

概念

绪论

计算机网络：

系统观点：把具有独立功能的计算机，通过通信介质和通信设备，按照一定的拓扑结构连接，根据网络协议相互通信，在数据交换基础上，实现资源共享的系统。

数据通信基础

数据：对客观事物的符号描述，有不同的形式

信号：数据的具体物理表现形式，具有确定的物理描述；模拟信号是随时间连续变化的量；数字信号是离散变化的量。

信道：是传输信息所经过的路径，包括传输介质和有关的中间设备。连接计算机和终端，实现数据高效、无差错的传输和转接。

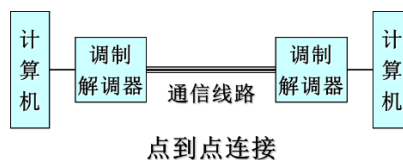
通信：数据由数据源（信源或发送端）经通信线路（也称信道）传输到数据的目的地（信宿或接收端）的过程。

模拟数据通信、数字数据通信：

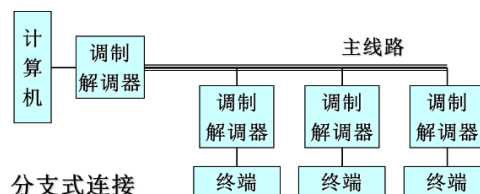
模拟数据是指连续变化的各种物理量，如声音的大小，光的强弱，电流；离散不连续的量是数字数据，如二进制信息的“0”和“1”。通信是数据由数据源（信源或发送端）经通信线路（也称信道）传输到数据的目的地（信宿或接收端）的过程。

通信线路的连接方式（点点、分支、集线）

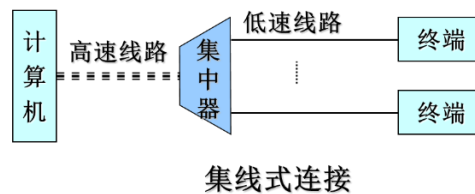
点点：终端或计算机和计算机之间直接或通过调制解调器 MODEM 用线路连接；



分支：多点通过主线路与计算机连接的方式；

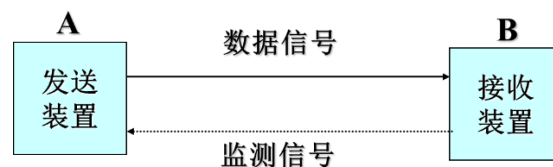


集线式连接：当多个终端设备都要与距离较远的计算机通信时，可把各终端先经集中器集中起来，再用一条频带较宽的高速线路与计算机连接；

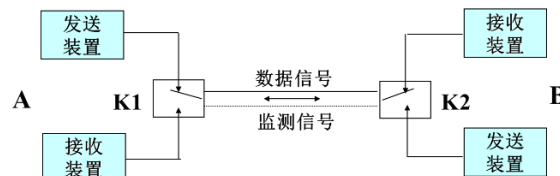


通信线路的通信方式（单工、半双工、全双工）

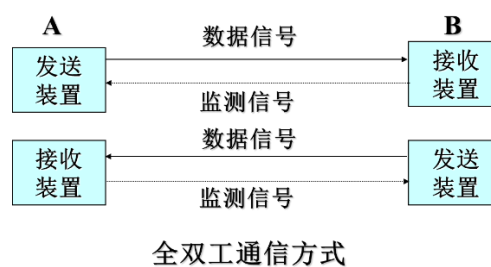
单工：通信线上的数据始终按一个方向传送



半双工：数据信息可以双向传送，但同一时刻一个信道只允许单方向传送；若想改变信息的传输方向，需由开关进行切换；



全双工：能同时两个方向进行通信，即有两个信道，可同时向两个方向传送信息；



数据传输方式（基带、频带、宽带传输）

基带：数字信号以原来的“0”、“1”形式原封不变地在信道中传送称为基带传输

频带：在计算机网络系统的远程通信中把数字信息调制成模拟音频信号后再发送和传输，到达接收端时再把音频信号解调成原来的数字信号的传输技术。

宽带：将信道分成多个子信道，分别传送音频、视频和数字信号，称为宽带传输。

计算机网络体系结构

网络体系结构：为了完成计算机间的通信合作，把每个计算机互联的功能划分成有明确定义的层次，规定了同层次进程间通信的协议及相邻层次之间的接口及服务。同层进程通信的协议以及相邻层接口统称为网络体系结构。

面向连接服务：通信双方在通信时，要事先建立一条通信线路，其过程有建立连接（通过三次握手的方式建立，建立连接是需要分配相应的资源如缓冲区，以保证通信能正常进行）、使用连接和释放连接三个过程。它可以保证数据以相同的顺序到达。

无连接服务：通信双方不需要事先建立一条通信线路，而是把每个带有目的地址的包（报文分组）送到线路上，由系统选定路线进行传输。它不要求发送方和接收方之间的会话连接，不保证数据以相同的顺序到达。

虚电路：在虚电路方式中，为进行数据传输，源和目的节点之间必须为分组的传输预先建立一条逻辑通路。一个逻辑通路中所有传输的路由是固定的，而且只在连接建立时进行一次路由选择。虚电路服务与数据报服务的本质差别表现为:是将顺序控制、差错控制和流量控制等通信功能交由通信子网完成，还是由端系统自己来完成。

数据报：数据报方式中，每个分组的传送是单独处理的，与先前传送的分组无关。每个分组被称为数据报。数据报必须包含目的端的完整地址信息。数据报所经过的路径可以不同，无法保证按发送的顺序到达，甚至可能有数据丢失。（与无连接服务类似）。

	数据报子网	虚电路子网
延时	分组传输延时	电路建立，分组传输延迟
路由选择	每个分组单独选择路由	建立虚电路时选择路由，所有分组都使用该路由
状态信息	子网无需保存状态信息	每个节点保存一张虚电路表
地址	每个分组包括源和目的地址	每个分组包含一个虚电路号
节点失败	除了在故障时正在由该节点处理的分组丢失外，无其他影响	所有经过的虚电路都被终止
拥塞控制	难于控制	如有足够的缓冲区分配给已建的虚电路，则容易控制

计算机局域网

CSMA/CD（载波监听多路访问/冲突检测）：在 CSMA 中，一旦两个帧发生冲突，在两个坏帧传输的时间内，其他站点都不能传输。如果帧比较长，还会浪费信道的容量。如果站点在传输中继续监听，则会减少这种因冲突而造成的浪费。这就是 CSMA/CD 对 CSMA 算法的改进。

CSMA/CD 的规则：(1) 若介质空闲，则传输；否则转步骤(2)；(2) 若介质忙，则一直监听到信道空闲，然后立即传输。(3) 若在传输中监听到冲突，则发出一个短小的干扰信

号，通知所有站点发生冲突，然后停止传输；(4) 发送干扰信号等待随机时间后，转步骤(1)。

令牌： 在令牌环网络中，有一种专门的帧称为"令牌"，在环路上持续地传输来确定一个结点何时可以发送包。谁有令牌谁就有传输权限。如果环上的某个工作站收到令牌并且有信息发送，它就改变令牌中的一位（该操作将令牌变成一个帧开始序列），添加想传输的信息，然后将整个信息发往环中的下一工作站。当这个信息帧在环上传输时，网络中没有令牌，其它工作站想传输数据就必须等待。

网络互联

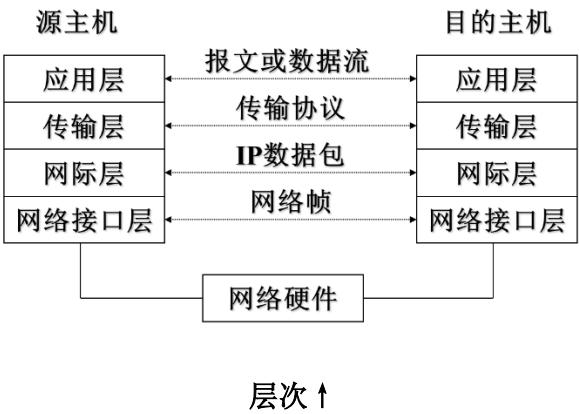
网络互联：采用各种网络互联设备将同一类型的网络或者不同类型网络及其产品相互联接起来，组成覆盖范围更大、功能更强的网络。网络互联也可以理解为将一个网络分解成若干个更小的子网，是计算机网络及技术发展到一定阶段的必然产物。

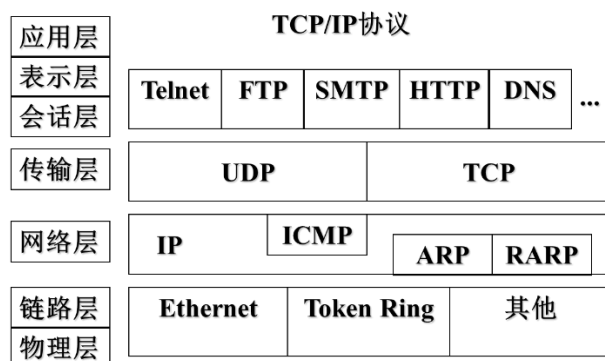
网络互联的形式：局域网互联；局域网与广域网互联；局域网与城域网互联

网络互联的层次：网络互联一般通过中间设备实现。网络互联层次主要是指网络间通过OSI 七层模型中的哪一层实现的。

TCP/IP 协议

TCP/IP 体系结构：





C/S（Client/Server）：客户机/服务器。包括两部分：接受用户要求并返回处理结果的部分(客户机程序)和根据用户请求进行数据处理部分(服务器程序)，称为客户机/服务器（C/S）结构。

B/S（Browser/Server）：浏览器/服务器。是 WEB 兴起后的一种网络结构模式，WEB 浏览器是客户端最主要的应用软件。这种模式统一了客户端，将系统功能实现的核心部分集中到服务器上，简化了系统的开发、维护和使用。

URL（Uniform Resource Locator）：统一资源定位符。是对可以从互联网上得到的资源的位置和访问方法的一种简洁的表示，是互联网上标准资源的地址。互联网上的每个文件都有一个唯一的 URL，它包含的信息指出文件的位置以及浏览器应该怎么处理它。

HTML（HyperText Markup Language）：超文本标记语言，标准通用标记语言下的一个应用。

WWW（World Wide Web）：万维网。是一个由许多互相链接的超文本组成的系统，通过互联网访问。

Telnet（远程终端协议）：Telnet 协议是 TCP/IP 协议族中的一员，是 Internet 远程登陆服务的标准协议和主要方式。它为用户提供了在本地计算机上完成远程主机工作的能力。在终端使用者的电脑上使用 telnet 程序，用它连接到服务器。终端使用者可以在 telnet 程序中输入命令，这些命令会在服务器上运行，就像直接在服务器的控制台上输入一样。可以在本地就能控制服务器。要开始一个 telnet 会话，必须输入用户名和密码来登录服务器。Telnet 是常用的远程控制 Web 服务器的方法。

DNS（Domain Name Service）：域名服务。因特网上作为域名和 IP 地址相互映射的一个分布式数据库，能够使用户更方便的访问互联网，而不用去记住能够被机器直接读取的 IP 数串。通过主机名，最终得到该主机名对应的 IP 地址的过程叫做域名解析(或主机名解析)。

FTP（File Transfer Protocol）：文件传输协议。文件传输协议是 TCP/IP 网络上两台计算机传送文件的协议。它属于网络协议组的应用层。FTP 客户机可以给服务器发出命令来下载文件，上传文件，创建或改变服务器上的目录。

HTTP (Hyper Text Transfer Protocol): 超文本传输协议。是我们浏览网页、看在线视频、听在线音乐等必须遵循的规则。

接入技术

接入: 把一个终端系统连接到一个网络系统的过程

交换网与宽带网

ATM: 异步转移模式(ATM)是一种以固定长度的分组方式,并以异步时分复用方式,传送任意速率的宽带信号和数字等级系列信息的交换设备。异步转移模式是用于实现宽带综合业务数字网(B-ISDN)的基础技术。它可综合任意速率的话音、数据、图像和视频的业务。

■ ATM

- **ATM综合线路交换实时性好、分组交换灵活特点,提供的数据传输和分组交换技术**
- **采用面向连接的高速交换技术,利用异步时分多路复用技术,将信息组成长度固定的信元独立传输。**
- **信元是长度固定,包括信头和有效数据。各种多媒体信息可以信元为单位传输。**

帧中继 (Frame Relay): 是一种用于连接计算机系统的面向分组的通信方法。它主要用在公共或专用网上的局域网互联以及广域网连接。

■ 帧中继

- **是一种快速分组交换技术,采用带宽按需分配的复用技术,将单条线路上多个用户站点信息汇集装载到帧中继网络;**
- **利用虚电路技术,将用户数据流分成多个分组(帧)进行传输,接收端再重新装配。**
- **帧中继传输数据的最小单位是帧。**
- **帧包括帧定界开始、帧头、用户数据、帧校验和帧结束定界等。**

计算机网络安全

数据加密: 确保信息不被其他的人截取和阅读。

验证: 提供通信对等实体和数据源的验证。**对等实体验证服务:** 用于两个开放系统对等层中实体建立连接时、对对方实体的合法性进行判断。**数据源验证服务:** 提供数据单元源的确认。但不提供对重复和修改数据单元的保护。

数字签名: 一种信息认证技术,利用数据加密、数据变换技术,根据某种协议来产生反

映被签署文件或签署人特征，以保证文件真实性和有效性，并防止接收者伪造或篡改的行为。

防火墙：防火墙是严格限制对网络指定资源的访问来实现组织安全策略的一个解决方案。

原 理

绪论

网络的组成部分包括：习题 1+

主机(服务器)：计算机网络中承担数据处理的计算机系统，可以是单机、多机系统、服务器群等；

终端(客户机)：网络中用量大、分布广的设备，直接面向用户，实现人机对话，并通过它与网络进行联系。终端种类很多，例如：PC、电子屏幕、智能终端、网络打印机、存储设备等。

通信处理机：节点计算机(NC: Node Computer)或前端处理机，是主机与通信线路间设置的计算机，负责通信控制和通信处理工作；以提高主机效率。

数据传输设备：包括集中器、信号变换器、多路复用器、通信线路等。主要解决数据和信号的传输及其控制。

网络的拓扑结构：见习题 2

数据通信基础

数据通信系统（组成、工作原理）：见习题 4.

线路交换（线路建立、数据传送、线路拆除）：习题 5.

存储转发交换（报文交换、报文分组交换）：习题 5.

多路复用（时分、频分、波分、码分复用）：习题 5+

- 码分多路复用CDM又称码分多址（Code Division Multiple Access, CDMA）
 - ◆ 共享信道频率和时间，是动态复用技术
 - ◆ 原理是每比特时间被分成 m 个更短的时间片，称为码片(Chip)。通常每比特有64或128个码片
 - ◆ 每个站点被指定一个唯一的 m 位的代码或码片序列
 - ◆ 各个站点的码片序列是相互正交的，当多个站点同时发送时，各路数据在信道中被线形相加

计算机网络体系结构

OSI 参考模型及各层功能（重点数据链路层、网络层、传输层）：习题 7

计算机局域网

Ethernet（以太网）结构、工作原理

Ethernet 是局域网中使用最广泛的共享总线型网络，采用带有冲突检测的载波监听多路访问控制技术 CSMA/CD，解决公用总线冲突问题。

Ethernet 由**工作站、网卡、Ethernet 总线**三部分组成。工作站是网络中的主要资源，通过它可以访问网络资源，为网络用户服务；网卡：(网络接口卡)控制和保证报文分组在物理信道上正确传输；Ethernet 总线是同轴电缆、T 型插头、终端匹配器及连接器的总称。大中型网络通过中继器连接各段。

以太网是一种广播网络，工作过程如下：一台主机要传输数据时将：
1、监听信道上有无信号在传输。如果有的话，表明信道处于忙状态，就继续监听，直到信道空闲为止。
2、若没有监听到任何信号，就传输数据
3、传输的时候继续监听，如发现冲突则执行退避算法，随机等待一段时间后，重新执行步骤 1（当冲突发生时，涉及冲突的计算机将发送数据返回到监听信道状态。
4、若未发现冲突则发送成功，所有计算机在试图再一次发送数据之前，必须在最近一次发送后等待 9.6 微秒（以 10Mbps 运行）。

令牌环网结构、工作原理：

令牌环网的媒体接入控制机制采用的是分布式控制模式的循环方法。在令牌环网中有一个令牌(Token)沿着环形总线在入网节点计算机间依次传递，令牌实际上是一个特殊格式的帧，本身并不包含信息，仅控制信道的使用，确保在同一时刻只有一个节点能够独占信道。当环上节点都空闲时，令牌绕环行进。节点计算机只有取得令牌后才能发送数据帧，因此不会发生碰撞。由于令牌在网环上是按顺序依次传递的，因此对所有入网计算机而言，访问权是公平的。

令牌在工作中有“闲”和“忙”两种状态。“闲”表示令牌没有被占用，即网中没有计算机在传送信息；“忙”表示令牌已被占用，即网中有信息正在传送。希望传送数据的计算机必须首先检测到“闲”令牌，将它置为“忙”的状态，然后在令牌后面传送数据。当所传数据被目的节点计算机接收后，数据被从网中除去，令牌被重新置为“闲”。令牌环网的缺点是需要维护令牌，一旦失去令牌就无法工作，需要选择专门的节点监视和管理令牌。

其它看 PPT net07 P32-44

令牌总线网结构、工作原理：

令牌总线网类似于令牌环网，其中，站点可在网络上进行发送之前，必须拥有一个令牌。但是，它们的拓扑结构和令牌传递方式是不同的。

令牌按照站点地址的序列号，从一个站点传送到另外一个站点。这个令牌实际上是按照逻辑环而不是物理环进行传递。在数字序列的最后一个站点将令牌返回到第一

个站点。这个令牌并不遵照连接到这条电缆的工作站的物理顺序进行传递。可能站点 1 在一条电缆的一端，而站点 2 在这条电缆的另外一端，站点 3 却在这条电缆的中间。

电缆的拓扑结构可以包括被长干线电缆连接的工作站的一些组。这些工作站从一种星形配置的集线器中分支出来，所以这个网络既是一个总线拓扑又是一个星形拓扑的网络。

令牌总线网是一种在总线拓扑中利用令牌作为控制节点访问公共传输介质的访问控制方法。令牌总线网在物理上是总线网，在逻辑上是环型网。

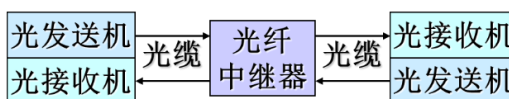
其它看 PPT net07 P45-60

FDDI 网结构、工作原理：

光纤分布式数据接口（Fiber Distributed Data Interface ,FDDI）是一种用于高速局域网技术，采用共享介质访问控制标准。

FDDI 采用新的编码技术，称为 4B/5B。每次对 4 位数据进行编码，每 4 位数据编码成 5 位符号，用光的存在与否表示 5 位符号中的每一位是 1 或者 0。

FDDI 网络是以光纤为传输介质组成的通信系统。由光端机、光纤（光缆）和光纤中继器组成。



光端机分为发送/接收光端机。发送端的光发送机将电信号调制成光信号，利用光源将光信号导入光纤，经光纤传送至光接收机，再将光信号转换成电信号，经放大、均衡判决后送给接收端。

光纤中继器用于延伸光纤的长度，防止光信号衰减。光波随传输距离增加，其功率逐渐下降，使用中继器放大信号。

无线局域网结构、工作原理

无线局域网 WLAN（Wireless Local Area Network）是计算机网络与无线通信技术结合的产物。利用微波扩频技术进行联网，在主机和设备之间采用无线连接和通信的局域网系统。以无线方式相连的计算机之间的资源共享，除支持传统的网络功能外，还可以在一定的区域实现移动并随时与网络保持联系。不受电缆束缚、可移动，满足便携机入网、局域网联网、远程接入、数据传输等功能。

网络互联

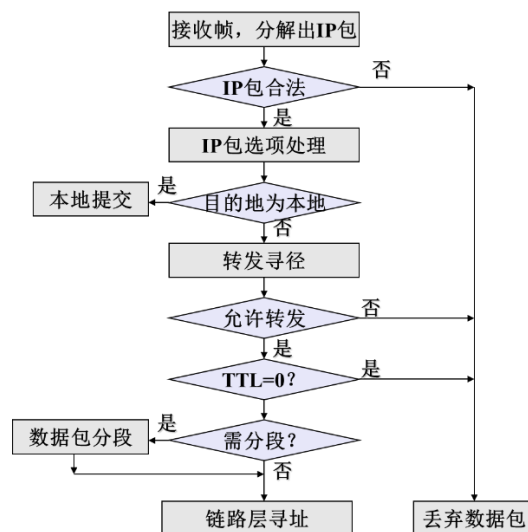
交换机工作原理：

交换机由多端口网桥发展而来。交换机按分组的 MAC 地址进行分组转发。

来自百度：工作在数据链路层，交换机拥有一条很高带宽的背部总线和内部交换矩阵。交换机的所有的端口都挂接在这条背部总线上，控制电路收到数据包以后，处理端口会查找内存中的地址对照表以确定目的 MAC（网卡的硬件地址）的 NIC（网卡）挂接在哪个端口上，通过内部交换矩阵迅速将数据包传送到目的端口，目的 MAC 若不存在，广播到所有的端口，接收端口回应后交换机会“学习”新的地址，并把它添加入内部 MAC 地址表中。使用交换机也可以把网络“分段”，通过对照 MAC 地址表，交换机只允许必要的网络流量通过交换机。通过交换机的过滤和转发，可以有效地减少冲突域，但它不能划分网络层广播，即广播域。交换机在同一时刻可进行多个端口对之间的数据传输。每一端口都可视为独立的网段，连接在其上的网络设备独自享有全部的带宽，无须同其他设备竞争使用。当节点 A 向节点 D 发送数据时，节点 B 可同时向节点 C 发送数据，而且这两个传输都享有网络的全部带宽，都有着自己的虚拟连接。

路由器工作原理

路由器的工作就是接收信息分组，根据当前网络拥塞、故障状况而导向最有效的路径。路由器先保存收到的分组，然后再按照目的路径转发出去。作用于网络层，在不同的网络间存储和转发分组，提供网络层上的协议转换。路由器从一条输入线路上接收分组，然后向另一条输出线路转发。这两条线路可以分属不同的网络，采用不同的协议。路由器检查网络分组头部，并根据其中的地址信息作出决定，当路由器将分组下载到数据链路层时，不关心具体的网络结构。



↑ 路由器工作流程

TCP/IP 协议

网络层协议（IP、ICMP、ARP/RARP 协议）：

网络层主要包括 IP、ICMP、ARP、RARP 等协议，主要功能由 IP 协议提供，实现端到端的分组转发和网际互联。

IP 协议的基本功能：无连接数据传送和数据包路由选择，即 IP 协议提供主机间不可靠的、无连接的数据包传送。IP 协议的主要任务是报文的分组和组装、寻址和路由选择。

互联网控制报文协议 ICMP，是在 IP 层中增加的特殊报文机制，使互联网能报告差错和提供有关意外情况信息。测试目的地的可达性和状态；测试报文不可达的目的地；数据包的流量控制；路由器路由改变请求；拥塞报告；ICMP 的报文是通过 IP 进行传送的。

地址转换协议 ARP，查找与给定 IP 地址对应的主机网络物理地址。IP 是网际范围内标识主机的逻辑地址，当传送报文时，必须知道物理地址。主机 A 使用 ARP 查找主机 B 的物理地址，可以广播一个 ARP 请求报文分组，其中有 B 的 IP 地址，B 收到报文后将自己的物理地址发回给 A。

RARP 协议主要解决物理地址到 IP 地址的转换。如无盘工作站启动时只有物理地址而不知道 IP 地址，可发送 RARP 报文给服务器获取其 IP。

传输层协议（TCP、UDP 协议）：

TCP 是传输层的一个主要协议，提供主机间端到端的面向连接的可靠的流服务。还提供多端口保证多进程的通信。PPTnet09 P118

UDP 协议：建立在 IP 协议基础上，UDP 不使用确认信息对报文的到达进行确认，不保证报文到达的顺序，不向源端反馈信息来进行流量控制，会出现报文丢失现象。UDP 协议提供了端口，提供了复用和解复用网络层服务的方法。报文到达时进入队尾，队满则丢弃该报文；当进程要接收时，从队列中移出一个报文，如队列空则阻塞该进程，直到数据报到达。PPT net09 P130

交换网与宽带网（net02 最后）

ATM 交换技术：ATM 综合线路交换实时性好、分组交换灵活特点，提供的数据传输和分组交换技术。采用面向连接的高速交换技术，利用异步时分多路复用技术，将信息组成长度固定的信元独立传输。信元是长度固定，包括信头和有效数据。各种多媒体信息可以信元为单位传输。

帧中继技术基本工作原理：是一种快速分组交换技术，采用带宽按需分配的复用技术，将单条线路上多个用户站点信息汇集装载到帧中继网络；利用虚电路技术，将用户数据

流分成多个分组(帧)进行传输,接收端再重新装配。帧中继传输数据的最小单位是帧。帧包括帧定界开始、帧头、用户数据、帧校验和帧结束定界等。

计算机网络安全

私有密钥密码体系: 习题 22 + PPT net 13-2 P41

公开密钥密码体系: 习题 22 + PPT net13-2 P48

防火墙的安全模型: 1.禁止没有被列为允许访问的服务:安全模型需要确定所有可以提供的服务及其安全特性,开放这些服务,封锁所有未列入的服务。2.允许没有被列为禁止访问的服务:安全模型需要确定哪些是不安全的服务,系统封锁这些服务,除此之外的其他服务则认为是安全的,允许访问。

基本类型: net13-4 P13

防火墙一般分为三类:报文过滤网关、电路层网关、应用层网关。

1. **报文过滤网关:** 最简单的防火墙,通常只对源和目的 IP 地址及端口进行检查,报文过滤器放在路由器,具有用户透明性,但不能进行用户区分。收到报文后先扫描报文头,检查报文类型(TCP 或 UDP 等协议)、源及目的 IP 地址、TCP/IP 端口,与过滤规则库中的规则比较后决定是否转发。
2. **电路层网关:** 实现 OSI 模型不同层次上的过滤。可根据安全级别的需要选择对应的 OSI 层进行设置。
3. **应用层网关:** 应用层网关并不是用简单的访问控制表来说明允许或拒绝的访问,而是运行一个接受连接的程序,需要进行口令确认和身份验证。应用层网关有三种类型:双源主机网关、屏蔽主机网关、屏蔽子网网关。

双源主机: 在代理服务器上装有两块网卡,并运行防火墙软件,使内外网络的通信必须通过代理服务器,不能直接进行。代理服务器本身不转发 TCP/IP 通信报文,网络中的所有服务均由此主机中的代理程序实现。

屏蔽主机: 代理服务器设置在内网,在内外网间加有报文过滤路由器,代理服务器运行防火墙软件,报文过滤路由器只允许外网访问内网中的代理服务器。内外网间的连接需要经过路由器和代理服务器中的两个访问控制列表来实现。

屏蔽子网: 在内外网间增加一个小型独立子网,对子网的访问受到路由器中的屏蔽规则保护,子网中的这些主机是唯一能被内外网访问到的系统。

IDS、??? 防病毒软件??? 工作原理

IDS: IDS 是网络中一种监视设备,帮助安全管理员识别进行中的攻击、终止攻击及攻击结束后的分析。两种主要的 IDS: 基于网络的入侵检测系统(监视网络流量)NIDS 和基于主机的入侵检测系统(监视个别计算机的行为)HIDS。IDS 通过比较数据包与特征

文件来判别某类已知的攻击。另外，IDS 能够检测到异常情况(行为)。

IDS 工作原理：数据收集（收集入侵的证据，包括分布式或集中式数据源；直接监控还是间接监控；基于主机还是基于网络的数据收集；使用外部探测器还是内部探测器）、数据分析（模式匹配，与已知特征或模式比较；统计分析，统计正常行为特征，发现异常行为；完整性分析，利用加密机制后中的消息摘要）。

术语及缩略语

- ATM:** Asynchronous Transfer Mode 异步传输模式
- ISDN:** Integrated Services Digital Network 综合业务数字网
- DDN:** Digital Data Network, 数字数据网
- FDDI:** Fiber Distributed Data Interface 光纤分布式数据接口
- CSMA/CD:** Carrier Sense Multiple Access with Collision Detection 基带冲突检测的载波监听多路访问技术(载波监听多点接入/碰撞检测)。
- CSMA/CA:** Carrier Sense Multiple Access with Collision Avoidance 载波侦听多路访问/冲突避免
- MAC:** Media Access Control 介质访问控制层
- LLC:** Logical Link Control 逻辑链路控制
- FTP:** File Transfer Protocol 文件传输协议
- HTTP:** HyperText Transfer Protocol 超文本传输协议
- HTML:** HyperText Markup Language 超文本标记语言
- WWW:** World wide web 万维网
- SMTP:** Simple Mail Transfer Protocol 简单邮件传输协议
- IIS:** Internet Information Services 互联网信息服务
- ISP:** Internet Software Provider 互联网服务提供商
- IP:** Internet Protocol 网络之间互连的协议
- TCP:** Transmission Control Protocol 传输控制协议
- UDP:** User Datagram Protocol 用户数据报协议
- ICMP:** Internet Control Message Protocol 网络控制报文协议
- ARP:** Address Resolution Protocol 地址解析协议
- RARP:** Reverse Address Resolution Protocol 反向地址转换协议
- ISO:** International Standardization Organization 国际标准化组织
- OSI/RM:** Open System Interconnection/ Reference Model 开放系统互连参考模型
- C/S:** Client/Server 客户机/服务器
- B/S:** Browser/Server 浏览器/服务器
- DNS:** Domain Name System, 域名系统
- LAN:** Local Area Network 局域网
- WAN:** Wide Area Network 广域网
- MAN:** Metropolitan Area Network 城域网
- PAN:** Personal Area Network 个人局域网
- WLAN:** Wireless Local Area Network 无线局域网
- VLAN:** Virtual Local Area Network 虚拟局域网
- VPN:** Virtual Private Network 虚拟专用网络
- VOIP:** Voice over Internet Protocol 网络电话协议(将模拟声音讯号(Voice)数字化,以数据封包(Data Packet)的形式在 IP 数据网络(IP Network)上做实时传递)

BSS: Base Station Subsystem 基站子系统，又称基站设备

ESS: Extended Service Set 扩展服务集合

SNMP: Simple Network Management Protocol 简单网络管理协议

SGMP: Simple Gateway Monitoring Protocol 简单网关监控协议