S8500交换机基本访问控制列表技术说明

罗淳榕 2006-08-07 发表

S8500基本访问控制列表技术说明

一、简单介绍

为了过滤通过网络设备的数据包，需要配置一系列的匹配规则，以识别需要过滤的对象。在识别出特定的对象之后，网络设备才能根据预先设定的策略允许或禁止相应的数据包通过。访问控制列表（Access Control List，ACL）就是用来实现这些功能。

ACL通过一系列的匹配条件对数据包进行分类，这些条件可以是数据包的源地址、目的地址、端口号等。ACL可应用在交换机全局或端口上，交换机根据ACL中指定的条件来检测数据包，从而决定是转发还是丢弃该数据包。S8500交换机支持的访问控制列表可以分为以下三类：

基本访问控制列表；

高级访问控制列表；

二层访问控制列表。

每一种访问控制列表都可以用名字或数字来标识。其中基本访问控制列表只根据源IP地址制定规则，对数据包进行相应的分析处理。

二、设备配置实例

1．组网需求

通过基本访问控制列表，实现在每天8:00～18:00时间段内对源IP为10.1.1.1主机发出报文的过滤（该主机从交换机的Ethernet4/1/1接入）。

2．组网图

基本访问控制典型组网图

3．配置步骤

(1)定义时间段

定义8:00～18:00时间段。

[Quidway] time-range huawei 8:00 to 18:00 daily

(2)定义基于名字的ACL

进入基于名字的基本访问控制列表视图，命名为traffic-of-host。

[Quidway] acl name traffic-of-host basic

定义源IP为10.1.1.1的访问规则。

[Quidway-acl-basic-traffic-of-host] rule 1 deny source 10.1.1.1 0 time-range huawei

(3)在端口上激活ACL

将traffic-of-host的ACL激活。

[Quidway-Ethernet4/1/1] packet-filter inbound ip-group traffic-of-host