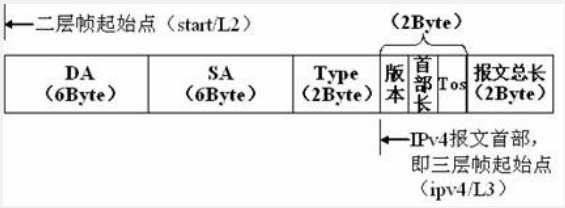
H3C S3610_S5510系列交换机使用自定义ACL匹配报文长度的方法

岳斌 2007-11-14 发表

H3C S3610_S5510交换机使用自定义ACL匹配
报文长度的方法

一、 需求描述：
当需要根据不同报文长度，对数据进行分类并进行不同处理时，在S3610、S5510交换机上可以使用“用户自定义ACL”的方式实现该功能。
用户自定义ACL的序号取值范围为5000～5999。规则配置的命令格式如下说明所示。
rule [*rule-id*] { **permit** | **deny** } [[**start** | **ipv4** | **ipv6** | **l2** | **l4**] { *rule-string rule-mask offset* }&<1-8>] [**time-range** *time-name*]
其中，
start：从报文头开始偏移。
ipv4：从IPv4报文头开始偏移。
ipv6：从IPv6报文头开始偏移。
l2：从二层帧头开始偏移。
l4：从四层报文头开始偏移。
rule-string：用户自定义的规则字符串，必须是16进制数组成，字符长度必须是偶数。
rule-mask：规则字符串的掩码，用于和报文作“与”操作，必须是16进制数组成，字符长度必须是偶数。
offset：偏移量，指定从第几个字节开始进行“与”操作。
&<1-8>：表示一次最多可以定义8个这样的规则。
下面通过不同应用对该ACL的配置方法予以说明。
二、 匹配精确长度的方法：
例如，通过配置ACL匹配长度为1200字节的报文时，rule规则的配置方法如下。
[H3C] acl number 5000
[H3C-acl-user-5000] rule permit start 04B0 ffff 16
或
[H3C-acl-user-5000] rule permit l3 04B0 ffff 2
说明如下：IP数据报文结构如下图所示。



从上图中可以看到，当选择“start”或“l2”关键字时，从二层帧起点向后偏移16字节即为报文总长度起点，“04B0”为1200的十六进制表示方法，“ffff”表示对带有“04B0”字段的报文进行完全匹配。
若选择“ipv4”或“l3” 关键字，则从三层帧起点向后偏移2字节即可。
三、 匹配长度范围的方法：
例如，通过配置ACL匹配长度在1200<=length<=1280字节范围内的报文时，rule规则的配置方法如下。
[H3C] acl number 5000
[H3C-acl-user-5000] rule permit start 04B0 fff0 16
说明：该rule匹配长度范围为1200<=length<=1215的报文。因为，
1199二进制表示如下0000 0100 1010 1111，十六进制表示如下04AF。
1200二进制表示如下0000 0100 1011 0000，十六进制表示如下04B0。
1215二进制表示如下0000 0100 1011 1111，十六进制表示如下04BF。
在1200～1215范围内，它们的前12个bit都相同，所以通过调整掩码中“1”的个数来匹配该范围内报文，即掩码前12个bit全“1”——“fff0”。
[H3C-acl-user-5000] rule permit start 04C0 ffc0 16
说明：该rule匹配长度范围为1216<=length<=1279的报文。因为，
1216二进制表示如下0000 0100 1100 0000，十六进制表示如下04C0。
1279二进制表示如下0000 0100 1111 1111，十六进制表示如下04FF。
在1216～1279范围内，它们的前10个bit都相同，所以掩码前10个bit全“1”——“ffc0”。
[H3C-acl-user-5000] rule permit start 0500 ffff 16
说明：该rule匹配长度为1280的报文。因为，
1280二进制表示如下0000 0101 0000 0000，十六进制表示如下0500。
通过精确匹配方式，即掩码全“1”——“ffff”来表示。

四、　　注意事项：

（1）报文匹配前不用将vlan tag的4个字节计入偏移量。

（2）在配置ACL过程中，通过修改掩码中“1”的个数来划分匹配范围。