

IP访问列表配置

目 录

第 1 章 配置物理端口IP访问列表	1
1.1 过滤IP报文	1
1.2 建立标准的和扩展的IP访问列表	1
1.3 应用访问列表	2
1.3.1 将访问列表应用到端口	2
1.3.2 将访问列表应用到VLAN	2
1.3.3 将访问列表应用到全局	3
1.4 扩展访问列表示例	3

第1章 配置物理端口IP访问列表

1.1 过滤IP报文

过滤报文帮助控制包在网络中的运动。这样的控制可以帮助限制网络传输并通过一定的用户或设备限制网络使用。为了从交叉指定的端口中使包有效或无效，本公司路由交换机提供了访问列表。可以用以下方式使用访问列表：

- 控制在端口上的包传输
- 控制虚拟终端线路访问
- 限制路由更新内容

本节概括了如何建立 IP 访问列表以及如何应用它们。

IP 访问列表是应用 IP 地址的允许和禁止条件的有序集合。本公司路由交换机的 ROS 软件在访问列表中逐个按规则测试地址。第一个匹配决定是否该软件接受或拒绝该地址。因为在第一个匹配之后，该软件停止了匹配规则，所以条件的先后次序是重要的。如果没有规则匹配，拒绝该地址。

在使用访问列表中有以下两个步骤：

- (1) 通过指定访问列表名及访问条件，建立访问列表。
- (2) 将访问列表应用到端口。

1.2 建立标准的和扩展的IP访问列表

用一个字符串建立 IP 访问列表。

注意：

标准的访问列表和扩展的访问列表不能用相同的名字。

为了建立标准的访问列表，在全局配置态执行下列命令。

命令	目的
ip access-list standard name	使用名字定义一个标准的IP访问列表。
deny {source [source-mask] any} or permit {source [source-mask] any}	在标准访问列表配置模式下，指定一个或多个允许或不允许条件。这决定该包通过还是不过。
Exit	退出访问列表配置模式。

为建立扩展的访问列表，在全局配置态执行下列命令：

命令	目的
ip access-list extended name	使用名字定义一个扩展的IP访问列表。
{deny permit} protocol source source-mask destination destination-mask [precedence precedence] [tos tos] {deny permit} protocol any any	在扩展访问列表配置模式下，指定一个或多个允许或不允许条件。这决定该包通过还是不过。(<i>precedence</i> 表示ip包优先级，TOS表示Type of Service)
Exit	退出访问列表配置模式。

在初始建立访问列表后，任何后续的增加部分(可能从终端键入)都放入表的尾部。换句话说，你不能从指定的访问列表选择增加访问列表命令行。但是，你可以使用 **no permit** 和 **no deny** 命令从名字访问列表中删除项。

注意：

当建立访问列表时，记住缺省时访问列表的结尾包含隐含的 **deny** 语句。进一步讲，标准的访问列表，如果从相关的 IP 主机地址访问列表指定中省略了掩码，那么 255.255.255.255 就假定是掩码。

在建立了访问列表后，必须将它应用到线路或端口上。如下一节“将访问列表应用到端口”所描述。

1.3 应用访问列表

1.3.1 将访问列表应用到端口

当建立了访问列表后，可以将它应用到一个或多个端口上，可以应用到入口。

在端口配置态使用以下命令。

命令	目的
ip access-group name	将访问列表应用到端口。

对于标准的入口访问列表，如果在该端口接收到报文之后，对照访问列表检查包的源地址。对于扩展的访问列表，该路由交换机也检查目标地址。如果访问表允许该地址，那么软件继续处理该报文。如果访问表不允许该地址，该软件放弃报文并返回一个 **ICMP** 主机不可到达报文。

如果指定的访问列表不存在，所有的包允许通过。

1.3.2 将访问列表应用到VLAN

当建立了访问列表后，可以将它应用到一个或多个 **VLAN** 上。

在全局状态下配置以下命令。

命令	目的
ip access-group name vlan word	将访问列表应用到 VLAN

WORD 代表了应用访问控制列表 vlan 号的集合，只有带有此集合中 vlan 标签的报文，而且 IP 地址匹配的情况下，访问列表才会发挥作用。对于标准的访问列表，报文的源 IP 地址需要与访问列表中 IP 地址匹配；对于扩展的访问列表，报文的源和目的 IP 地址需要与访问列表中源和目的 IP 地址相匹配。如果访问表允许该地址，那么软件继续处理该报文。如果访问表不允许该地址，该软件放弃报文并返回一个 ICMP 主机不可到达报文。

如果进入交换机报文未带有此集合中的 vlan 标签，或者 IP 地址没有与访问列表中 IP 地址相匹配，那么报文将不受访问控制。

命令	目的
ip access-group name vlan add word	向 word 集合中添加 VLAN 号。
ip access-group name vlan remove word	从 word 集合中删除 VLAN 号。

这两条命令用于添加或减少 WORD 集合中 VLAN，从而放大或缩小访问列表的控制范围。

1.3.3 将访问列表应用到全局

当建立了访问列表后，可以将它应用到全局。

在全局状态下配置以下命令。

命令	目的
ip access-group name	将访问列表应用到全局

把访问列表应用到全局后，所有进入交换机入口的报文，只要报文的 IP 地址与访问列表中的 IP 地址配置，报文将受到访问控制。如果访问表允许该地址，那么软件继续处理该报文。如果访问表不允许该地址，该软件放弃报文并返回一个 ICMP 主机不可到达报文。

1.4 扩展访问列表示例

在以下例子中，第一行允许新来的 TCP 与主机 130.2.1.2 的 SMTP 端口连接。

```
ip access-list extended aaa
permit tcp any 130.2.1.2 255.255.255.255 eq 25
interface g0/10
ip access-group aaa
```