1. **第1章 计算机网络概述**
2. **计算机网络的定义**

计算机网络是通过传输介质、通信设施和网络通信协议，把分散在不同地点的计算机设备互连起来，实现资源共享和数据传输的系统。

1. **计算机网络的物理结构**

通信子网和资源子网。

1. **计算机网络的拓扑结构**

总线型、环形、星形、树形、回路形、网状、不规则形、卫星等。

局域网：总线型、环形、星形。广域网：网状、不规则形。以太网：总线型

1. **熟悉常用的网络命令行程序（ping、ipconfig、arp、route、netstat、nslookup、tracert）**

设置和查看网络接口命令ipconfig

测试网络连接状态命令ping

查看和设置地址解析协议表项命令arp

1. **计算机网络的分类：**

a) 按网络用途分：公用网和专用网；

b) 按网络覆盖的地域范围分类：局域网(LAN,范围在10km以内)、城域网(MAN，范 围在100km以内)、广域网(WAN，范围在100~1000km以内)；

c) 按信息的传输交换方式分类:电路交换网络和存储转发网络；

电路交换网络

报文交换

存储转发网络 虚电路分组交换

分组交换

数据报分组交换

1. **第2章 计算机网络协议和体系结构**
2. **计算机网络协议3要素**

语法:即信息格式，协议数据单元的（PDU）的结构或格式。（怎么讲）

语义：即某些信息组合的含义。（讲什么）

同步：规定了事件的执行顺序。

1. **OSI参考模型**

OSI的7个层次的名称自顶向下依次为应用层、表示层、会话层、运输层、网络层、数据链路层、物理层。对应的协议数据单元（PDU）分别是A-报文、P-报文、S-报文、T-报文、分组、帧、位流。

1. **TCP/IP模型**

TCP/IP协议的层次结构自顶向下依次是应用层、TCP层（运输层）、IP层（互联网层）、网络接口层。

IP协议是一种不可靠的，无连接的数据报协议，提供“尽力而为”的服务。其PDU是IP数据报，也成为IP分组。

ICMP协议为因特网控制报文协议，用于监视与检测网络、报告意外事件的发生。ICMP协议数据单元封装在**IP数据报**中发送

ARP协议用于实现IP地址到物理地址（MAC地址）的转换。ARP协议数据单元封存在**以太帧**中发送。

RARP协议实现从物理地址到IP地址的转换。【域名系统DNS域名地址到IP地址】

TCP协议：可以提供可靠的数据传输，提供面向连接的服务，提供按字节流的有序的可靠传输，可以实现连接管理，差错控制，流量控制（使用可变大小的滑动窗口协议），拥塞控制等。

UDP协议：无连接不可靠，用于不需要或无法实现面向连接的应用中。

|  |  |  |
| --- | --- | --- |
| 应用层  HTTP、FTP、SMTP、SNMP、Telnet、TFTP、DNS | 应用层 | 应  用  层 |
| 表示层 |
| 会话层 |
| TCP、UDP | 运输层 | |  |
| ICMP、IGMP、  IP、  ARP、RARP | 网络层 | |
| 网络接口层 | 数据链路层 | |
| 物理层 | |

1. **局域网体系结构**

LAN的体系结构仅涉及计算机网络体系结构的低两层，即物理层和数据链路层，把数据链路层分成两个子层：介质访问控制（MAC）子层和逻辑链路（LLC）控制子层。

1. **OSI和TCP/IP模型的比较**

TCP/IP模型与OSI模型的一个重要区别是可靠性问题，OSI模型在所有各层都进行差错校验和处理。而TCP/IP仅在TCP层，即仅在端到端进行差错控制

1. **第3章 移动通信技术基础**
2. **网络中的时延及计算**

时延：是指数据从网络或链路的一端传送到另一端所需要的时间，有时也被成为延迟或迟延。

总时延：总时延=发送时延+传播时延+处理时延+排队时延

往返时间：从发送方发送数据开始，到发送方收到来自接收方的确认消息（接收方收到数据后立即发送确认），总共经历的时间。

1. **传输介质及其分类**

常用的有线传输介质：双绞线，同轴电缆和光纤。

常用的无线传输介质：电磁波谱、无线电、微波、红外线和光波传输。

双绞线中两根导线缠绕在一起，可以降低导线之间的电磁干扰。

1. **信道复用技术（频分、时分、波分、统计）**

a) 频分复用：频分复用（FDM）设计思想是，信道的带宽很宽，信道的可用带宽大于一路信号所需的带宽时，把信道划分为多个子信道，每个子信道传输一路信号。在子信道之间要留有隔离频带，对每路信号以不同子信道频段的要求，调到不同的子信道上传输，传输到目的地后再回复为原始信号。

b) 时分复用：时分复用（TDM）技术的依据是，信道的数据传输率大于一路信号传输所需要的数据传输率。可以把传输时间分成时间片帧，。每一时间片帧包含若干时间隙，每个时间隙对应一路信号的若干位。

c) 波分复用

d) 统计复用（STDM）

e) 码分复用

1. **交换技术（电路交换、报文交换、分组交换、信元交换）**

传统的交换技术有电路交换、报文交换和分组交换（面向连接的虚电路分组交换和无连接的数据报分组交换）。计算机网络较多使用的是分组交换和信元交换。

若要连续传输大量数据，或实时通信的应用宜采用电路交换，因为数据传输时间大于建立连接时间，在简历的连接之上独占带宽传输大量数据的效率比较高，但是电路交换的健壮性比较差，只要连接中的一段链路出现故障，通信就不能进行。

报文交换或分组交换都与存储、转发相联系，数据报文或数据报分组逐个节点传输，想接力赛一样，若一段链路出现故障，报文或分组可以绕过故障所在的节点或链路传输。

1. **知道CDMA是什么**

码分多址(CDMA)是一种崭新而成熟的无线通信技术，成为第三代移动通信的基础。

1. **第4章 应用层**
2. **常见应用、应用层协议、使用的底层传输层协议、端口**

常见应用：www、电子邮件、文本传输、IP电话通信、远程教学、视频会议以及QQ即时通信。主要应用层协议有：域名系统(DNS)，文件传输协议(FTP)，简单邮件传送协议(SMTP)，超文本传输协议([HTTP](http://baike.baidu.com/view/9472.htm))，简单网络管理协议(SNMP)， 远程登录协议(Telnet)。使用传输层的TCP协议：DNS、HTTP、FTP、SMTP、Telnet；使用UDP协议：DNS 、SNMP



1. **熟悉DNS、域名结构、服务器类型、解析过程（P96）**

DNS是TCP/IP协议中制定的层次结构名字管理机制，实现域名地址到IP地址解析

域名地址空间由ICANN管理。最上层是根域，之下是顶级域，顶级域之下再细分为子域，形成二级域名，以此类推。工商企业（.com）、网络服务机构（.net）、非盈利组织（.org）、军事部门（.mil）、国际性的组织（.int）

**服务器类型**：根域名服务器、顶级域名服务器、权威域名服务器和本地域名服务器。

**解析过程:**

1.客户机提出域名解析请求,并将该请求发送给本地的域名服务器。（递归查询）  
 2.当本地的域名服务器收到请求后,就先查询本地的缓存,如果有该纪录项, 则本地的域名服务器就直接把查询的结果返回。

3.如果本地的缓存中没有该纪录,则本地域名服务器就直接把请求发给根域名服务器,然后根域名服务器再返回给本地域名服务器一个所查询域(根的子域)的主域名服务器的地址。（迭代查询）  
 4.本地服务器再向上一步返回的域名服务器发送请求,然后接受请求的服务器查询自己的缓存,如果没有该纪录,则返回相关的下级的域名服务器的地址。  
 5.重复第四步,直到找到正确的纪录。  
 6.本地域名服务器把返回的结果保存到缓存,以备下一次使用,同时还将结果返回给客户机。

1. **HTTP协议、HTML、URL、HTTP协议的请求和应答，请求方法等（P105）**

HTTP请求报文的一些方法：

OPTION 请求一些选项的信息

GET 请求读取由URL所标志的信息

HEAD 请求读取由URL所标志的信息的首部

POST 给服务器添加信息

PUT 指明的URL下存储一个文档

DELETE 删除URL指明的资源

TRACE 进行环回测试的请求报文

CONNECT 用于代理服务连接

1. **FTP协议、控制链接、数据链接、主动被动模式、特点。（P110）**

文本传输协议（FTP）的工作原理：服务器主进程打开默认端口号21；等待客户机进程的连接请求；启动从属进程处理客户机进程发来的请求，处理完毕后从属进程终止；返回到等待状态，等待下一个客户机进程的请求连接。

FTP的客户和服务器之间需要建立并行的“控制连接”和“数据连接”，分别通过端口号21和20进行。

FTP 的数据连接分为主动数据连接和被动数据连接。由服务器DTP发起建立到客户机DTP的数据连接称为主动连接，反之称为被动连接。

1. **电子邮件，工作原理，SMTP、POP3协议在其中所起的作用。**

用户代理在向邮件服务器传送邮件时使用简单邮件传输协议（SMTP）。邮件服务器之间采用SMTP协议。用户代理从邮件服务器的信箱中读取邮件时使用POP3或IMAP协议，这取决于邮件服务器支持哪一种协议。

在访问采用的POP3协议的邮件服务器时，邮箱中的邮件被复制到用户的客户机中，用户在自己的客户机中阅读和管理邮件。在访问采用IMAP协议的邮件服务器时，用户可以选择邮件复制到客户机，也可以选择在IMAP服务器中保留副本。

1. **FTP、SMTP、HTTP协议比较（P124）**

HTTP协议和FTP协议都是文件传输协议，使用的运输层协议都是TCP。两个协议的主要差别是：FTP使用两个并行的TCP连接，控制连接用于在客户和服务器之间传输控制信息；FTP的控制信息是属于带外传送的，HTTP属于带内传输控制信息

1. **第5章**
2. **运输层提供的服务**

运输层为应用层提供可靠的运输服务，运输层协议处在计算机网络中的端系统之间，为应用层提供可靠的端到端的通信和运输连接。运输层为高层用户屏蔽了通信子网（网络核心）的细节运输层起着承上启下的功用。运输层除了要为应用进程提供**复用和分用，**还要为应用报文提供差错检测，包括:传输数据出错、传输数据丢失、应答数据丢失、重复、失序、超时等。运输协议要为端系统提供流量控制，并对尽力交付的网络提供拥塞控制等。还有连接建立与连接释放、连接控制和序号设置等

1. **网络地址之间的转换**

域名地址通过DNS协议，经过域名服务器进行域名解析找到对应的IP地址，IP地址经过ARP找到对应的物理地址。反之，物理地址通过RARP转换为IP地址。

IP地址与端口地址构成套接字(Socket)，用于标识不同的应用服务进程

1. **可靠数据传输原理，ARQ、序号、超时、窗口。等-等协议、回退N协议、选择重传协议。（P149-P156）**

当发送窗口和接收窗口的大小都等于 1时，就是停-等协议。

当发送窗口大于1，接收窗口等于1时，就是回退N协议。

当发送窗口和接收窗口的大小均大于1时，就是选择重传协议。

1. **TCP连接的建立与释放，三次握手、四次握手过程（P146）**

第一次握手：建立连接时，客户端发送 SYN 包(SYN=j)到服务器，并进入 SYN\_SEND 状态，等待服务器确认；（SYN：同步序列编号(Synchronize Sequence Numbers)）

第二次握手：服务器收到 syn 包，必须确认客户的 SYN（ACK=j+1），同时自己也发送一个SYN 包（SYN=k），即 SYN+ACK 包，此时服务器进入 SYN\_RECV 状态；

第三次握手：客户端收到服务器的 SYN＋ACK 包，向服务器发送确认包 ACK(ACK=k+1)，此包发送完毕，客户端和服务器进入 ESTABLISHED 状态，完成三次握手。

1. **流量控制与拥塞控制的区别**

流量控制是对一条通信路径上的流量进行控制，其目的是保证发送者的发送速度不超过接收者的接收速度，只涉及两个网络节点，属于是局部控制；拥塞控制是对整个通信子网的流量进行控制，其目的是保证通信子网的流量与资源相匹配，不出现系统性能恶化、甚至崩溃的局面，涉及网络中多个节点，属于是全局控制。

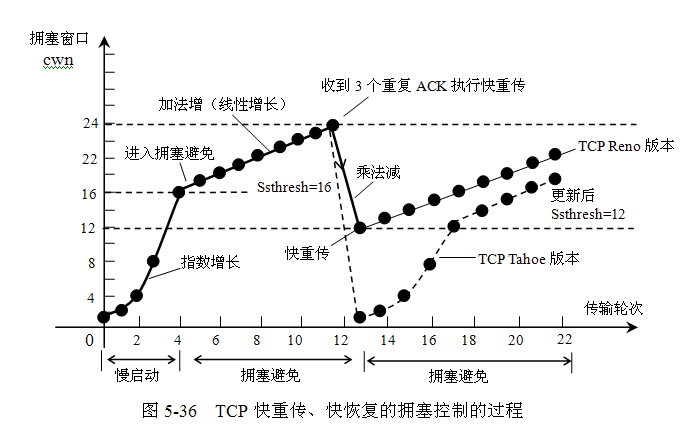
拥塞控制涉及到的层次有数据链路层、网络层和运输层

1. **TCP的滑动窗口机制、流量控制算法、序号、确认号、窗口**

TCP协议中的流量控制是通过协议数据单元中的接收窗口字段（该字段给出接收方的接收缓冲区当前可用的字节数）。发送方可以发送报文段的字节数还与拥塞窗口有联系，拥塞窗口是由发送方根据自己估计的网络拥塞程度设置的，是来自发送方的流量控制和拥塞控制

1. **TCP的拥塞控制算法，（慢起动、拥塞避免、快重传、快恢复），典型拥塞控制过程。（P172-P175）**

拥塞避免算法的设计思路是：拥塞窗口值超过阈值以后，按线性规律增加（加性增）拥塞窗口值，即每经过一个往返时延RTT，拥塞窗口增加一个MSS的大小，使拥塞窗口缓慢增大



1. **TCP协议的特点、了解TCP报文段格式（P169）**

是面向连接的、可靠的运输层协议。TCP的协议数据单元（PDU）是报文段，提供双向同时通信和可靠的数据传输，TCP连接的任何一方，不管是客户机或是服务器都可以发送和接受数据。TCP协议支持超时机制；由于采用双向同时传输，采用捎带确认和累计确认，不用专门发送确认报文段，提高了传输效率。TCP采用字节流传输数据，支持全双工和并发的TCP连接，提供确认、重传与拥塞控制。

TCP报文段包括协议首部和数据两部分，首部的固定部分有20个字节。

1. **UDP协议的特点、了解UDP报文段格式**

UDP协议的特点：

1. 在发送用户数据报之前不需要建立连接，好处是可以节省连接建立所需要的时间，有些应用层协议是不需要建立连接的，在有些情况下，也是无法或不能建立连接的，如在对网络进行故障检测时。
2. UDP采用尽力交付的方式为应用层提供服务。UDP协议简单，协议首部仅有8个字节，不需要维持包含许多参数、复杂的状态表。
3. UDP不支持拥塞控制，网络出现拥塞时，就简单的丢掉PDU，有些应用层的应用需要很低的时延，对在网络出现拥塞时丢失少量的PDU是可以容忍的，如IP电话。
4. UDP是面向报文（应用层的PDU）的，对应用程序交下来的报文不再划分为若干个报文段来发送，这就是要求应用程序要选择合适大小的报文。
5. UDP支持一对多、一对一、多对多和多对一的交互通信。

UDP的PDU由首部和数据两部分组成。UDP协议首部很简单，只有8个字节，由４个字段组成，每个字段都是两个字节（源端口、目的端口号、长度、校验和）。UDP协议的数据部分就是应用层的PDU。

1. **采用UDP的应用，采用TCP的应用**

TCP一般用于文件传输（FTP、HTTP对数据准确性要求高,速度可以相对慢），发送或接收邮件（POP、 IMAP、 SMTP对数据准确性要求高,非紧急应用），远程登录（TELNET 、SSH对数据准确性有一定要求,有连接的概念）、web/网页应用等；UDP一般用于即时通信（QQ聊天）,在线视频，网络语音电话。

1. **MTU和MSS**

MTU：最大传输单元。 MSS是TCP报文段中数据部分的最大长度，默认值是536字节

1. **第6章**
2. **网络层实现的功能**

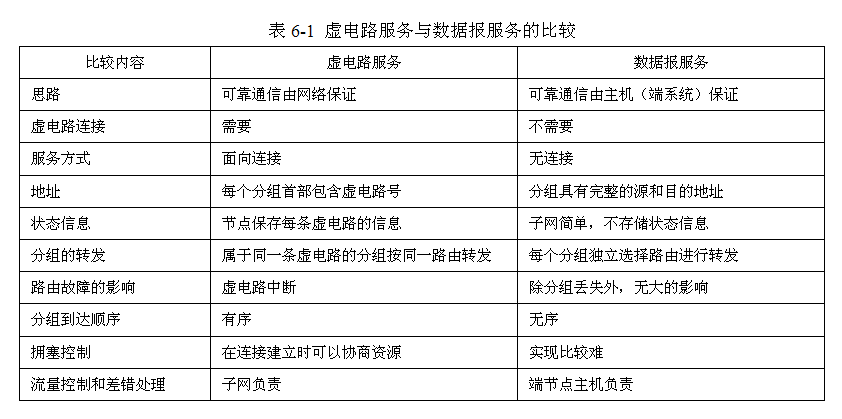
网络层实现的功能是最多的，网络层是网络核心（通信子网）的最高层，网络层的协议数据单元是分组。网络层需要解决的问题主要有：网络连接的建立和释放；路由选择；网络互连；网络寻址；拥塞控制；分片和组块；服务选择等。

网络层提供从发送节点（主机）到目的节点（主机）之间的可靠传输和分组的路由选择。发送节点到目的节点之间经过若干个节点（交换节点），节点之间均是点到点的连接，网络层与运输层之间的接口也用做通信子网与端用户的接口

1. **虚电路服务和数据报服务，比较**

虚电路VC(virtual circuit)服务是面向连接的网络服务：在双方通信之前先建立一条逻辑连接，通过发送呼叫连接请求分组，协商沿途经过的节点

数据报服务是“尽力交付（best-effort service）”的服务：是没有质量保证的服务，因特网采用的就是数据报服务。



1. **路由表、下一跳路由、会看网络拓扑图（能够写出网关、路由表）（P189）**
2. **直接交付和间接交付（P192）**

在同一个子网中的主机之间传输分组属于直接交付，不需要经过路由器.若是在不同子网中的主机之间传输分组，需要通过一个或多个路由器进行分组转发，属于间接交付

1. **静态路由和动态路由（老师未划重点）**

静态路由选择基本概念：静态路由的改变和设置是由人工完成的，一旦确定了分组路由，在一段时间内一般不会再重新设置路由。静态路由也称为非自适应性路由选择

静态路由选择算法的特点是：简单、开销小，以及路由过程是已知的

静态路由只用在小型的，网络拓扑结构不会经常变化的局域网中或是查找故障的试验网络中

动态路由选择是因特网中采用的技术。动态路由选择也称为自适应性的路由选择，能够适应网络状态的变化，动态的改变和设置路由。

动态路由选择可以分为三类：孤立式、集中式、分布式

1. **距离矢量路由选择原理及其计算(RIP)（P196）**
2. **链路状态路由选择原理及其计算(OSPF)（P200）**
3. **自治系统的概念，内部路由协议、外部路由协议（P206）**

因特网采用分层次的路由选择把互连网划分为多个自治系统AS。一个自治系统是具有一个单一的和明确定义的路由选择策略，由一组互连起来的具有相似IP前缀（一个或多个前缀）的路由器（节点）组成，由一个或多个网络管理员负责运行管理的系统。

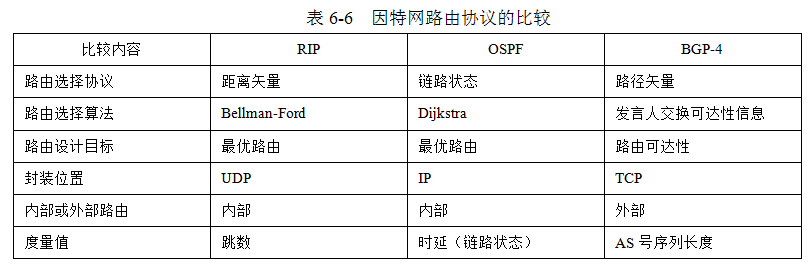
在自治系统内部运行的路由协议称为内部路由协议（IRP），也称为内部网关协议（IGP），与在其他自治系统内选用的路由协议无关。在自治系统之间运行的路由协议称为外部路由协议（ERP），也称为外部网关协议（EGP）。

1. **RIP、OSPF、BGP概念**

RIP是基于Bellman-Foed算法的距离矢量路由协议

OSPF协议是内部（网关）路由协议，采用链路状态路由选择算法。协议格式分为首部和数据部分，固定长度首部为24字节

外部路由协议：BGP采用路径向量（path vector）路由选择协议



1. **IP地址、分类、特殊地址、专用IP （P212-P215）**

IP协议中包含源IP地址和目的IP地址字段，各占32位二进制位。IP地址是一个逻辑地址。IP地址用来惟一标识网络中一个节点的连接，网络中的节点可以是主机或路由器。

**分类：**IP地址是将IP地址划分为若干个固定类。IP地址分为A、B、C、D、E共五类，最常用的是A、B、C三类。IP地址由网络标识字段（又称网络ID）和主机标识字段（又称主机ID）组成，IP地址可以标识为：

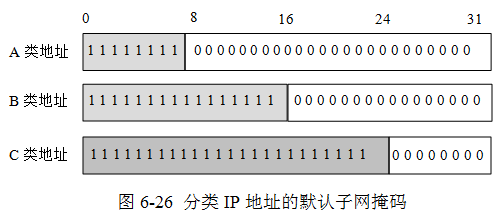
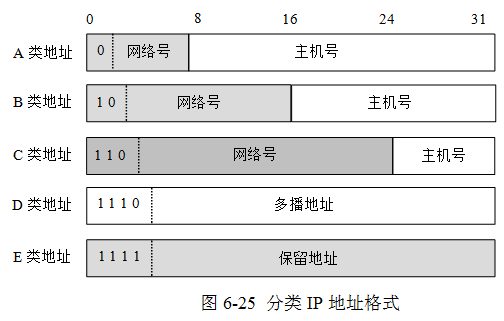
IP地址::＝{<网络标识>,<主机标识>}

对A、B、C类IP地址，对应的默认子网掩码依次是：255.0.0.0、255.255.0.0、 255.255.255.0

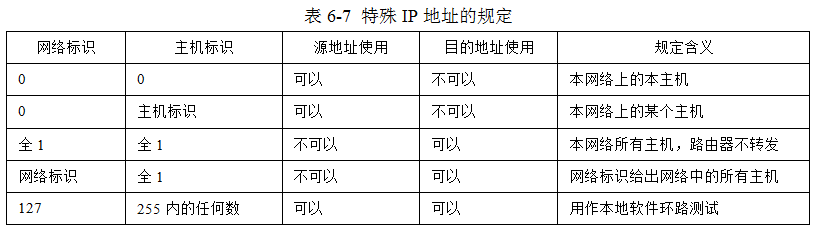
A类地址，1.0.0.0~127.255.255.255 B类地址，128.0.0.0~191.255.255.255

C类地址，192.0.0.0~233.255.255.255 D类地址用于多播，224.0.0.0~225.255.255.255

E类地址为保留地址，240.0.0.0~255.255.255.255



**特殊IP地址:** IP协议规定全0和全1的值不能用作普通的网络地址或主机地址。地址0.0.0.0用于标识本网络的本主机。网络地址为0的地址表示当前网络。全部为1的地址为网内广播地址。主机地址全为1的地址用于网内广播。127.X.Y.Z的地址为保留地址。



Intranet**专用IP地址**的三个地址范围是：

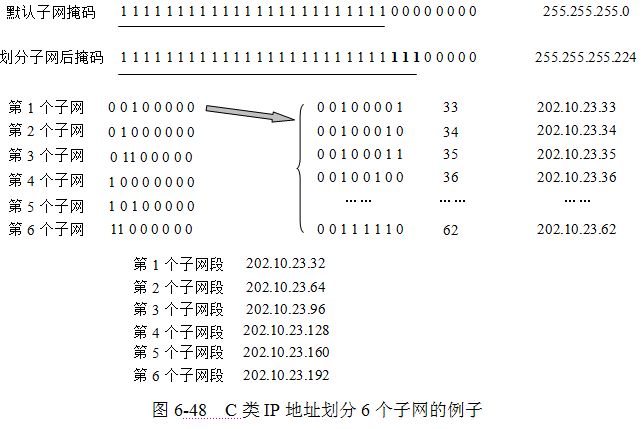
A类地址范围10.0.0.0—10.255.255.255，一个A类地址10

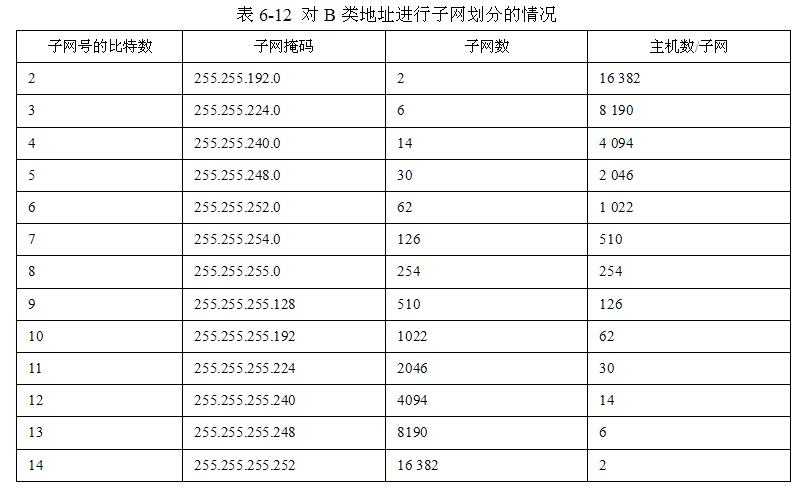
B类地址范围172.16.0.0—172.31.255.255 ，16个B类地址172.16—172.31

C类地址范围192.168.0.0—192.168.255.255，256个C类地址192.168.0—192.168.255

1. **子网划分、IP地址分配（P218-P220）**

用于子网划分的子网掩码(Subnet mask)是一个网络或一个子网的重要属性。子网的划分方法是，将原网络地址的主机地址分成两部分：一部分称为子网地址，也称为子网号，另一部分称为主机地址。





1. **IP分组、分片原理、分片过程（P216）**

当IP数据报的数据部分长度不适合底层网络MTU的要求时，需对IP数据报进行分片，IP数据报分片涉及到3个字段：标识；标志；片偏移

1. **ICMP报文概念**

ICMP（Internet Control Message Protocol）是用于监视与检测网络、报告意外事件的因特网标准协议，对应的技术文档是RFC 792

ICMP将检测的结果封装在IP分组中，ICMP报文作为IP分组的数据部分

ICMP允许主机或路由器报告差错情况和提供有关异常的报告，传送到给定的目的地，以实现对网络的监视和管理

ICMP将检测的结果封装在IP分组中，ICMP报文作为IP分组的数据部分

ICMP报文分为：询问报文和差错报告报文。ICMP报文的前4个字节采用统一的格式，有3个字段：类型；代码；校验和

1. **网络互联（P246）**
2. **网络互联设备、集线器、网桥、路由器**

网络互连设备

1. 协议转换器 是运输层及以上层（应用层）实现网络互联的设备
2. 路由器 是在网络层实现网络连接的设备
3. 网桥 是在数据链路上连接两个网络的设备（例:交换机）
4. 中继器 是在物理层实现网络互联的设备（例:集线器）

依次对应的层次为：运输层及以上层次、网络层、数据链路层、物理层

也就是说互连是在不同的层次上进行，越在高层次上实现互连，互连设备需要处理的东西就越多

1. **了解移动IP**

移动IP是发展最快的技术。为了实现网络中的移动通信，需要通过漫游(Roaming)和移动(Mobile)技术。漫游是指移动节点访问Internet上的资源；移动是指移动节点不仅要访问Internet上的资源，还要能够让Internet上的主机可以访问移动节点

支持移动性的Internet体系结构与协议称为移动IP

移动IP在网络层增加了新的特性，移动IP技术不仅可以用于跨越同类传输介质的网络，也适用跨越不同种类传输介质的网络

1. **第7章**
2. **数据链路层的作用**

数据链路层属于通信子网的层次，提供网络中相邻节点（一个源节点和一个目的节点）之间的可靠数据传输。

数据链路层的协议数据单元为帧

1. **了解HDLC和PPP协议（P266 老师未划重点）**
2. **局域网、LAN三要素、拓扑结构、传输介质、信道访问控制技术（P271）**

局域网LAN（Local Area Network）的属性涉及到网络地域范围的大小，一般把10千米范围内的网络划为LAN，LAN属于通信子网的范畴。

LAN的3个要素：拓扑结构，传输介质，信道访问协议

局域网常采用的拓扑结构有：总线型、星形、环形和树形。常用的传输介质有：双绞线、同轴电缆、光纤。常用的信道访问协议有：CSMA/CD、CSMA/CA等。

信道访问控制技术也可以分为两大类：静态划分信道和动态介质访问控制

**信道共享技术的分类如下：**

1. 固定信道划分协议，主要有时分复用、频分复用和码分多址等。
2. 随机访问协议，主要有：纯ALOHA、时隙ALOHA、CSMA、CSMA/CD、CSMA/CA等。
3. 轮流访问协议，主要有轮询协议和令牌传递协议。
4. **掌握CSMA/CD、工作原理、冲突处理方法（P277）**

载波侦听多路访问/冲突检测CSMA/CD协议，也称为“边讲边听”协议，即节点在侦听信道空闲时发送数据，发送数据以后还在继续侦听信道，看是否有冲突发生，进行冲突检测。

**工作原理**：节点发送前必须侦听信道，如果信道空闲，节点可以立即发送数据并进行冲突检测；如果信道忙，继续侦听信道，直到信道出现空闲，再发送数据并进行冲突检测。节点检测到冲突后立即停止发送，推迟一个随机时间再尝试发送。重复上述过程

冲突处理方法：

1）停止发送

2）强化冲突，发送一阻塞信号，让网络中的其他节点知道信道已经发送了冲突

3）根据冲突退避协议算法，退避一个随机时间后再尝试发送

1. **掌握ARP协议，同一网络和不同网络ARP协议工作过程，抓包分析。（P283）**

ARP是完成从IP地址到MAC地址转换的协议

网络中的主机B与同一个网络中的主机D通信，主机B只知道主机D的IP地址，当一台计算机需要进行地址解析时，广播发送一个ARP请求分组，其内容是查找给定 IP地址的主机的MAC地址。如“谁的IP地址是202.193.56.41”

节点在不同的LAN上的ARP解析过程：节点在两个不同的IP网络中，两个网络用不同网络ID标识，两个网络通过路由器R1和R2互连。在IP层抽象的互连网上只能看到IP数据报，IP数据报要经过R1和R2路由器转发，但在数据传输过程中IP数据报首部中源IP地址和目的IP地址始终没有变，两个路由器的IP地址并不出现在IP数据报首部中。

1. **以太网，MTU值，网段长度（P285）**

以太网MTU值为1500

局域网以太网中MAC地址为48位二进制位，使用时用12位16进制数标识。MAC帧由5个字段组成。第1、2字段分别为目的MAC地址和源MAC地址，各占用6个字节。第3个字段是类型字段，占用2个字节，用来标识上一层采用的协议

1. **了解CSMA/CA**

载波侦听多路访问（CSMA）协议分为非持续CSMA和持续CSMA两种机制，持续CSMA又分为1-持续和p-持续两种(1-持续是若信道空闲，立即发送数据，P-持续用于分隙信道)，也称为“边讲边听”协议

1. **了解VLAN、VPN、NAT的概念（P301老师未划重点）**

虚拟局域网VLAN（Virtual Local Area Network）：允许一组不同物理位置的用户群共享一个独立的广播域，可以在一个物理网络中划分多个VLAN，使得不同的用户群属于不同的广播域，这样的逻辑划分与物理位置无关，通过划分用户群控制广播范围。VLAN技术能够从根本上解决网络效率与安全性等问题。VLAN对广播域的划分是通过交换机软件来完成的

1. **二层交换机（原理，自学习）、三层交换机（P295 老师未划重点）**

交换机工作原理：通过交换机支持多个端口，把网络划分为多个冲突域，每个冲突域独立的执行CSMA/CD协议，一个冲突域只连接一台或很少的几台计算机，使在一个冲突域中的计算机可以获得较高的带宽，使整个系统具有更高的带宽

局域网采用三层交换技术主要有两种交换方法。第一种称为下一跳解析协议NHRP，第二种是Cisco公司提出的NetFlow交换，仍然是在第三层操作，目的是提高路由器的性能

1. **常见局域网接入方式**

电话拨号、路由器、ADSL、DDN专线、有线电视网络及高速以太网

1. **第8章**
2. **了解物理层解决的问题**

物理层的作用是屏蔽网络中各种网络设备和传输介质的差异，给上层数据链路层提供数据比特流服务

1. **了解常见接入技术**

xDSL技术、ADSL的连接、光纤同轴混合技术

1. **第10章（P362）**
2. **IPv6协议**
3. **选择题**（每空1分，共25分）

例如：在OSI参考模型中，实现端到端地应答、分组排序和流量控制功能地协议层是\_\_\_\_\_\_\_。

1. 数据链路层　　　 B、网络层　　　　　C、传输层　　　　　 D、会话层

二、**填空题**（每空1分，共25分）

例如： 计算机网络的物理构成由两级子网组成，即\_\_\_\_\_\_\_和\_\_\_\_\_\_\_。

三、**简答分析题**（每题6分，5题共30分）

类型有简答、抓包分析。

例如：简述TCP的链接建立和释放过程。

1. 论述/综合题：（共20分，共3道题）

计算、图例等类型