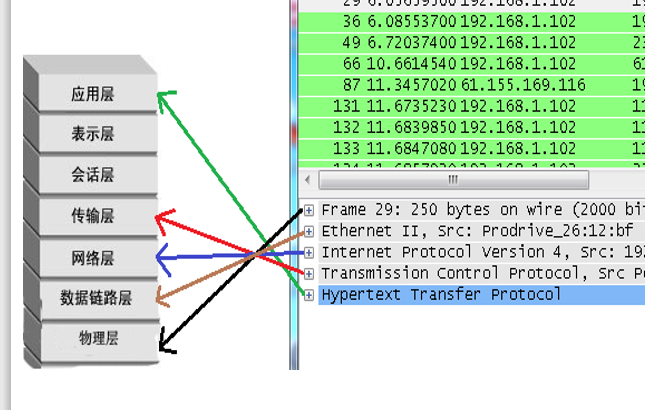
Wireshark知识总结



（1）抓包过滤器的使用

过滤语法：

* 1.Protocol（协议）

可能的值: ether, fddi, ip, arp, rarp, decnet, lat, sca, moprc, mopdl, tcp and udp.

* Direction（方向）

可能的值: src 原地址, dst目标地址, src and dst, src or dst

* Host(s)

可能的值： net, port, host, portrange.

如果没有指定此值，则默认使用"host"关键字。

例如，"src 10.1.1.1"与"src host 10.1.1.1"相同。

* Logical Operations（逻辑运算）

可能的值：not, and, or.

否("not")具有最高的优先级。或("or")和与("and")具有相同的优先级，运算时从左至右进行。

例如，

“not tcp port 3128 and tcp port 23”与“（not tcp port 3128） and tcp port 23”相同。

“not tcp port 3128 and tcp port 23”与“not （tcp port 3128 and tcp port 23）”不同。

**例子：**

udp dst port 60040

显示目的UDP端口为60040的封包。

ip src host 172.16.226.126

显示来源IP地址为172.16.226.126的封包。

host 10.1.2.3

显示目的或来源IP地址为10.1.2.3的封包。

src portrange 60040-60042

显示来源为UDP或TCP，并且端口号在60040至60042范围内的封包。

not imcp

显示除了icmp以外的所有封包。（icmp通常被ping工具使用）

src host 172.16.226.126 and not dst net 172.16.160.42/16

显示来源IP地址为172.16.226.126，但目的地不是172.16.160.42/16的封包。

(src host 10.4.1.12 or src net 10.6.0.0/16) and tcp dst portrange 200-10000 and dst net 10.0.0.0/8

显示来源IP为10.4.1.12或者来源网络为10.6.0.0/16，目的地TCP端口号在200至10000之间，并且目的位于网络10.0.0.0/8内的所有封包。

1. 显示过滤器

|  |  |
| --- | --- |
| 视频格式 | 动态载荷 |
| H261 | 31 |
| Mpeg2 | 33 |
| H263 | 34 |
| Mpeg4 | 97 |
| H264 | 106 |
| 音频格式 | 动态载荷 |
| G711A | 8 |
| G722 | 9 |
| G722.1.C Polycom | 98 |
| G728 | 15 |
| Mp 3 | 96 |
| MPEG4 AAC-LC | 102 |

h225 || h245

显示h225或h245的信令数据，通过此过滤方式可以只显示呼叫建立和释放的包信息

ip.src==172.16.226.126

显示数据包源的IP地址为172.16.226.126的所有信息，通过此过滤方式可只显示IP地址为172.16.226.126的主机所发出的所有数据包

ip.dst==172.16.160.42

显示数据包目的IP地址为172.16.160.42的所有信息，通过此过滤方式可只显示IP地址为172.16.160.42的主机所收到的所有数据包

udp.srcport==60048

显示udp包源端口地址为60048的所有信息，通过此过滤方式可只显示源端口地址为60048所发出的所有udp包

udp.dstport==60042

显示udp包目的端口地址为60042的所有信息，通过此过滤方式可只显示目的端口地址为60042所收到的所有udp包

ip.src==172.16.226.126 && udp.srcport==60048

显示数据包源的IP地址为172.16.226.126并且udp包源端口地址为60048的所有信息，通过此过滤方式可只显示IP地址为172.16.226.126的主机且由其60048端口所发出的所有udp包

ip.dst==172.16.160.42 && udp.dstport==60042

显示数据包目的IP地址为172.16.160.42并且udp包端口地址为60042的所有信息，通过此过滤方式可只显示IP地址为172.16.160.42的主机且由其60042端口所收到的所有udp包