H3C S9500交换机对Telnet用户的二层ACL控制配置

刘志伟 2006-11-03 发表

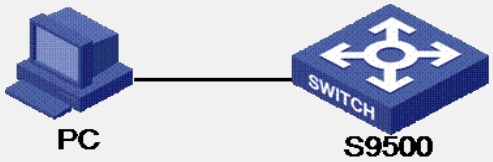
H3C S9500交换机对Telnet用户的二层ACL控制配置

一、组网需求:

通过配置对Telnet用户的ACL控制，可以在登录用户进行口令认证之前将一些恶意或者不合法的连接请求过滤掉，保证设备的安全。

本文主要介绍对Telnet用户的二层ACL控制配置，仅允许源MAC地址为000f-e201-0101和000f-e201-0303的Telnet用户访问交换机。

二、组网图:



三、配置步骤:

软件版本：S9500交换机全系列软件版本

硬件版本：S9500交换机全系列硬件版本

定义二层访问控制列表。

[S9500] acl number 4000 match-order config

定义子规则。

[S9500-acl-link-4000] rule 1 permit ingress 000f-e201-0101 0000-0000-0000

[S9500-acl-link-4000] rule 2 permit ingress 000f-e201-0303 0000-0000-0000

[S9500-acl-link-4000] rule 3 deny ingress any

[S9500-acl-link-4000] quit

进入用户界面视图。

[S9500] user-interface vty 0 4

引用二层访问控制列表，对用户界面的呼入进行限制。

[S9500-user-interface-vty0-4] acl 4000 inbound

四、配置关键点:

1.Telnet用户的ACL控制功能只能引用基于数字标识的访问控制列表。

2. Telnet用户引用基本访问控制列表或高级访问控制列表时，基于源IP或目的IP地址对呼入/呼出进行限制。因此引用基本访问控制列表和高级访问控制列表子规则时，只有源IP及其掩码、目的IP及其掩码、time-range参数有效。类似的，Telnet用户引用二层访问控制列表时，基于源MAC地址对呼入/呼出进行限制。因此引用二层访问控制列表子规则时，只有源MAC及其掩码、time-range参数有效。

3. 基于二层访问控制列表对Telnet用户进行控制时，只能限制呼入。