目 录

1 连接限制配置命令

1.1 连接限制配置命令

1.1.1 connection-limit default action

【命令】

connection-limit default action { **deny** | **permit** }

undo connection-limit default action [**permit**]

【视图】

连接限制策略视图

【缺省级别】

2：系统级

【参数】

deny：禁止对用户连接进行统计和限制。

permit：允许对用户连接进行统计和限制。

【描述】

connection-limit default action 命令用来设置缺省连接限制动作，即对于在连接限制策略规则中未指定的连接是否进行统计和限制。**undo connection-limit default action** 命令用来恢复缺省情况。

缺省情况下，不对用户连接进行统计和限制。

【举例】

设置缺省的连接限制动作为 **permit**，即允许对连接进行统计和限制。

```
<Sysname> system-view
[Sysname] connection-limit policy 1
[Sysname-connection-limit-policy-1] connection-limit default action permit
```

1.1.2 connection-limit default amount

【命令】

connection-limit default amount upper-limit *max-amount* **lower-limit** *min-amount*

undo connection-limit default amount [**upper-limit** *max-amount* **lower-limit** *min-amount*]

【视图】

连接限制策略视图

【缺省级别】

2：系统级

【参数】

upper-limit *max-amount*：指定连接数上限值。取值范围为 1～4294967295。

lower-limit *min-amount*：指定连接数下限值。取值范围为 0～4294967294，且 *min-amount* 应小于 *max-amount*。

【描述】

connection-limit default amount 命令用来设置缺省连接限制参数。**undo connection-limit default amount** 命令用来恢复缺省情况。

缺省情况下，连接数上限值为 50，下限制为 20。

【举例】

设置缺省连接数上限值为 200，下限值为 50。

```
<Sysname> system-view
[Sysname] connection-limit policy 1
[Sysname-connection-limit-policy-1] connection-limit default amount upper-limit 200
lower-limit 50
```

1.1.3 connection-limit policy

【命令】

connection-limit policy *policy-number*

undo connection-limit policy { *policy-number* | **all** }

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

policy-number：连接限制策略编号，取值范围为 0～19。

all：表示所有的连接限制策略。

【描述】

connection-limit policy 命令用来创建一个连接限制策略，并进入连接限制策略视图。**undo connection-limit policy** 命令用来删除一个或全部连接限制策略。

需要注意的是：

- 一个连接限制策略由一系列的连接限制规则组成，在规则中指明了对指定用户的连接数进行限制。缺省情况下，策略采用缺省的连接限制参数。
- 创建一个连接限制策略需要指定策略的编号，此编号用来唯一标识此策略。策略匹配按照编号从大到小顺序匹配。
- 如果连接限制策略已应用于 NAT 模块，则不允许修改策略中已配置的连接限制规则，但可以在该策略中添加或删除连接限制规则。

【举例】

创建编号为 1 的连接限制策略，并进入连接限制策略视图。

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

1.1.4 display connection-limit policy

【命令】

display connection-limit policy { *policy-number* | **all** } [**|** { **begin** | **exclude** | **include** } *regular-expression*]

【视图】

任意视图

【缺省级别】

1：监控级

【参数】

policy-number：显示指定编号的连接限制策略，取值范围为 0～19。

all：显示所有的策略。

|：使用正则表达式对显示信息进行过滤。有关正则表达式的详细介绍，请参见“基础配置指导”中的“CLI”。

begin：从包含指定正则表达式的行开始显示。

exclude：只显示不包含指定正则表达式的行。

include：只显示包含指定正则表达式的行。

regular-expression：表示正则表达式，为 1～256 个字符的字符串，区分大小写。

【描述】

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

相关配置可参考命令 **limit acl**。

【举例】

显示所有连接限制策略的配置信息。

```
<Sysname> display connection-limit policy all
 There is 1 policy:
 Connection-limit policy 1, refcount 0 ,3 limits
  limit 1 acl 2000 per-source amount 1111 10
  limit 2 acl 2001 per-destination amount 300 20
  limit 3 acl 2002 per-service amount 400 50
```

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

字段	描述
Connection-limit policy	连接限制策略编号
refcount 1, 2 limits	策略被引用的次数及策略中包含的规则数目

字段	描述
limit	策略下配置的连接限制规则，规则的具体含义请参考连接限制策略视图下的命令 **limit acl**

1.1.5 display connection-limit statistics

【命令】

display connection-limit statistics [**source** *src-address* { *mask-length* | *mask* }] [**destination** *dst-address* { *mask-length* | *mask* }] [**destination-port** { **eq** | **gt** | **lt** | **neq** | **range** } *port-number*] [**vpn-instance** *vpn-instance-name*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

【视图】

任意视图

【缺省级别】

1：监控级

【参数】

source *src-address*：显示指定源 IP 地址的连接限制统计信息。

destination *dst-address*：显示指定目的 IP 地址的连接限制统计信息。

mask-length：网络掩码的长度，取值范围为 1～32。

mask：网络掩码。

destination-port：按目的端口显示连接限制统计信息。

{ **eq** | **gt** | **lt** | **neq** | **range** }：表示限定端口范围的条件，包括以下几项：

- **eq**：表示等于指定的端口号；
- **gt**：表示大于指定的端口号；
- **lt**：表示小于指定的端口号；
- **neq**：表示不等于指定的端口号；
- **range**：表示指定端口号范围。

port-number：表示端口号，取值范围为 0～65535。参数为 **range** 时，*port-number* 为<*start-port*，*end-port*>表示的一个端口范围，需要先后输入 *start-port* 和 *end-port*，且 *start-port* 不能大于 *end-port*。

vpn-instance *vpn-instance-name*：指定用户连接所属的 VPN。*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1～31 个字符的字符串，区分大小写。如果未指定本参数，则表示待查询连接统计的用户连接属于公网。

|：使用正则表达式对显示信息进行过滤。有关正则表达式的详细介绍，请参见“基础配置指导”中的“CLI”。

begin：从包含指定正则表达式的行开始显示。

exclude：只显示不包含指定正则表达式的行。

include：只显示包含指定正则表达式的行。

regular-expression：表示正则表达式，为 1～256 个字符的字符串，区分大小写。

【描述】

display connection-limit statistics 命令用来显示连接限制统计信息。

【举例】

显示所有连接限制统计信息。

```
<Sysname> display connection-limit statistics
      source-ip       dest-ip         dest-port       vpn-instance
      192.168.0.210   ---             ---             ---
------------------------------------------------------------------------------
 NAT       amount          upper-limit     lower-limit     limit-flag
           2               200             100             0
```

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

字段	描述
source-ip	源 IP 地址，为“---”时表示连接中无该信息
dest-ip	目的 IP 地址，为“---”时表示连接中无该信息
dest-port	目的端口号，为“---”时表示连接中无该信息
vpn-instance	用户连接所属 MPLS L3VPN，为“---”时表示连接属于公网
NAT	应用连接限制策略的 NAT 模块
amount	当前用户的实际连接数
upper-limit	用户可建连接数上限值
lower-limit	用户可建连接数下限值
limit-flag	新连接是否还能建立标志，为 0 时可以再建，为 1 时不能再建

1.1.6 display nat connection-limit

【命令】

display nat connection-limit [**source** *src-address* { *mask-length* | *mask* }] [**destination** *dst-address* { *mask-length* | *mask* }] [**destination-port** { **eq** | **gt** | **lt** | **neq** | **range** } *port-number*] [**vpn-instance** *vpn-instance-name*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

【视图】

任意视图

【缺省级别】

1：监控级

【参数】

source *src-address*：显示指定源 IP 地址的连接限制统计信息。

destination *dst-address*：显示指定目的 IP 地址的连接限制统计信息。

mask-length：网络掩码的长度，取值范围为 1～32。

mask：网络掩码。

destination-port：按目的端口号显示连接限制统计信息。

{ eq | gt | lt | neq | range }：表示限定端口范围的条件，包括以下几项：

- **eq**：表示等于指定的端口号；
- **gt**：表示大于指定的端口号；
- **lt**：表示小于指定的端口号；
- **neq**：表示不等于指定的端口号；
- **range**：表示指定端口号范围。

port-number：表示端口号，取值范围为 0～65535。参数为 **range** 时，*port-number* 为*<start-port, end-port>*表示的一个端口范围，需要先后输入 *start-port* 和 *end-port*，且 *start-port* 不能大于 *end-port*。

vpn-instance *vpn-instance-name*：指定用户连接所属的 VPN。*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1～31 个字符的字符串。如果未指定本参数，则表示待查询连接统计的用户位于公网中。

|：使用正则表达式对显示信息进行过滤。有关正则表达式的详细介绍，请参见“基础配置指导”中的“CLI”。

begin：从包含指定正则表达式的行开始显示。

exclude：只显示不包含指定正则表达式的行。

include：只显示包含指定正则表达式的行。

regular-expression：表示正则表达式，为 1～256 个字符的字符串，区分大小写。

【描述】

display nat connection-limit 命令用来显示 NAT 模块的连接限制统计信息。

【举例】

显示 NAT 模块的连接限制统计信息。

```
<Sysname> display nat connection-limit
      source-ip       dest-ip         dest-port       vpn-instance
      192.168.0.210   ---             ---             ---
------------------------------------------------------------------------------
 NAT       amount          upper-limit     lower-limit     limit-flag
           2               50              20              0
```

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

字段	描述
source-ip	连接的源 IP 地址，为“---”时表示连接中无该信息
dest-ip	连接的目的 IP 地址，为“---”时表示连接中无该信息
dest-port	连接的目的端口，为“---”时表示连接中无该信息
vpn-instance	连接所属的 MPLS L3VPN，为“---”时表示连接属于公网
NAT	连接是通过 NAT 建立起来的

字段	描述
amount	当前用户实际连接数
upper-limit	用户可建连接上限值
lower-limit	用户可建连接下限值
limit-flag	用户能否再建连接标志，为 0 时表示用户还可再建连接，为 1 时表示用户不能再建连接

1.1.7 limit acl

【命令】

limit *limit-id* **acl** *acl-number* [{ **per-destination** | **per-service** | **per-source** } * **amount** *max-amount min-amount*]

undo limit *limit-id* [**acl** *acl-number* [{ **per-destination** | **per-service** | **per-source** } * **amount** *max-amount min-amount*]]

【视图】

连接限制策略视图

【缺省级别】

2：系统级

【参数】

limit-id：连接限制策略的规则编号，取值范围为 0～255。

acl-number：访问控制列表号，取值范围为 2000～3999。ACL 用来匹配用户的范围，对匹配 ACL 的用户的连接数进行统计和限制。

per-destination：按目的 IP 地址方式统计和限制，即到同一个目的 IP 地址的连接数目受限。

per-service：按服务方式统计和限制，即同一种服务（或应用）的连接数目受限。

per-source：按源 IP 地址方式统计和限制，即同一个源 IP 地址发起的连接数目受限。

amount：设置连接数限制。

max-amount：连接数上限值，取值范围为 1～4294967295。

min-mount：连接数下限值，取值范围为 0～4294967294。*min-mount* 必须小于 *max-amount*。

【描述】

limit acl 命令用来配置基于 ACL 的连接限制规则。**undo limit** 命令用来删除指定的连接限制规则。

需要注意的是：

- 如果只指定 **acl** 参数，不指定其它参数，则按照源 IP 地址方式，采用策略缺省的连接限制参数(连接数上下限值)进行统计和限制。缺省的连接限制参数配置请参见命令 **connection-limit default amount**。
- 如果同时指定 **per-destination**、**per-service**、**per-source** 参数中的多个，则各种统计和限制方式组合生效。例如，**per-destination per-service** 表示到同一个目的 IP 地址的同一种服务。

相关配置可参考命令 **connection-limit policy**、**display connection-limit policy** 和 **display nat connection-limit**。

【举例】

配置编号为 1 的连接限制规则，限制 192.168.0.0/24 网段的用户到同一个目的 IP 地址的连接数的上、下限值分别为 200 和 100。例如，如果此时内网有 192.168.0.1 和 192.168.0.100 两个用户访问某公网服务器，则按目的 IP 地址进行限制和统计，即要求与该公网服务器建立的连接数不超过 200，在连接数下降到 100 后允许新建连接。

```
<Sysname> system-view
[Sysname] acl number 2001
[Sysname-acl-basic-2001] rule permit source 192.168.0.0 0.0.0.255
[Sysname-acl-basic-2001] quit
[Sysname] connection-limit policy 1
[Sysname-connection-limit-policy-1] limit 1 acl 2001 per-destination amount 200 100
```

1.1.8 nat connection-limit-policy

【命令】

nat connection-limit-policy *policy-number*

undo nat connection-limit-policy *policy-number*

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

policy-number：指定连接限制策略编号，取值范围为 0～19。该连接限制策略必须已经存在。

【描述】

nat connection-limit-policy 命令用来在 NAT 模块上应用连接限制策略，即配置连接限制策略与 NAT 模块的绑定。**undo nat connection-limit-policy** 命令用来取消连接限制策略的应用。

需要注意的是，若要修改已经被 NAT 应用的连接限制策略的规则，需要先使用 **undo nat connection-limit policy** 命令取消已有的应用。

【举例】

将策略 1 与 NAT 模块绑定。

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

删除策略 1 与 NAT 模块的绑定。

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