计网

单选 10*1

填空 10*1

名词解释5*2

简答5*4

计算应用问答题5*10

大题（两套）：

1.IP层数据分片

IP为什么要分片，包括分片以后在首部的哪一个位置，

分完片后每一片的偏移是多少，标志是多少，首先决定分几片，每一片的长度是多少

举例：（难度：长度要会算）在上层协议TCP报文，在不考虑扩展功能的情况下，带用户数据100字节，IP和TCP都不考虑可选字段，问要不要分片？到10000要不要分片，怎么分片？

+首部20，IP首部20，100加起来140不需要分片，10040分片，10040÷1440再向上取整即分片数量。

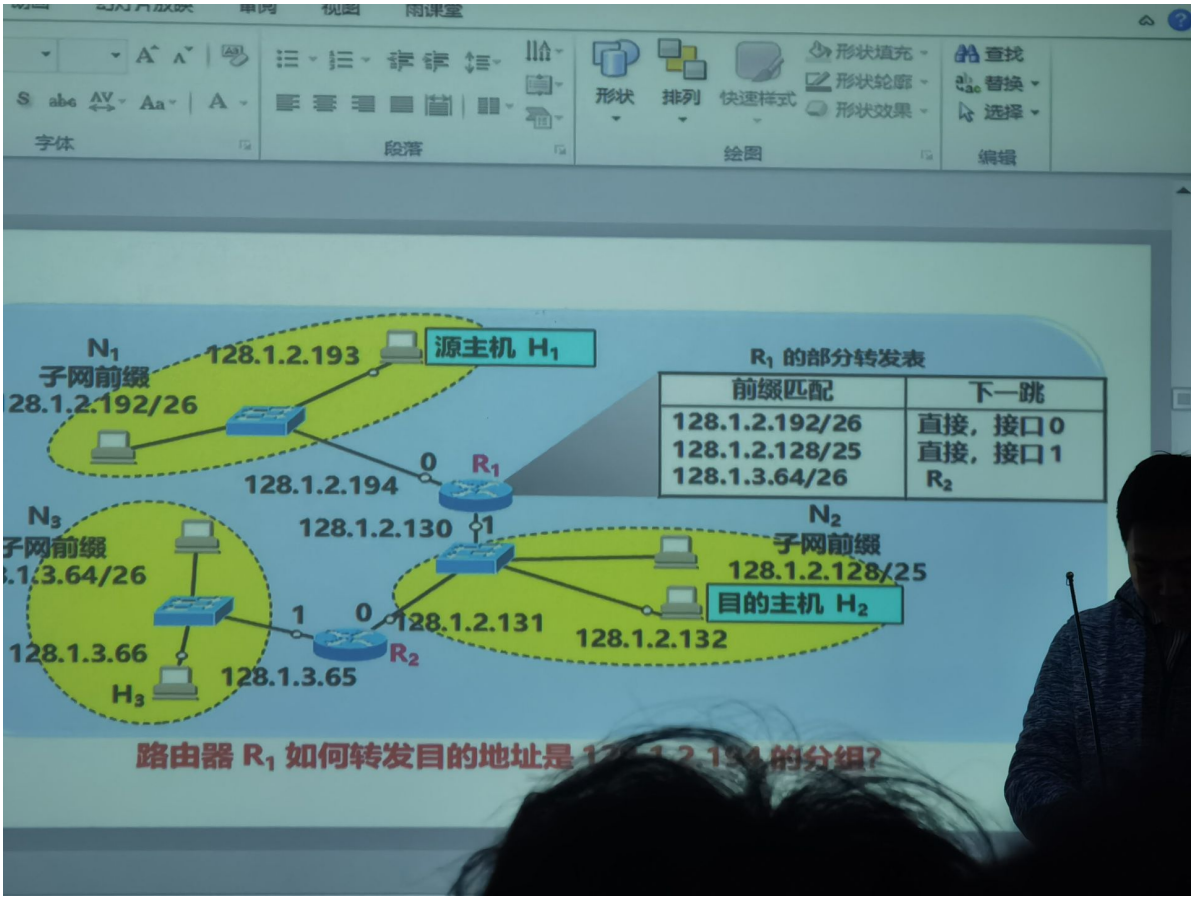
问每一片各自带多少长TCP数据，第一片多少，第二片多少

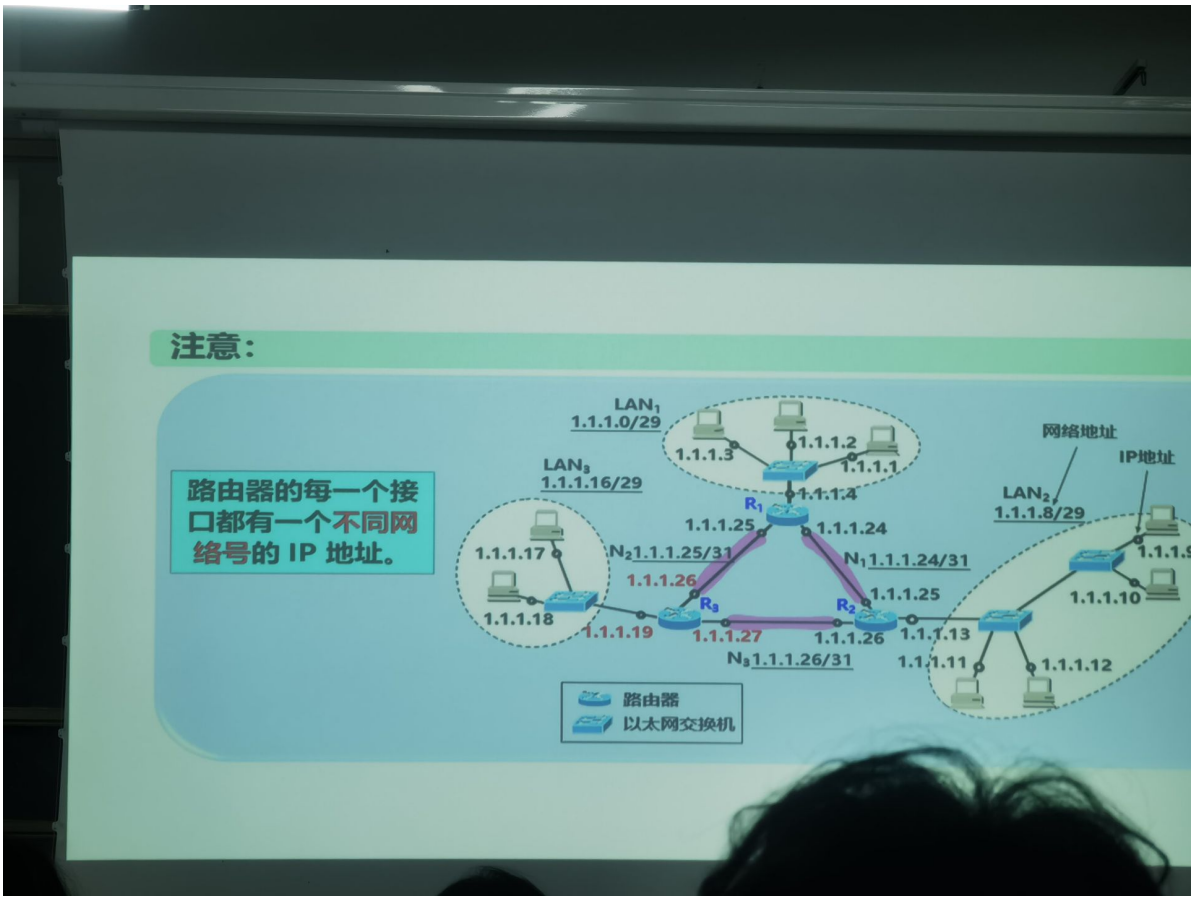
倒过来算：以太网数据链路层，MTU是1440，数据链路层分完片后的帧最多，MTU1440-20IP首部-20TCP首部，每一个最多带1400个字节的TCP数据，TCP总的用户数据是10000，10000÷1400再向上取整（分片数）

UDP用户数据带了多少个字节：UDP的首部长度是8字节

（网络层）

2.路由器图/写路由表





给一段地址1.1.1.0/25（25是优化后缀长度），根据要求

一个局域网有500台主机，60台，200台，每一个局域网里的主机数量不同，规划每一个局域网的后缀长度是多少，相应的路由器每个接口IP、局域网网络地址和后缀

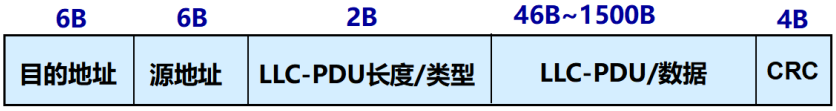
（网络层）

3.给一个原始的数据帧，分析长度和含义

从哪里开始是MAC帧，哪里是IP等，各自长度是多少，同时每一个字段的长度含义是什么

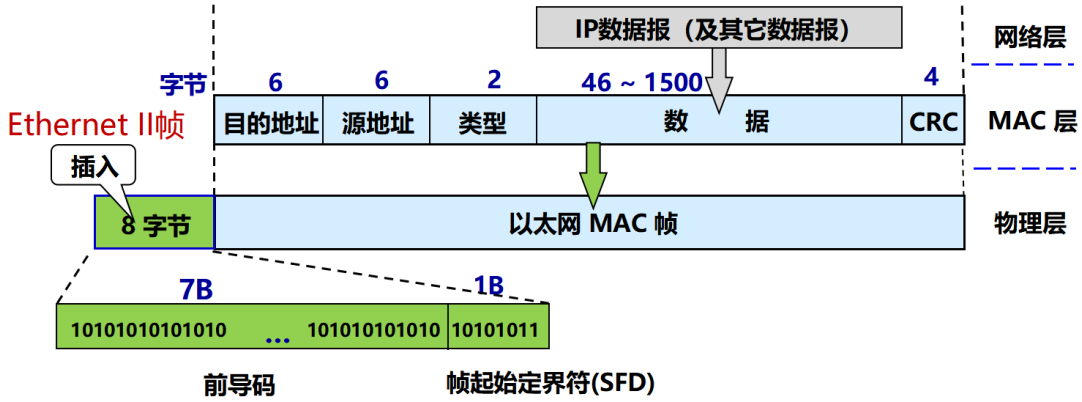
（数据链路层）

■以太网 MAC 帧格式有两种标准，通过帧中的长度/类型字段值来区分：



- 长度/类型>1536，Ethernet II 标准 (也称 DIX V2 标准)
- 长度/类型≤ 1500，IEEE 的 802.3 标准

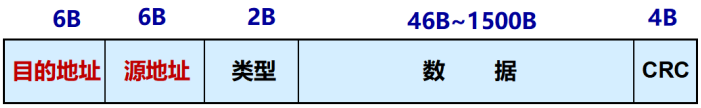
Ethernet II 帧



■在帧的前面插入（硬件生成）的 8 字节，包含两个字段

- 第一个字段是 7 个字节的前导码，用来迅速实现 MAC 帧的比特同步
- 第二个字段 是1 个字节的帧起始定界符，表示后面的信息就是 MAC 帧

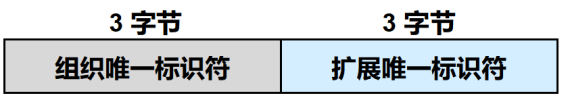
Ethernet II帧 - MAC地址字段（1）



■目的地址和源地址字段用于标识发送方地址和接收方地址，这个地址是硬件地址，又称为物理地址，或 MAC 地址

■IEEE 802 标准规定的 MAC 地址长48 比特（6字节）

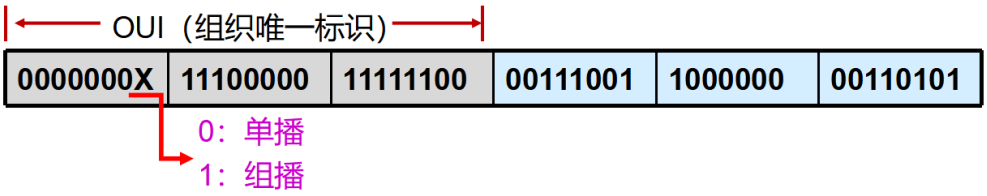
- 组织唯一标识符：前三个字节 (即高位 24 位)，由IEEE 的注册管理机构 RA 负责向厂家分配
- 扩展唯一标识符：后三个字节 (即低位 24 位)， 由厂家自行指派，必须保证无重复地址



Ethernet II帧 - MAC地址字段（2）

■ MAC地址分三种：单播地址、组播地址和广播地址

➢ IEEE 规定地址字段的第一字节的最低位用于标识单播还是组播地址



✓ 最高字节的最低位 = 0 时，是单播地址，只有一个站点拥有该地址

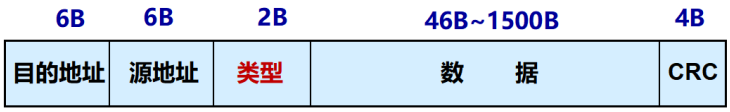
✓ 最高字节的最低位 = 1 时，是组播地址，有一组站点拥有该地址

➢ 48 位都为 1 时，为广播地址

11111111	11111111	11111111	11111111	11111111	11111111

➢ 组播地址和广播地址只能作为目的地址使用

Ethernet II帧 - 类型字段



■ 类型字段区分上层协议，以便接收方把帧里封装的数据交给正确的上层协议

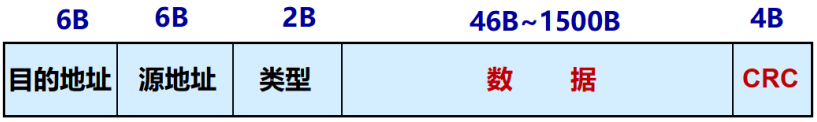
➢ 类型字段值 0x0800，表示这个帧内封装的是 IPv4 分组

➢ 类型字段值 0x0806，表示这个帧内封装的是ARP分组

➢ 类型字段值 0x8100，表示这个帧内封装的是IEEE 802.1Q帧

➢ 类型字段值 0x86DD，表示这个帧内封装的是IPv6分组

Ethernet II帧 - 数据字段、帧校验字段



■ 数据字段里封装的是上层协议的PDU

➢ 数据字段的最小长度46字节(最小帧长64B，首部和尾部共18B)

➢ 当数据字段的长度小于 46 字节时要进行填充，以满足以太网的最小帧长要求

■ 帧校验字段包含了差错检测信息，在这种情况下是CRC-32

一个原始的数据帧通常包括物理层和数据链路层的信息。以下是一个典型的以太网数据帧的结构：

1.前导码（Preamble）： 7个字节。前导码是一组特殊的比特模式，用于帮助接收设备同步时钟。在物理层中，前导码协助接收方在信号中找到比特的边缘。
2.帧起始定界符（Start Frame Delimiter）： 1个字节。帧起始定界符标志着数据帧的开始，它是前导码的最后一个字节。
3.目的MAC地址（Destination MAC Address）： 6个字节。指定数据帧的目标设备的物理地址。
4.源MAC地址（Source MAC Address）： 6个字节。指定发送数据帧的设备的物理地址。
5.类型/长度字段（Type/Length）： 2个字节。在以太网中，这个字段既可以表示上层协议的类型，也可以表示数据帧的长度。
6.数据（Data）： 最小46个字节，最大1500个字节。这是数据帧的实际载荷，包含上层协议的数据。
7.帧校验序列（FCS，Frame Check Sequence）： 4个字节。用于检测数据传输过程中是否发生错误的冗余校验字段。

如果上层协议是IPv4，那么数据部分的结构如下：

8.版本和首部长度（Version and Header Length）： 1个字节。指定IPv4协议的版本和首部的长度。
9.区分服务（Differentiated Services）： 1个字节。用于指定数据包的服务类别，包括优先级和流量分类。
10.总长度（Total Length）： 2个字节。指定整个IPv4数据包的长度，包括首部和数据。
11.标识、标志和片偏移（Identification, Flags, and Fragment Offset）： 2个字节。用于分片和重新组装数据包。
12.生存时间（Time to Live）： 1个字节。指定数据包在网络中的最大生存时间，每经过一个路由器减1。
13.协议（Protocol）： 1个字节。指定数据包上层协议的类型，例如TCP或UDP。
14.首部校验和（Header Checksum）： 2个字节。用于检测IPv4首部的错误。
15.源IP地址（Source IP Address）： 4个字节。指定数据包发送方的IP地址。
16.目标IP地址（Destination IP Address）： 4个字节。指定数据包接收方的IP地址。

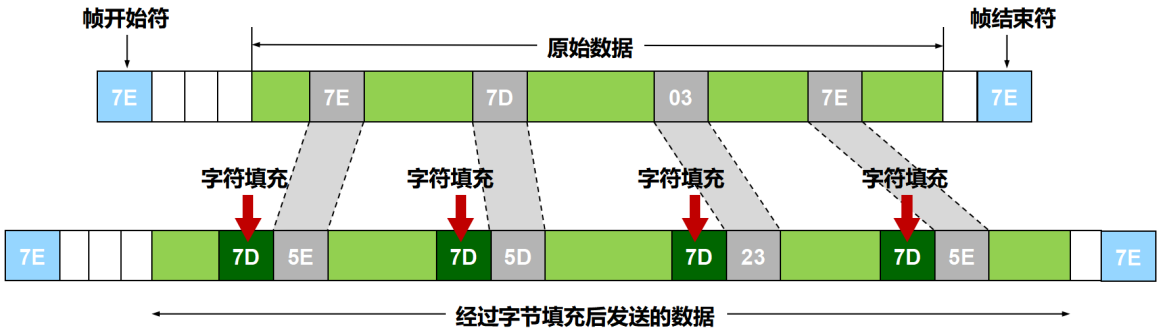
以上是以太网和IPv4数据帧的一般结构，实际协议、字段长度和含义可能会根据网络的具体配置和使用的协议而有所不同。在分析数据帧时，需要查看帧类型字段，确定上层协议，然后进一步解析相应协议的头部和数据。

4.字节填充法、比特填充法

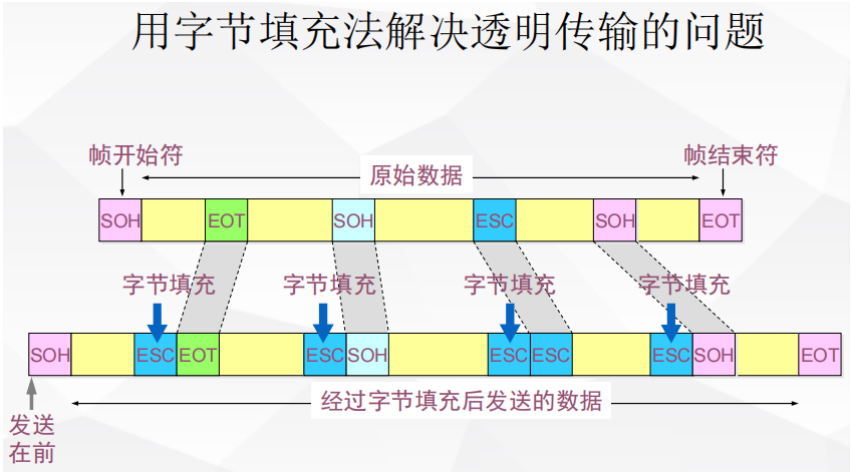
怎么去做填充，给一个原始用户数据，用两个方法发出去的和收到的数据，进行填充和恢复，填充之前的帧定界符是什么，两个方法各自是什么（其实一样）

（数据链路层）

字符填充法



- 对原始数据中出现的三种特殊字符，在前面用0x7D转义字符填充，并对特殊字符进行转义：
  - 对 0x7E（分界符），转换成 (0x7D, 0x5E)
  - 对 0x7D（转义字符），则转换成 (0x7D, 0x5D)
  - 对 ASCII 码的控制字符（小于 0x20 的字符），填充 0x7D，并将该字符的编码进行转义

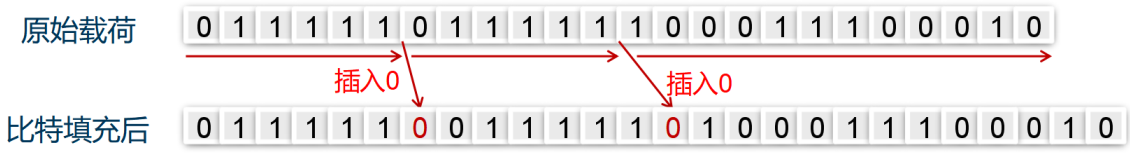


零比特填充法

- PPP 协议用在 SONET/SDH 链路时，使用同步传输（一连串的比特连续传送）。这时 PPP 协议采用零比特填充方法来实现透明传输。
- 在发送端，只要发现有 5 个连续 1，则立即填入一个 0。
- 接收端对帧中的比特流进行扫描。每当发现 5 个连续1时，就把这 5 个连续 1 后的一个 0 删除。

带比特填充的标志比特法

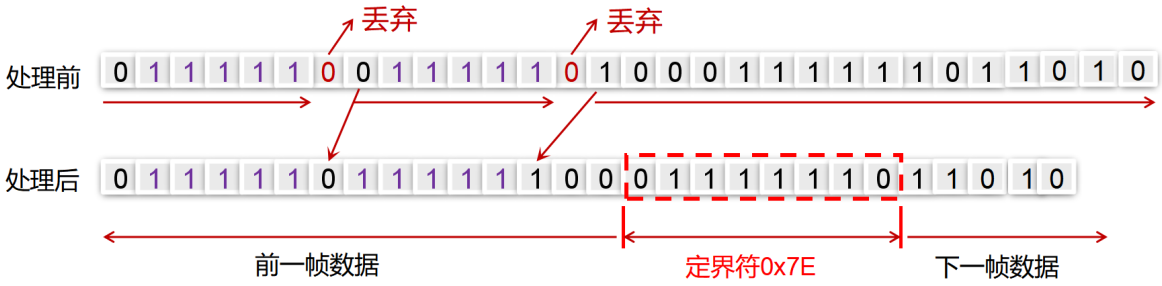
- 发送端的处理：比特填充
  - 发送方检查有效载荷，若出现了连续5个1比特后，则直接插入1个0比特，防止和定界符的比特模式 01111110 相同
  - 比特填充法是比特位操作，用0比特进行位插入和删除，硬件实现起来比较方便



带比特填充的标志比特法

■接收端的处理

- ➢检查接收到的比特流，若出现连续5个1后，则检查下一比特
- ➢若为0：则后面为有效载荷，该0比特是发送方填充进去的，直接丢弃
- ➢若为1：
  - ✓如果接下来的一比特是0，则构成定界符，一帧结束
  - ✓如果接下来一比特是1，则需要作出错或其他处理



在通信中，字节填充法和比特填充法是两种用于处理特定字符序列的方法，以确保数据的可靠传输。这两种方法的目的是在数据中插入特殊的字符，以避免与控制字符或帧定界符冲突，同时保持数据的完整性。
字节填充法：
发送端操作：

1.确定一个特殊的字节，通常称为填充字节。
2.在原始用户数据中，每当出现与填充字节相同的字符时，插入填充字节。
3.在数据的开头和结尾分别加上帧定界符。

接收端操作：

4.在接收到数据后，检测帧定界符，标志帧的开始和结束。
5.识别填充字节，将填充字节后面的字节当做原始数据处理。
6.去除开头和结尾的帧定界符。

比特填充法：
发送端操作：

7.确定一个特殊的比特序列，通常称为填充比特。
8.在原始用户数据中，每当连续的一定数量的相同比特序列出现时，插入填充比特。
9.在数据的开头和结尾分别加上帧定界符。

接收端操作：

10.在接收到数据后，检测帧定界符，标志帧的开始和结束。
11.识别填充比特，将填充比特后面的比特当做原始数据处理。
12.去除开头和结尾的帧定界符。

例子：
假设填充字节为0xAA，帧定界符为0x7E，原始用户数据为0x7E 0xAA 0x7E。
字节填充法：

13.发送前：0x7E 0xAA 0xAA 0x7E
14.接收后：去除填充字节，还原为原始数据：0x7E 0xAA 0x7E

比特填充法：

15.发送前：0x7E 0xAA 0x7D 0x5E 0x7E
16.接收后：去除填充比特，还原为原始数据：0x7E 0xAA 0x7E

在这两种方法中，填充字节或填充比特的选择是根据通信协议和特定需求而定的，关键是确保填充字符不与原始数据中的任何字符或比特序列冲突。

5.数据在某一类型路段传输时间

例如：长2km的一根导线，数据是100MB，电磁波在导线上的传播速率是200m/s，有一个1000字节的帧，从发送开始到接收结束需要持续多长时间（导线一端到另一端）。信号传播时间是信号在导线上传播的时间。

最常见的错误：1000➗100=网卡发完时间，导线上还没传完，类似火车过铁路桥。

如果相距最远的同时发送数据，要到什么时候才能检测出冲突，（冲突检测，两端同传）

常见错误：发生冲突和发现冲突

（物理层和数据链路层）

6.利用窗口进行流量控制

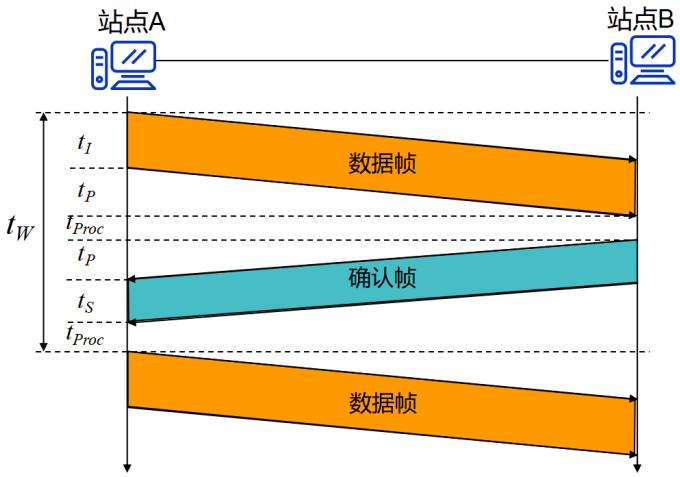
（数据链路层）

7.信道数据传输速率、传播时延？若利用率50%采用TCP停等协议时数据帧是多少

（物理层和数据链路层）

停等式协议性能评估：完成一帧发送所需的最短时间

- $t_W = t_I + 2t_P + 2t_{Proc} + t_S$
- t_I：发送端发送数据帧比特流时间（帧长/数据传输速率）
- t_S：接收端发送确认帧比特流时间（确认帧长/数据传输速率）
- t_P：信号传播延时（线路距离/信号传输速率）
- t_{Proc}：节点处理时间



停等式协议性能评估（无差错）

- 信道利用率：信道被占用的时间和总时间之比
- 有效数据传输率：单位时间内传输的有效数据位数
- 无差错情形时发送信道的利用率P

$$P=t_I/t_W$$

t_I：发送端发送数据比特流的时间

t_W：发送一帧的总时间

- 无差错情形时的有效数据传输率

$$S=N/t_W$$

N：一帧的有效数据比特数

停等式协议性能评估（有差错）

- 有差错时正确传送一帧的平均时间
  - 无差错情况下，发送一帧的最小时间间隔为t_W
  - 当出错率为 p 时，正确发送一帧的平均时间间隔t_V为（根据概率统计学）

$$t_V=t_W/(1-p)$$

- 系统最大吞吐量λ_{max} **(每秒成功发送的帧数)**

$$\lambda_{max}=1/t_V=(1-p)/t_W$$

- 极限吞吐量

$$M=1/t_I$$

- 系统传输效率：最大吞吐量/极限吞吐量

$$\eta=\lambda_{max}/M=(1-p)/(t_W/t_I)$$

信道利用率和有效数据传输效率计算实例

■ 假设条件

C = 数据流发送速率（10Mbps或10bit/ μs ）

S = 数据流在线路上传输速度（200m/ μs ）

D = 发送方与接收方的距离（200m）

t_{Proc} = 生成一帧的时间（1 μs ）

L_f = 一帧数据的比特数（200bit）

N = 一帧数据的有效数据比特数（160bit）

L_S = 一帧确认帧的比特数（40bit）

■ 计算结果

$t_W = t_I + 2t_P + 2t_{Proc} + t_S$

$t_I = L_f/C = 200/10 = 20(\mu s)$

$t_P = D/S = 200/200 = 1(\mu s)$

$t_{Proc} = 1(\mu s)$

$t_S = L_S/C = 40/10 = 4(\mu s)$

$t_W = 20 + 2\times1 + 2\times1 + 4 = 28(\mu s)$

发送信道利用率：

$P = t_I/t_W = 20/28 = 71.4\%$

有效数据传送速率：

$S = N/t_W$

$= 160/28 = 5.7Mbps$

8.画出网络拓补结构

（物理层和数据链路层）

星状拓扑 环状拓扑 总线型拓扑 网状拓扑 树状拓扑 混合型拓扑

简答

1.Internet和internet的区别

1.Internet (大写 "I"): "Internet" 是一个专有名词，它指的是全球范围内相互连接的计算机网络，即全球互联网。这是一个特定的网络，由许多子网络组成，通过标准化的通信协议进行连接，使得全球范围内的计算机能够相互通信和共享信息。互联网是一个大规模的、开放的、分布式的网络。
2.internet (小写 "i"): "internet" 是一个通用名词，指的是任何连接在一起的网络。这个词没有特定的技术含义，可以用来描述任何规模和范围的网络，包括组织内部的网络、局域网（LAN）、城域网（MAN）等。它只表示网络间的连接，而不涉及具体的技术规范或协议。

总体而言，"Internet" 是一个特定的网络，是全球范围内的互联网；而 "internet" 是一个通用的术语，可以用来描述任何连接在一起的网络，不限于全球性的互联网。

2.TCP/IP 拥塞和流量控制有什么区别和共同点

对比目的、方法、手段、结果

相同点：窗口控制

拥塞控制所要做的都有一个前提，就是网络能够承受现有的网络负荷。

拥塞控制是一个全局性的过程，涉及到所有的主机、所有的路由器，以及与降低网络传输性能有关的所有因素。

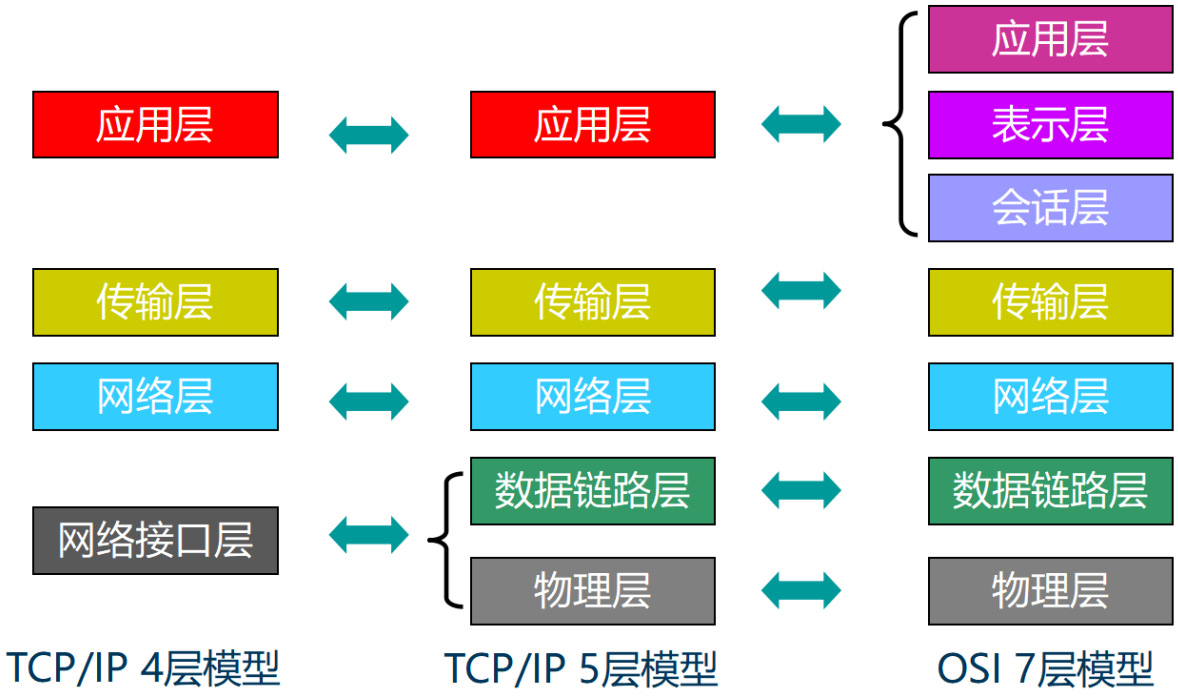
流量控制往往指在给定的发送端和接收端之间的点对点通信量的控制。

流量控制所要做的就是抑制发送端发送数据的速率，以便使接收端来得及接收。

3.TCP/IP和OSI模型分层

每一层的名字和作用，关系、功能

TCP/IP模型（4层）和OSI模型（7层/5层）



计算机网络通常采用五层体系结构，每一层都有不同的功能、数据传输单元、服务质量和协议。这五层通常被称为OSI（开放系统互连）模型：

1. *物理层：*

功能：负责传输比特流，将数据转换为电信号并在物理媒体上传输。
数据传输单元：比特（0和1）。
服务质量：不关心数据是否被正确接收。
常见协议：Ethernet、USB、RS-232。

2. *数据链路层：*

功能：负责数据帧的传输和错误检测、校正。
数据传输单元：数据帧。
服务质量：通常提供可靠的点对点数据传输。
常见协议：Ethernet、PPP、HDLC。

3. *网络层：*

功能：路由数据包，跟踪网络拓扑，进行寻址和转发。
数据传输单元：数据包。
服务质量：提供面向连接或无连接的服务，通常是不可靠的。
常见协议：IP（IPv4和IPv6）、ICMP、OSPF。

4. *传输层：*

功能：提供端到端通信，进行错误检测和纠正。
数据传输单元：段或报文。
服务质量：可靠（TCP）或不可靠（UDP）的端到端数据传输。
常见协议：TCP、UDP。

5. *应用层：*

功能：提供应用程序接口，支持应用程序之间的通信。
数据传输单元：消息、报文或数据。
服务质量：取决于具体应用，可以是可靠或不可靠。
常见协议：HTTP、FTP、SMTP、DNS。

1. **TCP/IP(四层)的名称，功能和主要协议**
2. *网络接口层（Network Interface Layer）*：
    - 功能：该层位于底层，主要负责物理硬件和数据链路层之间的通信，包括硬件设备的驱动和物理链路的访问。
    - 主要协议：在此层通常使用的协议包括以太网（Ethernet）、Wi-Fi、PPP（Point-to-Point Protocol）等，它们负责将数据帧从一个设备传输到另一个设备。
3. *互联网层（Internet Layer）*：
    - 功能：允许主机将数据包注入网络，让这些数据包独立传输至目的地，并定义了数据包格式和协议
    - 主要协议：IPv4协议和IPv6协议
4. *传输层（Transport Layer）*：
    - 功能：允许源主机与目标主机上的对等实体，进行端到端的数据传输。
    - 主要协议：主要协议包括传输控制协议（TCP）和用户数据报协议（UDP）。TCP提供可靠的连接导向数据传输，而UDP提供无连接的数据传输。
5. *应用层（Application Layer）*：
    - 功能：应用层包含了各种网络应用，如Web浏览、电子邮件、文件传输等。它提供了用户接口，使用户能够访问网络服务。
    - 主要协议：传输层之上的所有高层协议，如超文本传输协议（HTTP）、文件传输协议（FTP）、简单邮件传输协议（SMTP）、邮件访问协议（POP3/IMAP）等。这些协议支持各种应用程序的通信和数据交换。

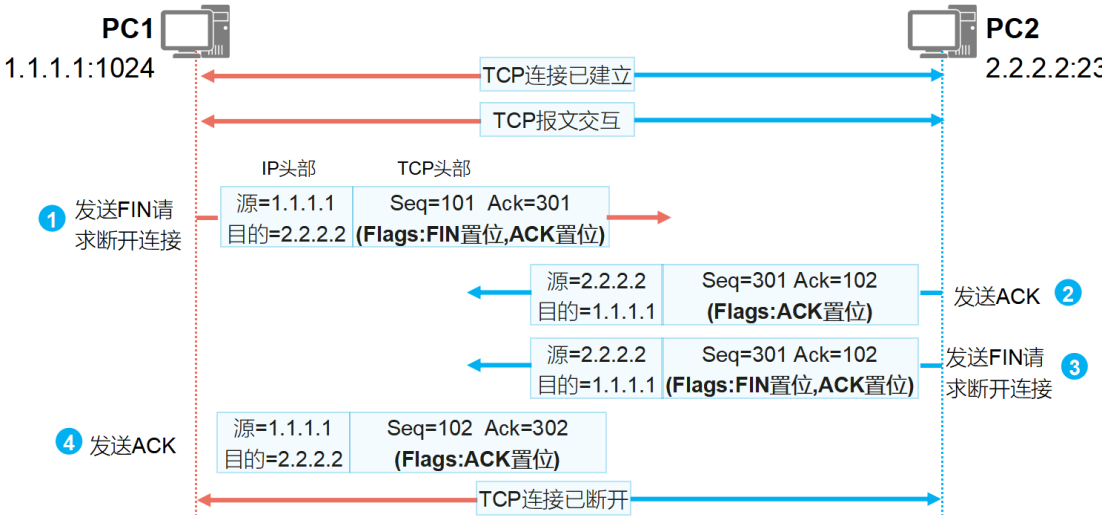
4.TCP建立和拆除连接需要3次/4次握手

过程画图，能不能3改4或4改3，描述哪一块合并或者拆分

（运输层）

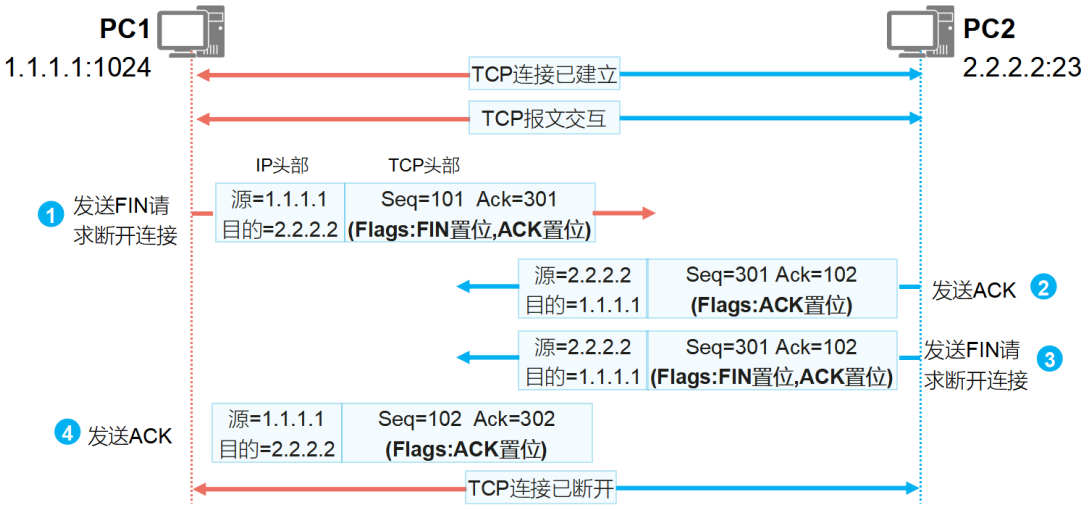
TCP的关闭 - 四次挥手

- 当数据传输完成，TCP需要通过"四次挥手"机制断开TCP连接，释放系统资源。



TCP的关闭 - 四次挥手

- 当数据传输完成，TCP需要通过“四次挥手”机制断开TCP连接，释放系统资源。

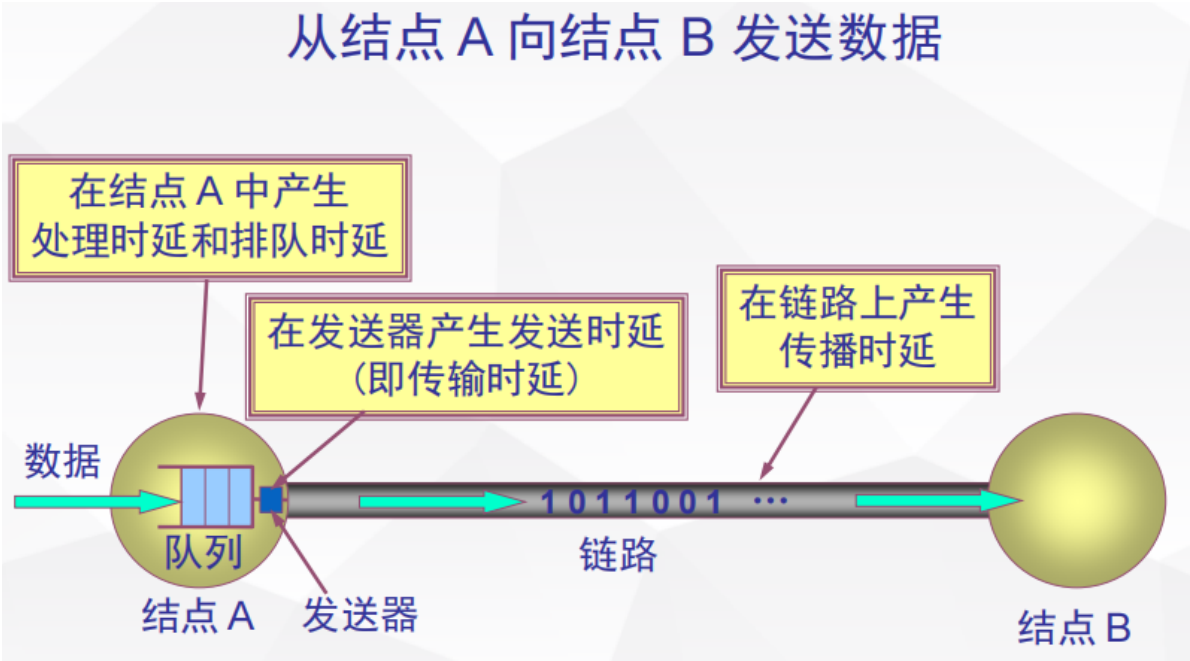


5.物理层、时延

数据发送的总时延的构成：4部分（排队、处理、传输、传播） 每一个时延在哪里产生

百兆无线局域网上网慢，升级至千兆网卡或者路由器会变快吗，哪一个有用

减少哪一部分的时延会对用户的体验有帮助



数据发送的总时延可以分为以下四部分，通常由排队时延、处理时延、传输时延和传播时延组成：

1.排队时延（Queueing Delay）： 在发送端等待将数据排入发送队列的时间

2.处理时延（Processing Delay）： 数据在结点（例如路由器、交换机）上进行处理所需的时间。

3.传输时延（Transmission Delay）： 数据从发送端传输到接收端所需的时间。

4.传播时延（Propagation Delay）：数据通过链路传输媒体传播所需的时间。

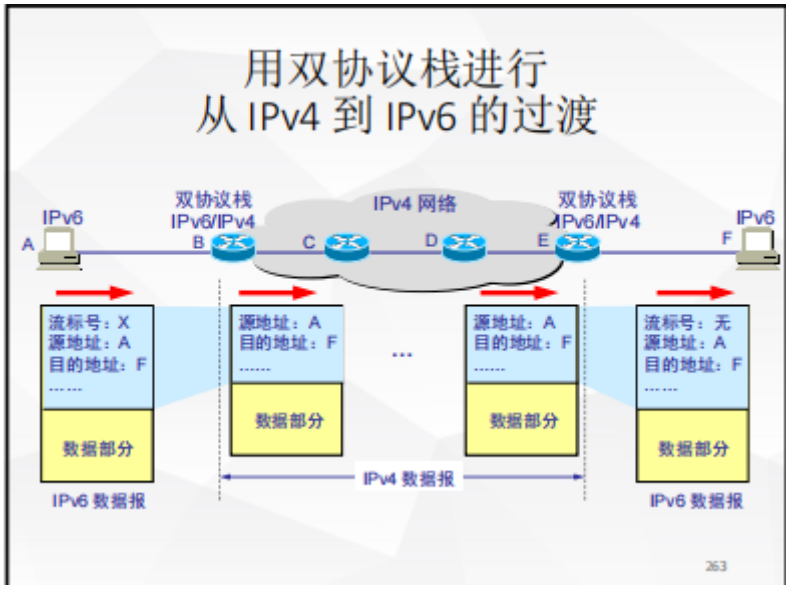
对于提升百兆无线局域网上网速度的问题：

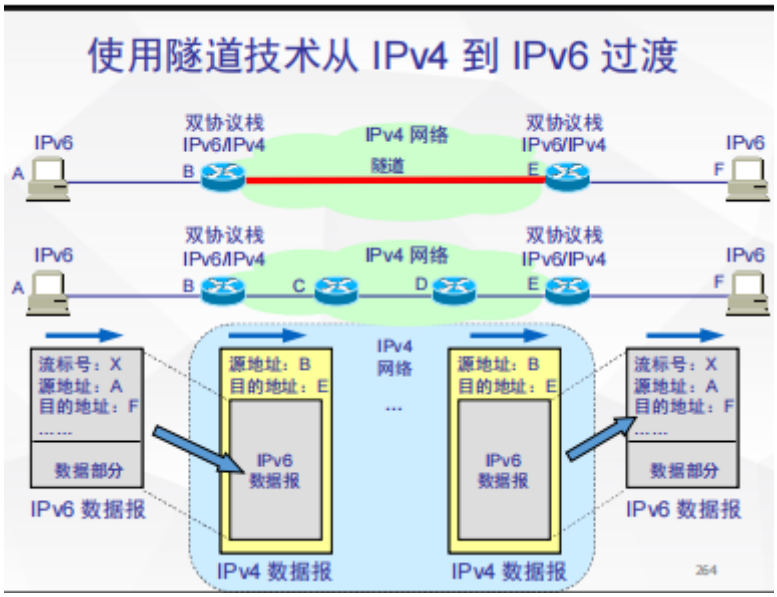
13.升级至千兆网卡或路由器是否有用：
14.如果瓶颈在局域网内部（例如，本地文件传输或内部网络通信），升级至千兆网卡或路由器可能提高数据传输速度。
15.如果瓶颈在互联网连接处，升级本地网络设备可能对上网速度影响较小，因为互联网速度受到服务提供商提供的带宽的限制。

减少哪一部分的时延会对用户体验有帮助：

16.排队时延和处理时延的减少： 优化网络设备和算法，以减少数据在网络节点上的排队和处理时延，可以提高实时性和响应性。
17.传输时延的减少： 提高网络带宽、使用更高速的传输媒体或采用压缩技术，可以减少数据在传输过程中的时延。
18.传播时延的减少： 缩短数据传输的物理距离或选择具有更高传播速度的传输媒体，可以降低传播时延。

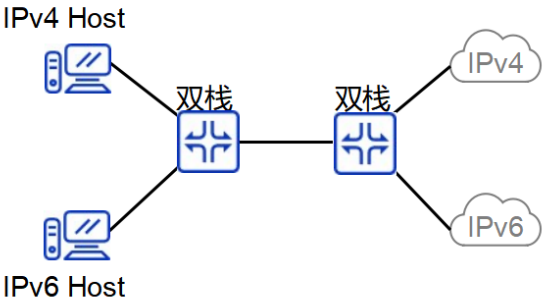
6.IPv4到6两策略 隧道/双栈技术对比





IPv4/IPv6双栈

- IPv4/IPv6在网络中并存、独立部署。对现有IPv4业务影响较小
- 演进方案简单、易理解。网络规划设计工作量相对更少。



隧道技术

- IPv6 over IPv4隧道：将IPv6流量封装在IPv4隧道中，在IPv4网络中实现IPv6孤岛互通。

- IPv4 over IPv6隧道：将IPv4流量封装在IPv6隧道中，在IPv6网络中实现IPv4孤岛互通。

7.为什么要用分层思想，有什么好处

各层之间是独立的。灵活性好。结构上可分割开。易于实现和维护。能促进标准化工作。

8.IP地址合法性，IPv6缩写规则

填空：域名、邮件名、IP地址合法性

- IPv6地址的长度为128 bit。一般用冒号分割为8段，每一段16 bit，每一段内用十六进制表示。

16 bit	16 bit	16 bit	16 bit	16 bit	16 bit	16 bit	16 bit
2001	0DB8	0000	0000	0008	0800	200C	417A

IPv6地址中的字母大小写不敏感，例如A等同于a。

- 与IPv4地址类似，IPv6也用“IPv6地址/掩码长度”的方式来表示IPv6地址。
  - 例如　2001:0DB8:2345:CD30:1230:4567:89AB:CDEF/64

IPv6地址： 2001:0DB8:2345:CD30:1230:4567:89AB:CDEF

网络前缀： 2001:0DB8:2345:CD30::/64

IPv6地址缩写规范

2001	0DB8	0000	0000	0008	0800	200C	417A

每组16 bit单元中的前导0可以省略，如果16 bit单元的所有比特都为0，那么至少要保留一个“0”；拖尾的0不能被省略。

2001	DB8	0	0	8	800	200C	417A

一个或多个连续的16 bit单元为0时，可用“::”表示，但整个IPv6地址缩写中只允许有一个“::”。

2001	DB8	::	8	800	200C	417A

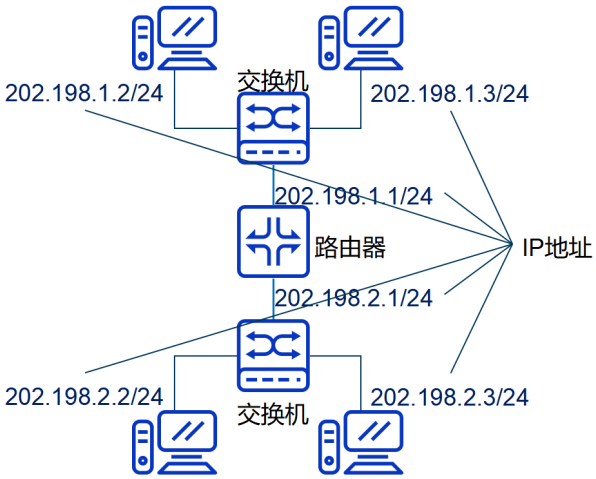
若缩写后的IPv6地址出现两个“::”，会导致无法还原为原始IPv6地址。

IPv6地址缩写示例

缩写前　0000:0000:0000:0000:0000:0000:0000:0001
缩写后　::1
缩写前　2001:0DB8:0000:0000:FB00:1400:5000:45FF
缩写后　2001:DB8::FB00:1400:5000:45FF
缩写前　2001:0DB8:0000:0000:0000:2A2A:0000:0001
缩写后　2001:DB8::2A2A:0:1
缩写前　2001:0DB8:0000:1234:FB00:0000:5000:45FF
缩写后　2001:DB8::1234:FB00:0:5000:45FF
或　2001:DB8:0:1234:FB00::5000:45FF

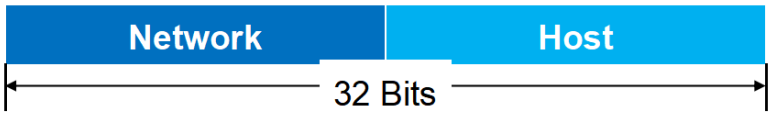
IP地址

- 网络中每个独立主机/路由器的每个接口必须有一个唯一的Internet 地址，也称为IP地址。
  - 通常路由器有多个接口，高端/核心路由器多至几十个接口
  - 主机通常有1个或2个接口（如以太网接口和WiFi）
- IP地址长度为32位（4个字节）。表示地址空间是232，或4,294,967,296（超过40亿个）。
- IP地址的表示方法：三种常用的表示方法
  - 二进制表示方法
  - 点分十进制表示方法
  - 十六进制表示方法。



IP地址的分类

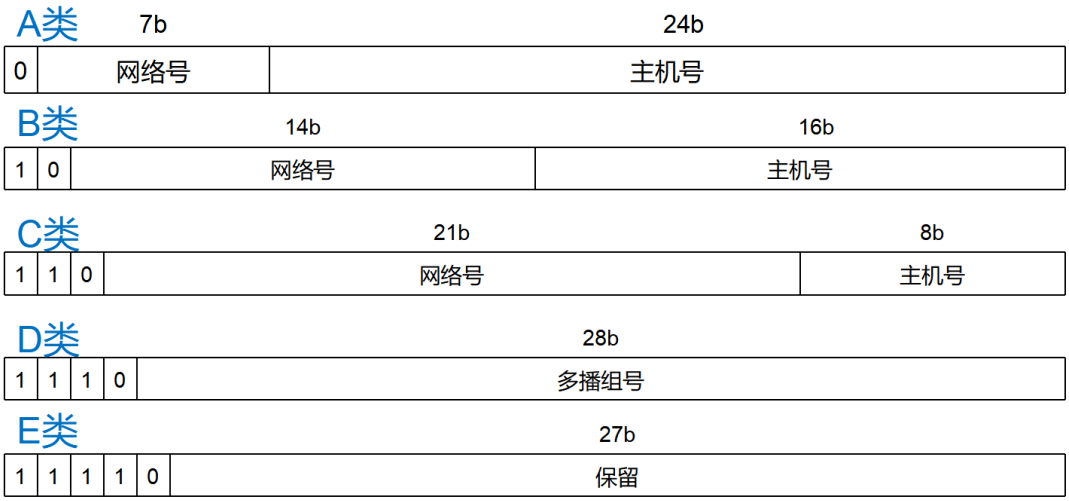
- IP地址采用两级结构，分为网络标识和主机标识



- IP地址被划分为若干个固定分类
- 每类IP地址由两个固定长度的字段组成：
  - 网络号 Network：标识主机（或路由器）所连接到的网络
  - 主机号 Host：在所连接到的网络中唯一标识该主机（或路由器）
- IP 地址在整个互联网范围内是唯一的

IP地址的分类

- IP地址按照层次结构划分成五类：A、B、C、D、E类。



IP地址的表示方法

- 二进制表示方法：用一个32位的比特序列表示IP地址，为了使这个地址有更好的可读性，通常在每个字节之间加上一个或多个空格做分隔

10000001 00001110 00000110 00011111

- 点分十进制表示方法：为了使32位地址更加简洁和更容易阅读，IP地址通常写成用小数点把各字节分隔开的形式。每个字节用一个小于256的十进制数表示

129.14.6.31

- 十六进制表示方法：每一个十六进制数字等效于4 bits

0x810E061F

各类IP地址的范围

类型	范围	网络数	每个网络主机数量
A	0.0.0.0 – 127.255.255.255	2^7 - 2	2^{24} - 2
B	128.0.0.0 – 191.255.255.255	2^{14}	2^{16} - 2
C	192.0.0.0 – 223.255.255.255	2^{21}	2^8 - 2
D	224.0.0.0 – 239.255.255.255		
E	240.0.0.0 – 247.255.255.255		
		>2百万	

特殊的IP地址

网络地址：主机号全为0的地址
网络IP地址不分配给任何主机，而是作为网络本身的标识，供路由器查找路由表用。
例：主机IP地址 202.198.151.136（C类地址，24bits掩码）所在网段的网络地址为202.198.151.0

32位全 0 IP地址：还没有分配到IP地址的主机在发送IP报文时用作源IP地址，用于DHCP协议

直接广播地址：主机地址为全“1”的IP地址不分配给任何主机，用作广播地址。
例：主机 202.198.151.136 （C类地址，24bits掩码）所在网段的直接广播地址为202.198.151.255

有限广播地址：32位为全1的IP地址称为有限广播地址。
例：有限广播地址为：255.255.255.255

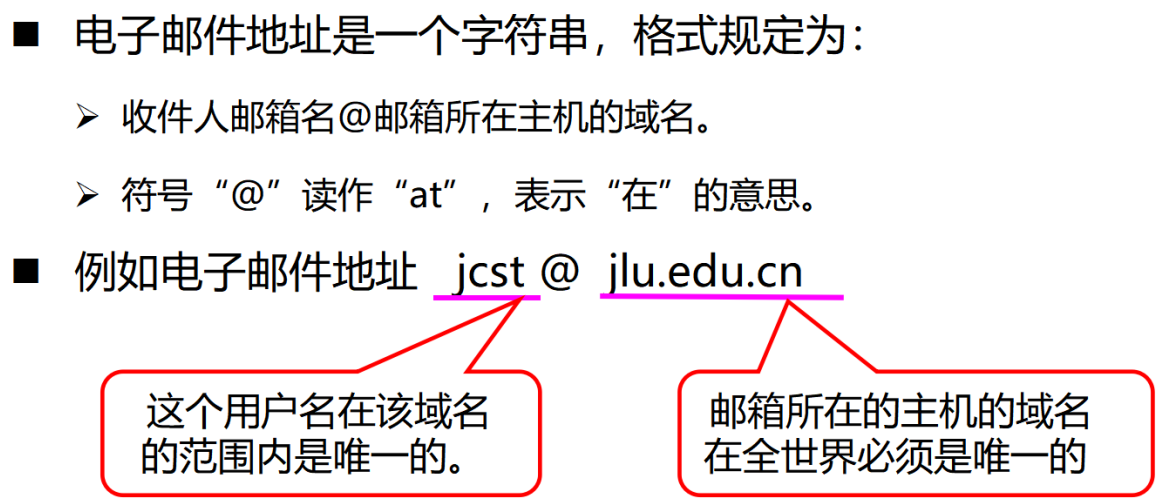
两者的区别：有限广播仅限于本网广播，路由器不转发该类数据包。直接广播可以跨网广播，可以通过路由器。

环回地址：第一个字节等于127的IP地址称为环回地址，用作主机或路由器的环回接口。
大多数主机系统把127.0.0.1分配给环回接口，常用于本机上软件测试和本机上网络应用程序之间的通信地址。

私有地址：
10.0.0.0　　— 10.255.255.255
172.16.0.0　— 172.31.255.255
192.168.0.0 — 192.168.255.255

企业内部网主机的IP地址可以设置成专用IP地址，进行企业内部的网络应用；并可通过NAT服务器访问Internet。这样只需要申请少量的全局IP地址，既解决了IP地址不足的问题，又解决了网络安全问题。

电子邮件的地址



9.TCP/IP防止网络拥塞的4方面措施

4阶段的4策略解释一下

1. 慢开始（启动）和拥塞避免
2. 快重传和快恢复

预分配缓冲区：常用于虚电路技术中，虚电路的建立会通知该节点为此虚电路预留缓冲区。

丢弃包：节点上收到过多的包而来不及处理或无法发送出去时，可丢弃一部分包。对突发性通信造成的拥塞有效。丢包的常用机制：尾丢弃（Tail Drop）随机早期检测（RED）

限制网内包数量：限制进入网内的包的数目，达到控制拥塞的目的。例如，在网内设置若干个许可证。

流量控制：接收端调节发送端发送数据的速率，防止到达接收端的数据速率超过接收端的处理速率。本质上流量控制和拥塞控制是不同的概念：流量控制是端到端　拥塞控制涉及中间节点

阻塞包：每个节点都监视其所有输出链路的使用情况。视情况决定是否向源结点发送阻塞包。

名词解释

P2P

在网络边缘的端系统中运行的程序之间的通信方式通常可划分为两大类：

• 客户−服务器方式（C/S 方式）即Client/Server方式

• 对等方式（P2P 方式）即 Peer-to-Peer方式

对等连接(peer-to-peer，简写为 P2P)是指两个主机在通信时并不区分哪一个是服务请求方还是服务提供方。

• 只要两个主机都运行了对等连接软件（P2P 软件），它们就可以进行平等的、对等连接通信。

• 双方都可以下载对方已经存储在硬盘中的共享文档。

多路复用技术

多路复用(multiplexing)利用一条链路同时传输多路信号，可以最大限度地利用系统所具有的传输能力

多路复用技术是将多个信号合并到单个通道传输的方法，以有效利用通信资源。它允许多个通信源共享同一通道，提高通信效率。

ARP协议

ARP（Address Resolution Protocol，地址解析协议）是用来将IP地址解析为MAC地址的协议。

端口

解决这个问题的方法就是在运输层使用协议端口号(protocol port number)，或通常简称为端口(port)。

• 虽然通信的终点是应用进程，但我们可以把端口想象是通信的终点，因为我们只要把要传送的报文交到目的主机的某一个合适的目的端口，剩下的工作（即最后交付目的进程）就由TCP/UDP 来完成。

TCP/IP协议栈

TCP/IP协议栈是一组通信协议，用于在计算机网络中进行数据通信。它是由两个主要协议组成的协议栈，分别是传输控制协议（TCP）和Internet协议（IP）。这个协议栈是互联网上的通信基础，它定义了数据在网络中的传输和处理方式。

数据通信系统：信源/信宿/信道

源系统（信源：产生要发送数据的设备，发送设备：对数据进行编码的设备）

传输系统（传输线路或网络）

目的系统（接收设备：将接收的信号变成数据，信宿：目的系统）

REP协议

？？？

DNS系统

域名系统（DNS，Domain Name System）是互联网重要的基础设施之一，向所有需要域名解析的应用提供服务，主要负责将可读性好的域名映射成IP地址

拥塞控制和流量控制

流量控制(flow control)就是让发送方的发送速率不要太快，既要让接收方来得及接收，也不要使网络发生拥塞。

在某段时间，若对网络中某资源的需求超过了该资源所能提供的可用部分，网络的性能就要变坏——产生拥塞(congestion)。

拥塞：网络或其一部分出现过多的包，导致网络性能下降的现象。对策：增加资源，或者降低负载

流量控制是一组过程，这组过程告诉发送方在收到接收方的应答之前，最多可以传送多少数据

使用停止-等待协议或者滑动窗口协议，控制了发送端发送数据的速度和节奏，确保接收端能够来得及正确接收数据，实现了流量控制

TCP是什么 P219

TCP：一种面向连接的、可靠的传输层通信协议，由IETF的RFC 793定义。

关注机构：名称，干了什么

IETA IRTF ICAN CNNIC

因特网协会 ISOC

因特网体系结构研究委员会 IAB

因特网研究部 IRTF

因特网研究指导小组 IRSG

因特网工程部 IETF

因特网工程指导小组 IESG

标准组织		在数据通信领域的主要工作
三大官方国际标准组织		
ITU-T	国际电信联盟	电信业务 IP 化、物联网
ISO	国际标准组织	网络互联模型
IEC	国际电工委员会	机械电气接口和互换性
三大民间国际标准组织		
IETF	互联网工程任务组	网络互联协议，标准主导者
IEEE	电气与电子工程师协会	Ethernet、WLAN
3GPP	第三代合作伙伴计划	无线IP
三大区域性标准组织		
CCSA	中国通信标准协会	设备形态、接口、标准支持
ETSI	欧洲电信标准化协会	宽带接入、终端
ANSI	美国国家标准局	美国标准审批

IRTF（Internet Research Task Force）的全名是互联网研究任务组。IRTF 是一个由互联网协会（Internet Society，ISOC）赞助的组织，旨在推动互联网技术的研究和发展。IRTF 的使命是促进互联网技术的长期发展，为互联网社区提供一个开放的论坛，以便研究和探讨各种技术问题。
IRTF 与 IETF（Internet Engineering Task Force，互联网工程任务组）有所不同。IETF 主要关注互联网标准的制定，而 IRTF 更专注于对未来互联网发展方向的研究。IRTF 的研究涵盖广泛的领域，包括网络协议、体系结构、安全性、隐私、性能、社会影响等方面。
IRTF 下设有多个研究组，每个研究组都关注特定的主题，例如分布式系统、未来互联网架构、网络测量、网络安全等。这些组通过组织讨论、研讨会、论文发表等方式，促进对互联网技术和发展方向的深入研究。
总体而言，IRTF 的目标是为互联网社区提供一个开放的平台，促进高质量的互联网技术研究，并为未来互联网的发展提供重要的指导和建议。

CNNIC 的全名是中国互联网络信息中心（China Internet Network Information Center）。中国互联网络信息中心是一个负责管理和运营中国国家顶级域名（.cn）的组织，同时也负责推动和协调中国互联网的发展。以下是CNNIC的主要职责和活动：

1.域名管理： CNNIC 负责管理和注册中国的顶级域名 .cn，以及其他一些与中国相关的域名。它维护域名注册系统，处理域名注册和管理相关的事务。
2.互联网基础设施建设： CNNIC 在互联网基础设施方面发挥重要作用，促进互联网的稳定、安全和可持续发展。这包括推动 IPv6 的部署，提高互联网的整体性能和可用性。
3.互联网统计和研究： CNNIC 进行关于中国互联网使用情况的调查和研究，发布《中国互联网络发展状况统计报告》等年度报告，提供关于互联网用户、网站、应用等方面的数据和趋势分析。
4.互联网安全： CNNIC 在互联网安全领域进行工作，包括发布安全警报、提供网络安全咨询和培训，以及参与国际互联网安全标准的制定。
5.推动互联网发展： 作为中国互联网的推动者，CNNIC 参与并组织各种互联网技术、政策和标准的制定，促进互联网产业的发展，推动数字经济的增长。

总体而言，CNNIC 在中国互联网发展中扮演着关键的角色，致力于促进互联网的可持续发展、提高网络安全水平，同时推动技术创新和数字化经济的发展。

每次数据传输单元

网络互联设备