利用established字段实现TCP的单向访问

ACL　程咪　2019-10-30 发表

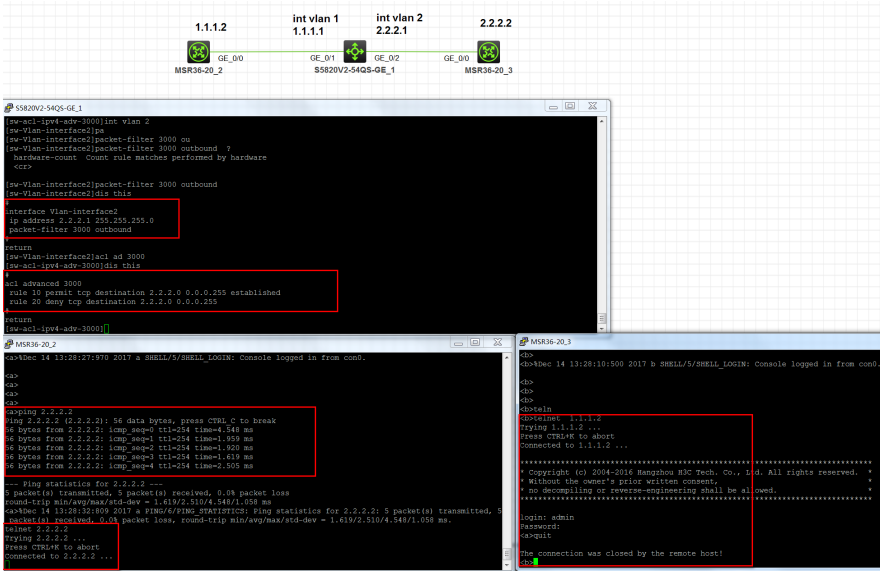
问题描述

利用established字段实现TCP的单向访问

解决方法

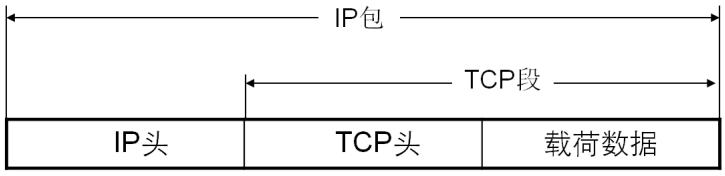
Tcp单向访问，主要是要理解ack置位和应用方向问题。
vlan2网段可以主动与其他网段建立tcp，但是其他网段不能主动和2网段建立tcp，可以如下操作：

tcp established匹配的是带有ack标志位的tcp连接报文，而tcp匹配的是所有tcp连接报文。
先匹配permit的，再匹配deny的。这样的结果是在出方向deny了不带有ack标志位的tcp连接报文，其它tcp连接报文均能正常通过。
因此Vlan 1所在网段发起tcp连接时第一个请求报文被deny而无法建立连接，Vlan 2所在网段发起tcp连接时，1所在网段回复的都是带有ack标志位的tcp连接报文，连接可以顺利建立。

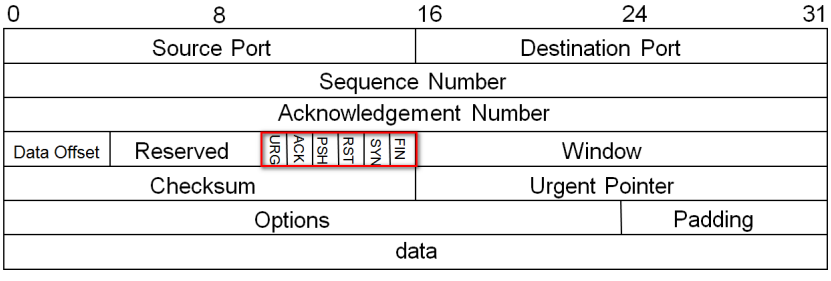


控制位如红框中字段，六个标志位从左至右是URG，紧急指针字段标志；ACK，确认字段标志；PSH，推功能；RST，重置连接；SYN，同步序列号；FIN，数据传送完毕。

TCP封装



TCP头格式



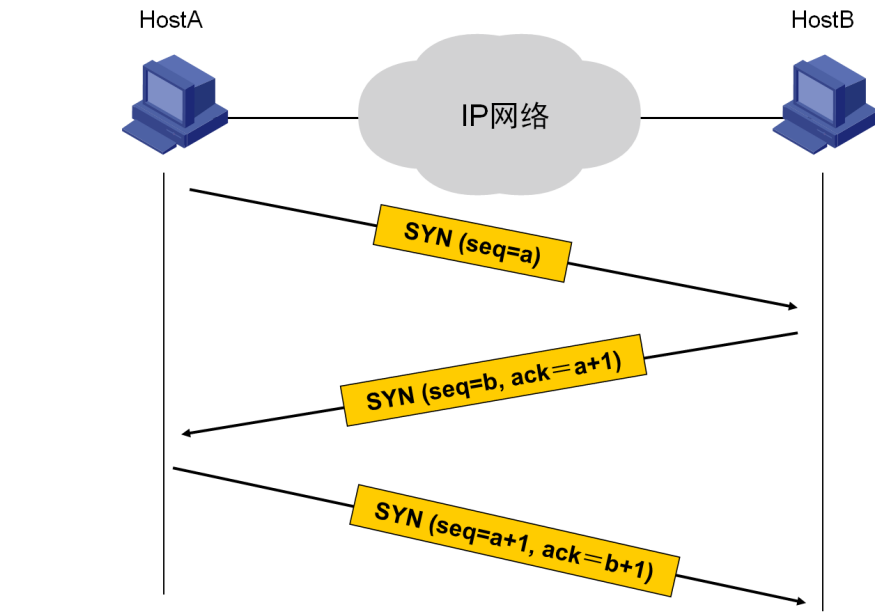
命令手册对于rule规则中tcp相关字段的说明：
1.1.18 rule (IPv4 advanced ACL view)

{ **ack** *ack-value* | **fin** *fin-value* | **psh** *psh-value* | **rst** *rst-value* | **syn** *syn-value* | **urg** *urg-value* } *	TCP 报文标识	定义对携带不同标志位（包括ACK、FIN、PSH、RST、SYN和URG六种）的TCP报文的处理规则	TCP协议特有的参数。表示匹配携带不同标志位的TCP报文，各*value*的取值可为0或1（0表示不携带此标志位，1表示携带此标志位） 如果在一条规则中设置了多个TCP标志位的匹配值，则这些匹配条件之间的关系为“与”。譬如：当配置为**ack** 0 **psh** 1时，表示匹配不携带ACK且携带PSH标志位的TCP报文

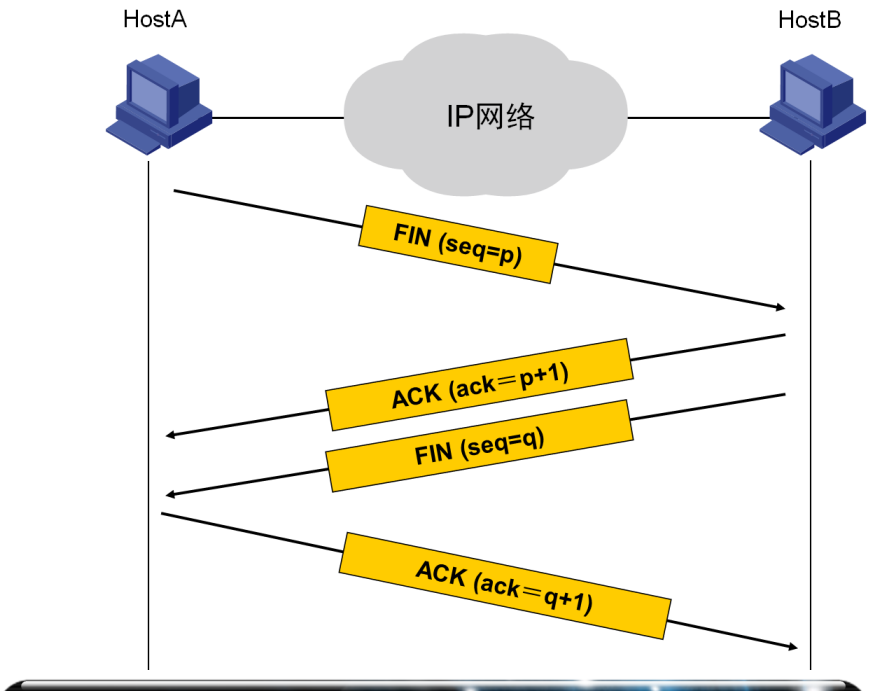
TCP的建立，拆除、传输、超时重传，滑动窗口过程截图如下：

Tcp建立过程发起方第一个发包，ACK无效，可以利用这个实现TCP单向访问。

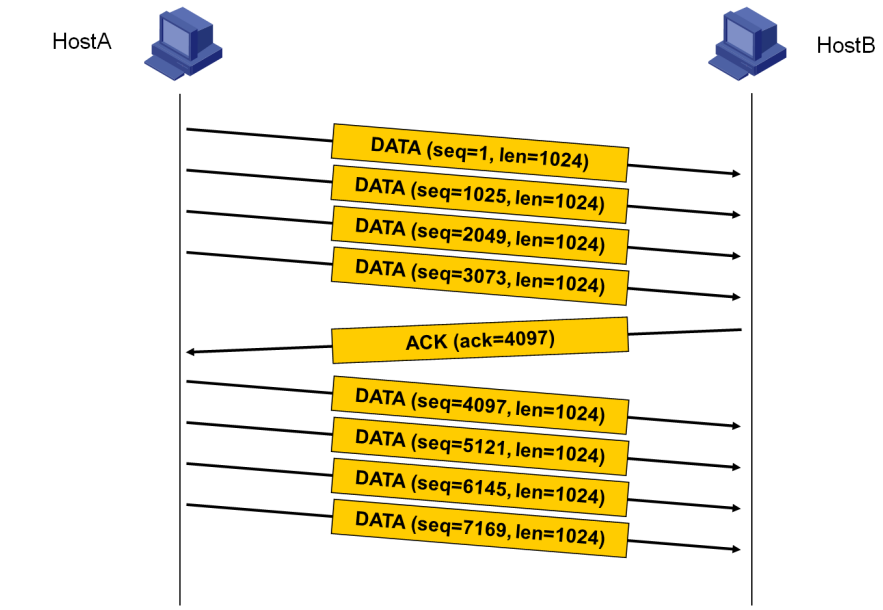
TCP连接的建立



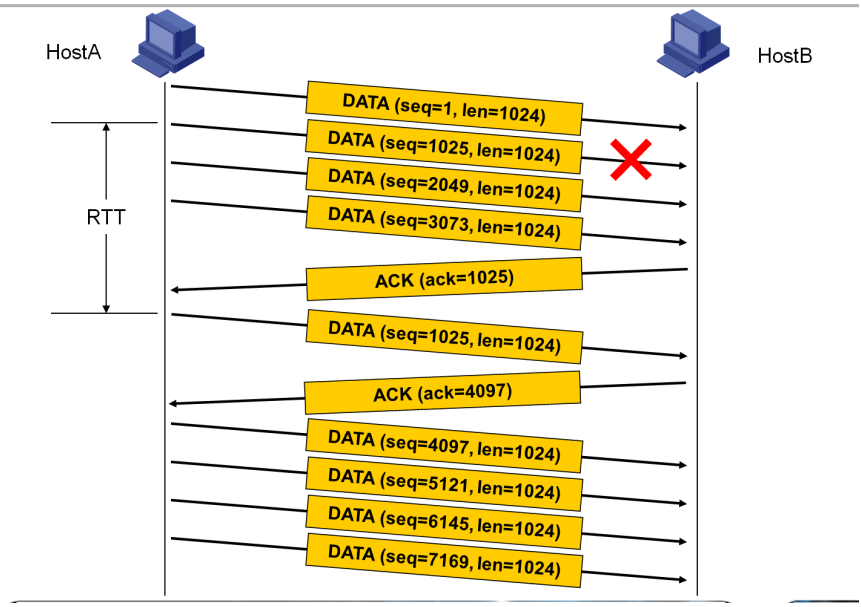
TCP连接的拆除



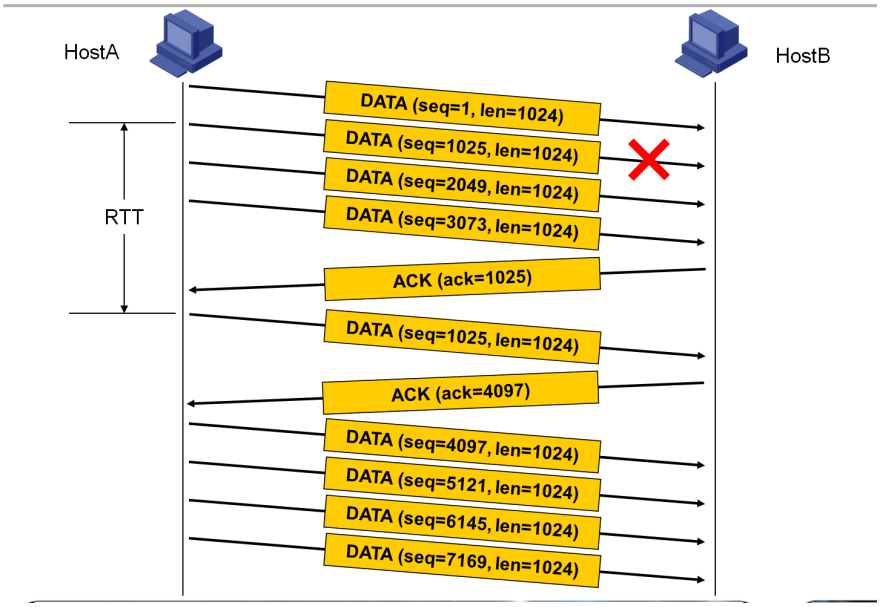
传输确认


HostA
HostB
DATA (seq=1, len=1024)
DATA (seq=1025, len=1024)
DATA (seq=2049, len=1024)
DATA (seq=3073, len=1024)
ACK (ack=4097)
DATA (seq=4097, len=1024)
DATA (seq=5121, len=1024)
DATA (seq=6145, len=1024)
DATA (seq=7169, len=1024)

超时重传


HostA
HostB
RTT
DATA (seq=1, len=1024)
DATA (seq=1025, len=1024)
DATA (seq=2049, len=1024)
DATA (seq=3073, len=1024)
ACK (ack=1025)
DATA (seq=1025, len=1024)
ACK (ack=4097)
DATA (seq=4097, len=1024)
DATA (seq=5121, len=1024)
DATA (seq=6145, len=1024)
DATA (seq=7169, len=1024)

超时重传


HostA
HostB
RTT
DATA (seq=1, len=1024)
DATA (seq=1025, len=1024)
DATA (seq=2049, len=1024)
DATA (seq=3073, len=1024)
ACK (ack=1025)
DATA (seq=1025, len=1024)
ACK (ack=4097)
DATA (seq=4097, len=1024)
DATA (seq=5121, len=1024)
DATA (seq=6145, len=1024)
DATA (seq=7169, len=1024)