网络协议分析实验整理

原创

qq_38941327 于 2019-05-28 21:39:43 发布 2366 收藏 18
分类专栏： class learning

本实验采用网络结构一，主机的IP地址使用172.16.0.0段。**两个人一组，每组提交电子报告。**

这门课需要上课做实验然后写报告，最后开卷考试，下面是我整理的问题，对应的答案在PDF中，太多了25页，有需要自取吧

链接：https://pan.baidu.com/s/1Gq0TM5lgZ5CgAltHqOaklA
提取码：l3x4
复制这段内容后打开百度网盘手机App，操作更方便哦

1. LLC帧的报头及长度（目的MAC-6、源MAC-6、协议类型或数据长度-2）
2. 实际以太网帧报头的长度：LLC帧的报头14+4字节的CRC
3. SAP的含义，三种LLC帧的控制字段的比较
4. 协议类型或数据长度字段的意思？该字段若>0600H(十进制1536），表示协议种类，小于，表示后面的数据长度，所以在实验1中，该字段为0040，指示了后面的数据长度为60（64-4,4位LLC的报头长度）
5. LLC广播帧的目的MAC是FFFFFFF-FFFFFF
6. IP地址和MAC地址的不同：位数、协议、分配依据、协议层不同
7. IPconfig命令查看本机IP、MAC、DNS、网关、MASK
8. route print查看本机路由表：表项包括：目的IP、网络掩码、网关、输出接口Interface、路径长度METRIC
9. 本机路由表中的缺省路由：Network Destination为0.0.0.0
10. IP协议报头及字段含义（会出给出十六机制以太网帧的字节信息，判断协议类型，IP地址，端口等），IP报文总长度=首部长度20Byte+数据长度
11. 协议类型或数据长度字段 常用值（十六进制）：0800：IP协议 8600：IPV6协议 0806：ARP协议
    1. IP协议中高层协议类型常用值（十六进制）：ICMP :01 IGMP:02 TCP06 UDP:11 OSPF:59
    2. 实验2中问题：查看捕获帧的长度是多少？是否与编辑的报文长度一致？不一致，因为IP报文经过了封装，捕获帧的长度是IP报文的总长度+LLC帧的长度14
    3. 实验2问题：为什么有目的端口不可达报文：因为编辑的包无传输层，无进程接收，所以...
    4. IPV6和IPV4的区别，字段对应？（NextHeader TTL HopLimit）
    5. IP广播
    6. IP分片（重点）：IP分片这次实验是使用PIng实现，由于Ping的原理是利用了ICMP查询报文，因此在IP数据部分存在8字节的ICMP报文头，因此，整个数据部分是ping的字节数+8字节，所以，若ping3000，分片为（3000+8）/1480=3片，最后一篇的IP数据长度为3008-1480*2=48，IP报文总长度为48+20=68字节，最后一片帧的总长度为82
    7. IP分片（ping），ping多长保证最后一个帧是82字节？1480*n+40
    8. netstat命令：-s显示本机已经接受和发送的IP报文个数 -r：显示本机路由表
    9. -e：查看以太网统计信息
    10. arp -a 查看缓存表内容
    11. ARP请求报文报头：MAC层-ARP层
    12. 不同网段内发送ARP报文原理（计算机网络中讲过），此过程中报文IP的不变，MAC的改变，TTL的改变（反应经过的网关数量）

13. ARP欺骗原理
14. IP冲突原理：免费ARP（ARP查询报文，源和目的IP都是自己的IP）
15. ARP缓存的作用：减少广播发送次数，提高解析速度
16. ARP表项为什么过一段时间会消失？具有老化机制
17. ICMP报文的格式和类型、代码，承载在IP层协议
18. ICMP时间戳报文和应答报文格式
19. ICMPV6和ICMPV4的比较
20. ICMP重定向（特征数据是什么？）
21. UDP检验和填0，表示不校验
22. UDP报文格式和检验和的手动计算
23. UDP端口不可达时，产生ICMP差错报文
24. UDP受限广播和直接广播，二者区别
25. DNS ：nslookup 域名 DNS报文编辑（正向查询和反向查询）
26. TCP三次握手序号和确认号的变化
27. TCP释放连接的变化
28. TCP实验中，主机发送的应答报文，是否会捕获到连续两个应答报文，且前者的ACK大于后者？会，有可能第一次对于报文的ACK丢失，接收方超时重传导致其后到达
29. UDP端口扫描
30. TCP端口扫描SYN（RST代表关闭，SYN/ACK代表打开）、FIN扫描（unix：关闭恢复RST，windows：都回复RST）
31. FTP命令、端口等，PORT的作用，控制连接和数据连接
32. HTTP协议
33. DHCP的四个阶段
34. DHCP报文格式
35. SMTP协议

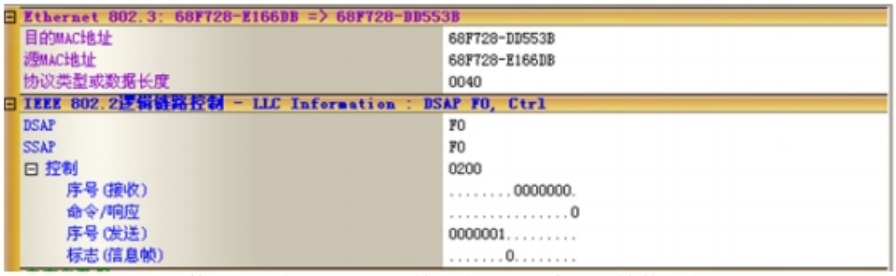
各类端口及其协议对应：

80：HTTP　　110：POP3
53：DNS.　　23：TELNET
20/21：FTP　　143：IMAP
25：SMTP

一、实验 1

1. LLC 帧（MAC 帧中的数据字段）：

在练习中，可以看出 LLC 信息帧报头长度是 4 字节（DSAP+SSAP+控制字段），如下：



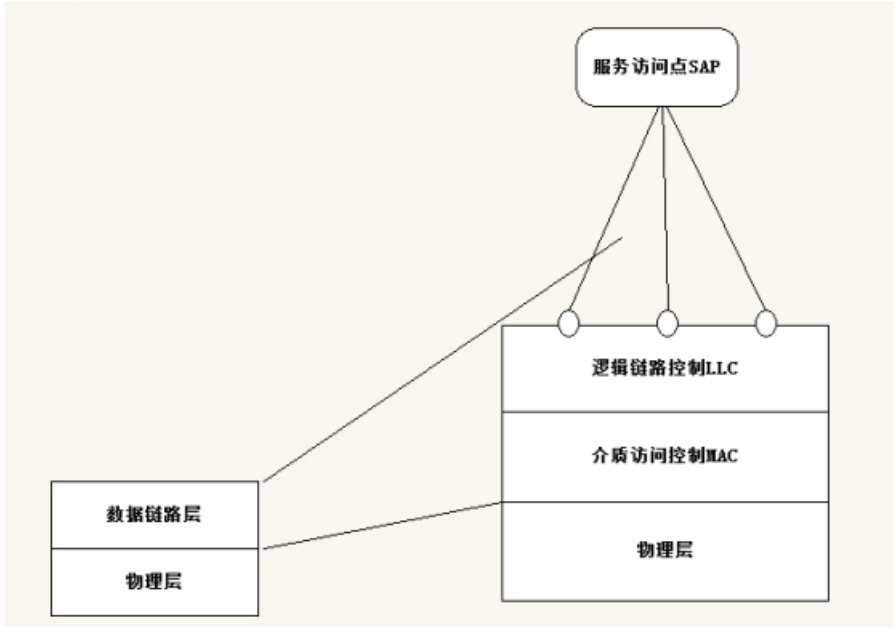
注意：**协议类型或数据长度字段是以太网帧的字段，用来指明帧数据字段的协议。**
若字段值>1536(十六进制：0600)时，该字段表示协议种类；若小于 1536，那么该字段指明了后面的数据长度

注：>0600:0800 对应 IP 协议；8600 对应 IPv6 协议；0806ARP 协议

所以 0040 会对数据区的长度有限制，0040（十六进制）=64，所以限制了数据字段只有 60（64-60）字节

注：实际中，以太网最小帧长为 64 字节，数据部分最少为为 64-18=46 字节； 而在此次试验中，以太网头只有 14 字节，实际是 14+4 字节的 CRC（循环冗余校验）码。 实际中，以太网最大帧长为 1500+18=1518 字节

在 IEEE802 中，数据链路层被划分为逻辑链路层（LLC）和介质访问控制 MAC 子层；如下图：



（1） 服务访问点（SAP）地址：SAP 提供了多个高层协议进程共同使用一个 LLC 层实体进行通信的机制（即为高层协议提供接口）。在一个网络结点上，一个 LLC 层可能同时为多个高层协议服务，LLC 协议定义了逻辑地址 SAP 及其编码机制，保证多个高层协议进程使用不同的 SAP 地址共享一个 LLC 层实体，允许高层协议进程同时使用多个 SAP 进行通信（并发）。
DSAP：目的 LLC 的 SAP 地址，最高位（I/G）为 0 表示 DSAP 是一个单地址，为 1 表示是一个组地址，此时 LLC 帧由 DSAP 标识的一组目的 LLC SAP 接收。
SSAP:源 LLC 的 SAP 地址，最高位（C/R）为 0 时，表示命令帧，为 1 是响应帧。

（2） 监控帧的控制字段如下：
对于一个监控帧，控制字段为 2 字节长。
1 位 1；一位 0；
2 位 SS 监控功能位中，00 表示准备接收、10 表示未准备接收、01 表示拒绝；
4 位 X 保留设置为 0；
1 位 P/F 命令或响应 LLC PDU 传输；
7 位 N(R) 接收序号

（3） 其他种类帧

下图表示了 LLC 三类帧的控制字段的比较。

信息帧

1 位	7 位	1 位	7 位
0	N(S)	P/F	N(R)
I-帧的控制字段			

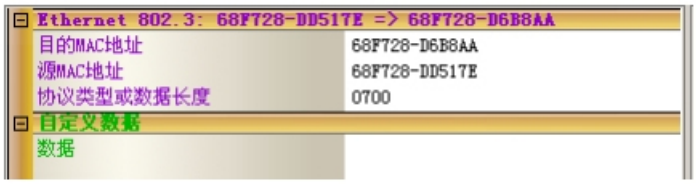
监控帧

1 位	1 位	2 位	4 位	1 位	7 位
1	0	SS	X	P/F	N(R)
S-帧的控制字段					

无编号帧

1	1	M	M	P/F	M	M	M
U-帧的控制字段							

2. 练习 2：自定义协议的数据帧



此帧的 0700>0600，表示协议类型，不再对数据长度有限制

3. 练习 3：LLC 广播帧
目的 MAC 地址：FFFFFF-FFFFFF
类型或长度：大于 0x0600（自定义协议类型）

4. 练习 4：MAC 地址在交换机和集线器的作用

A 向 C 发帧，B、C 均能收到，B 能收到是因为与 A 通过集线器连接，集线器会将数据转发给所有端口，交换机会根据地址转发到目的端口，由于集线器采用了共享带宽的方式，安全性较低，交换机是一个独享的信道，安全性较高。

5. 练习 5：IPconfig

该命令可以查看本机的主机名、IP、MAC、DNS、网关、MASK。

比较 IP 地址和 MAC 地址

1.两者的地址使用不同。IP 地址用于 Internet 协议，MAC 地址用于 Ethernet 协议

2.分配依据不同。IP 地址的分配基于网络拓扑，MAC 地址的分配基于制造商。

3.长度不同。IP 地址为 32 位，MAC 地址为 48 位。

4.寻址协议层不同。IP 地址应用于网络层，MAC 地址应用于数据链路层。

6. 练习 6：本机路由表

命令：route print：

Network Destination　是目的 IP 地址

Netmask：网络掩码

Gateway　：网关

Interface　：输出接口

Metric：是路由算法计算出的路径长度。

NetworkDestination	Netmask	Gateway	Interface	Metric
0.0.0.0	0.0.0.0	172.16.0.253	172.16.4.74	1

缺省路由：当一个数据包的目的网段不在你的路由记录中时，我的路由器将把这个数据包发送到哪里。缺省路由的网关是由你的链接上的 default gateway 决定的，当一个数据包的目的网段不在你的路由记录中时，会通过 172.16.4.74 这个接口发送到 172.16.0.253 这个地址。

二、实验 2

1. 练习 1：IP 协议

IP 数据包的编辑：总长度=首部长度 20Byte+数据长度