-number* **slot** *slot-number* [**cpu** *cpu-number*]] **dslite-peer** *b4-address* [**count**]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

context-admin

context-operator

【参数】

global：显示全局的 IPv4 统计节点列表。

interface *interface-type interface-number*：显示指定接口的 IPv4 统计节点列表，*interface-type interface-number* 表示接口类型和接口编号。

slot *slot-number*：显示指定单板上全局或全局接口的 IPv4 统计节点列表，*slot-number* 表示单板所在的槽位号。该参数仅在指定显示全局统计节点列表，或上述指定的接口为全局类型的接口（例如 VLAN 接口、Tunnel 接口）时可见。（独立运行模式）

chassis *chassis-number* **slot** *slot-number*：显示指定成员设备的指定单板上全局或全局接口的 IPv4 统计节点列表，*chassis-number* 表示设备在 IRF 中的成员编号，*slot-number* 表示单板所在的槽位号。该参数仅在指定显示全局统计节点列表，或上述指定的接口为全局类型的接口（例如 VLAN 接口、Tunnel 接口）时可见。（IRF 模式）

cpu *cpu-number*：显示指定 CPU 上全局或全局接口的 IPv4 统计节点列表，*cpu-number* 表示 CPU 的编号。只有指定的 **slot** 支持多 CPU 时，才能配置该参数。

deny-new：显示禁止创建新连接的 IPv4 统计节点列表。

permit-new：显示允许创建新连接的 IPv4 统计节点列表。

destination *destination-ip*：显示指定目的 IP 地址的 IPv4 统计节点列表。

service-port *port-number*：显示指定服务端口号的 IPv4 统计节点列表。

source *source-ip*：显示指定源 IP 地址的 IPv4 统计节点列表。

dslite-peer *b4-address*：显示指定 DS-Lite B4 设备的 IPv4 统计节点列表，*b4-address* 表示 B4 设备的 IPv6 地址。

count：显示 IPv4 统计节点的个数。如果配置本参数，将仅显示符合条件的（由 count 前面的参数决定）IPv4 统计节点的数量，而不显示 IPv4 统计节点的具体内容。如果不指定本参数，则显示符合条件的 IPv4 统计节点的具体内容。

【使用指导】

一个统计节点标识了连接数限制进行统计和限制的一个对象（一个连接或一类连接），包括该连接的报文特征（源/目的 IP 地址、服务端口号、传输层协议类型等）、对该连接所应用的连接限制策略、当前连接数目的统计值，以及当前是否允许创建新的连接。

如果指定 **source**、**destination**、**service-port**、**deny-new**、**permit-new** 中的一个或多个参数，则表示将按照多个条件来显示统计节点列表，比如指定了 **source** 和 **destination**，则显示同时符合指定源 IP 地址和目的 IP 地址的统计节点列表。.

如果不指定 **source**、**destination**、**service-port**、**deny-new**、**permit-new** 中任何一个参数，则表示显示所有的统计节点列表。

修改或删除连接数限制策略后，由该策略产生且已经生效的连接数限制统计节点不会受到影响。这些节点将在所统计的连接都断开后自动删除。

【举例】

显示所有单板上全局的所有 IPv4 连接数限制统计节点列表。（独立运行模式）

```
<Sysname> display connection-limit stat-nodes global
Slot 0:
There are no specified connection limit statistic nodes.
Slot 1:
 Src IP address          : Any
     VPN instance        : Vpn1
 Dst IP address          : Any
     VPN instance        : --
 DS-Lite tunnel peer     : --
 Service                 : All
 Limit rule ID           : 21(ACL: 2002)
 Sessions threshold Hi/Lo: 2000/1500
 Sessions count          : 1988
 Sessions limit rate     : 0
 New session flag        : Deny
```

显示接口 GigabitEthernet1/1/0/2 上的所有 IPv4 连接数限制统计节点列表。（IRF 模式）

```
<Sysname> display connection-limit stat-nodes interface gigabitethernet 1/1/0/2
Slot 1 in chassis 1:
 Src IP address          : Any
     VPN instance        : --
 Dst IP address          : 110.23.1.44
     VPN instance        : --
 DS-Lite tunnel peer     : --
 Service                 : udp/333
 Limit rule ID           : 19(ACL: 3307)
 Sessions threshold Hi/Lo: 10000/9900
 Sessions count          : 1001
 Sessions limit rate     : 0
 New session flag        : Permit
```

显示 1 号成员设备的上的 IPv4 连接数限制统计节点个数。（IRF 模式）

```
<Sysname> display connection-limit stat-nodes global chassis 1 slot 2 count
Slot 2 in chassis 1:
       Current limit statistic nodes count is 0.
```

显示 1 号单板的 0 号 CPU 上全局的所有 IPv4 连接数限制统计节点列表。（独立运行模式）

```
<Sysname> display connection-limit stat-nodes global slot 1 cpu 0
CPU 0 on slot 1:
 Src IP address          : Any
     VPN instance        : Vpn1
 Dst IP address          : Any
     VPN instance        : --
 DS-Lite tunnel peer     : --
 Service                 : All
```

```
 Limit rule ID           : 21(ACL: 2002)
 Sessions threshold Hi/Lo: 2000/1500
 Sessions count          : 1988
 Sessions limit rate     : 0
 New session flag        : Deny
```

显示接口 GigabitEthernet1/1/0/2 在 1 号成员设备的 1 号单板的 0 号 CPU 上的所有 IPv4 连接数限制统计节点列表。（IRF 模式）

```
<Sysname> display connection-limit stat-nodes interface gigabitethernet 1/1/0/2 chassis 1 slot 1 cpu 0
CPU 0 on slot 1 in chassis 1:
 Src IP address          : Any
     VPN instance        : --
 Dst IP address          : 110.23.1.44
     VPN instance        : --
 DS-Lite tunnel peer     : --
 Service                 : udp/333
 Limit rule ID           : 19(ACL: 3307)
 Sessions threshold Hi/Lo: 10000/9900
 Sessions count          : 1001
 Sessions limit rate     : 0
 New session flag        : Permit
```

显示全局接口 Vlan-interface10 在 2 号单板的 0 号 CPU 上的 IPv4 连接数限制统计节点个数。（独立运行模式）

```
<Sysname> display connection-limit stat-nodes interface vlan-interface 10 slot 2 cpu 0 count
CPU 0 on slot 2:
       Current limit statistic nodes count is 1.
```

显示 1 号成员设备的 2 号单板的 0 号 CPU 上的 IPv4 连接数限制统计节点个数。（IRF 模式）

```
<Sysname> display connection-limit stat-nodes global chassis 1 slot 2 cpu 0 count
CPU 0 on slot 2 in chassis 1:
       Current limit statistic nodes count is 0.
```

表1-4 display connection-limit stat-nodes 命令显示信息描述表

字段	描述
Src IP address	源IP地址
Dst IP address	目的IP地址
VPN instance	该地址所属的MPLS L3VPN的VPN实例名称，“--”表示不属于任何VPN
DS-Lite tunnel peer	DS Lite隧道对端的IP地址，“--”表示不属于任何DS Lite Tunnel
Service	协议名及服务端口号。如果不是知名协议则显示为“unknown(xx)”，xx为协议编号，此时不显示服务端口号。其中，对于ICMP协议，括弧内的数字为ICMP的type和code字段组合表示的十六进制数所对应的十进制数
Limit rule ID	匹配的规则编号，括号里为匹配的ACL编号
Sessions threshold Hi/Lo	连接数限制的上限值及下限值
Sessions count	当前连接计数
Sessions limit rate	每秒新建连接的最大数目

字段	描述
New session flag	是否允许创建新连接，Permit表示允许创建，Deny表示不允许创建  说明 当连接数增长到上限值（max-amount）时，New session flag 仍显示为 Permit，但此时不允许创建新连接。只有连接数超过上限值，New session flag 才会显示为 Deny

【相关命令】

- **connection-limit policy**
- **connection-limit apply global policy**
- **connection-limit apply policy**
- **limit**

1.1.9 limit

limit 命令用来配置连接数限制规则。

undo limit 命令用来删除指定的连接数限制规则。

【命令】

IPv4 连接数限制策略视图：

limit *limit-id* **acl** { *acl-number* | **name** *acl-name* } [**per-destination** | **per-service** | **per-source**] * { **amount** *max-amount min-amount* | **rate** *rate* } * [**description** *text* | **permit-new**] *

limit *limit-id* **acl ipv6** { *acl-number* | **name** *acl-name* } **per-dslite-b4** { **amount** *max-amount min-amount* | **rate** *rate* } * [**description** *text* | **permit-new**] *

undo limit *limit-id*

IPv6 连接数限制策略视图：

limit *limit-id* **acl ipv6** { *acl-number* | **name** *acl-name* } [**per-destination** | **per-service** | **per-source**] * { **amount** *max-amount min-amount* | **rate** *rate* } * [**description** *text* | **permit-new**] *

undo limit *limit-id*

【缺省情况】

不存在连接数限制规则。

【视图】

IPv4 连接数限制策略视图

IPv6 连接数限制策略视图

【缺省用户角色】

network-admin

context-admin

【参数】

limit-id：连接数限制规则编号，取值范围为 1～256。

acl：指定用于匹配用户范围的 ACL。该连接限制规则仅对匹配 ACL 规则的用户连接数进行统计和限制。

ipv6：表示引用 IPv6 ACL。若不指定该参数，则表示引用 IPv4 ACL。

acl-number：ACL 的编号，取值范围为 2000～3999。

name *acl-name*：ACL 的名称，为 1～63 个字符的字符串，不区分大小写，必须以英文字母 a～z 或 A～Z 开头。为避免混淆，ACL 的名称不允许使用英文单词 all。

per-destination：表示按目的地址进行统计和限制。

per-service：表示按服务（即按传输层协议和服务端口）进行统计和限制。

per-source：表示按源地址进行统计和限制。

per-dslite-b4：表示按照 DS-Lite 隧道的 B4 设备 IPv6 地址来进行统计和限制。该参数仅在 IPv4 连接数限制策略视图下存在。

amount：表示对连接数进行限制。

max-amount：指定的连接数上限，取值范围为 1～4294967294。若不配置 **permit-new** 参数，当某范围或某种类型的连接数值超过此值时，用户将不能建立新的连接，直到连接数下降到 *min-amount* 指定的连接数下限之下时，才允许用户建立新的连接。

min-amount：指定的连接数下限，取值范围为 1～4294967294，不能大于 *max-amount* 的取值。连接数的统计值降到此值之下时，允许用户建立新的连接。

rate：表示对新建连接速率进行限制。

rate：指定每秒新建连接的最大数目，取值范围为 5～10000000。若不配置 **permit-new** 参数，当某范围或某种类型的新建连接数速率超过此值时，用户将不能建立新的连接。

description *text*：表示连接数限制规则的描述信息，其中，*text* 为 1～127 个字符的字符串，区分大小写。

permit-new：当连接数或者新建速率超过设定的上限时，允许用户继续新建连接。设备将记录告警日志。

【使用指导】

每个连接数限制策略中可以定义多个规则，每个规则中需要指定引用的 ACL、规则的类型以及统计的上下门限值/新建速率限值。对于 **per-destination**、**per-source**、**per-service** 类型，可以在一条规则中单独指定其中之一或指定它们的组合。例如，同时指定 **per-destination** 和 **per-source**，就表示同时按照连接的报文源地址和目的地址进行统计和限制，具有相同源和目的的连接属于同一类连接，该类连接的数目将受到指定的阈值的限制。对于 **per-dslite-b4** 类型，只能在一条规则中单独指定。

对设备上建立的连接与某连接数限制策略进行匹配时，将按照规则编号从小到大的顺序依次遍历该策略中的所有规则，直到找到一条匹配的规则为止。

同一个连接数限制策略中的不同规则必须引用不同的 ACL。

当引用的 ACL 内容发生改变时，设备将按照新的连接数限制策略重新对已有连接进行统计和限制。

如果 **per-destination**、**per-service**、**per-source** 三个参数都不指定，则表示与本规则引用的 ACL 相匹配的所有连接将整体受到指定的阈值限制。

在 DS-Lite 隧道组网环境中，需要注意的是：

- **per-dslite-b4** 参数用于限制 DS-Lite 隧道每个 B4 设备连接的 IPv4 用户连接数，每个规则限制的 B4 设备由规则中指定的 IPv6 ACL 来匹配。
- 若 AFTR 设备上采用了 Endpoint-Independent Mapping 模式的 NAT 配置，则要基于 B4 设备来限制从 IPv4 外网主动访问 IPv4 内网的连接，配置了 **per-dslite-b4** 类型规则的连接数限制策略必须应用在 DS-Lite 隧道接口上或者应用在全局。

【举例】

在 IPv4 连接数限制策略 1 中创建一条规则，规则编号为 1，引用 ACL 3000，对匹配 ACL 3000 的连接同时按照报文的源地址和目的地址进行统计和限制，连接数的上限值为 2000、下限值为 1800。该规则用于限制 192.168.0.0/24 网段的每台主机最多只能同时向外网的同一个目的 IP 地址发起 2000 条连接，超过 2000 条时，需要等待连接数下降到 1800 以下之后，才允许新建连接，且每秒最多允许新建连接数为 10。

```
<Sysname> system-view
[Sysname] acl advanced 3000
[Sysname-acl-ipv4-adv-3000] rule permit ip source 192.168.0.0 0.0.0.255
[Sysname-acl-ipv4-adv-3000] quit
[Sysname] connection-limit policy 1
[Sysname-connlmt-policy-1] limit 1 acl 3000 per-destination per-source amount 2000 1800 rate 10
```

在 IPv4 连接数限制策略 1 中创建一条规则，规则编号为 1，引用 ACL 3000，对匹配 ACL 3000 的连接同时按照报文的源地址和目的地址进行统计和限制，连接数的上限值为 2000、下限值为 1800。该规则用于限制 192.168.0.0/24 网段的每台主机最多只能同时向外网的同一个目的 IP 地址发起 2000 条连接，超过 2000 条时，允许新建连接，但会产生告警日志，每秒最多允许新建连接数为 10，超过 10 时，允许新建连接，但会产生告警日志。

```
<Sysname> system-view
[Sysname] acl advanced 3000
[Sysname-acl-ipv4-adv-3000] rule permit ip source 192.168.0.0 0.0.0.255
[Sysname-acl-ipv4-adv-3000] quit
[Sysname] connection-limit policy 1
[Sysname-connlmt-policy-1] limit 1 acl 3000 per-destination per-source amount 2000 1800 rate 10 permit-new
```

在 IPv6 连接数限制策略 12 中创建一条规则，规则编号为 2，引用 ACL 2001，对匹配 ACL 2001 的连接按照报文的目的地址进行统计和限制，连接数的上限值为 200、下限值为 100。该规则用于限制 2:1::/96 网段的主机最多只能同时向外网的同一个目的 IP 地址发起 200 条连接，超过 200 条时，需要等待连接数下降到 100 以下之后，才允许新建连接，且每秒最多允许新建连接数为 10。

```
<Sysname> system-view
[Sysname] acl ipv6 basic 2001
[Sysname-acl-ipv6-basic-2001] rule permit source 2:1::/96
[Sysname-acl-ipv6-basic-2001] quit
[Sysname] connection-limit ipv6-policy 12
[Sysname-connlmt-ipv6-policy-12] limit 2 acl ipv6 2001 per-destination amount 200 100 rate 10
```

在 IPv6 连接数限制策略 12 中创建一条规则，规则编号为 2，引用 ACL 2001，对匹配 ACL 2001 的连接按照报文的目的地址进行统计和限制，连接数的上限值为 200、下限值为 100。该规则用于

限制 2:1::/96 网段的主机最多只能同时向外网的同一个目的 IP 地址发起 200 条连接，超过 200 条时，允许新建连接，但会产生告警日志，每秒最多允许新建连接数为 10，超过 10 时，允许新建连接，但会产生告警日志。

```
<Sysname> system-view
[Sysname] acl ipv6 basic 2001
[Sysname-acl-ipv6-basic-2001] rule permit source 2:1::/96
[Sysname-acl-ipv6-basic-2001] quit
[Sysname] connection-limit ipv6-policy 12
[Sysname-connlmt-ipv6-policy-12] limit 2 acl ipv6 2001 per-destination amount 200 100 rate 10 permit-new
```

【相关命令】

- **connection-limit**
- **display connection-limit**

1.1.10 reset connection-limit statistics

reset connection-limit statistics 命令用来清除连接数限制在全局或接口的统计信息。

【命令】

（独立运行模式）

reset connection-limit statistics { **global** | **interface** *interface-type interface-number* } [**slot** *slot-number* [**cpu** *cpu-number*]]

（IRF 模式）

reset connection-limit statistics { **global** | **interface** *interface-type interface-number* } [**chassis** *chassis-number* **slot** *slot-number* [**cpu** *cpu-number*]]

【视图】

用户视图

【缺省用户角色】

network-admin

network-operator

context-admin

context-operator

【参数】

global：清除全局的连接数限制统计信息。

interface *interface-type interface-number*：清除指定接口上的连接数限制统计信息，*interface-type interface-number* 表示接口类型和接口编号。

slot *slot-number*：清除指定单板上全局或全局接口应用的连接数限制统计信息，*slot-number* 表示单板所在的槽位号。该参数仅在指定清除全局的连接数限制统计信息，或上述指定的接口为全局类型的接口（例如 VLAN 接口、Tunnel 接口）时可见。（独立运行模式）

chassis *chassis-number* **slot** *slot-number*：清除指定成员设备的指定单板上全局或全局接口应用的连接数限制统计信息，*chassis-number* 表示设备在 IRF 中的成员编号，*slot-number* 表示单板所在的槽位号。该参数仅在指定清除全局的连接数限制统计信息，或上述指定的接口为全局类型的接口（例如 VLAN 接口、Tunnel 接口）时可见。（IRF 模式）

cpu *cpu-number*：清除指定 CPU 上全局或全局接口的连接数限制统计信息，*cpu-number* 表示 CPU 的编号。只有指定的 **slot** 支持多 CPU 时，才能配置该参数。

【举例】

清除 2 号单板上全局应用的连接数限制统计信息。（独立运行模式）

```
<Sysname> reset connection-limit statistics global slot 2
```

清除 1 号成员设备上 3 号单板上全局应用的连接数限制统计信息。（IRF 模式）

```
<Sysname> reset connection-limit statistics global chassis 1 slot 2
```

【相关命令】

- **display connection-limit statistics**