目 录

1 连接数限制

说明

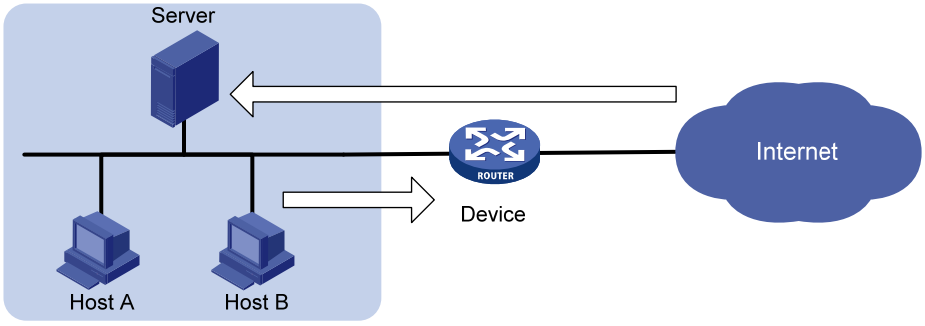
仅 WX2500H-WiNet 系列不支持 slot 参数。

1.1 连接数限制简介

图 1-1 所示的组网环境中，通常会遇到以下两类网络问题：某内网用户在短时间内经过设备向外部网络发起大量连接，导致设备系统资源迅速消耗，其它内网用户无法正常使用网络资源；某内部服务器在短时间内接收到大量的连接请求，导致该服务器忙于处理这些连接请求，以至于不能再接受其它客户端的正常连接请求。

连接数限制通过对设备上建立的连接数进行统计和限制，能够有效解决以上问题，实现保护内部网络资源（主机或服务器）以及合理分配设备系统资源的目的。

图1-1 连接数限制组网应用示意图



目前，设备仅支持基于接口的连接数限制：通过将已经配置好的连接数限制策略应用到全局或指定的接口上，对指定接口或所有接口上的用户连接数进行限制。

1.2 配置基于接口的连接数限制

1.2.1 基于接口的连接数限制配置任务简介

表1-1 基于接口的连接数限制配置任务简介

配置任务	说明	详细配置
创建连接数限制策略	必选	1.2.2
配置连接数限制策略	必选	1.2.3
应用连接数限制策略	必选	1.2.4

1.2.2 创建连接数限制策略

连接数限制策略用于定义具体的连接数限制规则，其中的规则规定了策略生效的范围和实施的参数。

表1-2 创建连接数限制策略

操作	命令	说明
进入系统视图	**system-view**	-
创建连接数限制策略，并进入连接数限制策略视图	**connection-limit** { **ipv6-policy** | **policy** } *policy-id*	缺省情况下，不存在任何连接数限制策略

1.2.3 配置连接数限制策略

一个连接数限制策略中可定义多条连接数限制规则，每条连接数限制规则中指定一个连接数限制的用户范围，属于该范围的用户可建立的连接数及新建连接速率将受到该规则中指定参数的限制。当某类型的连接数达到上限值（*max-amount*）时，设备将不接受该类型的新建连接请求并发送日志，直到设备上已有连接因老化而删除，使得当前该类型的连接数低于连接数下限（*min-amount*）后，才允许新建连接并发送日志。对于未匹配连接数限制规则的用户所建立的连接，设备不对其连接数进行限制。也可以选择对新建连接的速率进行限制（*rate*），每秒新建的连接数不能超过限制值。

目前，连接数限制支持根据 ACL 来限定用户范围，对匹配 ACL 规则的用户连接数进行统计和限制。

设备对于某一范围内的用户连接，可根据不同的控制粒度，按照如下各类型进行连接数限制：

- **per-destination**：按目的 IP 地址统计和限制，即到同一个目的 IP 地址的连接数目将受到指定阈值的限制。
- **per-service**：按服务统计和限制，即同一种服务（具有相同传输层协议和服务端口）的连接数目受限将受到指定阈值的限制。
- **per-source**：按源地址统计和限制，即同一个源 IP 地址发起的连接数目受限将受到指定阈值的限制。

如果在一条规则中同时指定 **per-destination**、**per-service**、**per-source** 类型中的多个，则多种统计和限制类型同时生效。例如，同时指定 **per-destination** 和 **per-service** 类型，则表示对到同一个目的地址的同一种服务的连接数进行统计和限制。若一条规则中不指定以上任何一种限制类型，则表示指定范围内的所有用户连接将整体受到指定的阈值限制。

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，因此在配置连接限制规则时，需要从整体策略考虑，根据各规则的内容来合理安排规则的编号顺序，推荐按照限制粒度和范围由小到大的顺序来设置规则序号。

表1-3 配置 IPv4 连接数限制策略

操作	命令	说明
进入系统视图	**system-view**	-
进入IPv4连接数限制策略视图	**connection-limit policy** *policy-id*	-
配置连接数限制规则	**limit** *limit-id* **acl** { *acl-number* | **name** *acl-name* } [**per-destination** | **per-service** | **per-source**] * { **amount** *max-amount min-amount* | **rate** *rate* } * [**description** *text*]	缺省情况下，连接数策略中不存在任何规则

操作	命令	说明
（可选）配置连接数限制策略的描述信息	**description** *text*	缺省情况下，连接数限制策略未配置任何描述信息

表1-4 配置 IPv6 连接数限制策略

操作	命令	说明
进入系统视图	**system-view**	-
进入IPv6连接数限制策略视图	**connection-limit ipv6-policy** *policy-id*	-
配置连接数限制规则	**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*]	缺省情况下，连接数策略中不存在任何规则
（可选）配置连接数限制策略的描述信息	**description** *text*	缺省情况下，连接数限制策略未配置任何描述信息

1.2.4 应用连接数限制策略

将已经配置好的连接数限制策略应用到全局或不同的接口上，实现对用户的连接数限制。接口上应用的连接数限制策略仅对本接口上处理的指定连接生效，全局应用的连接数限制策略对本设备处理的所有指定的连接生效。

如果在入接口、全局和出接口上分别应用了不同的连接数限制策略，则经过设备的连接将会依次受到入接口、全局、出接口连接数限制策略的多重限制，只要该连接的数目达到任何一处连接数上限，都不允许新建连接。

表1-5 在接口上应用连接数限制策略

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
在接口上应用连接限制策略	**connection-limit apply** { **ipv6-policy** | **policy** } *policy-id*	缺省情况下，接口上没有应用任何连接数限制策略 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

表1-6 全局应用连接限制策略

操作	命令	说明
进入系统视图	**system-view**	-

操作	命令	说明
全局应用连接限制策略	**connection-limit apply global** { **ipv6-policy** | **policy** } *policy-id*	缺省情况下，全局没有应用任何连接数限制策略 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

1.3 连接数限制显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示连接数限制配置后的运行情况，通过查看显示信息验证配置的效果。

在用户视图下执行 **reset** 命令清除连接数限制的相关信息。

表1-7 连接数限制显示和维护

操作	命令
显示连接数限制策略的配置信息	**display connection-limit** { **ipv6-policy | policy** } { **all** | *policy-id* }
显示连接数限制在全局或接口的统计信息	**display connection-limit statistics** { **global** | **interface** *interface-type interface-number* } [**slot** *slot-number*]
显示连接数限制在全局或接口的的统计节点列表	**display connection-limit** { **ipv6-stat-nodes** | **stat-nodes** } { **global** | **interface** *interface-type interface-number* } [**slot** *slot-number*] [**destination** *destination-ip* | **service-port** *port-number* | **source** *source-ip*] * [**count**]
清除连接数限制在全局或接口的统计信息	**reset connection-limit statistics** { **global** | **interface** *interface-type interface-number* } [**slot** *slot-number*]

1.4 连接数限制典型配置举例

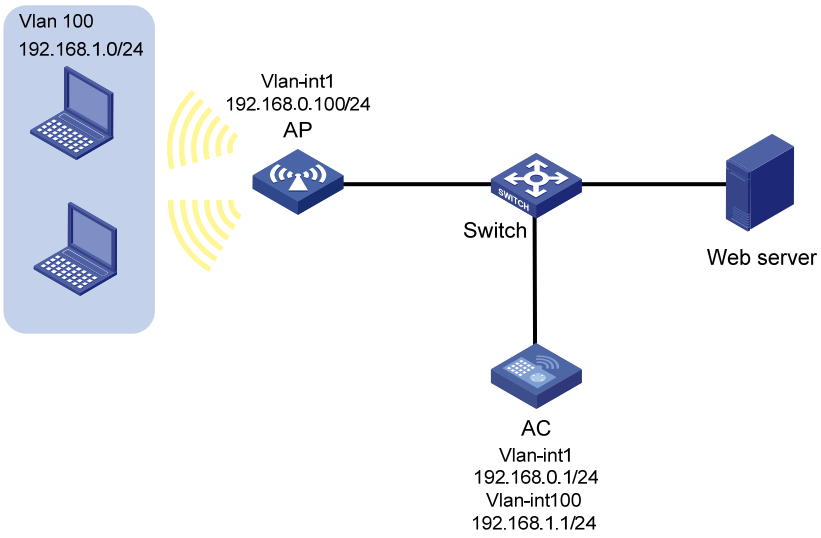
1.4.1 基于接口的连接数限制典型配置举例

1. 组网需求

某办公室内部所有主机通过无线网络访问 Web 服务器，所在网段地址为 192.168.1.0/24。为保障服务器资源的可用性，通过在 AC 上配置连接数限制功能，限制每台主机最多同时可与该 Web 服务器建立 100 条 HTTP 连接。

2. 组网图

图1-2 连接限制典型配置组网



3. 配置步骤

创建 ACL 3000，定义规则允许访问 Web Server 的 HTTP 请求报文通过。

```
<AC> system-view
[AC] acl advanced 3000
[AC-acl-ipv4-adv-3000] rule permit tcp source 192.168.1.0 0.0.0.255 destination-port eq 80
[AC-acl-ipv4-adv-3000] quit
```

创建连接数限制策略 1。

```
[AC] connection-limit policy 1
```

配置连接数限制规则 1，允许匹配 ACL 3000 的每台主机最多只能与外网建立 100 条连接，超过 100 时，需要等连接数恢复到 50 以下才允许建立新的连接。

```
[AC-connection-limit-policy-1] limit 1 acl 3000 per-source amount 100 50
[AC-connection-limit-policy-1] quit
```

在全局应用连接数限制策略 1。

```
[AC] connection-limit apply global policy 1
```

4. 验证配置结果

上述配置完成后，执行 **display connection-limit policy** 命令显示连接数限制的配置情况，具体内容如下。

```
[AC] display connection-limit policy 1
IPv4 connection limit policy 1 has been applied 1 times, and has 1 limit rules.
Limit rule list:
 Policy  Rule     Stat Type  HiThres  LoThres  rate    ACL
------------------------------------------------------------------------------
      1     1           Src      100       50  0       3000
 Application list:
     Global
```

1.5 连接限制常见配置错误举例

1.5.1 不同的连接限制规则中引用的ACL存在包含关系时，规则顺序错误

1. 故障现象

在 AC 上进行如下配置，希望限制主机 192.168.0.100/24 最多向某公网服务器发起 100 条连接请求，以及 192.168.0.0/24 网段的其他主机最多向某公网服务器发起 10 条连接请求。

```
<AC> system-view
[AC] acl basic 2001
[AC-acl-ipv4-basic-2001] rule permit source 192.168.0.0 0.0.0.255
[AC-acl-ipv4-basic-2001] quit
[AC] acl basic 2002
[AC-acl-ipv4-basic-2002] rule permit source 192.168.0.100 0
[AC-acl-ipv4-basic-2002] quit
[AC] connection-limit policy 1
[AC-connection-limit-policy-1] limit 1 acl 2001 per-destination amount 10 5
[AC-connection-limit-policy-1] limit 2 acl 2002 per-destination amount 100 10
```

实际运行过程中，主机 192.168.0.100 最多只能同时向外部网络的同一个目的地址发起 10 条连接，后续连接被拒绝。

2. 故障分析

在上述配置中，limit 1 和 limit 2 中指定的源 IP 地址范围存在包含关系，192.168.0.100 发起的连接既符合 limit 1 又符合 limit 2。由于在进行连接限制规则的匹配时，设备根据规则编号由小到大的顺序进行匹配，且以匹配到的第一条有效规则为准，因此对 192.168.0.100 向外部网络发起的连接将只按照 limit 1 进行限制，而不会使用 limit 2 来限制。

3. 处理过程

为实现本需求，需要对 limit 2 与 limit 1 的顺序重新安排，将两个规则的序号进行调换，即将限制粒度更细、限制范围更精确的规则置前。