Workshop 5：解码数据包 子网和超网 路由

1：解码因特网数据包（1）

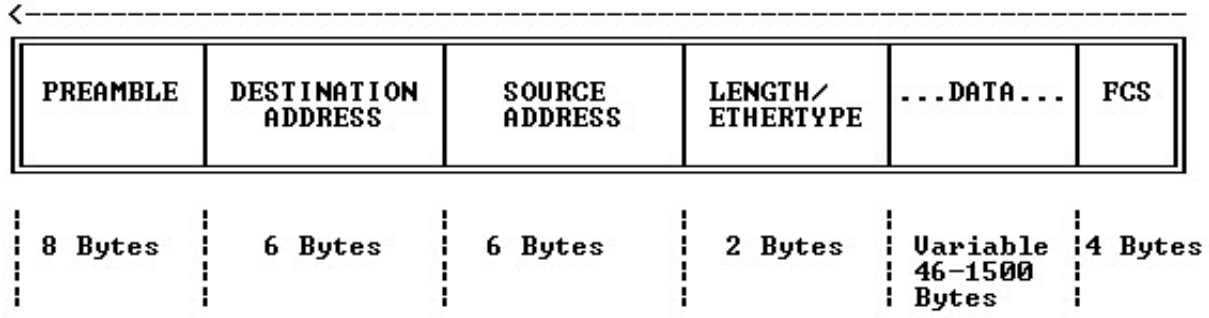
目标

本次课程的目标是来查看一下网络数据包和帧的真正内容，这将会帮助你理解为了网络传输网络层给有效载荷数据增加头部信息字段。

简介

在分组交换网，网络中的每一层需要传送信息给它的对等层。这是由传输首部来实现的。之所以叫做首部，是因为当有效数据载荷从应用程序向下依次到物理层的过程中，每一层都会附加头信息到有效数据载荷。
当然，在这之前，应用程序数据流（假设是数据流）会被分割成单元，这些单元要足够小，能够刚好放入一个用于在网络中传输的数据包中。
当接收到一个数据包，网络中连续的层开始依次处理和它们相关的头信息。每一层在移除当前首部后，要判断出是哪种上层协议将数据传给自己。

比如，这里有一个以太网帧的格式。



注意，这个帧在有效载荷后面还有一个校验字段。当这个帧被接收后，以太网链路层使用帧类型来计算出要将有效载荷传递给谁。如果帧类型是0800（十六进制），那么可以知道要将载荷发送到IP层。
这里给出了几种简单的以太网帧类型：

0800	IPv4
6559	帧中继
8035	ARP
809B	Appletalk
80D5	IBM SNA
8137	Novell IPX
8138	Novell IPX

1.1 IP 首部

当IP接收到一个数据包，任何链路层的首部和尾部都将被移除。下图显示了包大约前二十个字节的格式，请从左向右、从上到下阅读这幅图。

IPv4数据报格式

一些重要的字段：

- 版本: IP的版本号。对于IPv4来说总是4。
- 首部长度: IP首部的长度，是4字节的整数倍。一个IP首部如果没有可选字段是20字节长，因此首部长度值为5。
- 数据包长度: 包括IP首部在内的数据报总长度。
- 生存时间（寿命）: 数据报可以通过的路由器的数量。发送端将其设置成一个非零正整数（比如32）。每经过一个路由器此字段的值减少1，如果减少至0，路由器抛弃这个数据报。这样可以有效的减少路由环路所带来的影响。
- 类型 : 标识上层协议。参见下方表格。
- 首部校验和 : 确保首部信息是可用的。
- 源IP地址 : 发送数据报端的IP地址。
- 目的IP地址 : 接收数据报端的IP地址。

这里有一些简单的类型字段的值（十进制表示）：

1	ICMP
6	TCP
17	UDP

1.2 UDP 首部

在因特网中最重要的传输协议之一就是用户数据报协议，即UDP。IP将数据报发送给机器，UDP将数据报分解并将有效数据载荷传送给65535d个端口中的一个。
一个在主机上运行的UDP应用服务程序会监听UDP端口。比如因特网域名服务器总会监听发送到53端口的来自DNS客户端的请求。

八字节的UDP首部（如上图所示）包含以下字段：

- 源端口号: 在源机器上源应用程序使用的UDP端口号，在需要对方回信时使用。
- 目的端口号: 目的应用程序的UDP端口号。这在终点交付报文给正确的应用程序时使用。
- 长度: 数据报（包括UDP首部）的总长度
- 校验和 ： 用于确保首部和数据的正确性。

作为传输层协议，UDP并不去检测丢失的数据报，也不会去重发丢失的数据报。它不提供可靠的数据传输。

1.3 TCP 首部

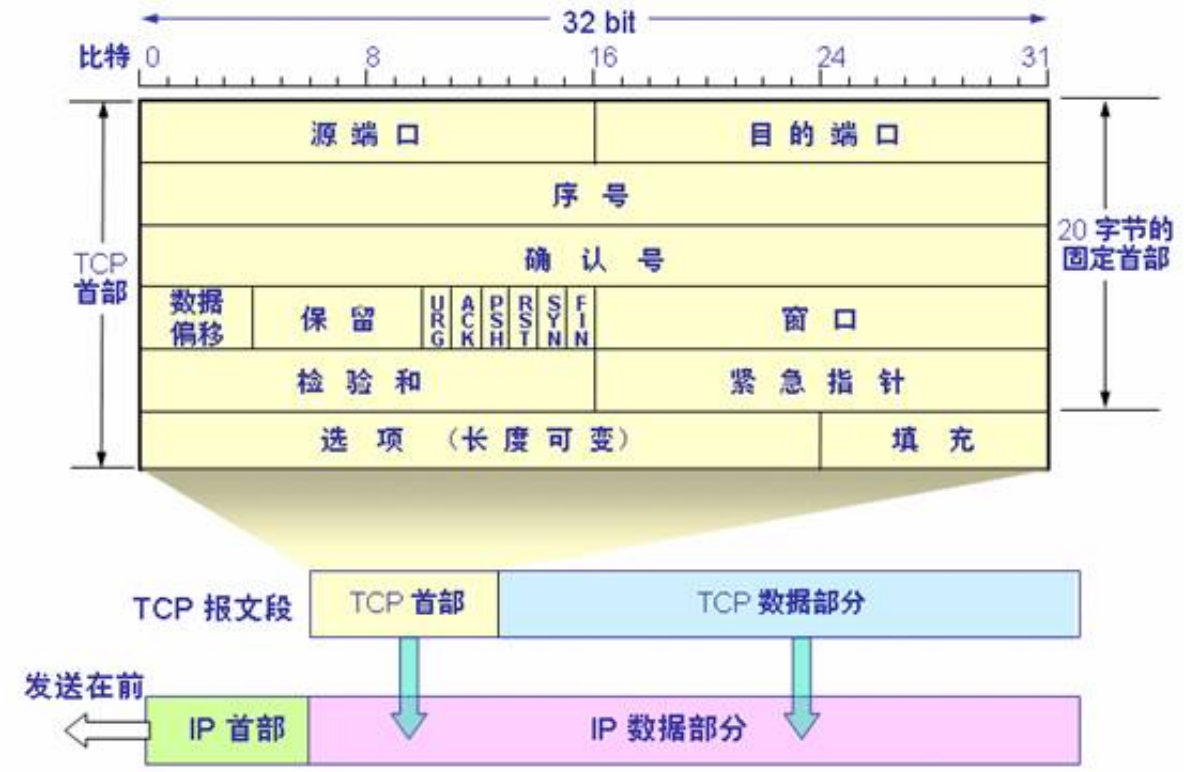
另一个更加重要的传输层协议是传输控制协议，其特点是：

- 检测丢失的或者坏掉的数据报
- 重传丢失或者坏掉的数据报
- 对无序的报文段进行排序
- 将数据段重装配成一个数据流

TCP 也提供了 65,536 个端口，但是这些端口和UDP端口是不同的。一些常用的端口号及其服务如下：

7	echo
13	daytime
21	FTP
23	Telnet
25	SMTP (email delivery)
70	gopher
80	HTTP
110	POP version 3

显然，TCP的首部要比UDP复杂一些。下面是20个字节的首部信息：



其中重要的字段有：

- 源端口：在源机器上源应用程序使用的TCP端口号，用于接收返回的数据信息。
- 目的端口：目的应用程序的TCP端口。
- 序号：用于流的重组和数据的重传 。
- 确认号：用于流重组和数据的重传。
- 校验和 ：用于确保头和数据的正确性。
- 比特代码：每一位代表一个布尔标志：
  - 0x20 URG：数据载荷是“紧急的”
  - 0x10 ACK：数据报确认
  - 0x08 PSH：推送数据
  - 0x04 RST：结束TCP连接
  - 0x02 SYN：创建一个TCP连接
  - 0x01 FIN：发送端发送数据完毕

  URG 和 PSH 标致位在本次实验中并不涉及，所以你可以暂时忽略他们。

1.4 TCP 的握手连接

TCP使用三次握手来建立连接：

1. 发送端发送一个SYN报文
2. 接收端向发送端发送回一个SYN报文作为回应
3. 发送端收到接收端传回的SYN报文，在回应一个ACK报文

连接建立之后，双方都可以向对方传输数据了。所有的数据报都会有一个返回的TCP ACK数据报来进行确认。
当所有的数据传输完毕，通过返回一个FIN报文来终端连接。

1.5 作业

手动对下面两个数据报进行译码，并根据上面所讲的报文的格式，确定各字段的值以及上面所描述中所对应的含义。这两个报文都有：

- 一个以太网的帧首部
- 一个IP首部
- 一个传输层首部（TCP或者UDP）
- 和一些用户数据

注意：已经将以太网的前导码和校验和尾部去掉了，并在每个数据包的不同部分之间用空行隔开了。

```
    Packet 1:                          Packet 2:

0800871c4218 00c04f88d4bc 0800         0800871c4218 00608cbee9d7 0800

4500 002c                              4500 0043
c013 4000                              f18b 4000
4006 468c                              ff11 5836
83ec 159e                              83ec 1509
83ec 16b6                              83ec 1606

0c8b 0015                              d1b1 0035
54ac 02ae                              002f e5e7
0000 0000
5002 4000                              a51d 0100
bfff 0000                              0001 0000
                                       0000 0000
0204 05b4                              076c 7073
                                       7461 6666
                                       0263 7304
                                       6164 6661
                                       026f 7a02
                                       6175 0000
                                       0100 01
```

将以太网地址用十六进制表示，但是将每对十六进制数字用冒号隔开。将IP地址转换成点分十进制表示法。将端口号转换为服务名称。尽可能多的标识出字段和它们的值。不需要对下列内容进行转化：IP服务类型，IP标记。你可以将校验和字段写成十六进制。

2：路由和子网实验

在本周的课程中我们学习了分组处理设备是怎样进行路由决定的，现在我们对这些概念做一些实验。

点击并运行所给材料中的PacketTracer方案：routing.pkt 。选择“simulation”标签和“simple routing”.

2.1 作业

运行所给方案，并回答下列问题：

1. 为什么第一个数据包没有通过任何的路由器？谁负责这个数据包的路由选择？
2. 在时刻6，点击位于路由器上的数据包2，试着回答此刻路由器发生了哪些操作。在路由器做出最终路由决定之前它是怎样在TCP/IP栈中一步步向上将帧打开的？在时刻7，交换机是怎样一步步向上解封数据帧的？
3. 切换到 ″louder, please!″，观察数据包从Moe到Karin的传输。检查数据包的细节信

息。为什么数据包丢失了？

点击并运行 subnetting.pkt 方案，进入“simulation”模式。左边的所有计算机是一个大型组织的一部分，拥有IP地址 200.17.0.0/16。因为一些原因，这个组织将网路划分成更小的子网：PC0到PC2这三台计算机使用的网络是 200.17.24.0/24, PC3 和 PC4 使用的地址是 200.17.38.0/24，这两个子网通过路由器A相连。路由器处于这个组织的边界处。

每一个在组织外部的人仅知道组织拥有地址和进入这个网路的入口点（A路由器）。为了回答这个问题，请继续。

2.2 作业

首先，查看路由器A、B和C的路由表，并回顾子网的相关概念和计算技巧。然后你需要运行模拟器来回答下列问题：

1. 在时刻9，PC6的子网掩码是多少？将子网掩码和目的地址相与（AND操作）的结果是多少？
2. 在时刻10，哪一层的数据报头部需要修改，怎样修改？

3：其它作业

3.1 单选或多选题

1．以下IP地址中属于B类地址的有（ ） 。
A）128.36.145.5
B）20.23.234.12
C）192.12.69.234
D）200.45.34.123

2．与下列掩码对应的网络前缀各多少位？（ ） 。
A）192.0.0.0
B）240.0.0.0
C）255.224.0.0
D）255.255.255.252

3．以下前缀中哪一个和地址152.7.77.159及152.31.47.252都匹配？（ ） 。
A）152.40/13
B）153.40/9
C）152.64/12
D）152.0/11

4．以下关于OSPF协议的描述中，最准确的是（ ） 。
A）OSPF协议根据链路状态法计算最佳路由
B）OSPF协议是用于自治系统之间的外部网关协议
C）OSPF协议不能根据网络通信情况动态地改变路由
D）OSPF协议只能适用于小型网络

5．OSPF和RIP都是Intemet中的路由协议，与RIP相比，OSPF有许多优点，以下选项中（)不是OSPF的优点。
A）有跳数的限制

B）更快的收敛性
C）支持层次化路由

D）更低的路由开销

6．以下关于OSPF的描述中不正确的是（ ）。
A）与RIP相比较，OSPF协议更安全
B）OSPF在进行路由表构造时，使用的是Dijkstra算法
C）OSPF具有路由选择速度快、收敛性好，支持精确度量等特点
D）OSPF是应用于自治系统之间的“外部网关协议”

7．下面对RIP的描述中，错误的是（ ）。
A）RIP限制最大跳数是15，即，在一条链路上最多有15个路由器
B）RIP使用广泛、配置简单，支持CIDR、VLSM及连续子网
C）RIP的路由更新时间为30秒，路由收敛速度慢
D）RIP通常使用单播方式发送路由更新信息

8．下面（ ）协议属于IGP协议
A）BGP

B）TCP
C）RIP

D）OSPF

9．RIP协议基于（ ）发送RIP消息，OSPF协议基于（ ）发送OSPF数据包，BGP协议基于（ ）发送BGP数据包。
A）IP

B）TCP
C）UDP

D）ARP

10．OSPF支持按区域划分的层次化路由，在骨干区域area0内部执行的路由协议是（ ）
A) BGP

B) OSPF
C) EGP

D) IGP

11．关于BGP协议，下列哪些叙述是错误的（ ）。
A）和RIP协议一样，BGP也存在产生路由环路的可能性；

B）BGP是路径向量类的路由协议
C）BGP主要用来在AS之间传递路由信息；

D）BGP路由考虑政治、安全等有关的策略

3.2 回答问题

1. P183习题：4-09

2. P184习题：4-17

3. P184习题：4-20

4. P184习题：4-21

5. P186习题：4-37

6. 对比RIP协议和OSPF协议的特点并说明两种协议的适用场合？