

考研计算机基础班讲义

计算机网络

主讲：白龙飞

欢迎使用新东方在线电子教材



新东方在线

www.koolearn.com

网络课堂电子教材系列

目 录

新东方计算机网络基础课程讲义	错误！未定义书签。
第一章 计算机网络学习方法	5
第二章 知识点分析	6
第三章 计算机网络体系结构	10
3.1 计算机网络概述	10
3.1.1 计算机网络的概念、组成与功能	10
3.1.2 计算机网络的分类	10
3.1.3 计算机网络与互联网的发展历史	10
3.1.4 计算机网络的标准化工作及相关的组织	10
3.2 计算机网络体系结构与参考模型	10
3.2.1 计算机网络分层结构	10
3.2.2 计算机网络协议、接口、服务等概念	10
3.2.3 ISO/OSI 参考模型和 TCP/IP 模型	11
第四章 物理层	15
4.1 通信基础	15
4.1.1 信道、信号、宽带、码元、波特、速率、信源与信宿等基本概念	15
4.1.2 奈奎斯特定理与香农定理	15
4.1.3 编码与调制	16
4.1.4 电路交换、报文交换与分组交换	16
4.1.5 数据报与虚电路	17
4.2 传输介质	17
4.2.1 双绞线、同轴电缆、光纤与无线传输介质	17
4.2.2 物理层接口的特性	17
4.3 物理层设备	18
4.3.1 中继器	18
4.3.2 集线器	18
第五章 数据链路层	19
5.1 数据链路层的功能	19
5.2 组帧	19
5.3 差错控制	19
5.3.1 检错编码	19
5.3.2 纠错编码	20
5.4 流量控制与可靠传输机制	20
5.4.1 流量控制、可靠传输与滑动窗口机制	20
5.4.2 停止-等待协议	20
5.4.3 后退 N 帧协议 (GBN)	20
5.4.4 选择重传协议 (SR)	20
5.5 介质访问控制	21
5.5.1 信道划分介质访问控制	21
5.5.2 随机访问介质访问控制	21
5.5.3 轮询访问介质访问控制：令牌传递协议	22
5.6 局域网	22

5.6.1 局域网的基本概念与体系结构	22
5.6.2 以太网与 IEEE 802.3	22
5.6.3 IEEE 802.11	22
5.6.4 令牌环网的基本原理	23
5.7 广域网	23
5.7.1 广域网的基本概念	23
5.7.2 PPP 协议	23
5.7.3 HDLC 协议	23
5.8 数据链路层设备	23
5.8.1 网桥的概念及其工作原理	23
5.8.2 局域网交换机及其工作原理	24
第六章 网络层	26
6.1 网络层的功能	26
6.1.1 异构网络互联	26
6.1.2 路由与转发	26
6.1.3 拥塞控制	26
6.2 路由算法	26
6.2.1 静态路由与动态路由	26
6.2.2 距离-向量路由算法	26
6.2.3 链路状态路由算法	27
6.2.4 层次路由	28
6.3 IPv4	28
6.3.1 IPv4 分组	28
6.3.2 IPv4 地址与 NAT	28
6.3.3 子网划分与子网掩码、CIDR	29
6.3.4 ARP 协议、DHCP 协议与 ICMP 协议	31
6.4 IPv6	33
6.4.1 IPv6 的主要特点	33
6.4.2 IPv6 地址	33
6.5 路由协议	33
6.5.1 自治系统	33
6.5.2 域内路由与域间路由	34
6.5.3 RIP 路由协议	34
6.5.4 OSPF 路由协议	34
6.5.5 BGP 路由协议	34
6.6 IP 组播	35
6.6.1 组播的概念	35
6.6.2 IP 组播地址	35
6.7 移动 IP	36
6.7.1 移动 IP 的概念	36
6.7.2 移动 IP 的通信过程	36
6.8 网络层设备	36
6.8.1 路由器的组成和功能	36
6.8.2 路由表与路由转发	36
第七章 传输层	1
7.1 传输层提供的服务	1

7.1.1 传输层的功能	1
7.1.2 传输层寻址与端口	1
7.1.3 无连接服务与面向连接服务	1
7.2 UDP 协议	1
7.2.1 UDP 数据报	1
7.2.2 UDP 校验	1
7.3 TCP 协议	1
7.3.1 TCP 段	1
7.3.2 TCP 连接管理	2
7.3.3 TCP 可靠传输	2
7.3.4 TCP 流量控制与拥塞控制	3
第八章 应用层	6
8.1 网络应用模型	6
8.1.1 客户/服务器模型	6
8.1.2 P2P 模型	6
8.2 DNS 系统	6
8.2.1 层次域名空间	6
8.2.2 域名服务器	6
8.2.3 域名解析过程	6
8.3 FTP	7
8.3.1 FTP 协议的工作原理	7
8.3.2 控制连接与数据连接	7
8.4 电子邮件	8
8.4.1 电子邮件系统的组成结构	8
8.4.2 电子邮件格式与 MIME	8
8.4.3 SMTP 协议与 POP3 协议	10
8.5 WWW	13
8.5.1 WWW 的概念与组成结构	13
8.5.2 HTTP 协议	13
第九章 网络实验入门	14
9.1 研究包大小和传输时间的关系	14
9.2 使用 tracert 和 ping 命令	16
9.3 学习使用 ethereal 观察网络	16
9.4 观察 web 简单过程	18
第十章 网络基础总结	19

第一章 计算机网络学习方法

“计算机网络”涉及计算机和通信两个领域，是计算机应用中一个不可或缺的方向，大纲将计算机网络列为考试科目，是为了使考生能深入地对其体系结构与协议等方面进行学习，整个大纲网络部分就是按照网络的层次结构安排的。该科目的知识点相当抽象，但考察的难度相对较低，如果能够深刻理解网络层次化的思想，复习难度将大大降低。

考核目标：

1. 掌握计算机网络的基本概念、基本原理和基本方法。
2. 掌握计算机网络的体系结构和典型网络协议，了解典型网络的组成和特点，理解典型网络设备的工作原理
3. 能够综合运用计算机网络的基本概念、基本原理和基本方法进行网络系统的分析、设计 and 应用

复习教材：

教材：《计算机网络》谢希仁 电子工业出版社

辅导书：《计算机网络知识要点与习题解析》哈尔滨工程大学出版社

《计算机专业基础综合辅导讲义》 北航出版社

《考研计算机专业基础综合真题名师讲解与 100 知识点聚焦》 北航出版社

习题集：《考研计算机专业基础综合考试大纲同步练习》 北航出版社

模拟题：《考研计算机专业基础综合全真模拟试题》 北航出版社

知识点：《考研计算机专业基础综合要点速记》 北航出版社

第二章 知识点分析（※代表知识点的重要程度）

一、 计算机网络体系结构

（一）计算机网络概述

1. 计算机网络的概念、组成与功能
2. 计算机网络的分类
3. 计算机网络与互联网的发展历史
4. 计算机网络的标准化工作及相关组织

（二）计算机网络体系结构与参考模型

1. 计算机网络分层结构※※※
2. 计算机网络协议、接口、服务等概念※※※※※
3. ISO/OSI 参考模型和 TCP/IP 模型※※※※※

二、 物理层

（一）通信基础

1. 信道、信号、宽带、码元、波特、速率、信源和信宿等基本概念
2. 奈奎斯特定理与香农定理※※※※※
3. 编码与调制
4. 电路交换、报文交换与分组交换※※※※※
5. 数据报与虚电路※※※

（二）传输介质

1. 双绞线、同轴电缆、光纤与无线传输介质
2. 物理层接口的特性

（三）物理层设备

1. 中继器
2. 集线器※※※

三、 数据链路层

（一）数据链路层的功能

（二）组帧※※

（三）差错控制

1. 检错编码※※
2. 纠错编码

新东方在线

www.koolearn.com

网络课堂电子教材系列

(四) 流量控制与可靠传输机制※※※※※

1. 流量控制、可靠传输与滑轮窗口机制
2. 停止-等待协议
3. 后退 N 帧协议 (GBN)
4. 选择重传协议 (SR)

(五) 介质访问控制

1. 信道划分介质访问控制

频分多路复用、时分多路复用、波分多路复用、码分多路复用的概念和基本原理。

2. 随机访问介质访问控制※※※※※

ALOHA 协议;CSMA 协议;CSMA/CD 协议;CSMA/CA 协议。

3. 轮询访问介质访问控制: 令牌传递协议

(六) 局域网

1. 局域网的基本概念与体系结构※※
2. 以太网与 IEEE 802.3
3. IEEE 802.11
4. 令牌环网的基本原理

(七) 广域网

1. 广域网的基本概念
2. PPP 协议
3. HDLC 协议

(八) 数据链路层设备

1. 网桥的概念及其工作原理
2. 局域网交换机及其工作原理。※※※※※

四、网络层

(一) 网络层的功能

1. 异构网络互联
2. 路由与转发
3. 拥塞控制

(二) 路由算法※※※※※

1. 静态路由与动态路由

2. 距离-向量路由算法

3. 链路状态路由算法

4. 层次路由

(三) IPv4※※※※※

1. IPv4 分组

2. IPv4 地址与 NAT

3. 子网划分与子网掩码、CIDR

4. ARP 协议、DHCP 协议与 ICMP 协议

(四) IPv6

1. IPv6 的主要特点

2. IPv6 地址※※

(五) 路由协议

1. 自治系统

2. 域内路由与域间路由

3. RIP 路由协议※※※※※

4. OSPF 路由协议※※※※※

5. BGP 路由协议※※※

(六) IP 组播

1. 组播的概念

2. IP 组播地址

(七) 移动 IP

1. 移动 IP 的概念

2. 移动 IP 的通信过程

(八) 网络层设备※※※※※

1. 路由器的组成和功能

2. 路由表与路由转发

五、传输层

(一) 传输层提供的服务

1. 传输层的功能

2. 传输层寻址与端口※※

新东方在线

www.koolearn.com

网络课堂电子教材系列

3. 无连接服务与面向连接服务

(二) UDP 协议

1. UDP 数据报
2. UDP 校验※※※※

(三) TCP 协议

1. TCP 段
2. TCP 连接管理※※※※
3. TCP 可靠传输※※※※
4. TCP 流量控制与拥塞控制※※※※※

六、应用层

(一) 网络应用模型

1. 客户/服务器模型
2. P2P 模型

(二) DNS 系统

1. 层次域名空间
2. 域名服务器
3. 域名解析过程※※※※※

(三) FTP

1. FTP 协议的工作原理※※※※※
2. 控制连接与数据连接

(四) 电子邮件

1. 电子邮件系统的组成结构
2. 电子邮件格式与 MIME※※※※※
3. SMTP 协议与 POP3 协议※※※※

(五) WWW

1. WWW 的概念与组成结构
2. HTTP 协议※※※※※

第三章 计算机网络体系结构

3.1 计算机网络概述

3.1.1 计算机网络的概念、组成与功能

计算机网络：就是利用通信设备和线路将地理位置不同的、功能独立的多个计算机系统互连起来，以功能完善的网络软件（即网络通信协议、信息交换方式、网络操作系统等）实现网络中资源共享和信息传递的系统。

3.1.2 计算机网络的分类

【例】下面不属于网络拓扑结构的是（ ）

- A. 环形结构 B. 总线结构 C. 网状结构 D. 层次结构

【答案】D

【分析】按照拓扑结构进行网络的分类，不包含层次结构。

3.1.3 计算机网络与互联网的发展历史

网络发展三阶段：面向终端的网络；计算机—计算机网络；开放式标准化网络。

3.1.4 计算机网络的标准化工作及相关组织

国际上制定通信协议和标准的主要组织有以下几个：（1）IEEE；（2）ISO；（3）ITU

3.2 计算机网络体系结构与参考模型

3.2.1 计算机网络分层结构

对于非常复杂的计算机网络协议，最好的方法是采用分层式结构。每一层关注和解决通信中的某一方面的规则。各层之间是独立的，灵活性好，结构上可以分开，易于实现和维护，促进标准化工作。

3.2.2 计算机网络协议、接口、服务等概念

1. 协议

协议总是指某一层协议，准确地说，它是对同等实体之间的通信制定的有关通信规则约定的集合。网络协议的三个要素：

(1) 语义 (Semantics)。 (2) 语法 (Syntax)。 (3) 同步即定时 (Timing)。

2 接口 (服务访问点)

同一系统中相邻两层的实体进行交互的地方。

3. 服务 (service)

为保证上层对等体之间能相互通信，下层向上层提供的功能。

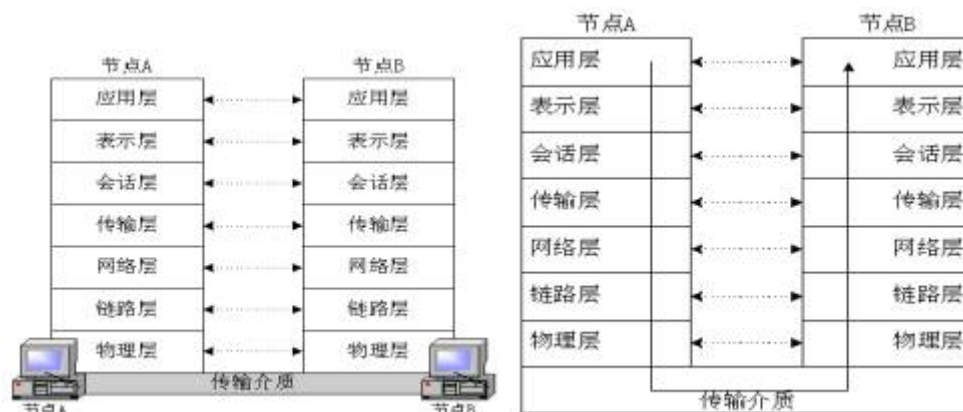
3.2.3 ISO/OSI 参考模型和 TCP/IP 模型

1. ISO/OSI 参考模型

各节点有相同的层次。

同一节点的相邻层之间通过接口通信。

下层为上层服务。



1、物理层

物理层是 OSI 参考模型的最低一层，也是在同级层之间直接进行信息交换的唯一一层。物理层负责传输二进制位流，它的任务就是为上层（数据链路层）提供一个物理连接，以便在相邻节点之间无差错地传送二进制位流。

有一点应该注意的是，传送二进制位流的传输介质，如双绞线、同轴电缆以及光纤等并不属于物理层要考虑的问题。实际上传输介质并不在 OSI 的 7 个层次之内。

- 电气特性：电缆上什么样的电压表示 1 或 0
- 机械特性：接口所用的接线器的形状和尺寸
- 过程特性：不同功能的各种可能事件的出现顺序以及各信号线的工作原理
- 功能特性：某条线上出现的某一电平的电压表示何种意义

2、数据链路层

数据链路层负责在两个相邻节点之间，无差错地传送以 “ 帧 ” 为单位的数据。每一帧包括一定数

量的数据和若干控制信息。

数据链路的任务首先要负责建立、维持和释放数据链路的连接。在传送数据时，如果接收节点发现数据有错，要通知发送方重发这一帧，直到这一帧正确无误地送到为止。这样，数据链路层就把一条可能出错的链路，转变成让网络层看起来就像是一条不出错的理想链路。

3、网络层

网络层的主要功能是为处在不同网络系统中的两个节点设备通信提供一条逻辑通路。其基本任务包括路由选择、拥塞控制与网络互联等功能。

4、传输层

传输层的主要任务是向用户提供可靠的端到端（ end-to-end ）服务，透明地传送报文。它向高层屏蔽了下层数据通信的细节，因而是计算机通信体系结构中最关键的一层。该层关心的主要问题包括建立、维护和中断虚电路、传输差错校验和恢复以及信息流量控制机制等。

5、会话层

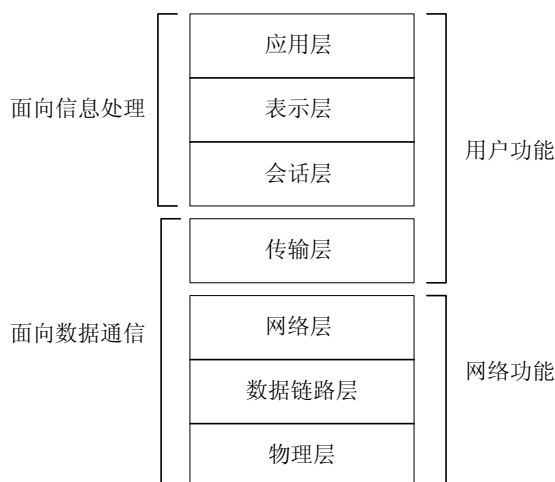
负责通讯的双方在正式开始传输前的沟通，目的在于建立传输时所遵循的规则，使传输更顺畅、有效率。沟通的议题包括：使用全双工模式或半双式模式？如何发起传输？如何结束传输？如何设置传输参数就像两国元首在见面会晤之前，总会先派人谈好议事规则，正式谈判时就根据这套规则进行一样。

6、表示层

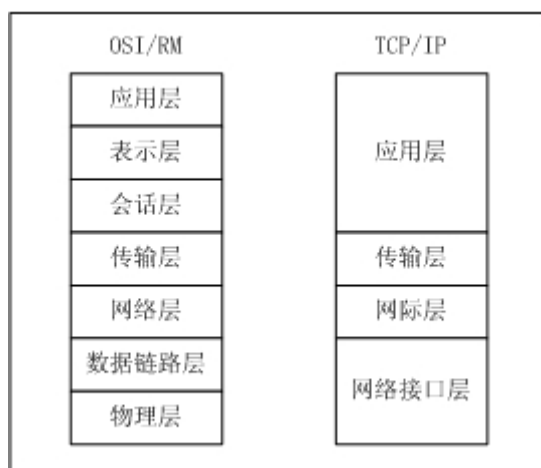
表示层处理两个应用实体之间进行数据交换的语法问题，解决数据交换中存在的格式不一致以及数据表示方法不同等问题。例如， IBM 系统的用户使用 EBCD 编码，而其它用户使用 ASCII 编码。表示层必须提供这两编码的转换服务。数据加密与解密、数据压缩与恢复等也都是表示层提供的服务。

7、应用层

应用层是 OSI 参考模型中最靠近用户的一层，它直接提供文件传输、电子邮件、网页浏览等服务给用户。



2. TCP/IP 模型



1、网络接口层（ network interface layer ）

在 TCP/IP 分层体系结构中,最底层是网络接口层,它 负责通过网络发送和接收 IP 数据报 。TCP/IP 体系结构并未对网络接口层使用权的协议做出强硬的规定,它允许主机连入网络时使用多种现成的和流行的协议,例如局域网协议或其他一些协议。

帧 是 独立的网络信息传输单元 。

2、网络层（ internet layer ）

网际层是 TCP/IP 体系结构的第二层,它实现的功能相当于 OSI 参考模型网络层的无连接网络服务。互联层负责将源主机的报文分组发送到目的的主机,源主机与目的主机可以在一个网上,也可以在不同的网上。

（ 1 ）处理来自传输层的分组发送请求。在收到分组发送请求之后,将分组建入 IP 数据报,填充报头,选择发送路径,然后将数据报发送到相应的网络输出线。

（ 2 ）处理接收的数据报。在接收到其他主机发送的数据报之后,检查目的地址,如需要转发,则选择发送路径,转发出去;如目的地址为本节点 IP 地址,则除去报头,将分组送交给传输层处理。

（ 3 ）处理互联的路径、流控与拥塞问题。

3、传输层（ transport layer ）

网际层之上是传输层,它的主要功能是负责应用进程之间的 端 - 端（ Host-to-host ）通信。在 TCP/IP 体系结构中,设计传输层的主要目的是在互联网中源主机与目的主机的对等实体之间建立用于 会话的端 - 端连接 。因此,它与 OSI 参考模型的传输层功能相似。

TCP/IP 体系结构的传输层定义了 传输控制协议（ TCP , transport control protocol ） 和 用户数据报协议（ UDP,user datagram protocol ） 两种协议。

TCP 协议是一种可靠的面向连接的协议,它允许将一台主机的字节流（ byte stream ）无差错地传送

到目的主机。

UDP 协议是一种不可靠的无连接协议，它主要用于不要求分组顺序到达的传输中，分组传输顺序检查与排序由应用层完成。

4、应用层（ application layer ）

在 TCP/IP 体系结构中，应用层是最靠近用户的一层。它包括了所有的高层协议，并且总是不断有新的协议加入。其主要协议包括：

- （ 1 ）文件传输协议（ FTP ,file transfer protocol ），用于实现互联网中交互式文件传输功能；
- （ 2 ）简单邮件传输协议（ SMTP simple mail transfer protocol ），用于实现互联网中邮件传送功能；
- （ 3 ）域名系统（ DNS, domain name system ），用于实现互联网设备名字到 IP 地址映射的网络服务；
- （ 4 ）超文本传输协议（ HTTP, byper text transfer protocol ），用于目前广泛使用的 Web 服务；
- （ 5 ）路由信息协议（ RIP, routing information protocol ），用于网络设备之间交换路由信息；

第四章 物理层

4.1 通信基础

4.1.1 信道、信号、宽带、码元、波特、速率、信源与信宿等基本概念

- (1) 信道：向某一个方向传送信息的媒体。
- (2) 数据：信息的承载实体。
- (3) 信号：数据的电磁或电气表现。
- (4) 带宽：媒介中信号可使用的最高频率和最低频率之差，或者说是频带的宽度；另一个定义是信道中数据的传送速率。
- (5) 码元：在使用时间域（简称时域）的波形表示数字信号时，代表不同离散数值的基本波形。
- (6) 波特：单位时间内传输的码元数。
- (7) 比特率：单位时间内传输的比特数。
- (8) 信息传播过程简单地描述为：信源→信道→信宿。

4.1.2 奈奎斯特定理与香农定理

奈奎斯特(Nyquist)无噪声下的码元速率极限值 B 与信道带宽 H 的关系：

$$\text{最大数据传输率 } B=2 \cdot H \text{ (Baud)}$$

奈奎斯特公式--无噪信道传输能力公式： $C=2 \cdot H \cdot \log_2 N$ (bps)

式中 H 为信道的带宽，即信道传输上、下限频率的差值，单位为 Hz； N 为一个码元所取的离散值个数。

香农公式--带噪信道容量公式： $C=H \cdot \log_2(1+S/N)$ (bps) 式中 S 为信号功率， N 为噪声功率， S/N 为信噪比，通常把信噪比表示成 $10\lg(S/N)$ 分贝(dB)。

【例】带宽 6 MHz，量化等级为 4，无噪声，最大数据传输率多大？

【答案】由 Nyquist 定理 $C=2 \cdot H \cdot \log_2 N$ (bps) $=2 \cdot 6 \log_2 4=24\text{Mbps}$

【分析】Nyquist 定理的直接应用。

【例】带宽 3 KHz，信噪比 20dB，二进制，最大数据传输率

【答案】 $R_{\max}^{\text{Shannon}} = B \log_2 \left(1 + \frac{S}{N}\right) = 3 \times \log_2(1+100) \approx 20\text{Kbps}$
 $R_{\max}^{\text{Nyquist}} = 2B \log_2 V = 2 \times 3 \times \log_2 2 = 6\text{Kbps}$

两个理论上限，不可逾越。取两者最小值： $R_{\max}=6\text{Kbps}$

【分析】香农和 Nyquist 定理的综合应用。

4.1.3 编码与调制

最基本的二元制调制方法有以下几种：（1）调幅(AM)：（2）调频(FM)： 3）调相(PM)：

4.1.4 电路交换、报文交换与分组交换

数据经编码后在通信线路上进行传输，按数据传送技术划分，交换网络又可分为电路交换网、报文交换网和分组交换网。

1 电路交换

（1）电路交换的三个过程

① 电路建立：数据传输：电路拆除：

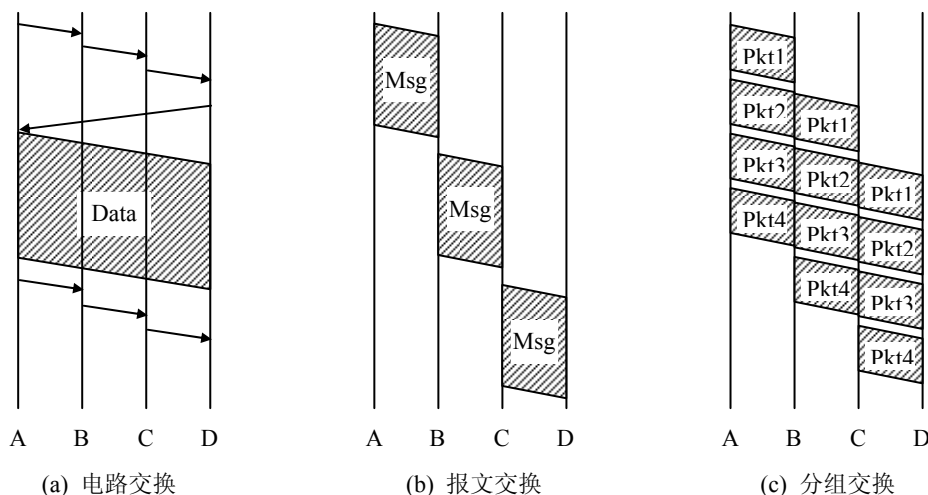
2 报文交换

报文交换方式的数据传输单位是报文，报文就是站点一次性要发送的数据块，其长度不限且可变。当一个站要发送报文时，它将一个目的地址附加到报文上，网络节点根据报文上的目的地址信息，把报文发送到下一个节点，一直逐个节点地转送到目的节点。

每个节点在收到整个报文并检查无误后，就暂存这个报文，然后利用路由信息找出下一个节点的地址，再把整个报文传送给下一个节点。因此，端与端之间无需先通过呼叫建立连接。

3. 分组交换

分组交换是报文交换的一种改进，它将报文分成若干个分组，每个分组的长度有一个上限，有限长度的分组使得每个节点所需的存储能力降低了，分组可以存储到内存中，提高了交换速度。它适用于交互式通信，如终端与主机通信。



三种交换方式的比较

4.1.5 数据报与虚电路

对比的方面	虚电路服务	数据报服务
思路	可靠通信应当由网络来保证	可靠通信应当由用户主机来保证
连接的建立	必须有	不需要
终点地址	仅在连接建立阶段使用, 每个分组使用短的虚电路号	每个分组都有终点的完整地址
分组的转发	属于同一条虚电路的分组均按照同一路由进行转发	每个分组独立选择路由进行转发
当结点出故障时	所有通过出故障的结点的虚电路均不能工作	出故障的结点可能会丢失分组, 一些路由可能会发生变化
分组的顺序	总是按发送顺序到达终点	到达终点时不一定按发送顺序
端到端的差错处理和流量控制	可以由网络负责, 也可以由用户主机负责	由用户主机负责

4.2 传输介质

4.2.1 双绞线、同轴电缆、光纤与无线传输介质

4.2.2 物理层接口的特性

物理层的主要任务描述为确定与传输媒体的接口的一些特性, 即:

(1) 机械特性: (2) 电气特性: (3) 功能特性: (4) 过程特性:

4.3 物理层设备

4.3.1 中继器

4.3.2 集线器

【例】用集线器连接的工作站集合（）

- A. 同属一个冲突域，也同属一个广播域 B. 不属一个冲突域，但同属一个广播域
C. 不属一个冲突域，也不属一个广播域 D. 同属一个冲突域，但不属一个广播域

【答案】A

【分析】对冲突域和广播域的理解，集线器的特点是 A。

第五章 数据链路层

5.1 数据链路层的功能

链路层的主要功能包括链路管理、帧同步、流量控制、差错控制、数据和控制信息分开、透明传输和寻址。

5.2 组帧

1 面向比特的方法

基本原理：将需要传输的数据块看作比特序列，在数据块前和后各加入一个特殊的比特序列（前文位模式和后文位模式，01111110），表示数据块的起始和结束，从而构成最终传输的帧。

2 面向字符的异步传输

基本思想,把需要传输的数据块看作字符序列,在数据块前和后各加入一个特殊点额字符序列(前文字符模式和后文字符模式,0x7E),表示数据块的起始和结束,从而构成最终传输的帧。

5.3 差错控制

5.3.1 检错编码

在数据链路层传送的帧中，广泛使用了循环冗余检验 CRC 的检错技术。

【例】设收到的信息码字为 110111，检查和 CRC 为 1001，生成多项式为: $G(x)=X^4+X^3+1$ ，请问收到的信息有错吗，为什么？

【答案】

$$\begin{array}{r}
 100110 \\
 \hline
 G(x) \rightarrow 11001 \) \ 1101111001 \\
 11001 \\
 \hline
 10110 \\
 11001 \\
 \hline
 11110 \\
 11001 \\
 \hline
 1111 \leftarrow R(X)
 \end{array}$$

因为余数 $R(x)$ 不为 0，所以收到的信息不正确。

【分析】采用 CRC 校验进行信息检测的实际应用例子，注意学会基本的运算原理。

5.3.2 纠错编码

当计算机存储或移动数据时,可能会产生数据位错误,这时可以利用汉明码来检测并纠错,简单的说,汉明码是一个错误校验码码集,由 Bell 实验室的 R.W.Hamming 发明,因此定名为汉明码。

5.4 流量控制与可靠传输机制

5.4.1 流量控制、可靠传输与滑动窗口机制

一般来说,凡是在一定范围内到达的帧,即使它们不按顺序,接收方也要接收下来。若把这个范围看成是接收窗口的话,由接收窗口的大小也应该是大于 1 的。

空闲 RQ: 发送窗口=1,接收窗口=1;

Go-back-N: 发送窗口>1,接收窗口>1;

选择重发: 发送窗口>1,接收窗口>1。

若帧序号采用 3 位二进制编码,由最大序号为 $S_{max}=2^3-1=7$ 。对于有序接收方式,发送窗口最大尺寸选为 S_{max} ;对于无序接收方式,发送窗口最大尺寸至多是序号范围的一半。发送方管理超时控制的计时器数应等于缓冲器数,而不是序号空间的大小。

5.4.2 停止-等待协议

5.4.3 后退 N 帧协议 (GBN)

GO-DACK-N 策略的基本原理是,当接收方检测出失序的信息帧后,要求发送方重发最后一个正确接收的信息帧之后的所有未被确认的帧;或者当发送方发送了 N 个帧后,若发现该 N 帧的前一个帧在计时器超时后仍未返回其确认信息,则该帧被判为出错或丢失,此时发送方就不得不重新发送出错帧及其后的 N 帧。这就是 GO-DACK-N(退回 N)法名称的由来。

5.4.4 选择重传协议 (SR)

另一种效率更高的策略是当接收方发现某帧出错后,其后继续送来的正确的帧虽然不能立即递交给接收方的高层,但接收方仍可收下来,存放在一个缓冲区中,同时要求发送方重新传送给出错的那一帧。一旦收到重新传来的帧后,就可以原已存于缓冲区中的其余帧一并按正确的顺序递交高层。这种方法称为选择重发(SELECTICE REPEAT)。

5.5 介质访问控制

5.5.1 信道划分介质访问控制

频分多路复用、时分多路复用、波分多路复用、码分多路复用的概念和基本原理。

多路复用技术就是把许多个单个信号在一个信道上同时传输的技术。频分多路复用 FDM 和时分多路复用 TDM 是两种最常用的多路复用技术。

3.5.2 随机访问介质访问控制

1.ALOHA 协议

纯 ALOHA 基本思想：是用户有帧即可发送,采用冲突监听与随机重发机制.这样的系统是竞争系统 (contention system)。它帧长统一，但两帧冲突或重叠，则会被破坏，因此效率不高。在泊松分布条件下，每个帧时间为尝试发送次数 $G=0.5$ 时，信道吞吐量 $S=0.184$ ，也就是说,只能用原信道吞吐量的 18.4%。

2.载波监听多路访问 (CSMA)。

CSMA 的原理是：当一个站点要发送数据前，需要先监听总线。如果总线上没有其他站点的发送信号存在，即总线是空闲的，则该站点发送数据；如果总线上有其他站点的发送信号存在，即总线是忙的，则需要等待一段时间间隔后再重新监听总线，再根据总线的忙、闲情况决定是否发送数据。

3.载波监听多路访问/冲突检测 (CSMA/CD)。

4.CSMA/CA(Carrier Sense Multiple Access with Collision Avoidance)

CSMA/CD 和 CSMA/CA 的主要差别对比如下：

CSMA/CD：带有冲突检测的载波监听多路访问，可以检测冲突，但无法“避免”

CSMA/CA：带有冲突避免的载波侦听多路访问，发送包的同时不能检测到信道上有无冲突，只能尽量‘避免’；

- ① 两者的传输介质不同,CSMA/CD 用于总线式以太网,而 CSMA/CA 则用于无线局域网 802.11a/b/g/n 等等；
- ② 检测方式不同,CSMA/CD 通过电缆中电压的变化来检测，当数据发生碰撞时，电缆中的电压就会随着发生变化；而 CSMA/CA 采用能量检测 (ED)、载波检测 (CS) 和能量载波混合检测三种检测信道空闲的方式；
- ③ WLAN 中，对某个节点来说，其刚刚发出的信号强度要远高于来自其他节点的信号强度，也就是说它自己的信号会把其他的信号给覆盖掉；

- ④ 本节点处有冲突并不意味着在接收节点处就有冲突；

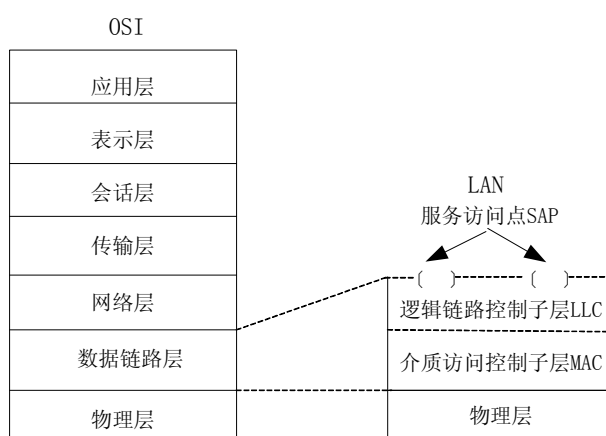
5.5.3 轮询访问介质访问控制：令牌传递协议

控制令牌是另一种传输媒体访问控制方法。它是按照所有站点共同理解和遵守的规则，从一个站点到另一个站点传递控制令牌

5.6 局域网

5.6.1 局域网的基本概念与体系结构

局域网是将小区域内的各种通信设备互联在一起的通信网络。



5.6.2 以太网与 IEEE 802.3

标准	主要使用的传输介质	速率	物理拓扑
10BASE5	50 Ω 粗同轴电缆	10Mbps	总线
10BASE2	50 Ω 细同轴电缆	10Mbps	总线
10BASE-T	3 类、4 类、5 类或超 5 类非屏蔽双绞线	10Mbps	星型
100BASE-TX	5 类或超 5 类非屏蔽双绞线	100Mbps	星型
100BASE-FX	光缆	100Mbps	星型

5.6.3 IEEE 802.11

802.11 的物理层实现方法：直接序列扩频 DSSS 正交频分复用 OFDM 跳频扩频 FHSS（已很少用）红外线 IR（已很少用）

标准	频段	数据速率	物理层	优缺点
802.11b	2.4 GHz	最高为 11 Mb/s	HR-DSSS	最高数据率较低，价格最低，信号传播距离最远，且不

				易受阻碍
802.11a	5 GHz	最高为 54 Mb/s	OFDM	最高数据率较高，支持更多用户同时上网，价格最高，信号传播距离较短，且易受阻碍
802.11g	2.4 GHz	最高为 54 Mb/s	OFDM	最高数据率较高，支持更多用户同时上网，信号传播距离最远，且不易受阻碍，价格比 802.11b 贵

5.6.4 令牌环网的基本原理

这种介质访问使用一个标记沿着环循环。当一个站要发送帧时，需等待空标记通过，然后将它改为忙标记。紧跟着忙标记，站把数据帧发送到环上。由于标记是忙状态，所以其它站不能发送帧，必须等待。发送的帧在环上循环一周后再回到发送站，将该帧从环上移去。同时将忙标记改为空标记，传至后面的站，使之获得发送帧的许可权。

5.7 广域网

5.7.1 广域网的基本概念

5.7.2 PPP 协议

PPP 协议是全世界使用最多的数据链路层协议，它已成为因特网的正式标准[RFC 1661]。

5.7.3 HDLC 协议

HDLC 是通用的数据链路控制协议，在开始建立数据链路时，允许选用特定的操作方式。所谓操作方式，通俗地讲就是某站点是以主站点方式操作还是以从站方式操作，或者是二者兼备。链路上用于控制目的的站称为主站，其它的受主站控制的站称为从站。主站对数据流进行组织，并且对链路上的差错实施恢复。由主站发往从站的帧称为命令帧，而从从站返回主站的帧称为响应帧。连有多个站点的链路通常使用轮询技术，轮询其它站的站称为主站，而在点-点链路中每个站均可为主站。

5.8 数据链路层设备

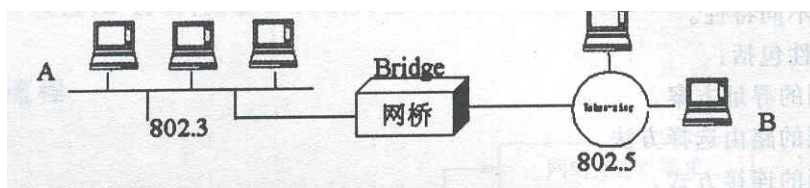
5.8.1 网桥的概念及其工作原理

1 网桥的概念

网桥是一种存储转发设备，用来连接类型相似的局域网。

假设一 802.3(CSMA/CD)局域网上的主机 A 与 802.5(Token Ring)局域网上的主机 B 通信，两个局域网

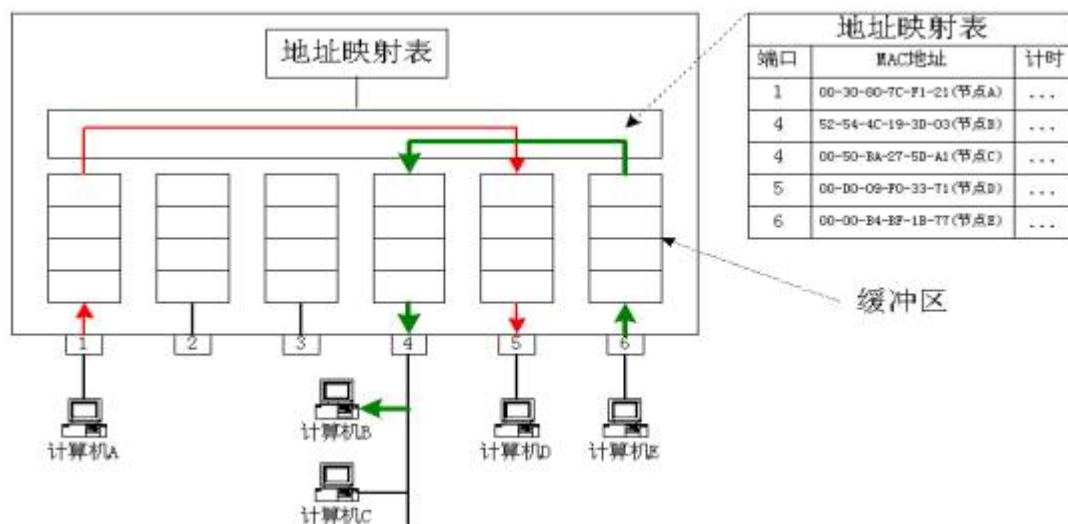
通过网桥互连，如图所示。



5.8.2 局域网交换机及其工作原理。

以太网交换机的原理很简单，它检测从以太网端口来的数据包的源和目的地的 MAC(介质访问层)地址，然后与系统内部的动态查找表进行比较，若数据包的 MAC 层地址不在查找表中，则将该地址加入查找表中，并将数据包发送给相应的目的端口。

以太网交换机的工作过程



1、端口 /MAC 地址映射表

(1) 二维表包含：端口、MAC、计时。

(2) 如何建立、更新端口 /MAC 地址映射表：“地址学习”法，动态更新，读取帧的源地址并记录帧进入交换机的端口（节点只要发送信息，交换机就能建立该表项），利用计时器维护表项的“新鲜”性。

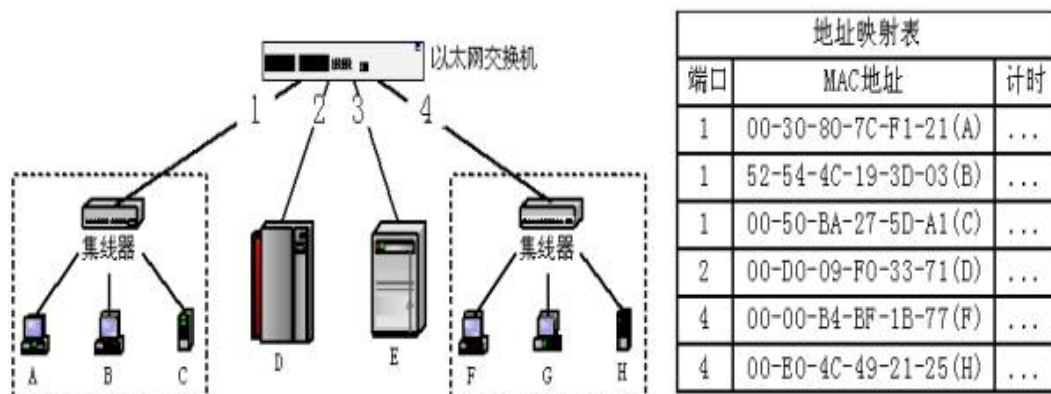
考虑：端口和 MAC 地址是否是一一对应的关系？

(3) 如何建立、更新端口 /MAC 地址映射表？

新建或更新的表项被赋予一个计时器，计时器超时，表项被删除。

(4) 如何过滤信息

目的：隔离本地信息，避免不必要的数据流动。



方法：利用端口 /MAC 地址映射表和帧的目的地址决定是否转发或转发到何处。

注意：如果地址表中不存在帧的目的地址，交换机则需要向除接收端口以外的所有端口转发。

考虑：CSMA/CD 对交换机是否适用？对用交换机组建的以太网是否适用？

以太网交换机的原理很简单，它检测从以太网端口来的数据包的源和目的地的 MAC(介质访问层)地址，然后与系统内部的动态查找表进行比较，若数据包的 MAC 层地址不在查找表中，则将该地址加入查找表中，并将数据包发送给相应的目的端口。

第六章 网络层

6.1 网络层的功能

6.1.1 异构网络互联

所谓虚拟互连网络也就是逻辑互连网络，它的意思就是互连起来的各种物理网络的异构性本来是客观存在的，但是我们利用 IP 协议就可以使这些性能各异的网络从用户看起来好像是一个统一的网络。使用 IP 协议的虚拟互连网络可简称为 IP 网。

6.1.2 路由与转发

6.1.3 拥塞控制

【例.】网络层的主要目的是（）

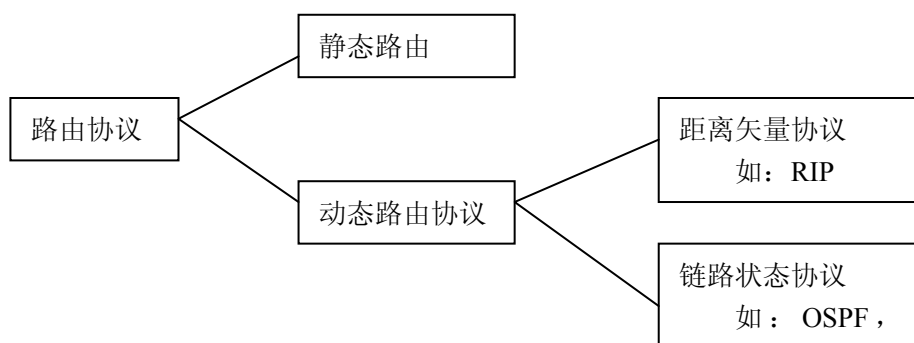
- A. 在邻接节点间进行数据包传输
- B. 在邻接节点间进行数据包可靠传输
- C. 在任意节点间进行数据包传输
- D. 在任意节点间进行数据包可靠传输

【答案】C

【分析】考察网络层的主要功能，注意概念上不要混淆。

6.2 路由算法

6.2.1 静态路由与动态路由

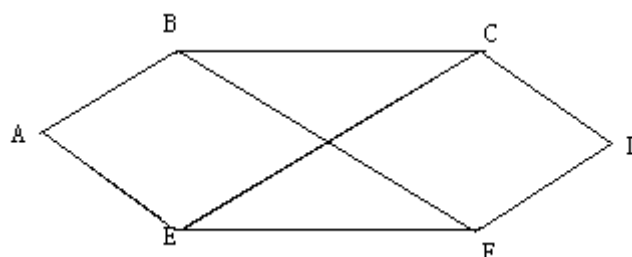


6.2.2 距离-向量路由算法

距离向量路由算法(Bellman-Ford Routing Algorithm)，也叫做最大流量演算法(Ford-Fulkerson Algorithm)，其被距离向量协议作为一个算法，如 RIP, BGP, ISO IDRP, NOVELL IPX。

【例】图所示的网络中，采用距离-向量路由算法。假设路由器 C 收到邻居发来的距离向量表，分别

为来自 B: (5, 0, 8, 12, 6, 2); 来自 D: (16, 12, 6, 0, 9, 10); 来自 E: (7, 6, 3, 9, 0, 4)。而 C 到 B、D 和 E 的距离分别为 6、3 和 5。请计算路由器 C 更新后的距离向量表以及 C 到每一个目的站点的最短路径所必须经过的下一邻居站点 (要求给出计算步骤)。【注: 假设线路是不对称的】



【答案】C 通过 B 到达每个站点的距离向量: (11, 6, 14, 18, 12, 8);

C 通过 D 到达每个站点的距离向量: (19, 15, 9, 3, 12, 13);

C 通过 E 到达每个站点的距离向量: (12, 11, 8, 14, 5, 9);

除 C 外, 对于每个目的站点取最小值可得 C 更新后的路由表为:

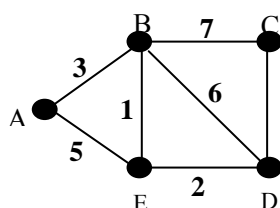
(11, 6, 0, 3, 5, 8), 对应的输出线路为: (B, B, --, D, E, B)。

【分析】对距离矢量算法的直接应用和计算, 要求掌握算法的核心。

6.2.3 链路状态路由算法

当路由器初始化或当网络结构发生变化 (例如增减路由器, 链路状态发生变化等) 时, 路由器会产生链路状态广播数据包 LSA (Link-State Advertisement), 该数据包里包含路由器上所有相连链路, 也即为所有端口的状态信息。

【例】下图是一个子网的拓扑结构及其相邻结点之间的传输延迟, 请采用 L-S 路由算法进行路由计算, 给出各结点的链路-状态报文, 并计算结点 A 的路由表。



【答案】

(1) 各结点的链路状态如下:

A:

B	3
E	5

B:

A	3
C	7
D	6
E	1

C:

B	7
D	4

D:

B	6
C	4
E	2

E:

A	5
B	1
D	2

(2) 采用 Dijkstra 算法，可以计算出结点 A 的路由表为：

线路	延迟
A	0
B	3
C	10
D	6
E	4

【分析】链路状态算法的具体应用。

6.2.4 层次路由

分层次的路由协议，其层次中最大的实体是 AS（自治系统），即遵循共同路由策略管理下的一部分网络实体。在每个 AS 中，将网络划分为不同的区域。每个区域都有自己特定的标识号。

6.3 IPv4

6.3.1 IPv4 分组



6.3.2 IPv4 地址与 NAT

1. IPv4 地址

网络号和主机号(net-id, host-id)。主机号为全 0 的网络地址定义为网络号，它标识因特网上的唯一网络。4 字节的 IP 地址，采用"点分十进制"的方法来表示，例如，202.119.224.93。每一个十进制数表示 4 个字节中的一个，排列次序从左到右。由于每个字节为 8 比特，所以每个十进制数只允许在 0~255 范围内。

2. 分类

根据因特网上的网络规模，IP 地址可分为 A 类、B 类、C 类、D 类和 E 类。

3. 特殊地址

对于因特网 IP 地址中有特定的专用地址，不作分配：

(1) 主机地址全为"0"

不论哪类网络，主机地址全为"0"表示指向本网，常用在路由表中。例如，18.0.0.0 表示其网络号为 18。

(2) 主机地址全为"1"

主机地址全为"1"表示广播地址，向特定的所在网上所有主机发送数据报。例如，IP 地址为 202.119.224.225，是要求指向 202.119.224 网上的所有主机转发数据报。

(3) 4 字节 32 比特全为"1"

若 IP 地址 4 字节 32 比特全为"1"，表示仅在本网内进行广播发送。

(4) 网络号 127

TCP/IP 协议规定网络号 127 不可用于任何网络。其中有一个特别地址：127.0.0.1 称之为回送地址 (loopback)，它将信息通过自身的接口发送后返回，可用来测试端口状态。

4. NAT

【例】以下对 IP 地址分配中描述不正确的是 ()

- A. 网络 ID 不能全为 1 或全为 0 B. 同一网络上每台主机必须有不同的网络 ID
C. 网络 ID 不能以 127 开头 D. 同一网络上每台主机必须分配唯一的主机 ID

【答案】B

【分析】同一网络上的主机必须有相同的网络 ID，因此选 B。

6.3.3 子网划分与子网掩码、CIDR

1. 子网划分

Internet 组织机构定义了五种 IP 地址，用于主机的有 A、B、C 三类地址。子网地址是借用基于类的网络地址的主机部分创建的。划分子网后，通过使用掩码，把子网隐藏起来，使得从外部看网络没有变化，这就是子网掩码。

2. 子网掩码

RFC 950 定义了子网掩码的使用，子网掩码是一个 32 位的 2 进制数，其对应网络地址的所有位都置为 1，对应于主机地址的所有位都置为 0。由此可知，A 类网络的缺省的子网掩码是 255.0.0.0，B 类网络的缺省子网掩码是 255.255.0.0，C 类网络的缺省子网掩码是 255.255.255.0。将子网掩码和 IP 地址按位进行

逻辑“与”运算，得到 IP 地址的网络地址，剩下的部分就是主机地址，从而区分出任意 IP 地址中的网络地址和主机地址。子网掩码常用点分十进制表示，我们还可以用网络前缀法表示子网掩码，即“/<网络地址位数>”。如 138.96.0.0/16 表示 B 类网络 138.96.0.0 的子网掩码为 255.255.0.0。

3. 子网划分与掩码的设置

子网划分是通过借用 IP 地址的若干位主机位来充当子网地址从而将原网络划分为若干子网而实现的。划分子网时，随着子网地址借用主机位数的增多，子网的数目随之增加，而每个子网中的可用主机数逐渐减少。

4. 子网划分的技巧

- (1) 所选择的子网掩码将会产生多少个子网?: 2^x (x 代表掩码位, 即 2 进制为 1 的部分。)
- (2) 每个子网能有多少主机?: 2^y (y 代表主机位, 即 2 进制为 0 的部分)
- (3) 有效子网是?: 有效子网号 = $256 - 10$ 进制的子网掩码 (结果叫做 block size 或 base number)
- (4) 每个子网的广播地址是?: 广播地址 = 下个子网号 - 1
- (5) 每个子网的有效主机分别是?: 忽略子网内全为 0 和全为 1 的地址剩下的就是有效主机地址. 最后有效 1 个主机地址 = 下个子网号 - 2 (即广播地址 - 1)

5. 无类别域间路由 (CIDR)

假设有一组 C 类地址为 192.168.8.0—192.168.15.0，如果用 CIDR 将这组地址聚合为一个网络，其网络地址和子网掩码应该为：

A. 192.168.8.0/21 B. 192.168.8.0/20 C. 192.168.8.0/24 D. 192.168.8.15/24

要求将 192.168.8.0—192.168.15.0 这组 C 类地址聚合为一个网络，我们先将 C 类地址的第三个八位组转换成二进制：

点分十进制 将第三个八位组转换成二进制

192.168.8.0 192.168.00001 000.0

192.168.9.0 192.168.00001 001.0

192.168.10.0 192.168.00001 010.0

192.168.11.0 192.168.00001 011.0

192.168.12.0 192.168.00001 100.0

192.168.13.0 192.168.00001 101.0

192.168.14.0 192.168.00001 110.0

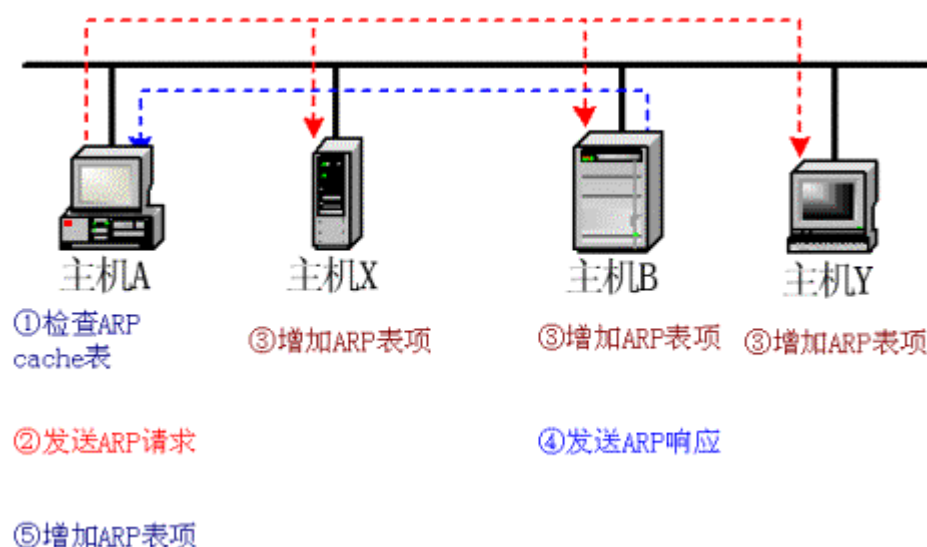
192.168.15.0 192.168.00001 111.0

从上表中可以看出，只要将网络位的低三位划分出来作为主机位，这些 C 类地址就被聚合在一个网络之中。因此，聚合后的网络地址应该为 192.168.8.0/21，正确答案为 A。主机地址只代表一个主机，只有网络地址才有聚合的意义。

6.3.4 ARP 协议、DHCP 协议与 ICMP 协议

1. ARP 协议

如下图所示，假设在一个以太网上的 4 台计算机，分别是计算机 A、B、X 和 Y，通过 TCP/IP 协议进行通信，那么双方的数据链路层必须知道对方的 MAC 地址。每台计算机都要在各自的高速缓存区中存放一张 IP 地址到 MAC 地址的转换表，称 ARP 表。其中存放着最近用到的一系列和它通信的同一子网的计算机的 IP 地址和 MAC 地址的映射。在主机初始启动时，ARP 表为空。现在源端计算机 A（IP 地址为 192.168.3.1）要和 IP 地址为 192.168.3.2 的计算机 B 通信。在计算机 A 发送信息前，必须首先得到计算机 B 的 IP 地址与 MAC 地址的映射关系。ARP 协议工作过程如下：



完整的 ARP 工作过程

（1）主机 A 首先查看自己的高速缓存中的 ARP 表，看其中是否有与 192.168.3.2 对应的 ARP 表项。如果找到，则直接利用该 ARP 表项中的 MAC 值把 IP 数据包封装成帧发送给主机 B。

（2）主机 A 如果在 ARP 表中找不到对应的地址项，则创建一个 ARP 请求数据包，并以广播方式发送（把以太网帧的目的地址设置为 FF-FF-FF-FF-FF-FF）。包中有需要查询的计算机的 IP 地址（192.168.3.2），以及主机 A 自己的 IP 地址和 MAC 地址。

（3）包括计算机 B 在内的属于 192.168.3.0 网络上的所有计算机都收到 A 的 ARP 请求包，然后将计

计算机 A 的 IP 地址与 MAC 地址的映射关系存入各自的 ARP 表中。

(4) 计算机 B 创建一个 ARP 响应包，在包中填入自己的 MAC 地址，直接发送给主机 A。

(5) 主机 A 收到响应后，从包中提取出所需查询的 IP 地址及其对应的 MAC 地址，添加到自己的 ARP 表中。并根据该 MAC 地址所需要发送的数据包封装成帧发送出去。

ARP 表的内容是定期更新的，如果一条 ARP 表项很久没有使用了，则它将被从 ARP 表中删除。

2. DHCP 协议

DHCP discover: 此为 client 开始 DHCP 过程中的第一个请求报文

DHCP offer: 此为 server 对 DHCP discover 报文的响应

DHCP request: 此为 client 对 DHCP offer 报文的响应

DHCP decline: 当 client 发现 server 分配给它的 IP 地址无法使用，如 IP 地址发生冲突时，将发出此报文让 server 禁止使用这次分配的 IP 地址。

DHCP ack: server 对 DHCP request 报文的响应，client 收到此报文后才真正获得了 IP 地址和相关配置信息。

DHCP nak: 此报文是 server 对 client 的 DHCP request 报文的拒绝响应，client 收到此报文后，一般会重新开始 DHCP 过程。

DHCP release: 此报文是 client 主动释放 IP 地址，当 server 收到此报文后就可以收回 IP 地址分配给其他的 client。

3. ICMP 协议

1、拥塞

(1) 什么是拥塞？路由器被大量涌入的 IP 数据报“淹没”的现象

(2) 拥塞产生的原因

路由器的处理速度太慢，不能完成数据报排队等日常工作

路由器传入数据速率大于传出数据速率。

(3) 拥塞控制：源站抑制

利用 ICMP 源抑制报文抑制源主机发送数据报的速率

2、发送源站抑制报文策略

路由器的某输出队列溢出后，抛弃新来的数据报，发送 ICMP 源抑制报文

为路由器的输出队列设置阈值，超过阈值后抛弃新来的数据报，发送 ICMP 源抑制报文

有选择地抑制 IP 数据报发送率较高的源主机

接收源站抑制报文

收到源抑制报文后，源主机可以降低发送 IP 数据报的速率

注意：拥塞解除后路由器不主动通知源主机

3、ICMP 重定向机制

主机在启动时具有一定的路由信息，但不一定是最优的

路由器检测到 IP 数据报经非优路由传输，就通知主机去往该目的地的最优路径

功能：保证主机拥有动态的、既小且优的路由表

ICMP 重定向机制只能在同一网络的路由器与主机之间使用

4、回应请求与应答

测试目的主机或路由器的可达性

5、时戳请求与应答

获取其他设备的当前时间

6、掩码请求与应答

从路由器获取本网的子网掩码

6.4 IPv6

6.4.1 IPv6 的主要特点

1. 全新的报文结构
2. 巨大的地址空间
3. 全新的地址分配方式
4. 对 QOS 更好的支持
5. 内置的安全性
6. 全新的邻居发现协议
7. 可扩展性
8. 移动性

6.4.2 IPv6 地址

6.5 路由协议

6.5.1 自治系统

自治系统是由同一个技术管理机构管理、使用统一选路策略的一些路由器的集合。AS 内部运行内部网关协议（IGP），AS 之间运行外部网关协议（EGP）。

【例】在自治系统内部实现路由器间自动传播可达信息、进行路由选择的协议称为（ ）

- A. EGP B. BGP C. IGP D. GGP

【答案】C

【分析】对自治系统中路由的概念考察，要求位系统内部，所以答案为 C。

6.5.2 域内路由与域间路由

当前 Internet 被划分为多个自治系统，自治系统是一个实体，一般是指隶属于一个管理机构的路由器集合。每个自治系统可以制定自己的路由策略。自治系统内部的路由器通过域内路由协议彼此交换路由信息，一般域内路由协议分为距离向量协议和链路状态协议，前者以 RIP 代表，后者常用的有 OSPF、IS-IS 协议；自治系统边界路由器通过域间路由协议交换路由信息，目前 Internet 上的域间路由协议事实标准是 BGP-4 协议。

6.5.3 RIP 路由协议

RIP (Routing Information Protocol) 路由协议就是一种动态路由协议，它采用距离矢量算法，距离矢量算法就是相邻的路由器之间互相交换整个路由表，并进行矢量的叠加，最后达到知道整个网络路由。它通过 UDP 报文交换路由信息，每隔 30 秒向外发送一次更新报文。如果路由器经过 180 秒没有收到来自对端的路由更新报文，则将所有来自此路由器的路由信息标记为不可达，若在其后 120 秒内仍未收到更新报文，就将这些路由从路由表中删除。

6.5.4 OSPF 路由协议

1. 基本原理

2. 最小生成树算法

Dijkstra 算法举例：

下面我们以路由器 A 为例，来说明最短路径树的建立过程：

(1) 路由器 A 找到了路由器 B、C，将它们列入候选列表 {B: 1; C: 2}。

(2) 从候选列表中找出最小代价项 B，将 B 加入最短路径树并从候选列表中删除。接着从 B 开始寻找，找到了 D，将其放入候选列表 {C: 2; D: 2}。

(3) 从列表中找出 C，再由 C 又找到了 D。但此时 D 的代价为 4，所以不再加入候选列表。最后将 D 加入到最短路径树。此时候选列表为空，完成了最短路径树的计算。

6.5.5 BGP 路由协议

BGP (Border Gateway Protocol) 是一种自治系统间的动态路由协议，它的基本功能是在自治系统间自动交换无环路的路由信息，通过交换带有自治系统号 (AS) 序列属性的路径可达信息，来构造自治区域的拓扑图，从而消除路由环路并实施用户配置的路由策略。与 OSPF 和 RIP 等在自治区域内部运行的协议对

应, BGP 是一类 EGP (Exterior Gateway Protocol) 协议, 而 OSPF 和 RIP 等为 IGP (Interior Gateway Protocol) 协议。

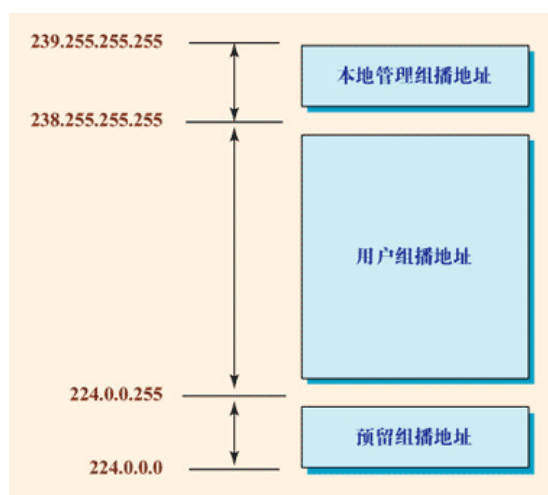
6.6 IP 组播

6.6.1 组播的概念

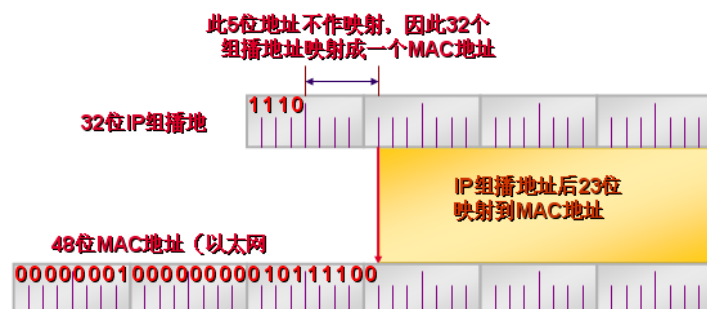
组播技术是 IP 网络数据传输三种方式之一, 在介绍 IP 组播技术之前, 先对 IP 网络数据传输的单播、组播和广播方式做一个简单的介绍:

6.6.2 IP 组播地址

1. 组播地址



2. 组播 MAC 地址



6.7 移动 IP

6.7.1 移动 IP 的概念

Mobile IP 是为了满足移动节点在移动中保持其连接性而设计的。Mobile IP 现在有两个版本，简单的说，移动 IP 是一种计算机网络通信协议，它能够保证计算机在移动过程中在不改变现有网络 IP 地址、不中断正在进行的网络通信及不中断正在执行的网络应用的情况下实现对网络的不间断访问。

6.7.2 移动 IP 的通信过程

- ① 代理发现 (Agent Discovery)
- ② 转交地址注册/取消注册 (Registration/Deregistration)
- ③ 数据的收发

6.8 网络层设备

6.8.1 路由器的组成和功能

6.8.2 路由表与路由转发

“转发” (forwarding) 就是路由器根据转发表将用户的 IP 数据报从合适的端口转发出去。

“路由选择” (routing) 则是按照分布式算法，根据从各相邻路由器得到的关于网络拓扑的变化情况，动态地改变所选择的路由。

1、主机 A 发送 IP 数据报

- (1) 构造目的地址为 B 的 IP 数据报
- (2) 对 IP 数据报进行路径选择：路由选择算法、IP 路由表
- (3) 决定将 IP 数据报传递到路由器 R2(如何发送到路由器 R)

主机 A 怎样将数据报发送给下一路由器呢？

在发送数据报之前，主机 A 调用 ARP 解析软件得到下一默认路由器 R1 的 IP 地址和 MAC 地址的映射关系，然后以该 MAC 地址为帧的目的地址形成一个帧，并将 IP 数据报封装在帧的数据区：帧 IP 数据报为帧的数据区，最后由具体的物理网络（以太网）完成数据报的真正传输。

2、路由器 R2 处理和转发 IP 数据报

- (1) 路由器 R2 收到主机 A 发送给它的帧，去掉帧头，将 IP 数据报交给 IP 软件处理。

考虑： 路由器如何接受数据帧？

IP 软件对 IP 数据报进行了何种处理？

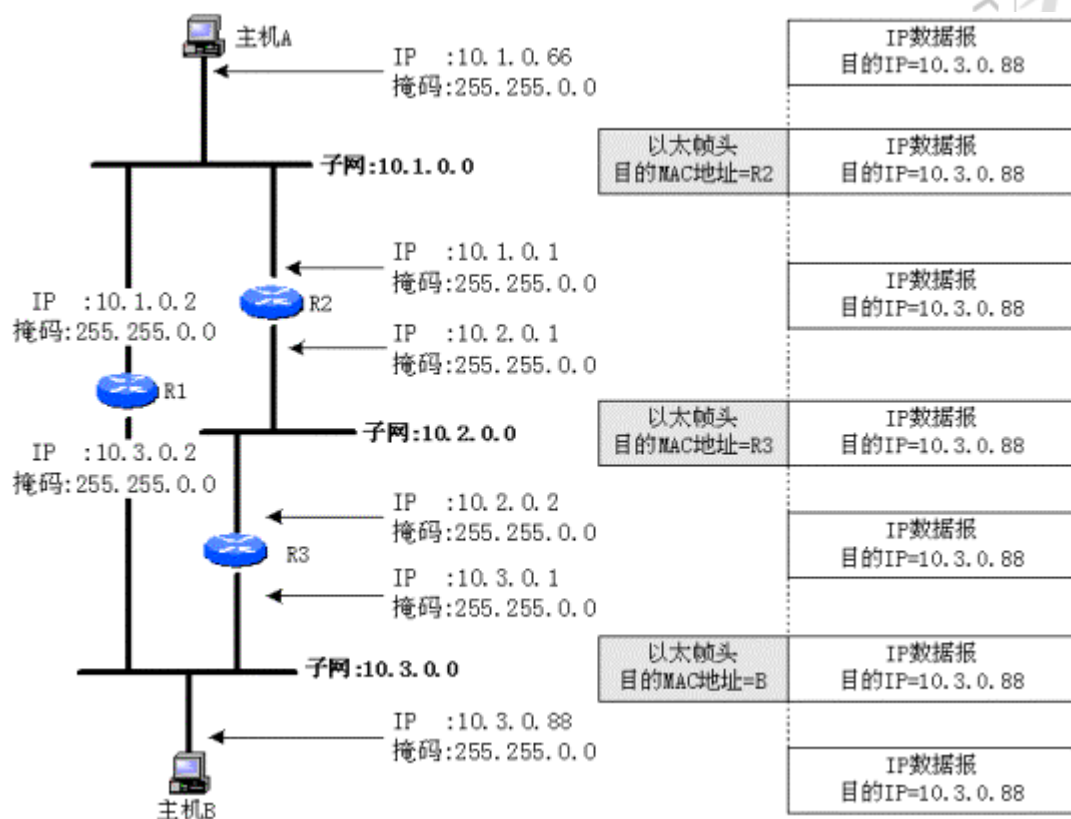
- (2) 对 IP 数据报进行路径选择：路由选择算法、IP 路由表
- (3) 决定将 IP 数据报传递到路由器 R2(如何发送到路由器 R)
- (4) 如何发送，同上

3、路由器 R3 处理和转发 IP 数据报

- (1) 路由器 R3 收到路由器 R2 发送给它的帧，去掉帧头，将 IP 数据报交给 IP 软件处理。
- (2) 对 IP 数据报进行路径选择：路由选择算法、IP 路由表
- (3) 决定将 IP 数据报直接投递到 10.3.0.0
- (4) 如何发送，同上

4、主机 B 接收 IP 数据报

- (1) 主机 B 收到路由器 R3 发送给它的帧，去掉帧头，将 IP 数据报交给 IP 软件处理。
- (2) 对 IP 数据报进行路径选择：路由选择算法、IP 路由表
- (3) 决定将 IP 数据报中的数据信息送交高层处理



IP 数据报在互联网中传输与处理过程

第七章 传输层

7.1 传输层提供的服务

7.1.1 传输层的功能

(1) 提高服务质量 (2) 多路复用 (3) 分段与重新组装。

7.1.2 传输层寻址与端口

硬件端口是不同硬件设备进行交互的接口，而软件端口是应用层的各种协议进程与传输实体进行层间交互的一种地址。

7.1.3 无连接服务与面向连接服务

面向连接服务就是在数据交换之前，必须先建立连接，当数据交换结束后，则应该终止这个连接。在无连接服务的情况下，两个实体之间的通信不需要先建立好一个连接，因此其下层的有关资源不需要事先进行预定保留，这些资源是在数据传输时动态地进行分配的。

7.2 UDP 协议

7.2.1 UDP 数据报

7.2.2 UDP 校验

【例】对 UDP 数据报描述不正确的是 ()

- A. 是无连接的 B. 是不可靠的 C. 不提供确认 D. 提供消息反馈

【答案】D

【分析】从 UDP 的首部字段和校验方法可知其不能提供消息反馈。

7.3 TCP 协议

7.3.1 TCP 段

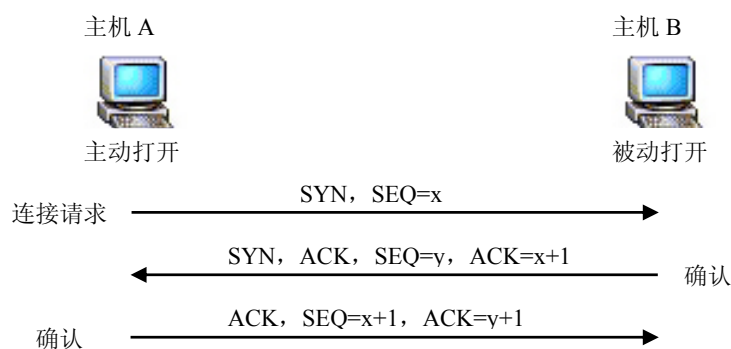
【例】在 TCP 分段中不包括的信息是 ()

- A. Source Port , Destination Port B. Sequence Number , Acknowledgment Number
C. 头部、数据区和伪包头校验和 D. 源 IP 地址和目的 IP 地址

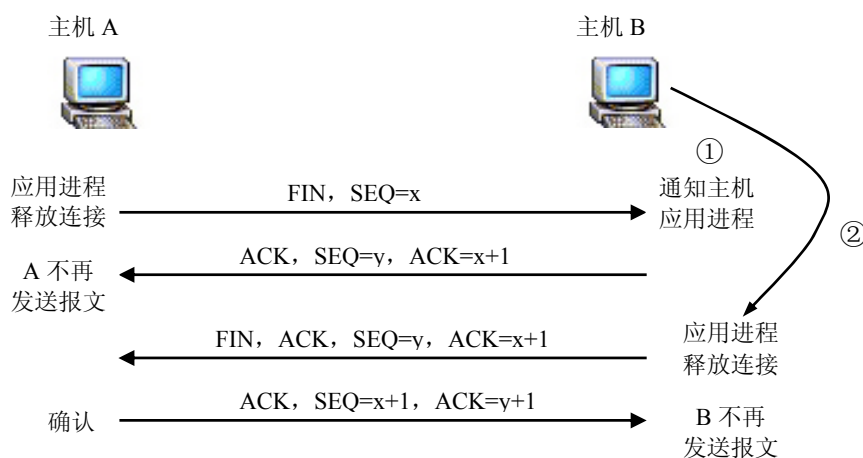
【答案】D

【分析】基本概念题，IP 地址的处理是网络层的主要功能，因此在 TCP 报文中不出现。

7.3.2 TCP 连接管理



TCP 连接的建立



TCP 连接释放过程

7.3.3 TCP 可靠传输

1 TCP 的编码和确认

2 TCP 的糊涂窗口综合症和 Nagle 算法

3 TCP 的超时与重传

重传计时器：为了控制丢失的或丢弃的报文段，TCP 使用了处理报文段的确认的等待重传时间的重传计时器。

坚持计时器：TCP 为每一个连接使用一个坚持计时器；当发送方的 TCP 收到一个窗口大小为零的确认时，就需要启动坚持计时器；当坚持计时器期限到时，发送方的 TCP 就发送一个特殊的探测报文段。

保持计时器：保持计时器又叫做激活计时器，它是用来防止在两个 TCP 之间的连接处以长时期空闲。

时间等待计时器：时间等待计时器是在连接终止期间使用的；当 TCP 关闭一个连接时，它并不认为这个连接马上就真正地关闭了。在时间等待期间中，连接还处于一种过渡状态；时间等待计时器的值

通常设置为一个报文段的寿命期待值的两倍。

重传计时器：为了控制丢失的或丢弃的报文段，TCP 使用了处理报文段的确认的等待重传时间的重传计时器。

坚持计时器：TCP 为每一个连接使用一个坚持计时器；当发送方的 TCP 收到一个窗口大小为零的确认时，就需要启动坚持计时器；当坚持计时器期限到时，发送方的 TCP 就发送一个特殊的探测报文段。

7.3.4 TCP 流量控制与拥塞控制

1 TCP 的滑动窗口机制

【例】TCP 连接建立的过程中，收发双方协商初始的窗口大小是 10B，要传输的数据为 30B，依次编号为 1-30，请回答如下问题：

- (1) 发送开始时，那些序号的报文不可发送。
- (2) 序号 1~5 的报文已经被确认，那些序号的报文不可发送。
- (3) 序号 5~10 的报文发生的确认，并且接收端通知窗口大小为 15B，那些序号的报文不可发送。

【分析】(1) 在连接建立的过程中，收发双方协商初始的窗口大小是 10B，那么发送端将自己的发送窗口定为 10，即序号 1~10 的报文可以在没有接收到确认的情况下连续地发送出去。发送开始时，窗口的指针在序号 1 的第一个字节位置，序号 1~10 的报文可以连续发送，而序号 11~30 的报文不可发送，如图 1 所示。

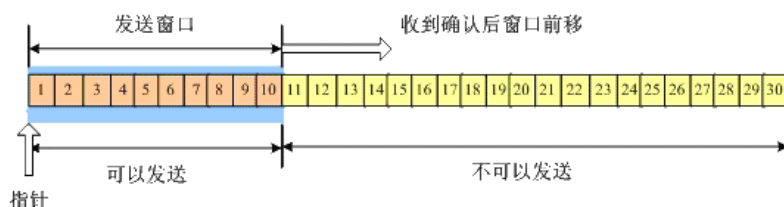


图 1 发送窗口大小为 10B

(2) 如图 2 所示，由于已经发送了序号 1~10 的报文，并且序号 1~5 的报文已经得到接收端的确认，因此，在窗口大小不变的情况下，平移到序号 6~15 的位置，指针滑动到 11 的位置。表明，已经发送了 10B，其中序号 1~5 的报文已经被确认，序号 6~15 的报文已发送的数据等待对方确认，可以继续发送 11~15 的报文。

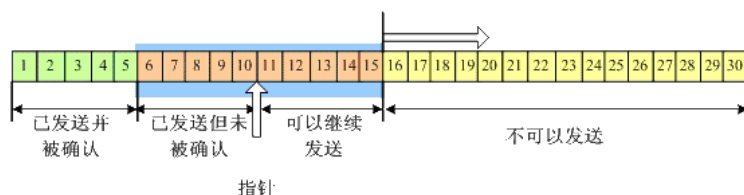


图 2 发送 10B,收到的确认序号为 6, 窗口大小不变, 还可继续发送 10B

(3) 如图 3 所示,。因此窗口的位置平移到序号 11~25 的位置。同时由于这一段时间没有发送新的数据段, 因此指针仍然在 11 的位置。表明, 已经发送的序号为 10 的报文已经被确认, 可以继续发送序号 11~15 的报文。

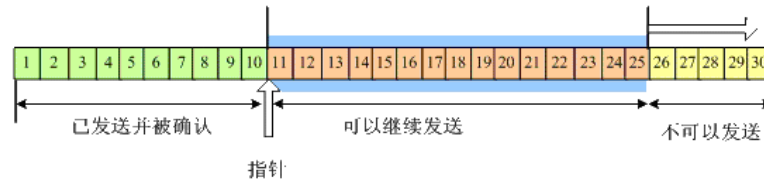


图 3 收到的确认序号为 11, 窗口增大为 15, 还可发送 15B

2 TCP 的慢启动和拥塞避免

针对 TCP 拥塞控制, 重点掌握慢启动, 具体步骤如下:

- (1) TCP 连接初始化。设置拥塞窗口初值, 不能大于 2 个报文段, 一般 $Cwnd=1MSS$; 设置慢启动门限初值 ($Cwnd$ 为拥塞窗口)。
- (2) TCP 开始发送过程, 发送窗口 $swnd$ 按式 $swnd=\min(Cwnd, rwnd)$ 计算, 一般, 通告窗口 $rwnd$ 足够大, 实际上, $swnd=Cwnd$ 。
- (3) 每次传输都调节一次拥塞窗口, 从而调节了发送窗口。 $Cwnd$ 从初值 1 开始, 每收到一个对新报文段的确认 ACK, $Cwnd=Cwnd+1$ 。这样, 第 1 次传输完, 收到 1 个 ACK, $Cwnd$ 增加到 2; 第 2 次传输完, 收到 2 个 ACK, $Cwnd$ 增加到 4; ...。因此, $Cwnd$ 按指数规律增长, 即每传输 1 次, $Cwnd$ 加倍。直到 $Cwnd>sssthresh$ (其中 $sssthresh$ 为慢启动门限), 进入拥塞避免。
- (4) 当在某时刻发生了拥塞, 则置 $sssthresh=\max(swnd/2, 2)$, 即将 $sssthresh$ 降到拥塞发生时 $swnd$ 的一半, 但不能小于 2, 并令 $Cwnd=1$, 开始慢启动过程。

说明: “慢启动”指每出现一次超时, 拥塞窗口降低到 1, 使报文慢慢注入网络;

“加速递减”指每出现一次超时, 就将门限窗口值减半;

“拥塞避免”指超过门限窗口后指数增长率降为线性增长率。

慢的含义: 不是指拥塞窗口增长速率慢, 而是使发送端在开始发送时向网络注入的分组数大大减少。

拥塞窗口的单位是: 报文段的个数, 而不是字节数。

3、超时重传时间的选择

重传机制是 TCP 中最重要和最复杂的问题之一。TCP 每发送一个报文段, 就对这个报文段设置一次计时器。只要计时器设置的重传时间到但还没有收到确认, 就要重传这一报文段。

- (1) 往返时延的方差很大, 由于 TCP 的下层是一个互联网环境, IP 数据报所选择的路由变化很大。

因而运输层的往返时间的方差也很大。

(2) 加权平均往返时间

TCP 保留了 RTT 的一个加权平均往返时间 RTTS (这又称为平滑的往返时间)。

第一次测量到 RTT 样本时, RTTS 值就取为所测量到的 RTT 样本值。以后每测量到一个新的 RTT

样本, 就按下式重新计算一次 RTTS:

新的 $RTTS = (1 - \alpha) \times (\text{旧的 } RTTS) + \alpha \times (\text{新的 RTT 样本})$

式中, $0 \leq \alpha < 1$ 。若 α 很接近于零, 表示 RTT 值更新较慢。若选择 α 接近于 1, 则表示 RTT 值更新较快。RFC 2988 推荐的 α 值为 1/8, 即 0.125。

(3) 超时重传时间 RTO

RTO 应略大于上面得出的加权平均往返时间 RTTS。

RFC 2988 建议使用下式计算 RTO: $RTO = RTTS + 4 \times RTTD$

RTTD 是 RTT 的偏差的加权平均值。RFC2988 建议这样计算 RTTD。第一次测量时, RTTD 值取为测量到的 RTT 样本值的一半。在以后的测量中, 则使用下式计算加权平均的 RTTD:

新的 $RTTD = (1 - \beta) \times (\text{旧的 } RTTD) + \beta \times |RTTS - \text{新的 RTT 样本}|$

β 是个小于 1 的系数, 其推荐值是 1/4, 即 0.25。

(3) Karn 算法

在计算平均往返时间 RTT 时, 只要报文段重传了, 就不采用其往返时间样本。这样得出的加权平均往返时间 RTTS 和超时重传时间 RTO 就较准确。

(4) 修正的 Karn 算法

报文段每重传一次, 就把 RTO 增大一些: 新的 $RTO = \gamma \times (\text{旧的 } RTO)$ 系数 γ 的典型值是 2。

当不再发生报文段的重传时, 才根据报文段的往返时延更新平均往返时延 RTT 和超时重传时间 RTO 的数值。实践证明, 这种策略较为合理。

3 快重传和快恢复。

第八章 应用层

8.1 网络应用模型

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 方式和对等方式（P2P 方式）即 Peer-to-Peer 方式。

8.1.1 客户/服务器模型

客户(client)和服务器(server)都是指通信中所涉及的两个应用进程。客户服务器方式所描述的是进程之间服务和被服务的关系。客户是服务的请求方，服务器是服务的提供方

8.1.2 P2P 模型

对等连接(peer-to-peer，简称为 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。

8.2 DNS 系统

8.2.1 层次域名空间

域名采用分层次方法命名，每一层都有一个子域名，子域名之间用点号分隔。具体格式如下：主机名·网络名·机构名·最高层域名

【例】域名服务系统（DNS）中，顶级域名 COM 代表的是（）

- A. 商业组织 B. 教育机构 C. 政府机构 D. 国家代码

【答案】A

【分析】考察域名系统中第一级域名的含义。

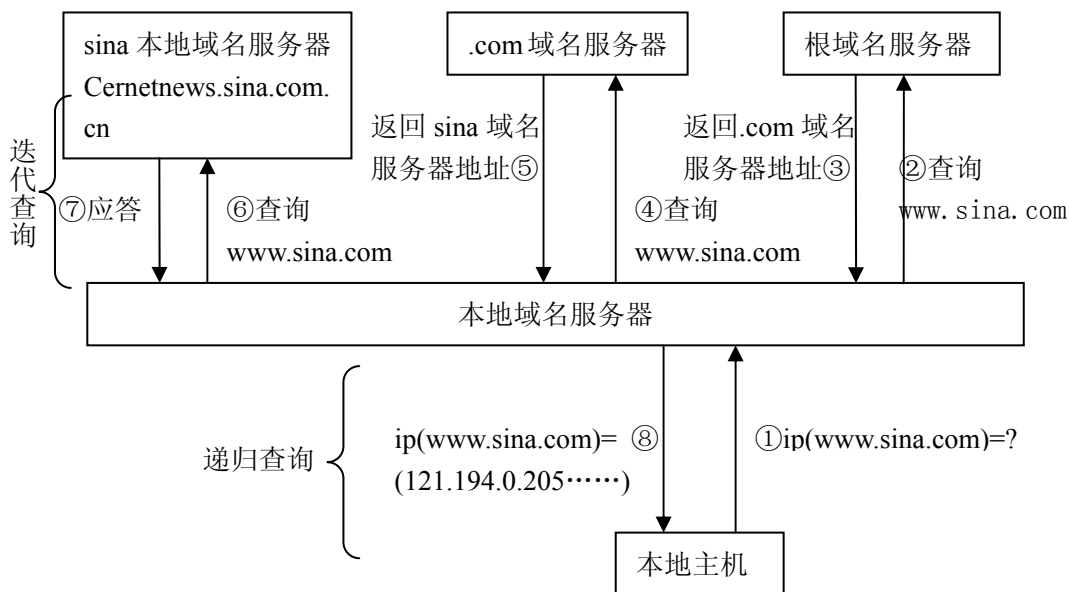
8.2.2 域名服务器

域名服务系统的主要功能是定义一套为机器取域名的规则，把域名高效率地转换成 IP 地址。域名服务系统是一个分布式的数据库系统，由域名空间、域名服务器和地址转换请求程序三部分组成。

根域名服务器。顶级域名服务器。权限域名服务器。本地域名服务器。

8.2.3 域名解析过程

图详细描述了解析 www.sina.com 的过程，基本分为八个步骤，其中第一步和最后一步为递归查询，其余为迭代查询的过程。



【例】域名服务 DNS 的正向解析是（ ）

- A. 将域名转换为物理地址
- B. 将域名转换为 IP 地址
- C. 将 IP 地址转换为物理地址
- D. 将 IP 地址转换为域名

【答案】B

【分析】DNS 的基本概念题，明确 DNS 的主要功能。

8.3 FTP

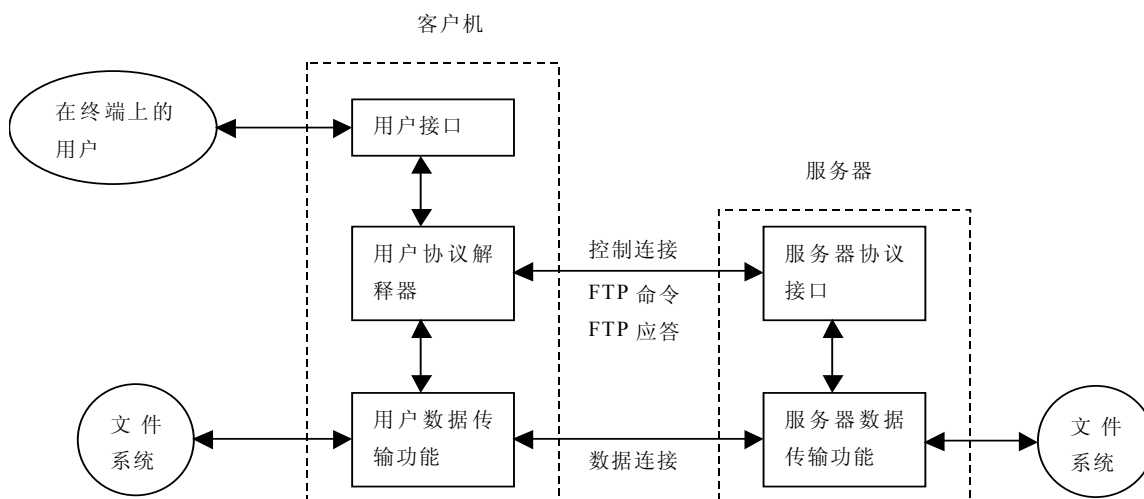
8.3.1 FTP 协议的工作原理

文件传送协议特点：

- (1) FTP 只提供文件传送的一些基本的服务，它使用 TCP 可靠的传输服务。
- (2) FTP 使用客户服务器方式。一个 FTP 服务器进程可同时为多个客户进程提供服务。

8.3.2 控制连接与数据连接

它采用两个 TCP 连接来传输一个文件，它们是控制连接和数据连接。图是工作原理的图示。



8.4 电子邮件

8.4.1 电子邮件系统的组成结构

在因特网上发送和接收电子邮件，实际并不是直接在发送方和接收方的计算机之间传送的，而是通过因特网服务提供商（Internet Service Provider, ISP）的邮件服务器（全天 24 小时都运行）作为代理环节实现的。

8.4.2 电子邮件格式与 MIME

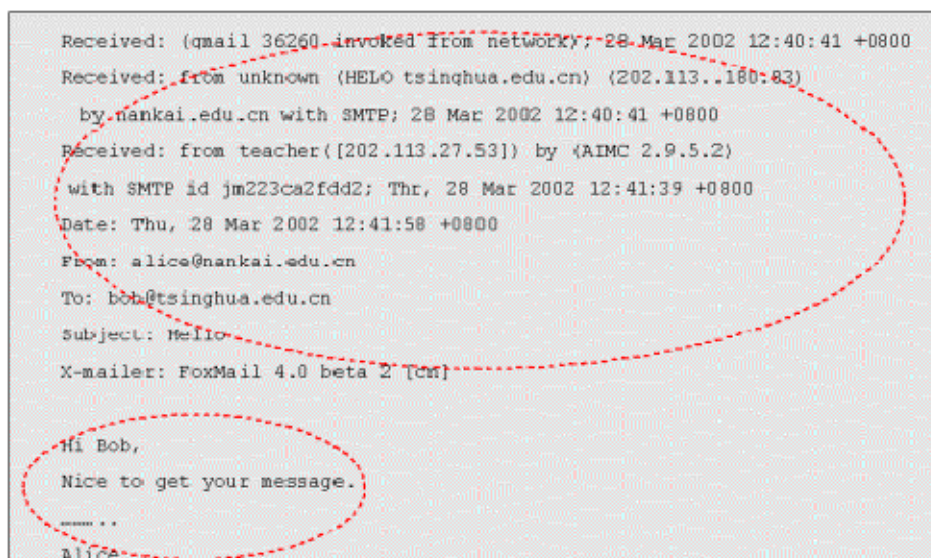
RFC822 和多用途因特网邮件扩展协议 MIME 对电子邮件的报文格式做出了具体规定。

1、电子邮件报文的组成

(1) 邮件头：邮件报文的控制信息，邮件头由多行组成，每行的基本语法：<keyword>: <value>。

(2) 邮件体：用户需要发送的邮件内容，RFC822 规定邮件体由 7 位 ASCII 字符串组成。

邮件头和邮件体之间用空行分隔。RFC822 对邮件的最大限制是邮件体由 7 位 ASCII 文本，而且 SMTP 中又规定传输邮件时将 8 位字节的高位清 0。因此，RFC822 邮件格式继续扩充。



```
Received: (qmail 36260 invoked from network); 28 Mar 2002 12:40:41 +0800
Received: from unknown (HELO tsinghua.edu.cn) (202.113.180.83)
    by nankai.edu.cn with SMTP; 28 Mar 2002 12:40:41 +0800
Received: from teacher([202.113.27.53]) by (AIMC 2.9.5.2)
    with SMTP id jm223ca2fdd2; Thu, 28 Mar 2002 12:41:39 +0800
Date: Thu, 28 Mar 2002 12:41:58 +0800
From: alice@nankai.edu.cn
To: bob@tsinghua.edu.cn
Subject: Hello
X-mailer: FoxMail 4.0 beta 2 [cn]

Hi Bob,
Nice to get your message.
-----
Alice
```

The image shows an email header and body. A red dashed circle highlights the header information, including the 'Received' lines, 'Date', 'From', 'To', 'Subject', and 'X-mailer' fields. Another red dashed circle highlights the body text, which starts with 'Hi Bob,' and 'Nice to get your message.', followed by a separator line and the name 'Alice'.

图 13.5 收件人收到的邮件示例

多用途因特网邮件扩展协议 MIME

1、MIME 解决的主要问题：多媒体等二进制信息能够利用电子邮件传输。

2、MIME 的基本思想：MIME 是对 RFC822 进行了扩充。MIME 继承了 RFC822 的基本邮件头和邮件体模式，增加了一些邮件头字段，并要求对邮件体进行编码（将 8 位的二进制信息变换成 7 位的 ASCII 文本）。

MIME 主要增加的邮件头字段：

- MIME-Version：表明该邮件遵循 MIME 标准的版本号。目前的主要标准为 1.0。

- Content-Type：指出邮件体包含的数据类型。7 种类型为：text、message、image、audio、video、application 和 multipart。

- Content-Transfer-Encoding：指出邮件体的数据编码类型：quoted-printable 和 base64。

```

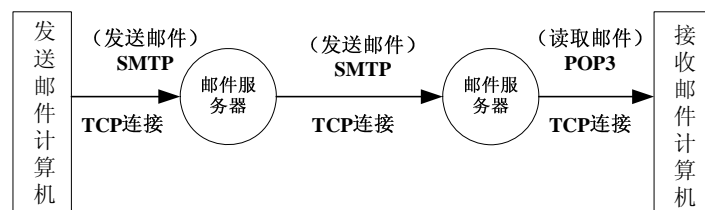
Received: (qmail 36260 invoked from network); 28 Mar 2002 12:40:41 +0800
Received: from unknown (HELO tsinghua.edu.cn) (202.113.160.83)
  by nankai.edu.cn with SMTP; 28 Mar 2002 12:40:41 +0800
Received: from teacher ([202.113.27.53]) by (AIMC 2.9.5.2)
  with SMTP id jn223ca2fd42; Thu, 28 Mar 2002 12:41:39 +0800
Date: Thu, 28 Mar 2002 12:41:58 +0800
From: alice@nankai.edu.cn
To: bob@tsinghua.edu.cn
Subject: Nice Picture
X-mailer: FoxMail 4.0 beta 2 [cn]
MIME-Version: 1.0
Content-Type: image/bmp
Content-Transfer-Encoding: base64

Qk34BAAAAAAAAAHYAAAAcAAAAAAADAAAAEAAQAAAAAAAAAADDDgAAw6AAAAAAAAAAAAAAAA
AAAAGAAgAAAAICAAIAAAACAAIAAgIAAAICAgADAwMAAAAD/ AAD/ AAAA/ / 8A/ wAAPEA/ wD/ / wAA
///AEREREEREzMREREREzMRERERMREEREREzMRERERMREERERExEEREEREzMRERETMRERE
REMREREREzMREREREzMREREREzMREREREzMREREREzMREREREzMREREREzMREREREzMRERERE
-----

```

使用 MIME 格式的电子邮件

8.4.3 SMTP 协议与 POP3 协议



简单邮件传输协议 SMTP

1、SMTP 的最大特点：简单、直观。

它只规定发送程序和接收程序之间的命令和应答，SMTP 协议中定义 命令和响应都是可读的 ASCII 字符串。

2、SMTP 邮件传输采用客户—服务器模式。

3、SMTP 服务器在 TCP 的 25 端口 守候。

常用的 SMTP 命令

命令	描述
HELO <主机域名>	开始会话
MAIL FROM: <发送者电子邮件地址>	开始一个邮递处理, 指出邮件发送者
RCPT TO: <接收者电子邮件地址>	指出邮件接收者
DATA	接收程序将 DATA 命令后面的数据作为邮件内容处理, 直到<CR><LF>.<CR><LF>出现
RSET	中止当前的邮件处理
NOOP	无操作
QUIT	结束会话

常用的 SMTP 响应

命令	描述
220	域服务准备好
221	系统状态或系统帮助应答
250	请求的命令成功完成
354	可以发送邮件内容
500	语法错误, 命令不能识别
502	命令未实现
550	邮箱不可用

SMTP 响应以 3 位数字开始, 后面跟有该响应的具体描述

SMTP 邮件传递过程分为 3 个阶段:

- (1) 连接建立阶段
- (2) 邮件传递阶段
- (3) 连接关闭阶段

发送方与接收方的交互过程	命令和响应解释	阶段
S: 220 Tsinghua.edu.cn C: HELO nankai.edu.cn S: 250 tsinghua.edu.cn	“我的域名是 tsinghua.edu.cn” “我的域名是 nankai.edu.cn” “好的, 可以开始邮件传递了”	连接建立
C: MAIL FROM: <alice@nankai.edu.cn> S: 250 OK C: RCPT TO: <bob@tsinghua.edu.cn> S: 250 OK C: DATA S: 354 Go ahead C: 邮件的具体内容..... C: C: <CR><LF>.<CR><LF> S: 250 OK	“邮件来自 alice@nankai.edu.cn” “知道了” “邮件发往 bob@tsinghua.edu.cn” “知道了” “准备好接收, 要发送邮件具体内容了” “没问题, 可以发送” 发送方发送邮件的具体内容..... “发送完毕” “好的, 都接收到了”	邮件传递
C: QUIT S: 221	“可以拆除连接了” “好的, 马上拆除”	连接关闭

注: S—服务器, C—客户, <CR>—回车, <LF>—换行

图 13.3 SMTP 通信过程示例

邮局协议 POP3

- 1、POP3 的主要功能：允许用户通过本地主机动态检索邮件服务器上的邮件
- 2、POP3 传输采用客户-服务器工作模式
- 3、POP 服务器在 TCP 的 110 端口守候
- 4、POP3 的命令和响应采用 ASCII 字符串形式

常用的 POP3 命令

命令	描述
USER <用户邮箱名>	客户机希望操作的电子邮箱
PASS <口令>	用户邮箱的口令
STAT	查询报文总数和长度
LIST [<邮件编号>]	列出报文的长度
RETR <邮件编号>	请求服务器发送指定编号的邮件
DELE <邮件编号>	对指定编号的邮件作删除标记
NOOP	无操作
RSET	复位操作，清除所有删除标记
QUIT	删除具有“删除”标记的邮件，关闭连接

POP3 的响应的两种基本类型：

- (1) 以 “+OK” 开始：命令已成功执行或服务器准备就绪等。
- (2) 以 “-ERR” 开始：错误的或不可执行的命令。

“+OK” 和 “-ERR” 后可以跟有附加信息，响应信息包含多行时，只包含 “.” 的行表示响应结束。

POP3 传输过程的 3 个阶段：

- (1) 认证阶段
- (2) 事务处理阶段
- (3) 更新阶段

发送方与接收方的交互过程	命令和响应解释	阶段
S: +OK POP3 mail server ready	“我是 POP3 服务器，可以开始了”	认证阶段
C: USER bob	“我的邮箱名是 bob”	
S: +OK bob is welcome here	“欢迎到这里检索你的邮箱”	
C: PASS *****	“我的密码是*****”	
S: +OK bob's maildrop has 2 messages (320 octets)	“你邮箱中有两个邮件，320 字节”	
发送方与接收方的交互过程	命令和响应解释	阶段
C: STAT	“邮箱中信件总数和总长度是多少？”	事务处理阶段
S: +OK 2 320	“2 个信件，320 字节”	
C: LIST	“请列出每个信件的长度”	
S: +OK 2 messages	“总共 2 个信件”	
S: 1 120	“第 1 个 120 字节”	
S: 2 200	“第 2 个 200 字节”	
S: .	“结束了”	
C: RETR 1	“请发送第 1 个信件给我”	
S: +OK 120 octets	“该信件 120 字节”	
S: 第 1 封邮件内容.....	第 1 封信件的具体内容.....	
S: .	“发完了”	
C: DELE 1	“删除第 1 个信件”	
S: +OK message 1 deleted	“好的，已为第 1 个信件作了删除标记”	
C: RETR 2	“请发送第 2 个信件给我”	
S: +OK 200 octets	“该信件 200 字节”	
S: 第 2 封邮件内容.....	第 2 封信件的具体内容.....	
S: .	“发完了”	
C: DELE 2	“删除第 2 个信件”	
发送方与接收方的交互过程	命令和响应解释	阶段
C: QUIT	“可以拆除连接了”	更新阶段
S: +OK POP3 mail server signing off (maildrop empty)	“已经将作过删除标记的邮件全部删除”	

POP3 传输过程举例

8.5 WWW

8.5.1 WWW 的概念与组成结构

8.5.2 HTTP 协议

HTTP：超文本传输协议。

HTTP 是一个简单的 ASCII 码协议。客户端只要与服务器的 80 端口建立一个 TCP 连接，就能够通过几条 HTTP 命令进行直接会话。这些命令包括：

GET：请求 WEB 服务器发送一个页面。如：GET/hypertext/www/project.html

HEAD：请求服务器仅发送一个页面的头部信息（如修改时间、大小等）

PUT：向服务器写入一页。用于远程建立 www 网页。

POST：向网页中添加数据。

DELETE：删除网页。

LINK 和 UNLINK：在已存的页面之间建立或解除连接。

HTTP/1.1 协议使用持续连接。

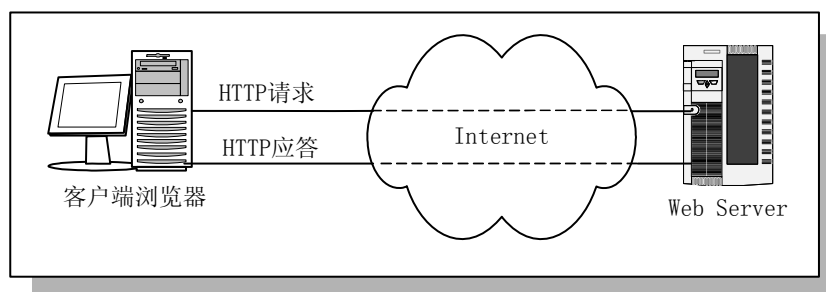
万维网服务器在发送响应后仍然在一段时间内保持这条连接，使同一个客户（浏览器）和该服务器可

以继续在这条连接上传送后续的 HTTP 请求报文和响应报文。这并不局限于传送同一个页面上链接的文档，而是只要这些文档都在同一个服务器上就行。目前一些流行的浏览器（例如，IE 6.0）的默认设置就是使用 HTTP/1.1。

持续连接的两种工作方式

非流水线方式：客户在收到前一个响应后才能发出下一个请求。这比非持续连接的两倍 RTT 的开销节省了建立 TCP 连接所需的一个 RTT 时间。但服务器在发送完一个对象后，其 TCP 连接就处于空闲状态，浪费了服务器资源。

流水线方式：客户在收到 HTTP 的响应报文之前就能够接着发送新的请求报文。一个接一个的请求报文到达服务器后，服务器就可连续发回响应报文。使用流水线方式时，客户访问所有的对象只需花费一个 RTT 时间，使 TCP 连接中的空闲时间减少，提高了下载文档效率。



【例】下列描述错误的是（）

- A. Telnet 协议 的服务端口为 23
- B. SMTP 协议的服务端口为 25
- C. HTTP 协议的服务端口为 80
- D. FTP 协议的服务端口为 31

【答案】D

【分析】该题是典型的概念题，要求掌握 ISO 参考模型的基本概念和层次划分。

第九章 网络实验入门

9.1 研究包大小和传输时间的关系

我们试着用 ping 命令把不同大小的数据发送给远程主机，这些数据会经过中间的路由器，然后从远程主机返回。命令可以在windows“运行”菜单中输入“cmd”进入的命令窗口运行，其基本格式是：

ping www.sina.com.cn -l 128

这里的 128 就是本次发送的数据的大小，默认情况下是32。

由于 ping 命令使用的是IP 协议的ICMP 功能，这个功能有时也被用于实现一种叫做DDOS 的网络黑客攻击技术，有很多主机或路由器是限制这种数据通过的，因此我们实验可以尝试不同的域名看是否有响应，至少我们可以尝试下一这几个域名：

www.163.net

www.google.com

这个实验的目的是看看不同大小的数据包在转发时有什么不同的表现，因此在完成这个实验后回答如下问题：

问题1. 填写下表:

访问主机: www.sina.com.cn

Sizes	TTL	Min	Max	Avg
512				
1024				
2048				
4096				

问题2. 平均响应时间和数据包的大小有没有关系? 有什么变化趋势?

问题3. 2048或者4096 大小的包怎末有和前面的数据不一样? 上网查一下为什么。

问题4. 发现TTL 的变化有什么规律? 上网查一下为什么。

附录1:

Ping是个使用频率极高的实用程序,用于确定本地主机是否能与另一台主机交换数据报,根据返回的信息我们就可以推断TCP/IP参数是否设置得正确以及运行是否正常。由于很多路由器和服务器为了防止DDOS攻击会关闭ICMP功能,如果因此而造成你访问的节点不响应ping的测试,你可以换一个IP或域名再试。

Ping 是一个测试程序,如果Ping 运行正确我们大体上就可以排除网络层、网卡、MODEM的输入输出线路、电缆和路由器等存在的故障,从而减小了问题的范围。按照缺省设置,Windows 上运行的Ping 命令发送4 组ICMP32 字节数据,如果一切正常我们能得到4 个回送应答。Ping 能够以毫秒为单位显示发送请求到返回应答之间的时间。如果应答时间短,表示数据报通过的路由器少或网络连接速度比较快。Ping 还能显示TTL 值(Time To Live生存时间),我们可以通过源地点TTL 起始值减去返回包的TTL 值从而推算数据包通过了多少个路由器。例如,如果返回TTL 值为249,TTL 起始值是256,源地点到目标地点要通过7 个路由器(256-249),一共是7 个hop。

正常情况下,当我们使用 Ping 命令来查找问题或检验网络运行情况时,我们需要使用一系列Ping 命令,如果所有步骤都运行正确,我们就可以相信基本的连通性和配置参数没有问题;如果某些Ping 命令出现运行故障,它也可以指明到何处去查找问题。下面就给出一个典型的检测次序及对应的可能故障:

ping 127.0.0.1

这个Ping 命令被送到本地计算机的IP 协议软件,如果没有成功就表示TCP/IP 协议的安装存在问题。

ping 本机的IP

这个命令被送到我们计算机所配置的IP 地址,计算机始终都应该对该Ping 命令作出应答,如果没有则表示本地配置或安装存在问题。出现此问题时,局域网用户请断开网络电缆,然后重新发送该命令。如果网线断开后本命令正确,则表示另一台计算机可能配置了相同的IP 地址。

ping 局域网其他电脑的IP

这个命令使数据经过网卡及网络电缆到达其他计算机再返回。收到回送应答表明本地网络中的网卡和载体运行正确。但如果收不到回送应答,表示子网掩码不正确、网卡配置错误或电缆系统有问题。

ping 网关的IP

这个命令如果应答正确,表示局域网中的网关路由器正在运行并能够作出应答。

ping 远程的某个IP

如果收到4 个应答,表示成功的使用了缺省网关。

ping localhost

localhost 是操作系统的网络保留名,它是127.0.0.1 的别名,每台计算机都应该能够将该名字转换成该地址。如果没有做到这一点,则表示主机文件(/Windows/host)存在问题。

ping www.sina.com.cn

对这个域名执行Ping www.sina.com.cn 地址,通常是通过DNS 服务器解析,如果这里出现故障,则表示DNS 服务器的IP 地址配置不正确或DNS 服务器有故障。

如果上面所列出的所有Ping 命令都能正常运行,计算机进行通信的功能基本上就可以放心了。但是这些命令的成功并不表示所有的网络配置都没有问题,例如某些子网掩码错误就可能无法用这些方法检测

到。

Ping 命令还有一些常用参数选项：

```
ping 某IP -t
```

9.2 使用 tracet 和 ping 命令

使用 ping 命令还可以分析目的主机和你的电脑中间的路由器数量，并观察转发延时。我们就先试着用ping 命令测试一下www.baidu.com

```
ping www.baidu.com
```

观察结果并回答以下问题：

- (1) 如果成功，Reply from 的IP 地址、bytes、time 和TTL 的值是什么？
- (2) 分析到eelab.nbu.edu.cn 的中间路由数量大约是多少？
- (3) 你判断中间路由器的依据是256 还是128,64 为基础的？上网查一下为什么？

我们还可以用 tracet 命令来进行验证转发路由器数量：

```
tracet IP address [-d]
```

该命令返回到达该IP 地址所经过的路由器列表，通过使用 -d 选项，将更快地显示路由器路径，因为 tracet 不会尝试解析路径中路由器的名称。

tracet 一般用来检测故障的位置，我们可以用tracet IP 测出在哪个环节上出了问题，虽然还是没有确定是什么问题，但它已经告诉了我们问题所在的地方。

我们进一步用 tracet 命令来测试一下：

```
tracet eelab.nbu.edu.cn
```

并回答以下问题：

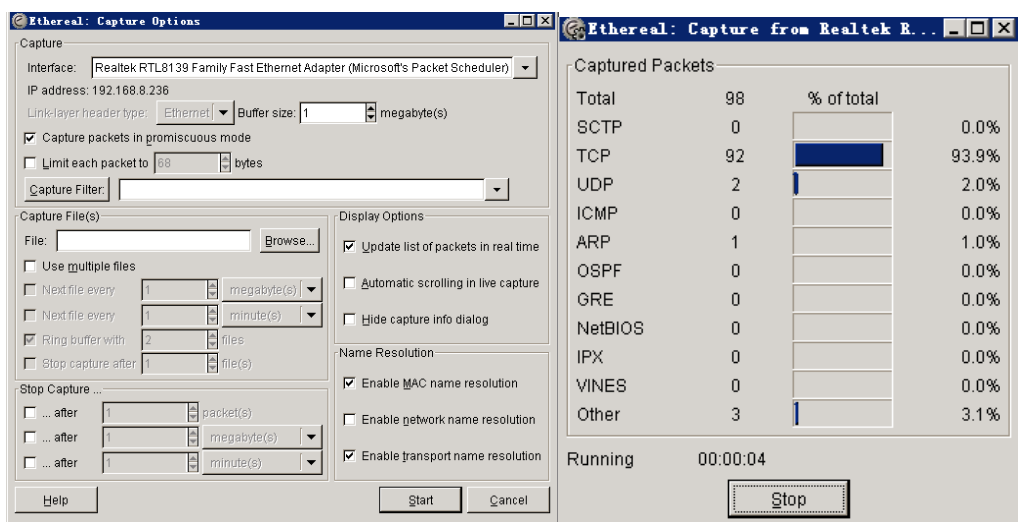
- (4) 到该网站的中间路由有多少个？和用ping 分析的结果一样吗？为什么？
- (5) 每个中间路由耗时各为多少？
- (6) 如果有某个中间路由没反应，可能的原因是？

9.3 学习使用 ethereal 观察网络

Ethereal 是经常要用到的协议分析软件，学习任何一个新的软件的最好方法是使用它！

1. 打开 Ethereal 软件，最初的时候窗口中都没有数据，因为Ethereal 还没有开始捕获包；

2. 开始包的捕获，选中 Capture 下拉菜单，选择Interface。你可以使用窗口中各选项的默认值，但网络接口（比如物理连接）要确认一下，如果你的电脑拥有多个网络接口，请选择正在接入网络的一个接口用来发送和接收包。选择网络接口（或者使用Ethereal 的默认接口），点击prepare则将会出现“Capture Options”窗口，如右图所示，使capture filter 保持为空，接下来勾选update list of packet in real time，点击start。包捕获现在将开始——你的电脑发送和接收的所有包都会被Ethereal 捕获；第一次配置好以后，下一次可以直接点击start进入捕获状态。



3. 当你开始包捕获，会出现一个包捕获摘要窗口，如左图所示。这个窗口概述了被捕获的各种类型包的量，Stop 按钮允许你停止包的捕获（现在还不要停止包的捕获）；

5. 你不需要在电脑上作任何操作，等大约 30-60 秒后在Ethereal 捕获窗口中按下stop按钮来停止Ethereal 的包捕获，Ethereal 的主窗口将会显示所捕获的包。

6. 恭喜你！现在，你拥有了刚才在你的电脑通过网络进行交换的协议消息，你已经完成了一次成功的协议数据捕获。

请回答以下问题：

问题1. 你没有手动进行网络访问操作，但还是抓到了一些数据，请列出你抓到的各种包的协议名称，并上网查询下这些包分别是起什么作用的？各是由谁发出的？

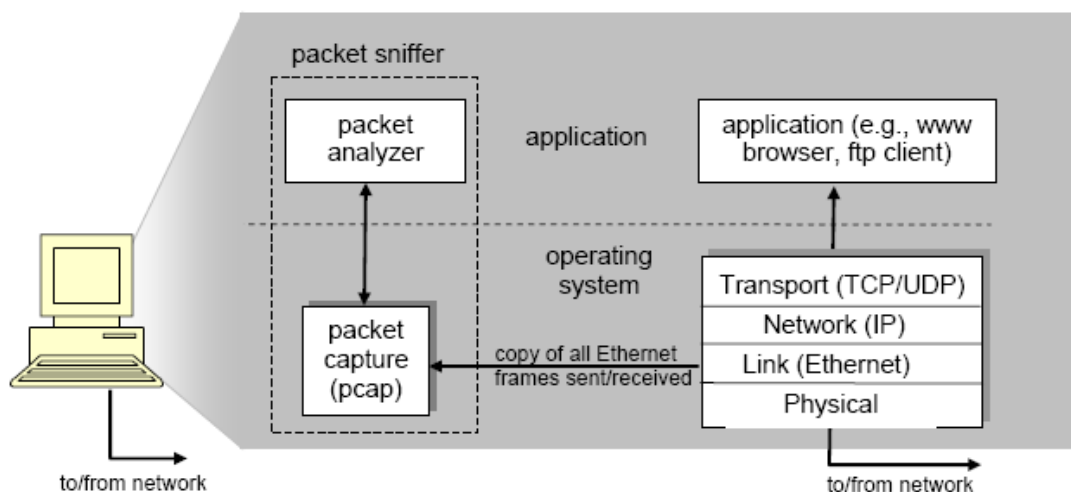
问题2. 从你抓到的第一个包到最后一个包持续的时间是多久？（默认time 列显示的是开始捕获后的以秒为单位的持续时间，如果要在time 列以time-of-day 格式显示，请选择Ethereal 的View 下拉菜单，然后选择时间显示格式为Time-of-day）

问题3. 导出这些数据，你可以在Ethereal 的File 命令菜单中选择save 菜单。

附录2 Ethereal 基础

我们观察执行协议的实体之间如何交换信息的基本工具是 packet sniffer，就如名字所示这是个包嗅探器，它在你的电脑发送消息或者接收消息时进行协议数据的捕获，同时有选择的显示这些协议数据的内容。包嗅探器本身是被动的，电脑所收发的数据包不写明是给包嗅探器的，而是由应用程序发送和接收时产生的，在包嗅探器收到包的同时应用程序数据收发仍然是正常进行的。

下图显示了一个包嗅探器的结构。



在图的右侧是协议和运行的应用程序，包嗅探器显示在用虚线围起来的框中，它侦听并接收每一个链路层帧的副本，当物理媒体是以太网时上层协议最终都将生成以太网帧，捕获所有的链路层帧就能收集所有在电脑上的应用程序和协议所收发的消息。包嗅探器的另一组成部分是包分析器，它显示一个协议消息中所有字段的内容，为了完成这些任务包分析器必须了解所有通过协议交换的消息的结构。例如我们对上图中通过HTTP 协议交换的消息所显示的区域感兴趣，包分析器需要了解以太网帧的格式，这样可以通过一个以太网帧来识别IP 数据包，同时它也需要了解IP 数据包的格式可以从IP 数据包中取出TCP 段，它也必须了解TCP 段的结构可以把包含在TCP 段中的HTTP 消息取出，最后它需要了解HTTP 协议等等，例如需要知道一个HTTP 消息的第一个字节将包含“GET”、“POST”或者是“HEAD”。

为了运行 Ethereal，你还需要支持Ethereal 和libpcap 包的捕获库，可以在安装Ethereal时的选项中勾选WinPcap 来安装。

9.4 观察 web 简单过程

1. 打开你的浏览器，打开 Ethereal 软件，最初的时候窗口中都没有数据，因为Ethereal 还有开始捕获包；

2. 开始包的捕获，当Ethereal 还在运行时，在浏览器中输入如下的URL 让它下载一个页面在你的浏览器中显示：

<http://www.baidu.com>

为了显示这个页面，你的浏览器将和www.baidu.com的HTTP 服务器进行联系，和服务器进行HTTP 消息的交换以下载这个页面，包含这些HTTP 消息的以太网帧将会被Ethereal 捕获：

3. 你的浏览器显示了这个页面后，在 Ethereal 捕获窗口中按下stop 按钮来停止包捕获，Ethereal 的主窗口将会显示所捕获的包。现在，你拥有了刚才在你的电脑通过网络进行交换的协议消息。HTTP 消息和www.baidu.com Web 服务器之间进行交换也在包捕获列表中出现，但是同样也有其他类型的包；

4. 在 Ethereal 主窗口的顶部的Filter 中，输入“http”，然后选择Apply，这样只有HTTP消息会被显示在包列表窗口；

5. 在包列表窗口中选择第一个 HTTP 消息，它应该是一个HTTP GET 消息，是由你的电脑发送给www.baidu.com 的 HTTP 服务器的。当你选中HTTP GET 消息后，以太网帧、IP 数据包、TCP 段以及HTTP 消息的头部将会显示在包头部窗口中。在包详细信息窗口的左边，选择扩展或收缩使显示的帧、以太网、IP 协议以及TCP 协议缩为最小而HTTP协议的信息被最大化。

6. 现在 Ethereal 显示的大致如下图所示：

在数据链路层里，数据链路层的基本概念和功能是必须掌握的，要明白数据链路层的组帧机制，差错

控制可以结合组成原理的这块的相关知识点来复习。流量控制和可靠传输控制是考试经常考的热点尤其是停止等待协议和连续 ARQ 协议。介质访问控制可以分为信道划分介质访问控制，随即访问介质访问控制和轮询访问介质访问控制，这里的每一知识点都是大家需要特别关注的地方。局域网与广域网也放在了数据链路层考查，要掌握局域网的基本概念和体系结构，广域网的基本概念。在局域网中重点是以太网，广域网中是 HDLC 协议和 ATM。最后同样是设备，数据链路层设备是网桥和交换机，要掌握网桥的概念；交换机的基本功能和实现原理。

在网络层里，首先要掌握住网路层的功能，尤其是路由与转发，这是最基本的。几个比较经典的路由算法像静态路由与动态路由的区别，距离-向量路由算法，链路状态路由算法等都是必须掌握的。网络层的主要协议是 IP 协议，对于这部分内容，要求掌握 IPv4 分组、IP 组播、IPv4 地址与 NAT、子网划分与子网掩码、CIDR。另外，还有与 IP 协议相关的其它层协议也将放在一起进行考查。作为新版本的 IP 协议 IPv6，需要掌握的是 IPv6 的主要特点、改进即地址表示方式等。要掌握 IP 组播的概念和 IP 组播的地址，移动 IP 的概念和移动 IP 的通信过程。网络层的主要设备是路由器，一定要掌握住路由器的组成和功能，路由表与路由转发。

传输层是网络的重点章节，一定要识记住传输层的功能和它所提供的服务，要掌握住面向连接的 TCP 协议与无连接的 UDP 协议之间的区别和联系，重点要弄懂 TCP 的连接过程，TCP 的可靠传输，TCP 的流量控制和拥塞控制。

应用层里经常用到耳熟能详的网络应用模型就是 B/S 模型，C/S 模型和 P2P 模型，大纲里面把后两者做为了考点，它们的架构，区别，它们之间的区别等。其它的一些应用比如 DNS 应用，FTP，邮件应用和 WWW 应用，大家一定都要了解，这些都是经常要用到的东西。重点要掌握 DNS 的解析过程，FTP 协议的工作原理，要明白 FTP 中控制连接和数据连接是分开的，HTTP 协议也关注一下。

预祝大家考研成功！