网络工程师笔记

目　录

第一章　数据通信基础

一、基本概念

码元速率：单位时间内通过信道传送的码元个数，如果信道带宽为 T 秒，则码元速率 $B=1/T$ 。

若无噪声的信道带宽为 W，码元携带的信息量 n 与码元种类 N 关系为 $n=\log_2^N$，则极限数据速率为

$R=B\log_2^N=2W\log_2^N$

有噪声的极限数据速率为

$C=W\log_2^{(1+S/N)}$　　$dB=10\log_{10}^{S/N}$

其中 W 为带宽，S 为信号平均功率，N 为噪声平均功率，S/N 为信噪比

电波在电缆中的传播速度为真空中速率的 2/3 左右，即 20 万千米/秒

编码：

单极性码：只有一个极性，正电平为 0，零电平为 1；

级性码：正电平为 0，负电平为 1；

双极性码：零电平为 0，正负电平交替翻转表示 1。

这种编码不能定时，需要引入时钟

归零码：码元中间信号回归到零电平，正电平到零电平转换边为 0，负电平到零电平的转换边为 1。这种码元自定时

不归零码：码元中间信号不归零，1 表示电平翻转，0 不翻转。

双相码：低到高表示 0，高到底表示 1。这种编码抗干扰性好，实现自同步。

曼彻斯特码：低到高表示 0，高到底表示 1。相反亦可。码元中间电平转换既表示数据，又做定时信号。用于以太网编码，编码效率为 50%

差分曼彻斯特码：每一位开始处是否有电平翻转，有电平翻转表示 0，无电平翻转表示 1。中间的电平转换作为定时信号。用于令牌环网，编码效率为 50%。

ASK、FSK 和 PSK 码元种类为 2，比特位为 1。DPSK 和 QPSK 码元种类为 4，比特位为 2。QAM 码元种类为 16。

一路信号进行 FSK 调制时，若载波频率为 fc，调制后的信号频率分别为 f1 和 f2 (f1<f2)，三者具有关系fc-f1=f2-fc。

编码技术：常用编码技术为脉冲编码调制技术。需要经过取样、量化和编码 3 个步骤。

在数字系统中，将数字信号转换成模拟信号成为调制；将模拟信号转换为数字信号成为解调。

尼奎斯特采样定理：采样速率大于模拟信号最高频率的 2 倍。

复用技术：

例：　10 个 9.6Kbps 的信道按照统计时分多路复用在一条线路上传输，假定信道只有 30%时间忙，复用线路开销为 10%，则带宽为：

$$9.6\times10\times30\%+9.6\times10\times30\%\times10\%=32$$

频分多路复用 FDM，时分多路复用 TDM，波分多路复用 WDM，码分多路复用（CDM）

T1 采用时分复用技术，将 24 条话音数据复用在一条高速信道上，其速率为 1.544Mbps，单个信道数据速率为 56KB/s

T2=4T1　T3=7T2　T4=6T3

E1 采用同步时分复用技术将 30 个语音信道，2 个控制信道（ch0 作为帧同步，ch16 传送信令）复合在一条高速信道上，其速率为 2.048Mbps，每条话音信道速率为 64Kb/s

OC-1 速率为 51.84Mb/s。

第三代通信技术：TD-SCDMA（中国），WCDMA（欧洲），CDMA2000（美国），WiMAX，其中 TD-SCDMA 属于时分双工模式，WCDMA 和 CDMA2000 属于频分双工模式。

奇偶校验码添加 1 位校验码，其码距变为 2。

海明码：利用奇偶性来检错和校验的方法。假设有 m 位信息码，加入 k 位校验码，则满足 $m+k+1\le 2^k$

一个码组内有 e 个误码，则最小码距 $d\ge e+1$

一个码组能够纠正 n 个误码，则最小码距 $d\ge 2n+1$

例：　求信息 1011 的海明码

解：由 $m+k+1\le 2^k$ 求得 k=3，即校验码为 3 位

校验码放在 2^n 位上

a7	a6	a5	a4	a3	a2	a1	位数
1	0	1		1			信息位
			r3		r2	r1	校验位

	r3	r2	r1
	0	0	0
a1	0	0	1
a2	0	1	0
a3	0	1	1
a4	1	0	0
a5	1	0	1
a6	1	1	0
a7	1	1	1

由上图得到监督关系式

r3=a5+a6+a7

r2=a3+a6+a7

r1=a3+a5+a7

将表中数值带入经异或运算得：

r3=a5+a6+a7=1+0+1=0

r2=a3+a6+a7=1+0+1=0

r1=a3+a5+a7=1+1+1=1

由此求得校验码为 001，填入表中得到海明码为 1010101

异或预算

1+1=0　　1+0=1

0+0=0　　0+1=1

偶数个 1 异或为 0

奇数个 1 异或为 1

第二章　局域网技术

一、预备知识

10BaseT 含义：10 表示传输速率为 10M（100M、1000M、10G）

Base 表示传输机制为基带（宽带 Broad）

T：代表传输介质为非屏蔽双绞线

C：为屏蔽双绞线

数字：为同轴电缆及电缆长度（10base5，10base2）

F 为光纤

Lx 为长波长 （1300nm、1310nm、1550nm）

Sx 为短波长（850nm）

综合布线测试参数：

双绞线：最大衰减值 回波耗损限值 近端串扰衰减值 开路/短路 是否错对

光　纤：最大衰减值　回波耗损限值　　波长窗口参数 时延 长度

光纤分类：

单模光纤：纤芯直径为 8~10*um*，包层 125um，采用激光光源，工作波长为 1310nm 或 1550nm，传输距离长（20 千米），容量大，带宽宽。

多模光纤：纤芯直径为 50*um* 和 62.5*um*，包层 125um，采用 LED 光源，工作波长为 850nm 或 1300nm，传输距离短（500 米），容量小，带宽窄。

电磁波在铜缆中传输速率约为真空中的 2/3，即 200000Km/s

RS232C 用于连接 DTE 和 DCE 设备，采用 25 芯 D 型连接器，微型机上一般采用 9 芯。-3v～-15v 表示 1，3v～15v 表示 0。采用 V.24 标准。电缆长度一般不超过 15m

二、局域网

2.1 拓扑结构

总线拓扑：采用主线传输作为公共传输媒体，网络中所有设备通过相应接口和电缆连接到这根总线。可采用令牌传递和 CSMA/CD 介质访问控制方法。

环形拓扑：由一系列首尾相连的中继器组成。使用令牌传递来实现介质的访问。*轻负载时效率低，重负载时利用率高*

星型拓扑：以中央节点为中心，把若干外围节点连接在一起的网络结构，

2.2 IEEE802 标准

IEEE802.1d 生成树协议

IEEE802.1q 虚拟局域网

IEEE802.1A 局域网体系结构

IEEE802.2　逻辑链路控制协议

IEEE802.3　CSMA/CD 与物理层规范

IEEE802.3u 快速以太网

IEEE802.3z 千兆以太网
IEEE802.3ae 万兆以太网
IEEE802.4 令牌总线标准 taken bus
IEEE802.5 令牌环标准 taken ring
IEEE802.10 局域网安全机制
IEEE802.11 无线局域网标准

2.3 数据链路层分为两个子层：目的是将与硬件相关和与硬件无关的部分分开。

逻辑链路控制子层（LLC）：目的是屏蔽不同子层的访问控制方法，向高层提供统一的服务和接口。LLC 帧结构如下图：

DSAP（8 位）	SSAP（8 位）	AC（8 位或 16 位）	DATA

DSAP 第 1 位为地址标识，后 7 位表示端口号。
SSAP 第 1 位为命令或响应标识。广播地址用 I/G=1 表示
LLC 地址作为 LLC 层的服务访问点，一个上层协议进程可以有多个服务访问点。
LLC 协议与 HDLC 协议兼容。主要提供如下 3 种服务：
A、无确认无连接的服务，不提供流控与差错控制，由高层软件完成。
B、面向连接方式服务，提供流控和差错控制，需要建立连接。
C、有确认无连接，提供有确认的数据报，但不建立连接。

介质访问控制（MAC）：局域网中，所有设备共享传输介质，需要一种方法有效的分配传输介质使用权。

根据控制方式不同分为**同步**和**异步**

同步传输：顺序连续传输，在传输前进行同步，然后传输双方以相同频率工作，适用于短距离高速数据传输

异步传输：各个字符分开传输，字符间插入**起始位**和**终止位**的同步信息，通常还需加入校验信息，适合长距离传输。

异步分配方法分为**循环（*令牌、FDDI*）、预约（IEEE802.6 定义的 *DQDB*）**和**竞争（*CSMA/CD*）**

2.4 IEEE802.3 标准（CSMA/CD 协议）

CSMA/CD 协议在发送数据前，先监听信道上是否有载波信号，有则说明信道忙，否则信道空闲，按照预定策略决定：

2.4.1 监听算法有 3 种：（*轻负载时效率较高*）

A、非坚持型监听算法：当一个站准备好数据帧，发送前先监听信道，如果信道空闲则立即发送（1），否则后退一个随机时间，在重复（1）。该方法**信道利用率低，增加了发送时延，减小了冲突概率。**

B、1-坚持型监听算法：当一个站准备好数据帧，发送前先监听信道，如果信道空闲则立即发送，如果信道忙则继续监听，直到信道空闲后再发送。该方法**有利于抢占信道，减少信道空闲时间，但增加了冲突概率**

C、P-坚持型监听算法：如果信道空闲则以 P 概率发送，以（1-P）概率延迟一个时间单位（1）（一个时间单位等于网络传输时延），如果信道忙则继续监听，直到信道空

闲转到（1），如果发送延迟一个时间单位，则重复（1）。该方法**吸取上述两种算法的优点**。

2.4.2 冲突检测

载波监听只能减小冲突概率，不能完全避免冲突。为充分利用带宽应采取边发送边监听的冲突检测方法：

（1）发送期间同时接收，并把数据与站中存储的数据进行比较；

（2）如果结果一致，则说明没有冲突，重复（1）

（3）如果结果不一致，则说明发生冲突，此时立即停止发送，并发送一个干扰信号 Jamming，使所有站停止发送，并等待一个随机的时间，重新监听，并试着发送。

2.4.3 二进制指数退避算法

按照该算法，后退时延的取值范围与重发次数 n 形成二进制指数关系。随着 n 的增减后退时延取值按 2 的指数增大。

为避免无限制的重发，对重传次数 n 进行限制。一般 n=16 时停止发送，丢弃该帧，并向上层报告。

该算法把后退时延的平均值与负载大小联系起来，因此**二进制指数退避算法能够解决在重负载下有效分解冲突的问题**

2.4.4 CSMA/CD 协议实现

对于基带和宽带总线来说，CSMA/CD 协议的实现方法基本相同，但也有差别：

差别一：（载波监听）基带系统是通过检测电压序列来实现载波监听，而宽带系统是监听站接受 RF 载波（射频）来判断信道是否空闲。

差别二：（冲突检测）基带系统是把直流电压加到信号上来检测冲突；宽带系统有两种方法来检测冲突：（1）把接收数据与发送数据逐位比对；（2）分裂配置，在端头检测是否有破坏的数据，这种数据的频率与正常的数据频率不同。

CSMA/CD 协议的载波监听、冲突检测、冲突强化、二进制指数后退等功能均由**硬件**来实现，这些硬逻辑包含在网卡中。网卡中的主要器件是以太数据链路控制器。

在 IEEE802.3 中使用 **1-坚持型监听算法**，这个算法有利于抢占信道，减少空闲，同时实现简单，在监听到网络空闲后，不立即发送而是等待一个**最小帧间间隔**(规定为 9.6us)时间，只有在这期间网络空闲才能开始发送。

在发送过程中继续监听，如果冲突，则发送 55555555 这是规定的阻塞信号。

接受站要对接受到的数据进进行校验，除了 CRC 校验，还要检查帧长度，如果小于最小帧长（64 字节）则认为是碎片。

线路利用率：

$$E=\frac{t_f}{t_p+t_f}=\frac{1}{\frac{t_p}{t_f}+1}=\frac{\frac{L}{R}}{\frac{d}{v}+\frac{L}{R}}=\frac{1}{a+1}\ 其中\ a=\frac{t_p}{t_f}=\frac{\frac{d}{v}}{\frac{L}{R}}=\frac{dR}{vL}$$

a（Rd 乘积）越大，线路的利用率越低

t_p 传播时延，信号在线路上传播的时间；

t_f 传输时延，数据帧加载到线路上所需时间；

d 为线缆长度 v 为信号传播速率；L 为帧长 R 为数据速率

2.5 以太网帧结构：

7	1	2/6	2/6	2	46-1500	0-46	4
P	SPD	DA	SA	L	DATA	PAD	FCS

P 为前导码，长度 7 个字节，1010..1010，用于使接收端进入同步状态

SPD 帧起始符，占 1 位，10101011，标识信息帧开始。

DA/SA（目的/源地址）占 2 个或 6 个字节。

L 数据字段长度，占 2 个字节，表示 DATA 字段长度及上层协议，0X0800 表示上层协议为 IP 协议；0X8137 表示上层协议为 IPX 协议。

PAD 填充字段，不大于 46 字节，主要解决帧不足 64 字节时，要加入填充位，使其满足要求。

DATA 数据字段，长度小于 1500 字节。用于存放高层 LLC 信息。

FCS 帧校验序列，占 4 字节，采用 CRC 字节。

最小帧长为 64 字节，最大帧长 1518 字节。

最短帧长计算： $L_{min}/R = 2L/v$,Lmin 为最小帧长，R 为数据速率，L 为两点间距离，v 为信号在介质中传播速率。

2.6 高速以太网：

2.6.1、快速以太网（100Mb/s），标准为 IEEE802.3u

与传统以太网采用**相同的帧格式**、**相同的介质访问控制方法**（CSMA/CD 协议）、**相同的接口**和**相同的组网方法。**

100BaseT4 ：使用 3 对 4 类 UTP，其中一对用于碰撞检测。

100BaseTX：使用 2 对 5 类 UTP，一对用于接收，一对用于发送。

100BaseFX：使用光纤

为能够检测到冲突，**采取保持最短帧长（64 字节）不变，将介质长度减少到 100 米，帧间间隔为 0.96us**(传统以太网为 9.6us)，采用 **4B/5B** 编码传统（传统以太网采用**曼彻斯特**编码）。

2.6.2、千兆以太网（1000Mb/s），标准为 IEEE802.3z

在 1000Mbps 的模式下，允许有**全双工**和**半双工**两种工作方式，与传统以太网采用的**相同帧格式，在半双工模式下，采用 CSMA/CD 协议**，在全双工不需要采用这种协议。IEEE802.3z，采用了帧突发方式，使一个站可以连续发送多个帧。

1000BaseTX：使用 4 对 5 类 UTP，最大段长 100 米

1000BaseCX：使用 2 对 STP，传输长度 25 米

1000BaseLX：使用多模光纤传输距离 550 米，使用单模光纤传输距离为 5 千米。

1000BaseSX：使用多模光纤传输距离 550 米

2.6.3、万兆以太网（10Gb/s），标准为 IEEE802.3ae

与传统以太网采用的**相同帧格式、最小和最大帧长**。仅支持**全双工模式**，不采用 CSMA/CD 协议，仅支持**单模**或**多模光纤**，不支持双绞线。定义了两种物理层：一种是**局域网物理层**，另一种是**广域网的物理层**。

2.7 虚拟局域网：

2.7.1、VLAN

VLAN（虚拟局域网），是一种将局域网设备从逻辑上划分成一个个网段，从而实现虚拟工作组的新兴数据交换技术。

VLAN 技术解决了局域网互联时无法限制广播的问题，每个 VLAN 一个广播域，同一 VLAN 内的主机通信跟一个 LAN 内一样，不同 VLAN 之间不能通信，如果需要通信，需要增加路由设备（三层交换机或者路由器）。

划分方法：

1、基于端口的划分（***属于静态划分 VLAN，其余属于动态划分***）

2、基于 MAC 地址的划分

3、基于网络层的划分

4、基于 IP 组播划分

5、基于规则划分

划分 VLAN 优点：

（1）控制网络流量，有助于控制广播风暴，减小冲突域、提高带宽利用率

（2）提高网络安全性。

（3）灵活的管理网络，可以突破地理位置限制而根据管理功能来划分网络。

2.7.2、VLAN 的中继模式（Trunk）

目前有两种通用标准，即 **IEEE802.1Q 和 Cisco ISL**，后者仅适用于 Cisco 设备。IEEE802.1Q 在原来的**以太网帧中增加了 4 个字节的帧标记字段。**

交换机支持的封装协议有 dot1q 和 ISL 两种。ISL 最多支持 1024 个 vlan；而 dot1q 支持 4096 个 vlan，其中两个保留，因此可用 4094 个

在划分 VLAN 的交换机上，端口分为两种：接入链路模式（Access）和中继链路模式（Trunk）。

接入链路模式：只能传送属于单个 VLAN 的数据包，所有端口均属于同一广播域。

中继链路模式：在进入中继端口前，在交换机的数据包中增加 VLAN 标记，在中继链路另一端的交换机不仅要根据目标地址，还要根据数据包中的 VLAN 标记进行决策。

2.7.3、VTP 协议与 VTP 修剪

VLAN 中继协议 VTP 用于在交换网络中简化 VLAN 管理。VTP 协议在交换网络中建立多个管理域，同一管理域共享 VLAN 信息，一台交换机只能参加一个管理域，不同管理域的交换机不能共享 VLAN 信息。

VTP 协议可以在一台交换机上配置所有 VLAN 信息，配置信息通过 VTP 报文发送到管理域内的所有交换机上。

VTP3 种模式：（*新交换机出厂时默认配置为 VLAN1，VTP 为服务器模式*）

服务器模式（server）：服务器上可以创建、删除、修改 VLAN 信息，服务器会自动将这些信息广播到同一域内的其他交换机上。

客户模式（client）：客户模式，不允许交换机上创建、删除、修改 VLAN 信息，只能被动接受服务器的 VLAN 信息。

透明模式（transparent）：透明模式下可以创建、删除、修改 VLAN 信息，但不广播自己的 VLAN 信息，它可以接收服务器发来的 VLAN 信息，但不使用，而是直接转发给别的交换机。

VTP 修剪：静态修剪　动态修剪

静态修剪：手工剪除中继链路上不活动的 VLAN。

动态修剪：允许交换机之间共享 VLAN 信息，也允许交换机从中继链路上动态的剪除不活动的 VLAN，使所得的所有 VLAN 都是活动的。当一台交换机端口加入新的 VLAN 时，则立即向周边交换机发送 VTP 报文，通知其他交换机，有新的 VLAN 加入。

2.8 生成树协议：IEEE802.1d，总延时为 50s

根桥的确定：（1）交换机 ID 最小（2 字节的优先级和 6 字节 MAC 地址组成）

（2）优先级值越小优先级越高，优先级高的的为根桥

（3）优先级相同，MAC 地址最小的为根桥

根端口确定：（1）最小路径开销的端口为根端口

（2）如果路径开销相同，取端口标识最小的为根端口。

端口开销规定：*10G 端口开销为 2；1000M 端口开销为 4；100M 端口开销为 19；10M 端口开销为 100*

端口状态：

阻塞：仅监听 BPDU，不转发数据帧，也不学习接受帧的 MAC 地址，延时 20s，防止启动交换机过程中产生交换环路。

监听：相互学习 BPDU 的信息，以便交换机可以学习网络中其他交换机的信息，延时 15s。此时不学习 MAC 帧的地址，不转发数据帧。

学习：处理学习到的 BPDU 信息，开始计算生成树协议。学习 MAC 地址，建立地址表，但不转发数据帧，该状态维持 15s。

转发：可以发送或监听 BPDU（用桥协议数据单元来传递交换机之间的生成树协议的信息），也可以转发数据帧

禁用：端口不参与生成树协议，不监听也不发送 BPDU，也不转发数据帧。

Portfast、uplinkfast 和 backbonefast 简介

Portfast（端口快速），使端口从阻塞状态快速恢复到转发状态，以达到快速收敛的目的。用于所有阻塞端口。

Uplinkfast（上行快速）使端口从阻塞状态快速恢复到转发状态，只用于接入层交换

机的阻塞上行级联端口（但不一定是 uplink 口），。

Backbonefast 与 uplinkfast 作用相同，但 backbonefast 配置在所有交换机上，可以诊断非直连链路故障，并且使生成树快速收敛。

交换机的分类：

以太网交换机按交换方式分为：直通式交换、存储转发式交换、碎片过滤式交换。

直通式交换：接收到数据包时检查包头，获取目的地址，立即将该数据转发，而不管数据是否出错，检错的任务交给节点主机完成。优点是交换延迟时间短，缺点是缺少差错检测能力，不支持不同输入输出速率端口之间的数据转发。

存储转发式交换：交换机完整接收数据并对数据进行差错检测，如果正确，根据目的地址将数据转发出去。优点是具备差错检测能力和支持不同输入输出速率端口之间数据转发，缺点是交换延迟时间长。是交换机的主流工作方式。

碎片过滤式交换：该方式是直通式转发的改进。在接收到数据后，判断数据包长度是否够 64 字节，小于 64 字节丢弃，大于 64 字节则发送。

交换机端口参数：

（1）端口类型

双绞线端口 RJ-45，可提供 100M 和 1000M 两种。

SC 端口，千兆光纤端口。

GBIC 端口，千兆光电转换接口

SPF 端口，是 GBIC 端口的升级，功能相同。

（2）传输模式：双工，半双工，自适应

（3）包转发率，指交换机数据包转发的能力

包转发率=千兆口数×1.488Mpps+百兆口数×0.1488Mpps

（4）背板带宽

交换机端口总带宽=端口数×2×端口速率

（5）MAC 地址数，指交换机的 MAC 地址表中可以存储的 MAC 地址数量。

（6）VLAN 表项，反映一台交换机所能支持的最大 VLAN 数。

（7）机架插槽数，指安装最大模块数。

2.9 无线局域网

IEEE802.11 定义了两种拓扑结构：

（1）基于基础设施网络：该方式所有无线终端通过 AP 访问骨干网络或者互访。AP 如同网桥，完成 802.11 与 802.3MAC 协议之间的转换。

（2）特殊网络（Ad Hoc）：该方式是一种点对点的网络，不需要有线网络和 AP，以无线网卡连接的终端设备之间可以互联通信。

802.11 工作在 2.4Ghz 频率，2Mb/s

802.11b 工作在 2.4Ghz 频率，11Mb/s

802.11g 工作在 2.4Ghz 频率，54Mb/s

802.11a 工作在 5.2Ghz 频率，54Mb/s

802.11h 工作在 5.2Ghz 频率

802.11n 利用 MIMO 技术和 OFDM(频分多路复用)结合在一起,理论上可提供 300Mbps 甚至是 600Mbps 的传输速率

无线局域网的关键技术

1、红外通信：

优点：A、红外频谱无限的，数据速率高

B、红外频谱不受管制

C、红外线可以被浅色物体漫反射。

缺点：室内环境可能因阳光或照明而产生强烈的光线，这将成为红外接收器的噪声。使得必须使用高能发送器，限制使用范围。

主要有以下 3 种技术：

定向光束红外线

全向广播红外线

漫反射红外线

802.11I 在数据加密方面定义了三种方式，即：TKIP，CCMP，WRAP 三种方式，TKIP 采用 WEP 中的 RC4 算法;CCMP 和 WRAP 基于 AES 算法。

2、扩展频谱通信

将信号散步到更宽的带宽上以减少阻塞和干扰的机会，其分为**跳频**和**直接序列**两种。**原理：**输入数据首先进入信道编码器，产生一个接近某中央频谱的较窄带宽的模拟信号，然后用一个伪随机序列对信号进行调制。调制的结果是大大的拓宽了信号的带宽。

跳频:信号按照看似随机的无线电频谱发送，每一个分组采用不同的发送频率。监听者只能收到一些无法理解的信号，干扰信号也只能破坏一部分传输信号。

直接序列：信号源中每一比特用成为码片的 N 比特来传输，这个过程在扩展器中进行，然后所有的码片用传统的数字调制器发送。

3、窄带微波：

分为 2 类：一类是申请许可证的窄带 RF；另一类是免申请许可证的窄带 RF

无线局域网访问控制机制

CSMA/CA 支持竞争访问、分布式协调和点协调功能支持无竞争的访问。

主要解决隐蔽终端和暴露站问题。

最常用的加密手段有 WEP（共享密钥），WPA/WPA2，WPA-PSK/WPA2-PSK 这三种算法中安全性最好的 WPA-PSK/WPA2-PSK，其加密过程采用了 TKIP 和 AES 算法

AP 安装与配置

安装原则：

（1）安装在高处，尽量避免障碍物，特别是金属物体。

（2）尽量处于房间中央。

配置：

（1）首先输入 AP 的管理员密码 SSID，用来标识不同的无线网络。然后根据 AP 预

设的 IP 地址和掩码设置客户端的地址和掩码，这样打开 AP 后，无线网卡将自行寻找。

（2）使用 AP 配置界面设置 IP 分配方式，它提供“静态分配”和“动态分配”两种。

（3）配置安装加密功能。默认情况下 AP 是不加密。

（4）避免信号干扰的方法对每个无线局域网采用不同的非重叠的信道。

3.0 结构化布线

结构化布线由 6 个子系统组成：

工作区子系统：有终端到信息插座的整个区域。包括信息插座、跳线、适配器。

原则：信息插座与电源插座保持在 30-150cm 的距离

信息插座据地面一般在 30cm，面积为 $9m^2$

UTP/STP 布线距离为 10m

水平子系统：各个楼层的接线间配线架到工作区信息插座之间的电缆构成。在结构化布线中，水平子系统起支线作用，它将用户端通过线缆连接至配线架上。**UTP/STP 布线距离为 90m**

管理子系统：对布线电缆进行端接和配线管理的子系统，通常设置在楼层的配线间内。由交联设备（双绞线配线架、光纤配线架）、集线器和交换机等交换设备组成。

干线子系统（垂直子系统）：连接管理间和设备间的子系统。一般由多对数的光缆和双绞线组成。语音系统采用三类大对数双绞线，数据通信采用高品质五类双绞线也可以采用光缆。**布线距离光纤一般 2000 米，STP 为 800 米，UTP 为 700 米。建议每 1.5 米设置一个线缆支撑点。**

设备间子系统：用于安放网络关键设备。

要求：湿度要求在 20%-80%，温度 20-30℃

综合考虑配电、安全接地和消防等因素

建筑群子系统：由连接楼群之间的通信传输介质和各种支持设备组成。**布线距离光纤一般 2000 米，STP 为 800 米，UTP 为 700 米。**

3.1 网络开发过程

网络生命周期至少包括系统构思与计划、分析和设计、运行和维护的过程。

常见的迭代周期分为四阶段周期、五阶段周期、六阶段周期。

网络开发过程根据五阶段迭代周期模型可被分为五个阶段：

需求分析、现有网络分析、确定网络逻辑结构、确定网络物理结构、安装与维护。

需求分析：收集不同用户的网络需求，主要包括,业务需求、用户需求、应用需求、计算机平台需求、网络通信需求和未来需求。

需求分析产生一份**需求规范**，需要管理者与设计者签字，这是规避网络建设风险的关键。

现有网络分析：主要目的是描述资源分布，以便在升级时保护已有的投资

该阶段给出一份**通信规范**说明文档，作为下一阶段的输入。主要包括：

（1）现有网络拓扑结构

（2）现有网络容量，新网络所需通信量和通信模式
（3）详细统计数据，直接反映现有网络新能的测量值
（4）Internet 接口以及广域网提供的服务质量报告
（5）限制因素列表，如电缆和设备清单

确定网络逻辑结构：根据需求规范和通信规范确定比较适宜的网络逻辑结构，并实施后续的资源分配规划、安全规划等内容

该阶段给出一份**逻辑设计文档**，内容主要包括：

（1）网络逻辑设计图
（2）IP 地址分配方案
（3）安全管理方案
（4）具体软硬件、广域网连接设备和基本网络服务
（5）招聘和培训网络员工的具体说明
（6）如硬件费用、服务提供费用和培训费用的估算

确定网络物理结构：对设备的具体物理分布、运行环境等的确定来使网络的物理连接符合逻辑设计要求

该阶段得到一份**网络物理结构设计文档**，主要包括：

（1）网络物理结构图和布线方案
（2）设备和部件的详细列表清单
（3）软硬件和安装费用估算
（4）安装日程表、说明服务的时间和期限
（5）安装后的测试计划
（6）用户的培训计划

安装与维护：根据前面的工程结果实施环境准备、设备安装调试的过程

网络结构设计：经典的三层模型，是将网络分为核心、汇聚和接入层

核心层：提供不同区域或者下层的高速连接和最优传输路径，主要设备是高端路由器或者交换机。

设计原则：采用冗余组件设计，具有高可靠性、高带宽和高吞吐率。尽量避免数据包过滤和策略路由等降低数据包转发处理的机制，已实现数据包的高速转发。

汇聚层：将网络业务连接到接入层，并且实施安全、流量负载和路由相关策略。主要设备是实现策略的路由器或者交换机。

汇聚层向核心层隐藏接入层的信息，汇聚层主要完成协议转换、策略路由、流量控制等

接入层：为终端用户访问网络提供接入。主要设备是低端交换机。

设计原则：接入层主要解决相邻用户之间的互访，同时还负责一些用户管理功能（如地址认证、用户认证、计费管理）和用户信息收集（IP 与 MAC 绑定、访问日志）工作。

单点故障：通过重复设置网络组件来避免因单个组件失效而导致应用失效。

传输速率=平均事务量大小×每位字节数×每个会话事物数×平均用户数/平均会话时长

网络安全的设计原则

从工程技术角度，网络安全应设计遵循以下原则

（1）**信息安全与保密的“木桶原则”。**强调对信息均衡、全面地进行安全保护。充分、全面、完整的对系统的安全漏洞和安全威胁进行分析、评估和检测使设计网络安全系统的必要前提条件

（2）**安全系统的整体性原则。**强调安全防护、检测和应急恢复。要求在网络发生被攻击情况下，尽快的恢复信息中心的服务，减少损失。

（3）**安全系统的有效性和实用性原则。**网络安全以不影响正常运行和合法用户的操作活动为前提

（4）**安全系统的“等级性”原则。**良好的安全系统必须划分不同的等级

（5）**自主和可控性原则。**网络安全产品不能依赖国外进口产品。

（6）**安全有价原则。**考虑网络安全问题解决方案时必须考虑性能和价格的平衡。不同的网络安全侧重点不同。

网络设备选型原则：

（1）**尽可能选择同一厂家产品。**这样的设备在互连性、协议的互操作性、技术支持和价格等方面有优势。

（2）**主干设备应考虑预留一定的扩展能力，低端设备够用即可。**

（3）**根据方案实际选型。**根据网络实际带宽性能需求、端口类型和端口密度选型。如果旧网改造，应尽可能保留用户原有网络投资，减少在资金投入的浪费。

（4）**选择性价比高、质量过硬的产品**

第三章　广域网和接入网技术

一、广域网技术

1、公共交换电话网

Internet 在网络层采用数据包服务，数据链路层采用协议 SLIP 协议（串行链路网际协议，主要用于低速交互型业务，仅支持 IP 协议，无差错控制）和 PPP 协议,PPPOA 和 PPPOE 均属于 PPP 协议的子集，PPPOA 应用于 ATM 专用网络，PPPOE 应用于以太网，目前大多采用 PPPOE 模式

DTE：用户的数据终端或计算机叫做数据终端设备 DTE

DCE：在通信网络的一边有个设备管理网络的接口，这个设备叫做 DCE，DCE 通常指调制解调器，主要提供建立、维持和拆除电路以及波形变化和编码等功能。

1.1 调制解调器

CCITT V.29 建议的 modem 以 9600b/s 的速率进行全双工或半双工传输，它采用正交调幅（QAM）由 4 种幅度 8 种相位结合产生 16 种码元，因而在 2400 的波特率下可得到 9600b/s（$2400\times\log_2^{16}$）的数据速率。

CCITT V.32 建议的 modem 采用网格编码调制 TCM 技术，这种 modem 的数据速率为 9600b/s。

CCITT V.33 建议的 modem 对 6 比特组进行幅度相位编码，增加 1 个冗余位，形成 7 比特的网格编码，因而在 2400 的波特率下可得到 14400b/s（$2400\times\log_2^{64}$）的数据速率。

ITU 的 V.90 建议的 modem 下行数据速率为 56KB/s，上行速率 33.6 KB/s。这种 modem 采用非对称工作方式。

1.2 公共数据网 X.25（也称分组交换网）

X.25 采用的是面向连接的虚电路服务

X.25 物理层采用 X.21 协议，主要定义物理网络之间的物理、电器、功能和过程特性。

X.25 的数据链路层（链路访问层）采用 LAPB 协议，该协议是 HDLC 协议的一部分，主要描述用户主机和分组交换机之间的数据可靠传输，包括帧格式定义和差错控制。

X.25 的网络层（分组层）采用 PLP 协议，该层主要定义分组、寻址、流量控制和拥塞控制等问题。其主要功能是允许用户建立虚电路（***支持交换虚电路 SVC 和永久虚电路 PVC***）和在已建的虚电路上传输最大长度为 128 字节的数据报文。

一个 DTE 设备最多建立 4095 条虚电路。

两个 X.25 网络互连使用 X.75 协议。

X.25 的流量和差错控制机制与 HDLC 相似。其默认窗口大小为 2。差错控制采用后退 N 帧 ARQ 协议。

X.25 由于复杂的差错校验机制，导致传输效率受到限制，同时传输速率不快，一般为 64kb/s，但主要优点有：

A、可以在一条物理链路上开放多条虚电路供多个用户使用；

B、具有动态路由功能和复杂完备的误码纠错功能；

C、可以满足不同速率和不同型号的终端与计算机间、计算机与计算机间以及局域网和局域网间的数据通信。

HDLC 协议时一种**面向比特的同步数据链路控制协议**，由 6 个字段组成。其用一种特殊的位模式 01111110 作为帧的边界标志。

01111110	地址 8 位	控制 8 位	信息	FCS（16 或者 32 为）	01111110

HDLC 定义了三种帧：信息帧（I 帧）、管理帧(S 帧)、无编号帧（U 帧），其中控制字段第一位或者前两位用于区别三种不同的帧（I 帧控制字段第一位为 0，S 帧前两位为 01，U 帧前两位为 11）

1.3 流量控制与差错控制

1.3.1、停等协议：发送站发送一帧，然后等待应答信号后再发送下一帧；接收站每收到一帧都回一个应答信号 ACK，表示愿意接受下一帧，如果接受站不送信号则发送站必须等待。

线路利用率 $E=\frac{t_f}{2t_p+t_f}=\frac{1}{2\frac{t_p}{t_f}+1}=\frac{\frac{L}{R}}{2\frac{d}{v}+\frac{L}{R}}=\frac{1}{2a+1}$ 其中 $a=\frac{t_p}{t_f}=\frac{\frac{d}{v}}{\frac{L}{R}}=\frac{dR}{vL}$

t_p 传播时延，信号在线路上传播的时间；

t_f 传输时延，数据帧加载到线路上所需时间；

d 为线缆长度 v 为信号传播速率；L 为帧长 R 为数据速率

1.3.2、滑动窗口协议：如果接收端维持能容纳 W 个帧的缓冲区（即窗口大小为 W），那么发送端可以连续发送 W 个帧而不必等待应答信号，但在收到接收端的应答信号前，则滑动窗口不滑动。接收端收到一个帧时，就发送一个应答信号，并把滑动窗口滑动到 i=W-i+1 的位置，表明 i 之前的已正确接收，期待接收后续 W 个帧。

则线路利用率 $E=\frac{Wt_f}{2t_p+t_f}=\frac{W}{2a+1}$

1.3.3、差错控制

ARQ 技术：利用差错检测技术自动的对丢失帧和错误帧请求重发的技术

1.3.3.1、停等 ARQ 协议：发送站发送一帧必须等待应答信号 ACK，收到信号后才能发送下一帧；如果收到否定应答信号 NAK 后重发该帧；如果在一定时间内未收到应答信号必须重发。

1.3.3.2、连续 ARQ 协议：分为选择重发 ARQ 和后退 N 帧 ARQ 两种。其中**选择重发 ARQ** 只重发出错的帧，后面的帧被缓存。这种协议窗口大小的最大值应为帧编号数的一半，即 $W \le 2^{k-1}$；

后退 N 帧 ARQ 是从出错处重发已发过的 N 个帧其窗口大小为 $W \le 2^k-1$

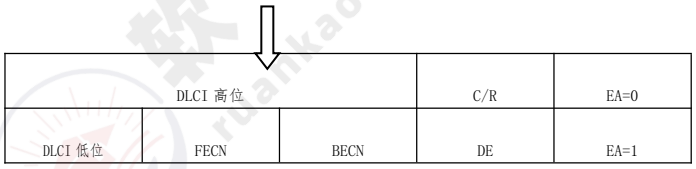
1.4 帧中继 frame-relay（也称快速分组交换网）

帧中继工作在物理层和数据链路层，其在数据链路层建立虚电路，用帧方式承载数据业务。帧中继的帧只进行检错和拥塞控制。

帧中继支持交换虚电路 SVC 和永久虚电路 PVC，但相对来说永久虚电路 PVC 用的较多。

帧中继协议为 LAP-D（D 信道链路规程），LAP-D 帧头和帧尾都是一个字节的帧标志字段 01111110，信息字段可变，默认最大长度为 1600 字节，该协议增加了拥塞控制。

01111110	地址	信息	FCS（2）	01111110



帧头中 2 字节地址中包含 DLCI 字段，DLCI 不同代表不同的虚电路，DLCI0 用于信令传输，其中 FECN 位为 1 表示向前拥塞控制；BECN 位为 1 表示与传送方向相反的方向上出现拥塞；DE（优先丢弃比特位）位为 1 表示该帧被优先丢弃。

帧中继主要优点：

A、基于分组交换的透明传输，可提供面向连接的服务

B、帧长可变，长度 1600-4096 字节，可承载各种局域网的数据帧

C、速率可达 2-45Mb/s

D、既可按需提供带宽，也可应付突发数据传输

E、没有流控和重传机制，**仅进行拥塞控制**，开销少，效率高

缺点：不适于对延迟敏感的应用（音频、视频），无法保证可靠提交。

1.5 ATM（异步传输）

ATM 以异步时分复用为基础，每个时间片没有固定的占有者，各子信道的信息按照优先级和排队规则按需分配时间片。为区分信息所属，在信息头部增加报头。报头和信息构成 ATM 的信元，信元大小为 53 字节，其中信头 5 字节，数据域 48 字节。*差错控制和流量控制放在高层处理。*

1.5.1、ATM 网络工作在物理层和数据链路层，其中数据链路层被分为 ATM 适配子层（AAL）和 ATM 子层。

物理层分为物理介质相关子层 PMD 和传输汇集子层 TC。PMD 负责正确的传输和接受比特流；TC 负责信元流和比特流的转换。

ATM 适配子层由 CS 子层和 SAR 子层组成。CS 子层提供接口，SAR 子层负责对数据进行分段和重装配。

ATM 子层主要定义信元头的结构，VPI 用于标识不同的虚路径；VCI 用于标识虚路径中的虚通道（***每个 VPI 可复用 65535 个 VCI***）。该层的主要功能：

A、信元汇聚和分拆；

B、VPI/VCI 的管理；

C、信元头的拆装和信元速率调整。

AAL 主要定义高层 PDU 和信元中数据域的拆装方法。主要目的是将高层数据转换为适合 ATM 网络传输的格式

CCITT 通信业务分类

A 级 支持有实时性要求的恒定位速率业务 CBR，采用面向连接的工作方式，比特率恒定，要求同步；AAL1 支持此类业务，常用业务为 64KB/s 的话音、固定码率的非压缩视频。

B 级 支持有实时性要求的可变位速率业务 VBR，采用面向连接的工作方式，比特率可变，要求同步。AAL2 支持此类业务，常用业务为压缩的语音通信和压缩的视频通信。

C 级 支持无实时性要求的可变速率业务 ABR，采用面向连接工作方式，比特率可变，不要求同步。AAL3/4 支持此类业务，适用于文件传递和数据网业务。

D 级 支持面向无连接的数据传输业务 UBR，采用无连接工作方式，比特流可变，不要求同步。AAL3/4 和 AAL5 均支持此类业务，适用于数据报业务和数据网业务

ATM 通信管理采取的主要措施

（1）**连接准入控制**是防止网络因超载而出现拥塞的第一道防线；

（2）**参数控制**来避免用户滥用资源而引起网络拥塞

（3）通信量整形用来平滑通信量、减小信元堆积、公平分配资源、减小延迟。

1.6 ISDN 综合业务数据网

ISDN 即支持线路交换也支持分组交换，其系统组成为：设备终端 TE、网络终端 NT、适配器 TA。

TE（终端设备）分为 TE1 和 TE2。TE1（标准 ISDN 设备）直接和 NT 相连；TE2（称为非 ISDN 设备）需经过 TA（终端适配器）与 NT 相连。

NT 分为 NT1 和 NT2。NT1 是第一网络终端，被放在用户设备和 ISDN 之间，起到插板作用，同时还具有管理和维护功能。NT2 仅具有集线和交换功能。

ISDN 分为窄带 ISDN（N-ISDN）和宽带 ISDN（***B-ISDN，关键技术为 ATM，采用五类双绞线和光纤传输，数据速率可达 155Mb/s***）。其中窄带 ISDN 是基于电路交换网的技术，采用时分多路复用技术，其提供两种速率接口：

基本速率接口（2B+D）：2 条速率 64kb/s 的 B 信道（话音和数据信道）和 1 条速率 16kb/s 的 D 信道（信令信道）组成，合计 144kb/s。允许用户使用模拟电话进行数据的存数字通信。

一次群速率接口（30B+2D）：B 信道和 D 信道（信令信道）速率均为 64kb/s，享有高达 2.048Mb/s 的速率

窄带 ISDN 分为三层，多路复用属于物理层功能，数据链路层采用 LAPD 协议，网络层支持电路交换

和分组交换。

缺点：数据传输速率太低，不适合传输视频信息。

二、接入网技术

1.7 XDSL 技术：基于普通电话线的宽带接入技术，其有以下几种模式：（ADSL 采用频分多路复用技术，可同时存在 3 个信道）

ADSL：非对称 DSL 技术，下行速率 1～8Mb/s，上行速率 512 kb/s～1Mb/s，传输距离 3-5 千米。同时可传输 4KHZ 的语音数据。成熟的标准有 G.DMT（***全速率 ADSL，速率为 8 Mb/s，用户端需要安装 POTS 分离器将话音与数据分开，ISP 端安装接入多路复用器 DSLAM 连接 Internet，适用于小型办公网络 SOHO。***）和 G.Lite（***速率较低，仅为下行 1.5 Mb/s，上行速率 512Kb/s，不需安装分离器，适用于家庭***）两种。

ADSL 接入方式分为：*虚拟拨号和专线*

VDSL：采用非对称技术，是各种 DSL 中速率最快的（13-52Mb/s）。

RADSL：采用非对称技术，能在但对双绞线上以高速率下载数据，低速率上传数据，并保持原有语音通信（64Kb/s-12Mb/s）。

HDSL：采用对称技术，为企业用户提供 2Mb/s 的链路。

SDSL：采用对称技术，上行与下行速率均为 1.5Mb/s，但技术不成熟。

1.8 HFC（hybird fiber-coax）

HFC 网综合运用了模拟和数字传输技术、同轴和光纤技术的宽带接入网络，它由光纤干线网（星型）和同轴分配网（树型）组成。

对于 HFC 网络，用户需要安装电缆调制解调器（Cable Modem），该设备提供三种连接：

A、使用同轴电缆连接到机顶盒，在连接到用户电视机；

B、使用一对双绞线连接到用户的电话机；

C、通过四对双绞线连接到用户的计算机。

HFC 利用电缆调制解调器（Cable Modem），在发送端对数据进行调制，在接收端进行解调。

Cable Modem 采用频分复用技术，将信道分为上行信道（10Mb/s）和下行信道（30Mb/s），*一般安装在用户端，不是成对的使用*。采用 MAC（***媒体访问控制协议***）协议。使用 Cable Modem 远程接入需要依赖于运营商一端的线缆调制解调器终结设备 CMTS，该设备向 Cable Modem 提供高速连接。CMTS 的以太网口可以直接与以太网相连，同时可以通过中继线路连接 PSTN 网络；在 HFC 区域中，可以借助光电收发器、光电转换器完成信号的中继和传递，连接至 Cable Modem。

主要优势：

A、仅需要一个光纤节点进行信号转发、转换，节省器件；

B、具有 1000MHZ 的带宽，可传输电话语音业务、高速数据业务和个人通信业务。

C、比传统的 CATV 网络具有更高的资源利用率。

1.9 FTTx 接入

FTTx 是指接入网络光纤化，范围从区域电信机房的局端设备到用户终端设备。

主要分类：

FTTCab：（Fiber To Zhe Cabinet）光纤到交换箱

FTTC：（Fiber To Zhe Curb）光纤到路边

FTTZ：（Fiber To Zhe Zone）光纤到小区

FTTB：（Fiber To Zhe Building）光纤到大楼

FTTH：（Fiber To Zhe Home）光纤到用户，需要光电转换器。

2.0 宽带无线接入

802.11 工作在 2.4Ghz 频率，2Mb/s

802.11b 工作在 2.4Ghz 频率，11Mb/s

802.11g 工作在 2.4Ghz 频率，54Mb/s

802.11a 工作在 5.2Ghz 频率，54Mb/s

802.11h 工作在 5.2Ghz 频率

802.11n 利用 MIMO 技术和 OFDM（频分多路复用）结合在一起，理论上可提供 300Mbps 甚至是 600Mbps 的传输速率

PoE（Power Over Ethernet）技术使用一条以太电缆同时提供以太网信号和直流电源。主要完成对无线 AP、IP 电话机、安全网络摄像机等终端传输数字信号和提供直流电源。提供 44V-57V 的直流电压，功率一般控制在 15.4W。

2.1 SDH 同步数字系列

SDH 主要有两种方式：

IP over SDH：该方式以 SDH 网络作为 IP 网络的物理传输网络，使用链路适配器和帧协议（PPP）对数据包进行封装，然后按字节同步方式将封装后的数据包映射到 SDH 网络中进行传送。IP over SDH 为提供的接口主要是 **POS。**该接口可以提供 **STM-1**（155.52M）及其以上的传输速率。

PDH（准同步数字系列）：这种方式的 STM-1 中封装 63 个 E1 信道，可同时为 63 个用户提供 2Mb/s 的接入速率。该方式提供两种接口，即 **E1 接口**和封装了多个 E1 的 **CPOS 接口。**

几个常用的基本速率：E1 速率为 2.048Mb/s，T1 速率为 1.544Mb/s，OC-1 速率为 51.84Mb/s。

几种关系式：E2=4E1　E3=4E2 E4=4E3

T2=4T1 T3=7T2　T4=6T3

OC-3=3OC-1

E1 采用分时复用技术，共有 32 个时隙，每个时隙提供 64Kb/s 的数据速率，其中 30 个时隙用于传输数据，CH0 用于帧同步，CH16 用于传输信令；

T1 信道采用时分复用技术，共有 24 个时隙，每个时隙提供 56Kb/s 的数据速率。

2.2 VPN 技术

VPN 技术是通过公共网络实现远程用户与远程局域网的互联。

VPN 的关键技术包括：**隧道技术、加密解密技术、密钥管理技术和使用者与设备身份认证技术。**

VPN 技术主要基于数据安全传输协议来完成，主要包括：

二层协议：主要是对传统拨号协议 PPP 的扩展。典型协议为 **L2TP 和 PPTP**。

三层协议：定义了在一种网络层协议封装另一个协议的规范。典型的协议时 **IPSEC 和 GRE**。

IPSEC 主要包括：

网络认证协议 AH：为 IP 网络提供数据源认证，数据完整性、反重播保证和保护通信免受篡改，但**不提供保密服务**。支持的认证算法：HMAC-MD5 和 HMAC-SHA1。

封装安全载荷协议 ESP：为数据包提供完整性检查、认证和加密、机密性和防篡改。

密钥管理协议 IKE：IKE 完成两个任务：（1）安全关联的集中化管理，减少连接时间（2）密钥生成和管理

MPLS VPN 技术：

MPLS 技术主要是为了提高路由器转发速度提出的。核心思想是利用标签交换取代路由运算和路由交换。其技术实现的核心是在 IP 数据包之外封装一个 32 位的 MPLS 包头（MPLS 标签被插入在以太帧头和 IP 头之间）。

MPLSVPN 承载平台由 PE 路由器、CE 路由器和 P 路由器组成，其中 P 路由器是 MPLS 核心网中的路由器，PE 路由器是 MPLS 核心网上的边缘路由器，与 CE 路由器相连，负责待传数据包的 MPLS 标签生成和弹出。CE 路由器直接与电信运营商相连额用户端路由器，该设备不存在任何带有标签的数据包

第四章 因特网

一、预备知识

网络地址：主机为全为 0 的地址

广播地址：主机位全为 1 的地址

狭义Internet 是指由上述网络中采用 IP 协议的网络互联而成的，狭义Intrenet 加上所有能通过路由选择至目的站的网络，便构成了广义Intrenet。

优点：Intrenet 体系结构具有良好扩充性，因为它基于树型结构，具有层次性和单向依赖性。

缺点：对核心网关结构依赖严重，一旦出现故障，整个Intenet 的工作将受到影响，这种结构将逐渐被对等主干结构所取代。

二、网络互连设备

2.1 网络设备

中继器：主要是对接受信号进行再生和发送，其不解释也不改变接收到数字信号。工作在物理层。

集线器：是一个多端口的中继器。

网桥：通过分析帧地址字段，来决定是否将收到的帧发送到另一个网段上。其工作在数据链路层。

交换机：是一个多端口网桥。

路由器：工作在网络层，主要完成协议转换。

网关：对不同的传输层、会话层、表示层和应用层的协议进行翻译和转换。

2.2 广播域与冲突域

冲突域：连接在同一导线上的所有工作站的集合。

中继器和集线器连接的所有节点处在**同一冲突域**中，网桥、交换机和路由器可以分割冲突域。

广播域：指接受同样广播消息的节点的集合。

网桥和交换机连接的所有节点处在**同一广播域**，路由器和三层交换设备可以分割广播域。

2.3 IP 协议

IP 协议时 Internet 中网络层协议，提供无连接的服务

2.3.1 IP 协议提供的服务

IP 协议控制传输的协议单元称为 IP 数据报。IP 数据报中包括收/发双方的 IP 地址。IP 协议提供**不可靠、无连接的、尽力投递**的数据报投递服务。

2.3.2 IP 地址（IPV4）

一个 IP 地址由**网络号**和**主机号**组成，由 4 个字节共 32 位二进制数组成。一般用点分十进制表示。

IP 地址	第一字节	二进制固定	二进制网络	网络数	二进制主机	主机数

分类	十进制范围	高位	位数		数	
A 类	1-126	0	8	126	24	$2^{24}-2$
B 类	128-191	10	16	2^{14}	16	$2^{16}-2$
C 类	192-223	110	24	2^{21}	8	$2^{8}-2$
D 类	224-239	1110	组播地址			
E 类	240-254	11110	留给实验用			

IP 地址配置原则：

（1）网络地址第一个数字不能为 127，127 的地址用于测试连接。

（2）网络地址不能全为 0，也不能全为 255。

（3）只有 A、B、C 类的 IP 地址可以分配给计算机或者网络设备。

私有地址（不允许出现在互联网上）

10.0.0.0-10.255.255.255　　A 类

172.16.0.0-172.31.255.255　　B 类

192.168.0.0-192.168.255.255　　C 类

特殊 IP 地址

0.0.0.0 严格讲这不是一个 ip 地址，在本网络上的本主机。可做源地址。

127.0.0.1 本机地址，用于测试 TCP/IP 协议能否正常工作。

255.255.255.255 限制广播地址。同一广播域的所有主机，这个地址不被路由转发。可以做目的地

169.254.X.X（自动专有地址）当 DHCP 服务器出现故障或者响应时间太长而超出系统规定时间，Windows 会分配一个这样的地址。

224.0.0.0 是一个组播地址。224.0.0.1 指所有主机；224.0.0.2 指所有路由器；224.0.0.5 OSPF 路由协议专用。

2.3.3 子网划分与子网掩码

子网（subnet）：在 TCP/IP 网络上用路由器连接起来的网段。同一子网内的 IP 地址必须有相同的网络地址

无类别 IP 地址（classless）：引入子网划分后的 IP 地址

子网掩码：与 IP 地址成对出现，子网掩码中为 1 的部分表示网络号，为 0 的部分表示主机位。

可变长度子网掩码（VLSM）：允许一个网络使用不同的子网掩码适应不同规模的网络。

子网数= 2^k (k 为子网借用位数)

可用子网数= 2^k-2 (k 为子网借用位数)

例：172.16.0.0/16 规划为 250 个主机的网络 172.16.0.0/24,则可用子网数= $2^{24-16}-2$ 个

可用主机数=2^n-2（n 为主机位数）

有效 IP 地址范围：在一个网段中除去前面一个网络地址和后面一个广播地址后剩余的地址范围

使用路由汇聚时，路由匹配结果应选择最长网络前缀的路由（即，子网掩码最长的作为路由）

2.3.4 IP 协议

IP 数据报由头部和数据部分组成，头部由两部分组成，其中头部固定部分为 20 字节，头部可变部分长度为 4 字节的整数倍。

ARP 协议（报文封装在以太网帧中传送）网络层协议

如果主机 A 向主机 B 发送数据，主机 A 向自己的 ARP 缓存表中寻找主机 B 对应的 MAC 地址，如果有，直接发送；如果没有，主机 A 向网络中发送广播，主机 B 收到广播后，就会将主机 A 的 MAC 写入 ARP 缓存表并以**单播方式**发送 ARP 应答，（内容包括主机 B 的 IP 地址、MAC 地址、主机 A 的 IP 地址、MAC 地址，）主机 A 收到应答后会更新其 ARP 缓存表，并发送数据。

ICMP 报文控制协议（报文封装在 IP 数据报中数据部分传送）ICMP 报文控制协议属于网络层协议

差错控制报文：

目标不可达：不能把 IP 数据报送达目标主机，发送该报文

源抑制：网络出现拥塞，发送该报文

超时：IP 数据报的生存期已超时（TTL=0），发出该报文

参数问题：当判断出 IP 数据报头部字段或语义出错，发送该报文

路由重定向：告诉主机一个更短的路由路径。

询问报文

回送请求：测试两点之间线路是否畅通（ping 命令）

时间戳请求：测试两点之间通信延迟（traceroute 命令 Unix 系统，tracert 命令 windows 系统）

2.4 IPV6 协议

IPV6 数据报包有一个 **40 字节**的基本首部，其后允许有 0 个或多个扩展首部，然后是数据部分。扩展首部和数据部分统称为有效载荷。IPV6 使用了两种安全性扩展，即 IP 身份验证头和 IP 封装安全性净荷

IPV6 地址空间采用 128 位地址长度。其表示方法有：

（1）IPV6 地址长度 128 位，采用冒号分开十六进制表示。

（2）某些 IPV6 地址中有一长串 0，此时可将连续的 0 压缩为一个 0。也可以将连续多个 0000 用双冒号替代。

例：21DA：0000：0000：0000：00C2：0EF0：A57E：78EA

21DA：0：0：0：C2：EF0：A57E：78EA

21DA:: C2: EF0: A57E: 78EA

（3）0 压缩只能出现 1 次

特殊地址

全 0 的地址表示为（::）表示为一个未指明的地址，不能将该地址分给一个接口或者目的地址。

回环地址:（:: 1）用于标识一个回环接口，相当于 IPV4 中的 127.0.0.1。ping:: 1 可以测试本地 IPV6 协议栈是否正常。

兼用 IPV4 地址（:: 192.168.0.1）用于使用公共 IPV4 地址的 IPV6 网络。

IPV4 地址映射

0000: 0000: 0000: 0000: 0000: FFFF:（192.168.0.1）

表示为 :: FFFF:（192.168.0.1）

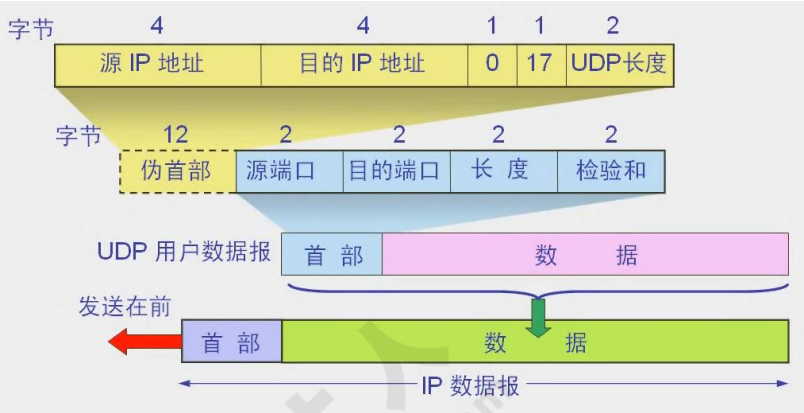
用于仅支持 IPV4 的节点表示 IPV6 地址

2.5 TCP 传输控制协议和 UDP 用户数据报协议

TCP 与 UDP 属于传输层协议

2.5.1 UDP

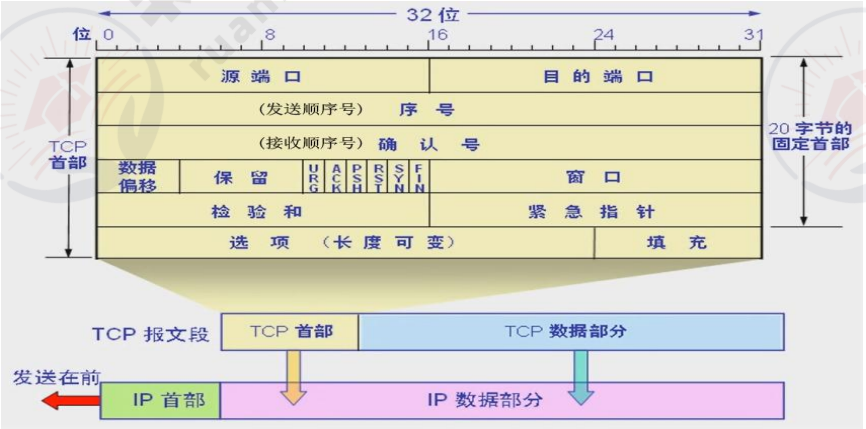
UDP 协议支持**无连接的、不可靠的**数据报投递投递服务，常用于数据量较小的数据传输。



UDP 首部字段 8 个字节，在多媒体应用中，TCP 传输数据，UDP 传输音频、视频。

2.5.2 TCP 协议支持面向连接的、可靠的、面向流的投递服务

TCP 模块之间进行全双工的数据流交换。



允许长达16位的端口值，所以TCP软件可以提供216个不同的端口。

2.5.3 TCP 三次握手，目的是防止产生错误连接

A 发送 SYN，请求建立连接① Seq=X Ctl=SYN → B 返回 SYN 和 ACK ②

Seq=Y ACK=X+1 Ctl=SYN，ACK → A 发送 ACK③ Seq= X+1ACK=Y+1 Ctl=ACK → 建立连接

TCP 四次断开

A 发送 FIN=1，请求断开① Seq=U Ctl=FIN，ACK → B 返回 ACK②

ACK=U+1 Ctl= ACK → A

B 发送 FIN=1，请求断开③ Seq=E ACK=U+1 Ctl=FIN，ACK → A 返回 ACK④

ACK=E+1 Ctl= ACK → B

TCP 进行流量控制的方法是采用可变大小的滑动窗口协议

2.5.4 TCP 连接状态详解

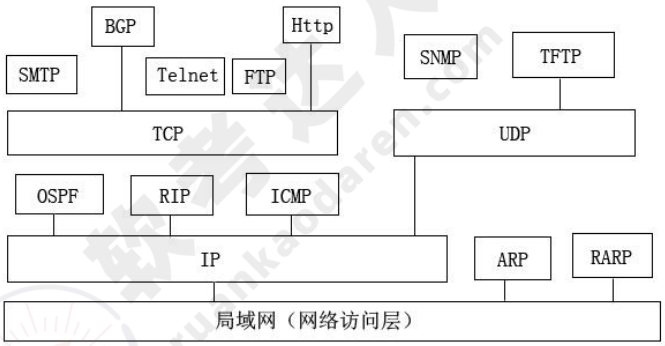
Listen：侦听对方建立连接请求的状态

SYN-SENT：已主动发出建立连接请求

SYN-RECEIVED：收到对方的连接建立请求。

FIN-WAIT 等待对方的连接释放请求

2.6 Internet 体系结构中各个协议图



2.6.1 端口号分类

保留端口号 1-1023，固定的分给一些应用协议使用。常用如下

端口号	传输层协议	用途

20	TCP	FTP 数据
21	TCP	FTP 控制
23	TCP	telnet 远程
25	TCP	Smtp
53	TCP/UDP	DNS
69	UDP	TFTP
80	TCP	Http
110	TCP	POP3
161	UDP	SNMP
162	UDP	SNMP(trap)
443	TCP	https

注册端口号 1024-49151，需要在 IANA 注册防止重复

动态端口号 49152-65535，用来分配给请求通信的客户进程

2.7 域名系统 DNS

名称解析方法：

Hosts 表：是一个没有扩展名的文本文件。其中存放一些常用的主机域名和其对应的 IP 地址映射，文件中每一行对应一个条目。

NIS 系统：由 sun 公司开发的域名系统。用于中小型系统。

DNS 系统：规定域名中的标号由英文字母和数字组合而成，每个标号不能超过 63 个字符，为方便记忆一般不超过 12 个字符。

DNS 查询过程：

本地解析：客户机平时查询得到的 DNS 记录均保存在本地 DNS 缓存中，当有进程提出 DNS 查询时，DNS 客户端先使用本地缓存的信息来解析，如果可以解析则直接应答查询而不必向 DNS 服务器查询。**本地解析有两个来源：Hosts 表和 DNS 缓存。**

直接解析：如果本地解析不能找到 DNS 信息，则客户端向其所设定的 DNS 服务器发出查询请求，服务器收到请求后先检查本地配置区域中是否有所需查询信息，如果有则作出应答，如果没有，服务器则检查能否通过其缓存的查询信息来解析，如果有则作出应答。

递归解析：如果 DNS 服务器不能解析该查询信息，则服务器向上级 DNS 服务器查询，直到查询到该信息为止。**（服务器默认配置）**

迭代解析：如果 DNS 服务器不能解析该查询信息，服务器不会向上级 DNS 服务器查询该信息，而是将上级 DNS 服务器地址告诉给客户端，由客户端向上级 DNS 服务器查询该信息。

```
C:\>nslookup
Set type=ptr
>ip 地址
```

将 IP 地址转换为域名

DNS 对象类型与资源记录

A： 域名到 IP 地址的映射。

PTR： 将 IP 地址转换为域名

NS： 指明授权服务器

MX： 邮件交换

CNAME: 允许多个域名指向同一台服务器（别名）

SOA： DNS 数据库的来源

2.8 远程登录协议 Telnet　端口 23

用户在本地使用虚拟终端（NVT）通过 TCP 连接可以登录到远程的主机或服务器，像使用本地主机一样使用远程资源。

其他协议

FTP 文件传输服务　控制端口 21　　数据端口 20

FTP 常用命令：

Get： 从远端传送文件至本地主机

Open ip 打开 FTP

Dir 显示服务端那些文件可以下载

! dir 显示客户端目录文件

Put 上传文件

List： 请求远端返回当前目录下的目录和文件

Lcd： 改变当前本地主机的工作目录

Bye 推出

DHCP 服务过程：工作在 UDP 基础上应用层协议，采用客户机/服务器模式，服务器使用 **UDP 端口 67**，客户端使用 **UDP 端口 68**

客户机 —向网络中广播 DHCPdiscover 数据包，数据报中附加来源地址 0.0.0.0，目的地址 255.255.255.255→ **服务器**

←服务器收到 DHCPdiscover 数据包，通过广播 DHCPoffer 数据包作出响应，包含 IP，mac，租约期等

选择第一个收到 DHCPoffer 包作出响应，发送 DHCPrequest 广播包，告诉所有 DHCP,它将采用哪个服务器的 IP 地址。同时客户机还发送 ARP 数据报，查询网络中是否有该 IP 地址，如果该 IP 被占用将会发出 DHCPdecline 数据报给服务器，拒绝其 DHCPoffer，并重新发送 DHCPdiscover

服务器收到 DHCPrequest 数据包后，便向客户机提供包含 IP 地址及其它设置的 DHCPpack 的确认信息。租约期默认为 8 天

当租约期过一半时（50%）重新向服务器发送 DHCPrequest 数据包，以便继续租用原来 IP，如果租约成功，更新租约，否则继续使用原来 IP。

当租约过一半没有租约成功，则在剩下的租约期限再过一半（87.5%）时，发出 DHCPdiscover 广播包，向其它服务器获取新的租约。**DHCP 是 BOOTP 协议的扩展**

HTTP 协议提供的主要操作：

Get：读取一个网页

Head：读取头部信息

Post：把消息加载到指定的网页上

NAT 把内部私有地址转换成为外部全局地址，主要分为静态 NAT、动态 NAT 和端口复用 NAPT

2.9 网关协议

自治系统内部网关之间交换路由信息执行内部网关协议 IGP;

不同的自治系统之间交换路由信息执行外部网关协议 EGP

外部网关协议

最新的外部网关协议 EGP 叫做边界网关协议 BGP。

BGP 特点

BGP 报文通过 TCP 连接传送（端口 179）。

BGP 属于距离矢量路由算法协议

采用增量更新，触发更新

周期性的发送 Keepalive 信息验证 TCP 连接

支持路由汇总 CIDR 技术

BGP 三张表：邻居表、BGP 转发表、路由表

BGP 具体有四种报文：

Open 报文：用于建立邻居关系

Update 报文：用于发送新的路由信息

Keepalive 报文：用于对 open 的应答和周期性的确认邻居关系

通告报文：用于报告检测到的错误

基本配置命令：

Router bgp 64512(自治系统号)

Neighbor {ip-address|peer-group-name remote-as autonomous-system}

Network network-number mask network-mask

例：Router bgp 65102

Neighbor 192.168.0.1 remote-as 65101

Network 172.16.4.0 mask 255.255.0.0

RIP 原理与配置命令（rip 基于 Bellman-Ford 算法）

RIP 属于**距离矢量**算法的路由选择协议，通过**广播方式周期性（30s）**的通告路由表，其最大跳步数为 **15 跳**。

RIP 有两个版本分别为 RIPv1 和 RIPv2。区别在：

（1）RIPv1 不支持可变长度子网掩码（VLSM），而 RIPv2 支持 VLSM；

（2）RIPv2 支持明文和 MD5 密文认证；

（3）RIPv1 采用广播方式更新路由，而 RIPv2 采用组播方式更新路由，组播地址 224.0.0.9；

（4）RIPv2 采用触发更新方式来加速路由收敛。

（5）RIPv2 采用水平分割方法来消除路由循环，即，一条路由信息不会发给该信息的来源方。

（6）RIPv2 支持路由汇总 CIDR

1、**最大度量值**，最大跳步数为 15，当为 16 时，认为网络不可达，丢弃数据包。

2、**水平分割**来避免路由环路，即，一条路由信息不会发给该信息的来源方。

3、**路由中毒**。标记该路由为无穷大，中毒路由被发给邻居路由器，通知该路由失效。

4、**反向下毒**。当邻居路由器被成功下毒后，邻居路由器会向毒源方向下毒。

5、**保持时间**，让路由器保持 down 状态一段时间，直到所有路由器均学习到该路由的状态，同时在保持时间为超时是，不再接收邻居路由器发来关于该路由的更新信息

基本配置命令

Router rip //启用 RIP 路由进程

Version 2 //声明 RIP 版本为第二版

Network 192.168.5.0 //发布直连网段，可以写上掩码，不写 RIP 会根据接口 IP 自动判断

OSPF 原理与配置命令（ospf 基于 Dijkstra 算法）

OSPF 开放式最短路径优先协议，是一种**链路状态路由协议。**OSPF 主要**优点**

（1）OSPF 没有跳数限制。

（2）OSPF 支持 VLSM 和 CIDR

（3）OSPF 采用触发更新，收敛速度快

三张表：邻居表 拓扑表 路由表

OSPF 网络一般划分为两个逻辑的级别层次：**骨干区域**一般记为 **area0，非骨干区域**

运行 OSPF 的路由器通过邻接的路由器发送 hello 报文，来发现邻居路由器，路由器核实 hello 报文后，宣布邻居关系。

DR 指定路由器，担任 LSA 信息集中点

BDR 备份指定路由器。LSA 信息第二集中点，通过计时器监视 DR 的更新活动。

DR 与 BDR 选举

路由器**优先级**（默认为 1）高的为 DR，优先级相同则为 **router ID 大**的为 DR,一般 router ID 为**最大的 IP** 地址，如果有回环口，则**回环口 IP** 优先为 ID。

优先级为 0 不参加选举，优先级影响一个选区进程，但不强制更新已生效的 DR 和 BDR 路由器。

Hello 报文采用**组播方式发送**,地址为 **224.0.0.5**,其大小为 50 字节。LSA，链路状态通告，LSU，链路状态更新包。

在 OSPF 网络中，路由器定时发出 Hello 分组与特定的邻居进行联系，默认情况下 40s 没收到该分组就认为对方不存在了。

OSPF 协议支持 4 种网络类型，分别是广播多址、非广播多路访问、点对点、点对多。其中广播多址网络包括 Ethernet 和 FDDI；非广播多路访问包括帧中继、X.25 和 ATM；点对点网络包括 PPP、HDLC 和 Lapb。

基本配置命令

Router ospf process-id //启动 ospf 进程

Network address *反掩码* area *area-id*

ip ospf priority 10 //范围为 0-255

ip ospf cost 200 //范围 1-65535

例：

Router ospf 50

Network *10.0.0.0 0.255.255.255* area *0* *//发布的直连网段*

Network *10.1.1.2 0.0.0.0* area *0* *//发布的时直连 IP 地址，此时反掩码应写为 0.0.0.0*

IGRP 原理与配置命令

IGRP 是**距离矢量路由协议**，由 cisco 公司设计，每 90s 发送一次路由更新广播，如果 **270s** 没有收到路由更新，则认为路由不可访问，**630s** 后清除该路由。

IGRP 采用**带宽、延迟、可靠性和负载**作为度量标准，量度最小的做最佳路径，不支持 VLSM 和不连续子网。

基本配置命令

Router igrp 109 //109 自治系统号

Network network-number //发布直连网段

Bandwidth 带宽 **单位为 Kbps**

Clock rate 时钟

EIGRP 是 cisco 在 IGRP 基础上的一种新的改进型协议，其度量值有：**带宽、延迟、可靠性、负载、最大传输单元。**支持 VLSM 和 CIDR

EIGRP 基本配置命令

Router eigrp 109 //109 自治系统号

Network network-number //发布直连网段，**网段是子网时带反掩码**

No auto-summary //处理不连续子网时关闭汇总

常见路由协议管理距离

RIP 管理距离 120，IGRP 管理距离 100，EIGRP 管理距离 90，OSPF 管理距离为 110，直连网段管理距离为 0

第五章 路由器与交换配置

路由器基本配置命令

Route>　　//用户模式
enable　//进入特权模式
config terminal　//进去全局配置模式
hostname *route1*　//设置路由器的名称为 route1
enable secret *123*　//设置 enable 加密口令为 123（以密文显示，权限高）
enable password *123* //设置 enable 口令（以明文显示，两者同时配置，前者生效）
no ip domain-lookup　//取消域名解析
ip classless　//开启 IP 无类别策略。目的是告诉路由器，当收到无法转发的数据包时将其传递给默认路由，而不是简单的丢弃，与默认路由一起使用。
ip subnet-zero　//支持零子网
line console 0　//进入控制台线路配置模式(超级终端)
password *123*　//设置 console 登录密码为 123
exec-timeout *30 30*　//设置路由器超时时间为 30 分钟，30 秒后自动弹出到用户模式，设置为 0 0 则永远不超时。
Login　//要求登录时输入口令
line vty 0 4　//进入虚拟终端线路配置模式（telnet）
exec-timeout *30 30*　//设置路由器超时时间为 30 分钟，30 秒后自动弹出到用户模式，设置为 0 0 则永远不超时。后一个 30 的单位是秒。
password *123*　//设置 VTY 登录密码为 123
login　//要求登录时输入口令
exit　//退出当前模式
copy running-config startup-config　//将更改保存到 nvram
service password-encryption　//对所有密码加密
interface *fa0/0*　//进入 fa0/0 接口配置模式
ip address *192.168.1.1 255.255.255.0*　//设置接口 IP 地址
no shutdown　//激活接口
interface *s0*　//进入 s0 接口

ip address *192.168.2.2 255.255.255.0*
clock rate 9600　//设置时钟频率
no shutdown
exit
ip routing　//允许路由配置。没有该语句将导致配置的路由无效。
No ip routing　//禁用路由配置
ip route *目标网段 子网掩码 下一跳入口 IP 地址*　//静态路由
ip route 0.0.0.0 0.0.0.0 *下一跳入口 IP 地址*　//默认路由
exit
end　//退出到特权模式（与 ctrl+z 一样）
show ip route　//查看路由表
show interface *fa0/0*　//查看 fa0/0 接口信息
show ip protocol　//查看路由协议
show ip interface brief　//查看端口简要信息

IPV6 配置

Config terminal
Hostname R1
Ipv6 unicast-routing　//开启 ipv6 单播路由
Interface f0/0
Ipv6 address 2005:CCCC::1/64
No shutdown
Exit
Interface serial0/2/0
Ipv6 address 2007:CCCC::1/64
Clock rate 128000
Exit
Ipv6 route 2004:CCCC::/64 serial0/2/0

IPV6 GRE 隧道配置

Interface tunnel 0　//启用通道 0
Tunnel source s1/0　//通道源地址为 s1/0，（本端路由器接口）
Tunnel destinaltion 202.100.2.2　//通道目的地址，（对端路由器地址）

Ipv6 address 2005:AAAA::1/64 //为通道配置 ipv6 地址
Tunnel mode gre ipv6 //通道模式为 ipv6 的 gre 隧道
Ipv6 rip test enable //在路由器通道 0 上启用 rip，并命名为 test
Interface f0/0
Ipv6 rip test enable //在路由器 f0/0 上启用 rip，并命名为 test

IPV6 NET-PT(静态)

Config terminal
Interface e0
Ip address 192.17.5.1 255.255.255.0
Ipv6 nat //在接口上启用 nat-P
Interface e1
Ipv6 address 2001:aaaa::1/64
Ipv6 nat
Exit
Ipv6 nat prefix 2001:aaaa:0:0:0:1::/96 //说明在 ipv6 域内使用的 ipv6 前缀
Ipv6 nat v4v6 source 2001:aaaa::2 192.17.5.200 //将源 ipv6 地址输出的 ipv6 数据包转成 ipv4 数据包
Ipv6 nat v4v6 source 192.17.5.2 2001:aaaa:0:0:0:1::8 //将源 ipv4 地址输出的 ipv4 数据包转成 ipv6 数据包

IPV6 NET-PT(动态)

Config terminal
Interface e0
Ip address 192.17.5.1 255.255.255.0
Ipv6 nat //在接口上启用 nat-P
Interface e1
Ipv6 address 2001:aaaa::1/64
Ipv6 nat
Exit
Ipv6 nat prefix 2001:aaaa:0:0:0:1::/96 //说明在 ipv6 域内使用的 ipv6 前缀
Ipv6 nat v6v4 pool ipv4-pool 192.17.5.10 192.17.5.20 prefix-length 24 //指定名为 ipv4-pool 的 ipv4 地址池

Ipv6 nat v6v4 source list ipv6 pool ipv4-pool //**配置** NAT-PT **映射**

RIP 配置

Router rip //启动 rip 协议
Version *2* //设置 rip 版本为第 2 版
Network *192.168.1.0* //发布直连网段
No auto-sumary //取消路由协议自动汇总
ip split-horizon //配置水平分割
Exit
interface *fa0/0* //进入接口配置模式
ip rip send version 1 2 //该接口发送 ver1 和 ver2 报文
ip rip receive version 1 2 //该接口接收 ver1 和 ver2 报文

IGRP 配置

Interface fa0/0
Ip address 192.168.3.1 255.255.255.0
No keepalive //不监测 keepalive 信号，即不连接设备时可激活该接口
Exit
Interface serial 0
Ip address 192.168.4.1 255.255.255.0
Bandwidth 1544 //设置带宽为 1.544Mbps
Clock rate 512000
Exit
Router igrp 100
Network 192.168.3.0
Network 192.168.4.0

EIGRP 配置

Router eigrp 100 //启动 eigrp 协议进程，100 为自治系统号
Network 192.168.1.0 //发布直连网段
Network 172.16.4.4 0.0.0.3 //此处地址为子网地址，需写出反掩码
Network 172.16.4.12 0.0.0.3
No auto-sumary //取消路由协议自动汇总

Ospf 配置

Router ospf 1　//启动 ospf 协议进程，1 为进程号
Network 192.168.1.0 0.0.0.255 area 0　//发布直连网段
Network 192.168.2.1 0.0.0.0 area 0　//发布的网络为端口地址时，反掩码为 0.0.0.0
Show ip ospf　//查看 ospf 信息

Frame-relay 配置

Interface s0　//进入 s0 接口配置模式
Encapsulation frame-relay　// 对 串 口 s0 进 行 frame-relay 封 装
frame-relay lmi-type ansi　//设置帧中继的 lmi 类型
Interface s0.1 point-to-point　//进入子接口配置模式
Ip address 192.168.1.1 255.255.255.0
Frame-relay interface-dlci 100　//设置 dlci 编号为 100
Frame-relay map ip 192.168.1.2 100 broadcast　//设置 ip 地址与帧中继 DLCI 之间的映射，并允许广播（*另外一种配置*）

NAT 配置

静态 nat

Config terminal
ip nat inside source static *192.168.1.2* *25.98.192.2*　源地址　目的地址
　//手动定义转换映射关系
ip nat inside source static *192.168.1.3*　*25.98.192.3*

ip nat inside source static *192.168.1.4*　*25.98.192.4*
ip address *192.168.1.1* *255.255.255.0*
ip nat inside　//定义内部接口
interface fa0/2
ip address *25.98.192.254* *255.255.255.0*
ip nat outside　//定义外部接口

动态 nat

Config terminal
Ip nat pool cisco *25.98.192.2* *25.98.192.254* netmask 255.255.255.0　//定义目的地址范围

access-list 1 permit *10.1.1.2 0.0.0.255* //定义访问控制列表
ip nat inside source list 1 pool cisco //启用 nat，私有地址来源于 list1，使用 pool 名为 cisco 地址池内的公网 ip 进行转换
interface fa0/1
ip address *10.1.1.1 255.255.255.0*
ip nat inside
interface fa0/2
ip address *25.98.192.1 255.255.255.0*
ip nat outside

动态复用地址转换

Config terminal
access-list 1 permit 10.1.1.2 0.0.0.255
ip nat inside source list 1 interface fa0/2 **overload** //启用 nat，私有地址来源于 list1，使用 fa0/2 上的公网 ip 转换，overload 使用端口转换
ip address 10.1.1.1 255.255.255.0
ip nat inside //定义内部接口
interface fa0/2
ip address 25.98.192.254 255.255.255.0
ip nat outside //定义外部接口

访问控制列表 ACL

标准访问控制列表仅检查源地址，列表号为 1-99；扩展访问控制列表不仅要检查源地址，也检查包的目的地址，也可以检查协议类型、端口号和其它参数

（1）允许网络地址 172.16.0.0 通过，但拒绝 172.16.19.2 通过

Config terminal
Access-list 1 deny host 172.16.19.2
Access-list 1 permit 172.16.0.0 0.0.255.255
Interface fa0/1
Ip access-group 1 out

(2)禁止主机 A（172.16.16.2）远程登录路由器 B（172.16.17.1）

Access-list number permit|deny protocol source destination

Config terminal

```
Access-list 110 deny tcp host 172.16.16.2 host 172.16.17.1 eq telnet
Access-list 110 permit ip any any
Interface fa0/1
Ip access-group 110 out
```

(3)允许主机 A（172.16.16.2）远程登录路由器 B（172.16.17.1）

```
Config terminal
Access-list 110 permit tcp host 172.16.16.2 host 172.16.17.1 eq telnet
Interface fa0/1
Ip access-group 110 out
```

交换机基本配置命令

```
Switch>     //用户模式
enable  //进入特权模式
config terminal  //进入全局配置模式
hostname sw1  //设置交换机的名称为 sw1
enable secret 123  //设置使能密码（以密文显示，权限高）
enable password 123 //设置使能口令 (以明文显示, 与使能密码同时使用时, 使能密码有效)
no ip domain-lookup  //取消域名解析
line console 0  //进入控制台线路配置模式(超级终端)
password 123    //设置 console 登录密码为 123
exec-timeout 30 30  //设置路由器超时时间为 30 分钟，30 秒后自动弹出到用户模
                    式，设置为 0 0 则永远不超时。
Login              //要求登录时输入口令
line vty 0 4  //进入虚拟终端线路配置模式（telnet）
exec-timeout 30 30  //设置路由器超时时间为 30 分钟，30 秒后自动弹出到用户模
                    式，设置为 0 0 则永远不超时。后一个 30 的单位是秒。
password 123    //设置 VTY 登录密码为 123
login          //要求登录时输入口令
exit
interface vlan1  //进入 vlan1 配置模式
ip address 192.168.1.1 255.255.255.0  //ip 地址为 192.168.1.1
no shutdown  //启用该接口
```

exit
ip default-gateway 192.168.1.254 //设置默认网关为 192.168.1.254
ip name-server 192.168.2.1 //设置域名服务器
ip domain-name wqs.com //设置域名
interface fa0/1
speed 100 //设置带宽为 100Mbps bandwidth 单位为 Kbps
duplex full //设置为全双工模式

VTP 配置

Vlan database // 进入 vlan 配置模式
Vtp version 2 //启用版本 2 的 vtp
Vtp domain *305* //设置域名为 305
Vtp domain *server/client/transparent* //设置交换机为服务器模式（客户模式或者透明模式）
Vtp password 123 //配置 vtp 口令
Vtp pruning //启动 VTP 修剪功能
Vlan 1 name *aa* //创建 VLAN1 名为 aa
Vlan 2 name *bb* //创建 VLAN2 名为 bb
Vlan 3 name *cc* //创建 VLAN3 名为 cc
Exit
Show vtp status //查看 VTP 配置信息

生成树协议 STP

Congfig terminal
Spanning-tree vlan *2* root primary //配置为根交换机
Spanning-tree vlan *2* root secondary //设置为从根交换机
Spanning-tree vlan *2* priority *4096* //修改交换机优先级。数值为 4096 的倍数，值越小，优先级越高。
Interface fa0/1
Spanning-tree vlan *2*port-priority 10 //端口优先级为 10，默认值是 128，取值范围是 0-255
Spanning-tree vlan *2* cost 30 //设置 vlan2 生成树路权值为 30
Spanning-tree port-fast //设置端口为快速端口

（1）创建 VLAN1 和 VLAN2 并将 1-8 口分配给 VLAN1，9-23 口分给 VLAN2，将 24 口设置为干道

Enable　　//进入特权模式
vlan database　//进入 VLAN 配置模式
Vlan 3 name *shichang*　//建立 VLAN3 并命名为 shichang
Vlan 4 name *yingxiao*　//建立 VLAN4 并命名为 yingxiao
exit
Config terminal　　//进入配置模式
Interface range *fa0/1-8*　//进入组配置模式
Switchport mode access　//设置这组接口为接入模式
Switchport access vlan 3　//将组接口分配给 VLAN3 下的接口
Interface range *fa0/9-23*
Switchport mode access
Switchport access vlan 4
Interface fa0/24　//进入接口配置模式
Switchport mode trunk　//设置 24 口为中继模式
Switchport trunk encapsulation dot1q　//设置 trunk 封装
switchport trunk allowed vlan *all*　//设置允许从该接口交换数据 vlan
End
Show vlan　//查看 vlan 信息

> **注:**交换机支持的封装协议有 **dot1q** 和 **ISL** 两种。ISL 最多支持 **1024** 个 vlan；而 dot1q 支持 **4096** 个 vlan，其中两个保留，因此可用 4094 个

交换机 B 为客户模式。24 口为干道模式

交换机 A:

enable
Vlan database
Vtp domain *305*　　//设置域名为
Vtp mode server　//设置本交换机为服务器模式
Vlan 1 name *aa*　//建立 VLAN1 并命名为 aa
Vlan 2 name *bb*　//建立 VLAN2 并命名为 bb

```
exit
Config terminal
Interface range fa0/1-8
Switchport mode access
Switchport access vlan 1
Interface range fa0/9-23
Switchport mode access
Switchport access vlan 2
Interface fa0/24
Switchport mode trunk
Switchport trunk encapsulation dot1q  //设置 trunk 封装
switchport trunk allowed vlan all  //设置允许从该接口交换数据 vlan
```

交换机 B:

```
Enable
Vlan database
Vtp domain 305
Vtp mode client  //设置本交换机为客户模式
exit
Config terminal
Interface range fa0/1-8
Switchport mode access
Switchport access vlan 1
Interface range fa0/9-23
Switchport mode access
Switchport access vlan 2
Interface fa0/24
Switchport mode trunk
Switchport trunk encapsulation dot1q  //设置 trunk 封装
switchport trunk allowed vlan all  //设置允许从该接口交换数据 vlan
```

（3）VLAN 间路由

交换机:

```
enable
vlan database
vlan 10
vlan 20
exit
config terminal
interface E0/1
swichport mode access
switchport access vlan 10
no shutdown
interface E0/2
switchport mode access
switchport access vlan 20
no shutdown
interface E0/3
switchport mode trunk
switchport trunk encapsulation dot1q
switchport trunk allowed vlan all  //设置允许从该接口交换数据 vlan
no shutdown
```

路由器

```
config terminal
interface e0/0.1  //进入子接口配置模式
encapsulation dot1q 10  //设置封装模式
ip address 192.168.0.1 255.255.255.0
interface e0/0.2
encapsulation dot1q 20
ip address 10.10.10.1 255.255.255.0
exit
interface e0/0
duplex full
no shutdown
```

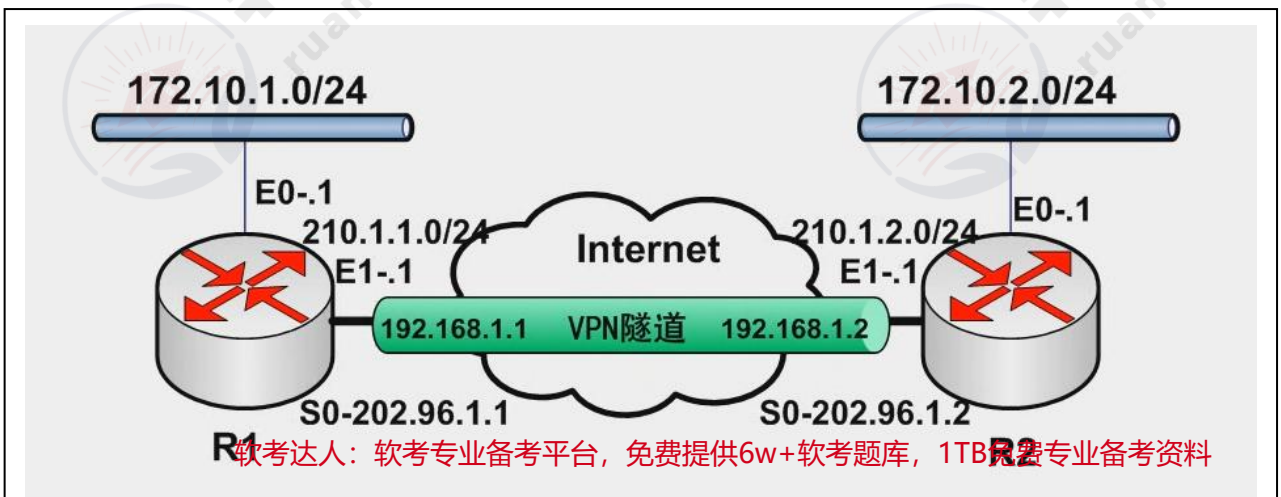
（4）stp 配置

交换机 A 的 fa0/0 对应 trunk1，其 vlan1-3（path cost18），vlan4-5（path cost30）；fa0/1 对应 trunk2，其 vlan1-3（path cost30），vlan4-5（path cost18）。

交换机 A：

```
Config terminal
Interface fa0/0
switchport mode trunk
switchport trunk encapsulation dot1q
switchport trunk allowed vlan all
Spanning-tree vlan 3 cost 18
Spanning-tree vlan 2 cost 18
Spanning-tree vlan 1 cost 18
Spanning-tree vlan 4 cost 30
Spanning-tree vlan 5 cost 30
exit
Interface fa0/1
switchport mode trunk
switchport trunk encapsulation dot1q
switchport trunk allowed vlan all
Spanning-tree vlan 1 cost 30
Spanning-tree vlan 2 cost 30
Spanning-tree vlan 3 cost 30
Spanning-tree vlan 4 cost 18
Spanning-tree vlan 5 cost 18
```

VPN 配置



以 R1 为例

Config terminal

Cypto isakmp enable //启用 ike

Cypto isakmp policy 1 //配置 IKE 策略，1 为策略号，自定义

Group 1 //1 的参数密钥长度为 768 位，2 的参数密钥长度为 1024 位,默认为 DES 算法

Authentication pre-share //采用预先共享密码认证方式

Lifetime *86400* //调整 SA 周期，单位是秒

Cypto isakmp key *123456* address *202.96.1.2* //设置对等体的共享密钥为 123456。**202.96.1.2** 为对端路由器地址，根据实际修改

Cypto ipsec transform-set test ah-md5-hmac esp-des //设置名为 test 的交换集，ah 的散列算法为 md5，esp 加密算法为 des

Cypto map *tt* 10 ipsec-isakmp //设置加密图，名称为 tt，序号为 10，使用 IKE 来建立 IPSEC 安全关联，以保护由该加密图所指定的数据流

Set peer *202.96.1.2* //标识对方路由器的合法 ip 地址

Set transform-set test //将加密图用于交换集

Access-list 130 permit host 202.96.1.1 host 202.96.1.2
源地址 目的地址

match address 130 //设置匹配 130 的访问列表

interface tunnel 0 //定义隧道接口

ip address 192.168.1.1 255.255.255.0 //定义隧道接口 IP

no ip directed-broadcast

tunnel source 202.96.1.1 //定义隧道接口源地址

tunnel destination 202.96.1.2 //定义隧道借口目的地址

cryto map tt //将加密图应用于此端口

interface s0

ip address 202.96.1.1 255.255.255.252

no ip directed-broadcast

cryto map tt //将加密图应用于此端口

Interface e0/1

```
Ip address 210.1.1.1 255.255.255.0
no ip directed-broadcast
Interface e0/2
Ip address 172.10.1.1 255.255.0.0
no ip directed-broadcast
ip classless
ip route 0.0.0.0 0.0.0.0 202.96.1.2
ip route 172.10.1.2 255.255.0.0 192.168.1.2  //设置内网静态路由
```

PIX 防火墙的配置

```
Config terminal
Nameif eth0 outside security 0  //外部接口命名并定义安全级别
Nameif eth1 inside security 100
Nameif dmz security 50
Interface eth0 auto  //设置 eth0 为自适应网卡类型
Interface eth1 100full  //设置 eth1 为 100M 全双工
Interface eth1 100full shutdown  //关掉此接口
ip address outside 61.144.51.42 255.255.255.248 //配置外网地址
ip address inside 192.168.0.1 255.255.255.0  //配置内网地址
```

```
nat (inside) 1 0 0  //启用 nat，内网所有主机访问外网
nat (inside) 1 172.16.5.0 255.255.0.0  //172.16.5.0 网段可以访问外网
```

```
global (outside) 1 61.144.51.42-61.144.51.48
        //使用网段 61.144.51.42-61.144.51.48 为内网提供 IP 地址
global (outside) 1 61.144.51.42
        //访问外网时，所有主机统一使用 61.144.51.42 地址
```

global (outside) number ipaddress-ipaddress *[netmask mask]*

```
Static(inside,outside) outside-ipaddress inside-ipaddress
Static (inside,outside) 61.144.52.62 10.0.1.3  //创建内网地址 10.0.1.3 与
    外网地址 61.144.52.62 之间的映射
Static(dmz,outside) 211.48.16.2 172.16.10.8  //创建 dmz 地址 172.16.10.8
      与外网地址 211.48.16.2 之间的映射
```

Conduit Permit|deny global_ip port protocol foreign_ip

Conduit permit tcp host 192.168.0.8 eq www any //允许任何外部对全局地址 192.168.0.8 主机进行 http 访问（*主机提供 http 服务*）

Conduit deny tcp any eq ftp host 61.144.51.89 //禁止外部主机 61.144.51.89 访问内部 ftp

Conduit permit icmp any any //允许 icmp 消息通过

Fixup protocol ftp 21 //启用 ftp 协议并指定端口为 21

Fixup protocol http 80

Fixup protocol http 8080 //指定 http 协议运行的端口为 80 和 8080

No fixup protocol smtp 80 //禁用 smtp 协议

Route(inside|outside) 0 0 gateway-ip number //number 表示 gateway 跳数，通常为 1，

Route outside 0 0 61.144.51.168 1 //指向边界路由器 61.144.51.168 的默认路由

Route inside 10.1.1.0 255.255.255.0 172.16.0.1 1 //创建一条从 10.1.1.0 网络到 172.16.0.1 的静态路由

ISDN 配置

Config terminal

Isdn switch-type basic-net3 //设置 iSDN 交换类型

Interface bri 0 //进入 BIR 接口配置模式

Ip address 192.168.0.1 255.255.255.0

Encapsulation ppp //封装协议为 PPP

Dialer string 888888 //设置拨号串,R2(对端路由器)的 ISDN 号码

Dialer-group 1 //设置拨号组号 1，把 bri 0 接口与拨号列表 1 相关联

No shutdown

Exit

Dialer-list 1 protocol ip permit //设置拨号列表 1

Ppp anthentication chap //设置认证方式

Dialer map ip 200.10.1.1 name R2 broadcast 888888 //设置协议地址与电话号码的映射（对端 IP 和 ISDN 号）

Ppp multilink //启用多多链路

Dialer load-threshold 128 //设置启用另一个 B 通道的阀值

Clock rate speed //设置 DCE 端的线速度

策略路由配置

希望部分 IP 走 A 线路 1.1.1.1，另一部分走 B 线路 2.2.2.2

Config terminal

==========第一步创建匹配源列表==========

Access-list 1 permit 192.168.1.0 0.0.0.255 //匹配地址列表

Access-list 2 permit 192.168.2.0 0.0.0.255

==========第二步配置 Route-map==========

Route-map test permit 10 //创建路由映射规则

Match ip address 1 //匹配列表 1

Set ip next-hop 1.1.1.1 //执行动作是送往 1.1.1.1

Exit

Route-map test permit 20

Match ip address 2 //匹配列表 2

Set ip next-hop 2.2.2.2 //执行动作是送往 2.2.2.2

Exit

==========第三步在接口上应用 Route-map==========

Interface f0/0

Ip address 192.168.1.1 255.255.255.0

Ip policy route-map test

第六章 网络安全

一、网络安全威胁

网络安全威胁的主要种类：窃听、假冒、重放、流量分析、拒绝服务、数据完整性破坏、非授权访问、陷门和木马、病毒和诽谤。

网络攻击的手段：被动攻击、主动攻击、物理临近攻击、内部人员攻击和分发攻击。

网络安全措施：数据加密、数字签名、身份认证、防火墙和入侵检测。

1.1 数据加密

基本思想：通过**变换**信息的**表现形式**来伪装需要保护的敏感信息，非授权者不能了解被加密的内容。

明文：需要隐藏的信息

密文：产生的结果

密码算法：加密时使用的变换规则

信息安全的核心是密码技术，密码技术的目的是研究数据保密

一个加密系统采用的基本工作方式成为**密码体制**，密码体制的基本要素是**密码算法**和**密钥**，其中密码算法分为**加密算法**和**解密算法**，密钥分为**加密密钥**和**解密密钥**。

1.1.1 密码体制分为**对称密码体制**和**非对称密码体制**。

对称密码体制：加密密钥和解密密钥相同，或者从一个可以导出另一个，拥有加密能力就拥有解密能力。

对称密码体制的**保密强度高，开放性差**，需要**可靠的密钥传递渠道**。

要求发送和接收数据的双方使用相同的**对称密钥**对明文进行加密和解密运算。

常用算法有：DES，IDEA，TDEA,AES,RC2,RC4,RC5。

DES：属于**对称密码体制**，将分组为 64 位的明文加密称 64 为密文。其密钥长度为 56 位附加 8 为奇偶校验。加密过程执行 16 个加密循环。

三重 DES：使用**两个密钥**，执行**三次 DES 算法**，在第一和第三层使用相同的密钥，其主密钥长度为 112 位。

IDEA：属于**对称密码体制**，将分组为 64 位的明文加密成 64 为密文。使用

128 位密钥，加密过程执行 17 个加密循环。

AES 支持 128、192 和 256 位三种密钥长度。

非对称密码体制：又称**公开密钥**，加密和解密是分开的，即，**加密密钥公开，解密密钥不公开**，从一个区推导另一个是不可行的。

非对称密码体制适用于开放的使用环境，密钥管理简单，但工作效率低于对称密码体制，常用于实现数字签名与验证。

RSA 算法：非对称密码体制。理论基础是数论中大素数分解。

加密密钥公开称为**公钥，解密密钥**隐藏在个体中称为**私钥**。私钥带有个人特性，可以解决**数据的签名验证**问题。**公钥用于加密和认证，私钥用于解密和签名**

该算法特点实现效率低，不适用于长明文加密，长与对称密码体制相结合使用。

主要的非对称密钥算法有：RSA 和 ECC

例：

已知两个奇数 p,q,公钥 e，求 d

解：

两个数同余运算 $r=p\times q$

根据 Euler 函数 $z=(p-1)(q-1)$

取小于 r 的整数 e 并且与 z 没有公约数。这里 e 已知。

找到 d 满足 $ed-1$ 能被 z 整除

1.1.2 加密的基本方法：置换和异位

置换：改变明文内容的表现形式，但内容元素的相对位置不变。

异位：改变明文内容相对位置，但表现形式不变。

数据加密的方式：链路加密、节点到节点加密、端到端加密

链路加密：数据在信道中是密文，在节点中呈现明文

节点到节点加密：解决了节点中数据是明文的缺点。在中间节点中装有加密与解密保护装置，由其来完成密钥的变换。

端到端加密：数据在没有到达最终节点前不被解密，对于中继节点，数据是密文。通常使用**对称密钥**

1.2 数字签名

认证分为**实体认证**和**消息认证，**主要是解决网络通信过程中通信双方身份

认可。

实体认证：识别对方身份防止**假冒**，可采用**数字签名。**

消息认证：验证消息在传送或存储过程中有没有被**篡改**，可采用**报文摘要。**报文摘要可以为指定的数据产生一个不可仿造的特征，**主要的方法有：MD5，SHA 和 HMAC**

三种认证技术：基于共享密钥的认证，needham-schroeder 认证协议，基于公钥认证

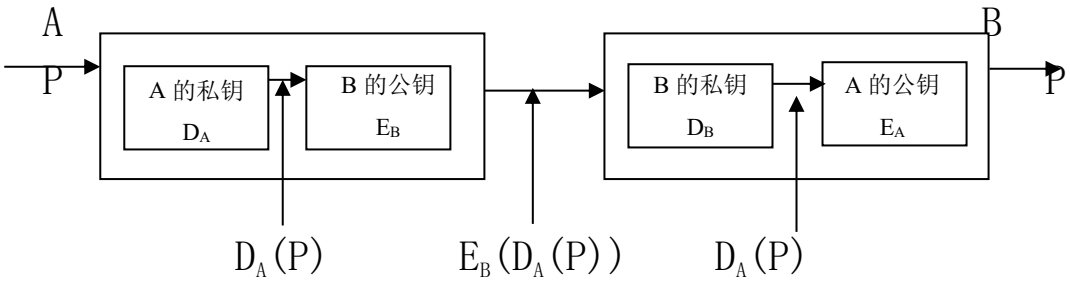
1.2.1 数字签名

数字签名应满足 3 点：

（1）接收者能够核实发送者

（2）发送者事后不可抵赖对报文的签名

（3）接收者不能伪造对报文的签名



发送方 A 先利用自己的私钥 D_A 对消息 P 进行加密，得到 $D_A(P)$，以此代表 A 对 P 的签名。A 从 CA 获得 B 的公钥 E_B 对密文 $D_A(P)$ 进行加密，得到 $E_B(D_A(P))$，然后将密文传送给 B，接收方 B 收到密文先用自己的私钥 D_B 进行解密，得到 $D_A(P)$，B 从 CA 中获得 A 的公钥 E_A 对密文 $D_A(P)$ 进行解密，得到消息，如果与 P 相同，则认为签名有效，否则认为签名无效。

数字签名可以利用 DES、公钥密码体制来实现，常用方法是建立在公钥密码体制和 MD5 或 SHA 的组合基础上。

1.2.2 报文摘要

MD5 算法以任意长的报文作为输入，输出产生一个 **128 位**报文。

SHA 全称为安全散列算法，该算法建立在 MD5 基础上，输入报文小于 2^{64} 位，产生 **160 位**的报文摘要。

HMAC 全称散列式报文认证码，**HMAC-MD5** 被用于 Internet 安全协议 **IPSEC** 的验证机制。

密钥管理：

数字证书：一个经认证中心 CA 数字签名的包含**公开密钥拥有者信息**和**公开密钥**的文件。用户使用自己的**私钥**进行**解密和签名**，使用**公钥**进行**加密和验证**。

X．509 证书标准包括：版本号、序列号、签名算法、发行者、有效期、主题名、公钥、发行者 ID、主体 ID、扩充域和认证机构的签名。

PKI 包括：

证书管理中心 CA：负责证书的颁发与管理，是可信任的第三方。**签发证书**

注册机构 RA：帮助远离 CA 的实体在 CA 处注册证书。**申请证书**

政策审批机构 PAA：制定整个体系结构的安全策略和下级机构的安全策略。

1.3 计算机安全：

机密性：保证信息不被非授权访问，**数据加密**

完整性：保证信息非法篡改 ，**报文摘要**

抗否认性：保证用户对所产生信息否认，**数字签名**

可用性：保证合法用户可以随时访问信息资源

可审计性：记录信息访问过程中的详细操作过程和安全事件。

可靠性：在规定的环境和规定的时间内完成工作的概率

1.4sniffer

Sniffer 工作前提

（1）必须是共享以太网

（2）网卡设置为混杂模式

网络监听的防范方法：

1、确保网络整体安全

2、数据加密与身份验证

网卡接受数据状态：
Unicast：单播模式
Broadcast：广播模式
Muticast：多播模式
Promiscuous：混杂模式

Sniffer 对所遇到的每一个帧均产生**硬件中断**，提醒主机处理该报文。主要攻击有：**捕获用户名和口令，获得更高级的访问权限，窥探低级协议信息**。其通常运行在**路由器**或**有路**

ARP 欺骗

在局域网中，攻击源主机不断发送 ARP 欺骗报文，诱使其他主机通过攻击源主机连接网络。

网络中只要存在攻击源主机，其它主机上网就会不稳定，严重时网络会瘫痪。

欺骗方式：（1）冒充网关欺骗主机、冒充主机欺骗网关、冒充主机欺骗其它主机（2）虚构 MAC 地址欺骗（3）ARP 泛洪（5）基于 ARP 的 DoS

鉴别方法：（1）检查网关 MAC 地址（2）检查三层设备的 ARP 表，如果多个 IP 对应同一个 MAC 则说明对应次 MAC 的计算机中了 ARP 病毒。

Windows XP 系统：Arp -s gateway-ip gateway-mac

DNS 欺骗

检测方法：被动监听检测 虚假报文检测 交叉检测查询

IP 欺骗

WEB 欺骗

Email 欺骗

口令破解与拒绝服务攻击 DoS

1.5 安全套接层 SSL

SSL 介于 Http 协议和 TCP 协议之间的可选层。当发出访问请求时，SSL 层借助下层协议的信道安全协商出一份**加密密钥**，并用此密钥**加密 Http 请求**；在 TCP 层与服务端口建立连接，传输 SSL 层处理后的数据，接受端与此过程相反。

SSL 分为**握手协议**和**记录协议**，握手协议用来**协商密钥**；记录协议用于**定义传输格式。**

默认情况下，SSL 协议使用端口号为 443

传输层安全性 TLS，工作于 TCP/IP 之上，HTTP 协议之下。它**提供了客户机与服务器之间的安全连接。**

1.6 安全超文本传输协议 S-HTTP

该协议为 HTTP 客户机和服务器提供了多种安全机制，是结合 HTTP 而设计的消息安全通信协议。工作在应用层

HTTPS 是一种安全 HTTP 协议，它使用 **SSL** 来保护信息安全，使用 TCP 的 **443** 端口来发送和接收报文。工作在传输层

安全电子交易 set

SET 使用“电子认证”技术为保密电子交易安全进行的基础，**认证过程**使用 **RAS 和 DES** 算法

提供的 3 种服务：

（1）在交易的双方之间提供安全信道

（2）使用 X.509 证书实现安全电子交易

（3）保证信息的机密性

SET 发生的先决条件：每个客户必须有一个**唯一的电子（数字）证书**，且由**客户设置口令**，并利用这个口令对数字证书、私钥、信用卡号及其它信息进行**加密存储**。

PGP

PGP 工作过程：用一个随机生成的密钥（每次均不同）使用 IDEA（128 位密钥）对明文进行数据加密，使用 MD5 进行数据完整性认证，然后用 RSA 对该密钥进行加密。既有 RSA 的保密性，又有 IDEA 的快捷性。

主要特征：

（1）使用 PGP 对邮件加密，防止非法阅读

（2）给邮件加数字签名，使得收件人能够确认发件人

（3）能够机密文件

Kerberos 属于对称密钥（DES 算法），在不安全的网络环境中为用户对远程服务器的访问提供**自动鉴别、数据完整性和安全性服务、以及密钥管理**

Kerberos 要求用户使用**用户名和口令**作为自己的标识，而客户机与服务器之间的交互则使用对应的用户名和口令生成的会话密钥。当用户需要通信时，用户先向认证服务器 AS 申请初始票据；用户收到 AS 响应的初始票据后，在向票据授权**服务器获得 TGS 申请会话密钥**；用户收到 TGS 响应的会话密钥后，再向服务器请求相应的服务。

为了防止中途报文被截获再重发，通信双方提供**时间戳**，再根据对方发来的时标判断这个请求是否是攻击者截获的旧信息。

Kerberos 系统的目标有三方面的：认证、授权和记帐审计

KerberosV4 系统中使用时间戳防止重发

KerberosV5 系统使用 seq 序列号来防止重发，目前主流是 V5。

Windows 五种身份认证：

匿名认证:不需要提供经过身份认证的用户凭据；

基本身份认证：用户必须输入 ID，访问是基于用户 ID 的。但该方式的用户 ID 和密码以明文形式在网络上传输。

集成 Windows 身份验证：该验证使用了 KerberosV5，能够提供较高的安全级别。

摘要式身份验证：该方式需要用户 ID 和密码，可提供中等安全级别。与基本身份验证相同，但克服可基本身份验证的缺点。

1.7 隔离技术

隔离技术的目标是确保把有害的攻击隔离，在可信网络之外和保证可信网络内部信息不泄露前提下，完成网间数据安全交换。

第一代：完全隔离

第二代：硬件卡隔离

第三代：数据转播隔离

第四代：空气开关隔离

第五代：安全通道隔离

完全隔离会使网络处于信息孤岛，目前隔离技术的发展方向是安全通道隔离。

1.8 入侵检测系统 IDS

主要功能：检测出正在发生的攻击活动、发现攻击活动的范围和后果、诊断并发现攻击者的入侵方式和入侵地点并给出建议、收集并记录入侵活动的证据。

IDS 系统不仅能针对外部入侵，还可以检测、监控内部用户行为，防止出现内部攻击者。

IDS 系统分类：基于主机的 IDS、基于网络的 IDS、分布式 IDS

IDS 系统的服务功能：**异常检测、滥用检测和攻击告警**

IDS 部署位置

（1）服务器区域的交换机上

（2）Internet 接入路由器之后的第一台交换机上

（3）重点保护网段的局域网交换机上

1.9 病毒

病毒分类：寄生病毒、存储器驻留病毒、引导区病毒、隐形病毒和多形病毒。

网络安全审计系统的基本思想是：对网络数据实时采集，对上层应用协议数据实时分析与还原，对网络中的使用情况进行监控，对各种网络违规行为实时报告，甚至封锁某些特定的主机，以帮助管理员对信息资源进行有效的管理和维护。

从时间上说审计是事后的，因此不能防止信息不泄露；从目标角度讲，**审计的目的是希望达到信息不外泄。**

计算机系统安全等级

D 级：级别最低，保护措施少，没有安全功能；

C 级：自定义保护级

C1 级：自主安全保护级。

C2 级：受控访问级实现更细粒度的自主访问控制，通过登录规程、审计安全性事件以隔离资源。Windows NT 4.0 属于 C2 级。

B 级：强制保护级

B1 标记安全保护级

B2 结构化安全保护级

B3 安全域

A 级：可验证的保护

A1：拥有正式的分析和数学方法。

第七章　网络管理

一、预备知识

1.1 文件系统

FAT16：管理最大分区为 2G，每个分区有 65525 个簇。

FAT32：管理最大分区为 2T。

NTFS：为网路管理安全特性设置的格式，支持更大的分区空间，速度快，安全性好。能够实现自动错误修复和文件级安全性以及支持文件压缩。

EXT2：linux 文件系统

EXT3：是 EXT2 的带日志版本

AWAP：linux 交换分区文件系统

VFAT：与 windows 系统兼容的 linux 长文件名系统，

1.2 工作组和域

域模型是 Windows 系统中将网络管理和安全性策略集中的方案，每个域都有一个**主域控制器**和**归属的工作站**，当域规模较大时，安装**备份域控制器**来缓解主域控制器的管理工作。

主域模型： 拥有一个主域控制器，一个或多个备份域控制器，主域控制器支持 2500 个验证账号，适合网络用数目少的情况。

多主域模型：拥有 2 个或 2 个以上主域，主域用作账号管理，其它域称为资源域，不管理用户账号，但提供网络资源共享，主域之间相互信任。适合四万用户以上组织。

完全信任模型：拥有多个主域，每个域都有账号和资源，域间完全信任

二、网络管理系统的功能与组成

网络管理系统分为：集中式、分布式、分层式

2.1 网络管理功能

配置管理：负责检测和控制网络的配置状态。对网络拓扑结构、资源配备、操作日志、使用状态等配置信息进行定义、检测和修改。

性能管理：保证有效的运营管理和提供约定的服务质量，并在保持各种业务服务质量的同时，提高网络资源的利用率。

故障管理：发现和纠正网络故障，动态的维护网络有效性。故障管理的功能：

报警、故障定位、测试、业务恢复和维护故障日志。

安全管理：提供信息的保密、认证和完整性保护机制，使网络中的服务、数据和系统免受侵扰和破坏。主要功能包括：风险分析、安全服务、告警、日志和报告。

计费管理：正确的计算和收取用户网络服务费用，进行网络资源利用率的统计和成本效益核算。

2.2 网管系统构成：

主要包括：网络管理协议、网络管理工作站(manager)、被管理组件(agent)、管理信息库 MIB

管理工作的流程

（1）在被管理组件上预置代理

（2）管理者利用网络管理协议从代理的 MIB 中取得被管理组件的管理信息，并存入自己的 MIB 中。

（3）管理软件通过对 MIB 的分析，达到网络监控的管理目的。

2.3 简单网络管理协议 SNMP *（采用**轮询**和**事件驱动**实现管理功能）*

SNMP 是在 TCP/IP 协议基础上定义并依赖于 UDP 数据报的**应用层协议**，采用 UDP 协议不会增加网络负载，但 UDP 协议不可靠，所以 SNMP 报文容易丢失，为此，**SNMP 的每个管理信息单独发送，报文限制在 484 字节。**

在 SNMPV3 版本中，管理站和代理站统一叫做 SNMP 实体。

在 SNMPV3 版本中把网络协议的安全威胁分为主要和次要的两类：（1）篡改管理信息和假冒合法用户是 SNMPV3 安全模块必须防护的两种主要威胁；

（2）修改报文流和消息泄露 SNMPV3 安全模块必须提供防护的两种次要威胁；

（3）拒绝服务和通信分析是 SNMPV3 安全模块不必防护的。

目前是 SNMPV3 版本，它提供了数据源标识、报文完整性认证、防止重放、机密性、授权和访问控制、远程配置和高层管理。

SNMPv1 和 SNMPv2 使用团体名进行认证，但 **SNMPv1 共同体名**使用**明文传送**，而 **SNMPv2** 可以进行**鉴别和加密**；**SNMPv3** 定义了**基于用户**的**安全模型**，可以使用**预先共享密钥**进行**报文认证**

管理进程使用 UDP161 端口进行 get 或者 set 操作；代理进程使用 UDP162 端口，进行 trap 操作。

简单网络管理协议 SNMP 周期性的向被管对象发出探寻信息，探寻的好处使系统相对简单，限制管理信息的通讯量，同时允许被管对象发出 trap 信息来通报特殊事件

管理站支持的设备数 N 与轮询时间 T（单位：秒）、单个轮询时间 t 之间关系为： $N \leq T/t$

Snmp5 种报文：

Get-Request: 从代理处提取一个或多个变量

Get-NextRequest： 从代理处提取紧跟当前参数的下一个变量值

Set-Request： 设置代理进程一个或多个变量

Get-Response： 返回参数值，该操作由代理进程发出，是前 3 种操作的响应。

Trap： 代理进程主动发出的报文，通知管理进程某些事件。

管理进程与代理进程之间关系称为**共同体**，在 SNMP 中，只有**同一共同体之间才能通信**，只有管理进程和代理进程之间交换管理信息时才使用共同体，**共同体**实际就是实现管理应用实体之间的**身份鉴别**，为一个字符串，是管理进程与代理进程之间的口令，采用明文方式，默认为 public。

SNMP MIB 中被管对象的 ACCESS 属性包括，只读、只写、读写和不可访问 4 种。

SNMPV2 实体接收报文处理的步骤

（1）对报文进行语法检查，丢弃出错报文

（2）把 PDU 部分、源和目的端口交给认证服务器，如果认证失败就发出一个陷入，丢弃该报文。

（3）如果认证通过，则将 PDU 转化成 ASN.1 的形式。

（4）协议实体对 PDU 做句法检查，如果通过，则根据团体名和适当访问策略做相应处理。

SNMPV2 实体发送报文处理的步骤

（1）根据实现协议构造 PDU

（2）把 PDU、源和目的端口地址以及团体名交给认证服务器，认证服务器产生认证代码或对数据加密并返回结果。

（3）加入版本号和团体名，构造报文。

（4）进行 BER 编码，产生 0/1 比特串，发送出去

远程网络监控 RMON 和 SNMP 的主要区别：

RMON 提供整个子网的管理信息，而 SNMP 管理信息库只包含本地设备的管理信息。RMON 扩充了管理信息库 MIB-2，在不改变 SNMP 的条件下增强了网络管理功能，进一步解决了 SNMP 在日益扩大的分布式网络中所面临的局限性。

2.4 Windows 基本管理配置命令

Winipcfg 等价于 ipconfig,但 Winipcfg 用在 winME、WIN98 和 WIN95 之上。

Ipconfig/all 显示所有适配器完整 TCP 配置信息

Ipconfig/renew 手动更新 DHCP 配置信息

Ipconfig/release DHCP 客户端手动释放 IP

Ipconfig/flushdns 清除并重设 DNS 缓存信息

Ipconfig/registerdns 手动注册 DNS

Ipconfig/displaydns 显示本地 DNS 内容

Ping -t 连续发送请求信息到目的地，按 ctrl+C 终止。

Ping -a 对目的地 IP 进行反向名称解析

Ping -n count 指定发送请求信息的次数，默认为 4

Ping -l size 发送消息中数据字段的长度

Tracert -d 防止将路由器的 IP 解析成名称

Tracert -h max-hops 搜索目标路径中指定跃点的最大数

Tracert name|IP 指定目标的路径

Route -f 删除路由表中的网络路由

Route -p 与 add 命令结合是添加一条路由；

与 print 结合是显示**持久路由**。*保存在注册表中的路由*

Route -p add 目标地址 mask 子网掩码 下一跳地址

Route add 添加路由

Route change 修改已有路由

Route delete 删除路由

Route print 显示本机路由，与 netstat -r 命令相同

Route [-f|-p] [command 目标地址] [mask netmask] [gateway]

Netstat -a 显示所有活动 TCP 连接以及侦听的 TCP 和 UDP 端口

Netstat -e 显示以太网统计信息，包括收发字节数，常与-s 结合使用

Netstat -s 按协议显示统计信息

Netstat -r 显示本机路由，与 Route print 等价
Netstat -p protocol 显示指定的协议连接，与-s 可以联合使用
Netstat -n 显示活动的 TCP 连接，但以数字形式表现地址和端口

Arp -s IPaddress MAC 在 arp 表中添加静态表项
arp -d IPaddress 删除指定一个表项
arp -a ipaddress 显示指定 IP 地址的 arp 表项，不带参数则显示所有表项

2.5 Linux 系统

Linux 支持多种分区格式，其采用 ext2 和 ext3，安装时至少需要一个根分区（/）和一个交换分区（swap），交换分区应该为计算机内存容量的 2 倍。

2.5.1 Linux 下的文件包含内容

/ 为根目录，在 linux 系统中根目录只有一个
/var 包含正在操作的文件、记录文件、加密文件和临时文件
/home 除 root 用户外的所有用户配置文件,个性化文件和主目录 ★
/etc 操作系统配置文件 ★
/dev 设备文件
/lib 程序和核心模块共享库
/usr/local/bin 用户安装的应用程序
/lost+found 一些丢失的文件可以在这里找到
/mnt 外部设备的挂载点
/proc 这是临时目录，存放内存读取的进程信息，该目录中的内容关机后不被保存
账号记录在 etc/passwd ★
密码记录在 etc/shadow ★
用户组记录在 etc/group ★
用户组密码记录在 etc/gshadow
etc/sysconfig/network 包括主机基本网络信息，用于系统启动 ★
etc/hostname 包含完整域名 ★
etc/hosts IP 地址与主机映射，进行域名解析（与 Windows 相同） ★
etc/host.conf 解析主机域名方法 ★
etc/resolv.conf 置 DNS 文件配★
etc/service 端口与服务器名之间的映射 ★
etc/gateways 建立动态路由

2.5.2 文件权限（用八进制数字表示文件权值）

drwxrwx--- d 表示文件类型，r 表示可读我，w 表示可写，x 表示可执行

4 2 1

新建目录的权限 drwxrwxrwx，权值为 777。新建文件的全新 rwrwrw，权值为 666

- 表示为普通文件；b 表示块专用文件；c 表示字符专用文件；d 表示目录文件；l 表示符号链接文件

Chmod g+rwx filename 与文件所有者同组用户增加权限

Chmod a+rwx filename 文件所有者，同组用户和其他人增加权限

Chmod u+rwx filename 为文件所有者增加权限

Chmod o+rwx filename 为其它用户增加权限

+号表示增加权限，- 号表示取消权限，=表示唯一权限。

Chown *拥有者 文件名* 改变文件拥有者

Chgrp *组名 文件名* 改变文件组

2.5.3 Linux 常见命令

cd 改变当前工作目录，cd 与目录名间有空格，不带任何参数时返回 root 目录。

pwd 显示当前所在目录

mkdir 建立新目录，-p 一次可建立多个目录，-m 给目录设定权限

ls 产看文件及目录 -a 显示所有目录和文件，包括隐藏文件；-l 以长格式显示文件信息，包括类型、权限、所有者、组、大小、创建和修改时间。

cp 复制文件和目录，-f 表示覆盖文件目录，且不提示

rm 删除文件及目录

mv 移动文件及目录，-f 表示覆盖文件目录，且不提示

cat 串联并显示文件，可同时显示多个文件

ps 显示当前进程

tac 从最后一行显示文件内容

more 一页一页的显示内容

less 显示文件时允许用户即可向前也可向后翻阅文件

vi 创建或打开文件

kill<pid>终止某个进程

man 获得在线帮助

tar 打包

whereis 查找文件　whatis 获取命令简介

grep 在文件中搜索指定字符，-i 不区分大小写。

ln 为某一文件在另外一个位置建立文件链接

按 ESC 输入:wq 保存并退出当前文件，:q 不保存退出

Useradd -c 注释 *user* 创建带注释的 user

Useradd -g 组名 *user* 创建属于某组的 user

Userdel -r *user* 删除 passwd 中的对应用户，包括 shadow 和 group 中的信息

Passwd *user* 设置 user 用户口令

Passwd -u *user* 解锁 user 用户

-f *user* 强制 user 用户下次登录修改口令

Groupadd -g *ID group-name* 创建带 ID 的组，$ID > 499$

Groupdel *group-name* 删除组

Groupmod -n *new-groupname old-groupname* 更改组名

Ifconfig -a *eth0* 显示 eth0 接口信息，包括 ip、掩码、广播地址和接口状态

Ifconfig *eth0 ipaddress* netmask *mask* broadcast *广播地址* 设置 eth0 口的 IP 地址、子网掩码和广播地址。

Ifconfig *eth0* down|up 关闭或者开启 eth0

Ping IPaddress 测试 ip 地址是否连通

-c 次数 发送数据包的个数 **Ping -n 相同**

Arp -n 列出当前 ARP 缓存条目

-s 添加一个静态 ARP 条目， arp -s IPaddress MAC

-d 删除 ARP 条目， arp -d IPaddress

Route 显示本机路由

Route add|del [-net|-host] *IPaddress* [gw *gateway*] [netmask *mask*] [dev *interface*] 添加或者删除路由

例：route add -net 10.1.1.0 添加一个网络路由

Route add -host 10.2.1.1 gw 10.1.1.2 主机 10.2.1.1 的网关 10.1.1.2

2.6 网络故障诊断

物理故障 逻辑故障 路由故障 主机故障

Ping 127.0.0.1 如果不通说明本机的 TCP/IP 协议不能正常工作
Ping 本机 IP 如果通则表明网络适配器工作正常，否则适配器故障
Ping 网段内其他工作正常的主机，如果不通则说明线路故障
Ping 本地网关，不通则不能上网
Ping DNS 地址，不通则 DNS 故障
Tracert 命令可以判断数据报走的路径，

故障诊断的一般步骤：

（1）确定故障现象，分析可能造成的原因
（2）收集需要的用于帮助隔离可能故障的信息。从网络系统、协议分析、路由诊断命令输出的报告或者软件说明书中收集信息。
（3）根据收集到的情况考虑可能的故障原因。

2.7 数据备份

数据备份的策略：

完全备份：备份系统中所有数据。特点是备份时间长，恢复时间短，操作方便。适用于数据量不大的系统
增量备份：只备份上次备份以后变化后的数据。特点是备份时间短，恢复麻烦，操作方便。
差分备份：只备份上次完全备份以后变化的数据。特点是备份时间适中，恢复方便。

2.8 网络存储

直连式存储 DAS：在服务器上外挂大容量磁盘，存储设备与服务器主机之间采用 SCSI 通道连接。这种方式难以扩展存储容量，不支持数据容错，当服务器出错时，造成数据丢失。
网络附加存储 NAS：将存储设备连接到现有网络上，来提供数据存储和文件访问服务。采用 raid 方式管理，能有效保护数据
存储区域网络 SAN：是一种连接存储设备和存储管理子系统的专用设备，专门提供数据存储与管理功能。SAN 是一种专用高速网络，采用光纤通道实现网络互联，SAN 不仅提供大容量的数据存储，而且地域上可以分散部署。

磁盘冗余阵列 RAID

RAID0 需要两块以上磁盘，每个磁盘划分不同的区块，数据采用交叉存取和并行传输。这种**磁盘利用率高**，读写**速度最快**，但由于没有数据差错控制，因此

很容易发生数据错误。

RAID1 由磁盘对组成，每个工作磁盘均有对应的映像，上面保存着与工作盘完全相同的数据，具有**最高的安全性**，但**利用率为 50%**。

RAID2 采用海明码纠错技术。输出速率与驱动器中速度最慢的相等。

RAID3 把**奇偶校验码**（只能查错不能纠错）**存在一个独立的磁盘**，如果一个磁盘失效，其上的数据可以通过其他盘上数据进行异或运算得到，**读盘速度快，但写入速度慢**。适用于图像处理等要求高吞吐率的场合，**磁盘利用率为** $n-1/n$。

RAID5 各块**磁盘进行条带化分割**，相同的条带进行**奇偶校验**，检验数据平均分配在每一块硬盘上。**磁盘利用率为** $n-1/n$。

RAID0+1 是 RAID0 与 RAID1 组合形式，它提供 RAID1 的安全保障同时提供 RAID0 近似的访问速度。

2.9 系统可靠性与失效率计算

串联系统的失效率 $\lambda=\lambda 1+\lambda 2+.....+\lambda n$

并联系统的失效率

$$\lambda=\frac{1}{\frac{1}{\lambda}\sum_{n=1}^{n}\frac{1}{n}}$$

平均无故障时间与失效率之间关系 $MTBF=\frac{1}{\lambda}$

串联系统的可靠度 $R=R1\times R2\times.....\times Rn$

并联系统的可靠度 $R=1-(1-R1)\times(1-R2)\times.....\times(1-Rn)$

可靠度与失效率之间关系 $R=e^{-\lambda t}$ (t为时间)

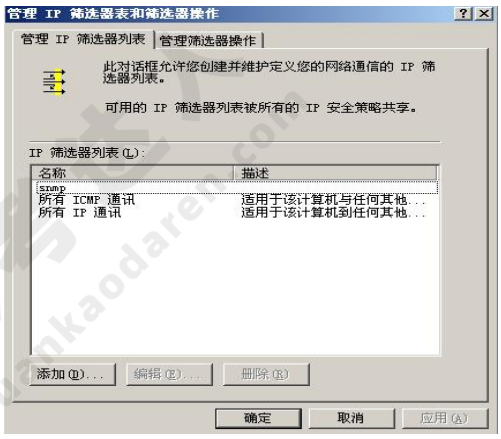
SNMP 消息是以明文形式发送的。这些明文消息很容易被“Microsoft 网络监视器”这样的网络分析程序截取并解码。未经授权的人员可以捕获社区名称，以获取有关网络资源的重要信息。“IP 安全协议”(IP Sec)可用来保护 SNMP 通信。您可以创建保护 TCP 和 UDP 端口 161 和 162 上的通信的 IP Sec 策略，以保护 SNMP 事务。

创建筛选器列表

要创建保护 SNMP 消息的 IP Sec 策略，先要创建筛选器列表。方法是：单击开始，指向管理工具，然后单击本地安全策略。

展开安全设置，右键单击“本地计算机上的 IP 安全策略”，然后单击“管理

IP 筛选器列表和筛选器操作”。



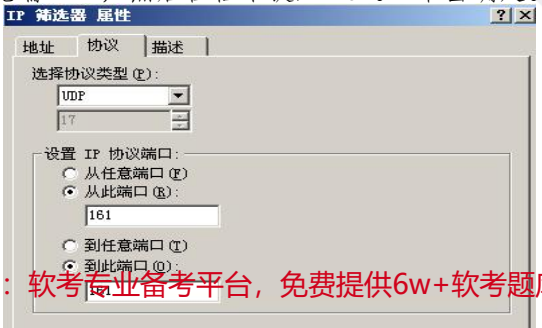
单击“管理 IP 筛选器列表”选项卡，然后单击添加。

在 IP 筛选器列表对话框中，键入 SNMP 消息(161/162)（在名称框中），然后键入 TCP 和 UDP 端口 161 筛选器（在说明框中）。

单击使用“添加向导”复选框，将其清除，然后单击添加。

在“源地址”框中，单击“任意 IP 地址”。在“目标地址”框中，单击我的 IP 地址。单击“镜像。选中“与源和目标地址正好相反的数据包相匹配”复选框。

单击协议选项卡。在“选择协议类型”框中，选择 UDP。在“设置 IP 协议端口”框中，选择“从此端口”，然后在框中键入 161。单击“到此端口”，然后在框中键入 161。 单击确定。



在 IP 筛选器列表对话框中，选择添加。

在“源地址”框中，单击“任意 IP 地址”。在“目标地址”框中，单击我的 IP 地址。选中“镜像、匹配具有正好相反的源和目标地址的数据包”复选框。

单击协议选项卡。在“选择协议类型框中，单击 TCP。在“设置 IP 协议”框中，单击“从此端口”，然后在框中键入 161。单击“到此端口”，然后在框中键入 161。单击确定。

在 IP 筛选器列表对话框中，单击添加。

在“源地址”框中，单击“任意 IP 地址”。在“目标地址”框中，单击我的 IP 地址。单击“镜像，匹配具有正好相反的源和目标地址的数据包”复选框，将其选中。

单击协议选项卡。在“选择协议类型”框中，单击 UDP。在“设置 IP 协议”框中，单击“从此端口”，然后在框中键入 162。单击“到此端口”，然后在框中键入 162。 单击确定。

在 IP 筛选器列表对话框中，单击添加。

在“源地址”框中，单击“任意 IP 地址”。在“目标地址”框中，单击我的 IP 地址。单击“镜像。匹配具有正好相反的源和目标地址的数据包”复选框，将其选中。

单击协议选项卡。在“选择协议类型框中，单击 TCP。在“设置 IP 协议”框中，单击“从此端口”，然后在框中键入 162。单击“到此端口”，然后在框中键入 162。 单击确定。

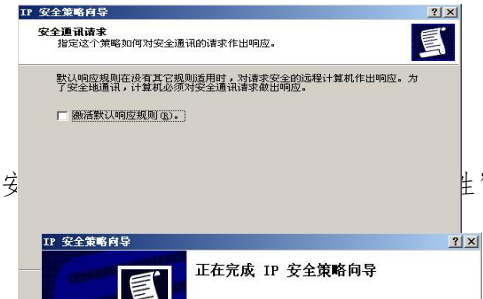
在 IP 筛选器列表对话框中单击确定，然后单击“管理 IP 筛选器列表和筛选器操作”。单击应用，关闭。

创建 IPSec 策略。

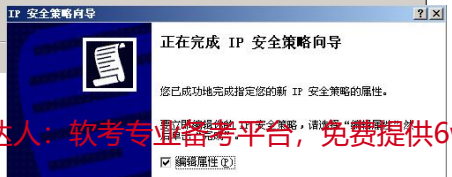
要创建 IPSec 策略来对 SNMP 通信强制实施 IPSec，请按以下步骤操作： 右键单击左窗格中“本地计算机上的 IP 安全策略”，然后单击创建 IP 安全策略。 “IP 安全策略向导”启动。 单击下一步。

在“IP 安全策略名称”页上的名称框中键入 Secure SNMP。在说明框中，键入 Force IPSec for SNMP，然后单击下一步。

单击“激活默认响应规则”复选框，将其清除，然后单击下一步。

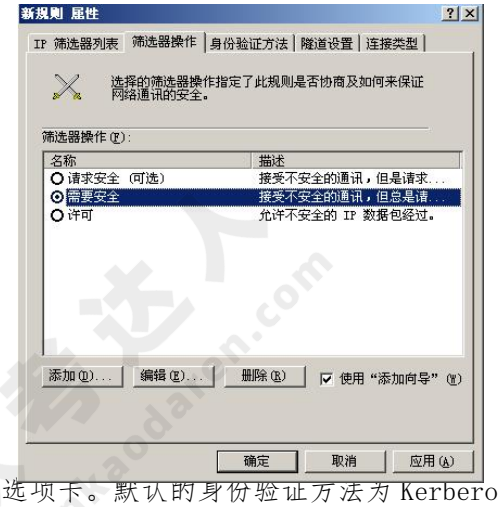


在“正在完成 IP 安 性”复选框已被选中，然后单击完成。



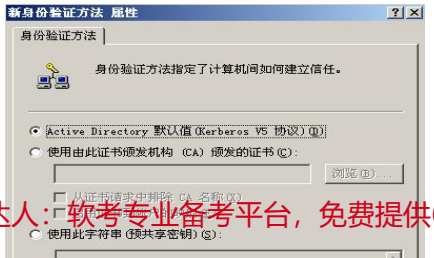
在“Secure SNMP 属性”对话框中，单击使用“添加向导”复选框，将其清除，然后单击添加。 单击 IP“筛选器列表”选项卡，然后单击 SNMP 消息(161/162)。

单击筛选器操作选项卡，然后单击需要安全。



单击身份验证方法选项卡。默认的身份验证方法为 Kerberos。如果您需要另一种身份验证方法，则请单击添加。在新身份验证方法属性对话框中，从下面的列表中选择要使用的身份验证方法，然后单击确定：

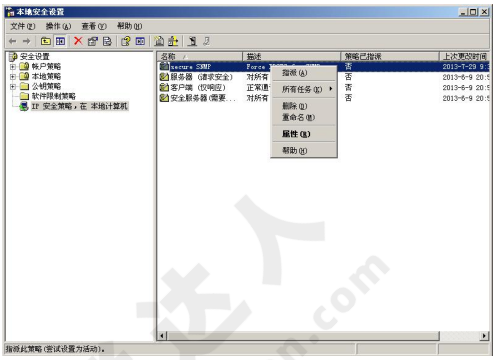
ActiveDirectory 默认值（KerberosV5 协议） 使用此字符串（预共享密钥）



在新规则属性对话框中，单击应用，然后单击确定。

在 SNMP“属性”对话框中，确认 SNMP“消息(161/162)”复选框已被选中，然后单击确定。

在“本地安全设置”控制台的右窗格中，右键单击安全 SNMP 规则，然后单击指派。



在所有运行 SNMP 服务的基于 Windows 的计算机上完成此过程。SNMP 管理站上也必须配置此 IPSec 策略。

第八章　计算机基础知识

一、计算机硬件基础

1.1 数据表示

原码：最高位为符号位，0 表示正数，1 表示复数。其中数值 0 有+0 与-0 之分。其数值范围 $-(2^{n-1}-1)\sim 2^{n-1}-1$。8 位时范围-127～+127

反码：正数的反码与原码相同；负数符号位不变，其余位取反。数值 0 有两种表示方式。数值范围 $-(2^{n-1}-1)\sim 2^{n-1}-1$。8 位时范围-127～+127

补码：正数的补码与原码相同；负数的补码在反码基础上加 1。数值 0 只有一种表示法，即：0000 0000。数值范围 $-2^{n-1}\sim 2^{n-1}-1$。8 位时范围-128～+127，**适合数字加减运算**

移码：在补码基础上符号位取反，数值 0 只有一种表示法，即：1000 0000。**适合浮点数阶码。**

1.2 校验码

码距：在一个编码系统中，任意两个合法编码之间至少有多少个二进制位不同

奇偶效验码：通过在编码中增加 1 的个数为奇数或者偶数从而使码距为 2。

海明码：利用奇偶性来检错和校验的方法。假设有 m 位信息码，加入 k 位校验码，则 $m+k+1\le 2^k$

循环冗余校验码 CRC：

1.3 计算机的结构

1.3.1 CPU 由运算器、控制器和寄存器组成

运算器：完成算术运算、逻辑运算和移位操作。主要部件算术逻辑单元 ALU、累加器、标志寄存器、寄存器组、多路转换器和数据总线。

控制器：实现指令读入、寄存、译码和执行过程有序的发出控制信号。主要部件：程序计数器 PC、指令寄存器、指令译码器、时序产生器和信号发生器组成。

寄存器：暂存寻址和计算过程的信息。通常分为数据寄存器、地址寄存器、状态寄存器、控制寄存器。

指令周期：取出并执行一条指令所需时间。

总线周期：CPU从存储器或者I/O接口存取一个字节所需时间。

时钟周期：CPU处理动作的最小单位

相互关系：一个指令周期可以划分成一个或多个总线周期；

一个总线周期可以分为几个时钟周期。

1.3.2 主存储器：又称内存或主存，用来存放正在使用或者随时使用的数据和程序，CPU可以直接访问。

主存储器指标：

（1）存储容量：存储器可容纳的二进制信息量。

$1KB=1024B=2^{10}B$，$1MB=2^{20}B$，$1GB=2^{30}B$,$1TB=2^{40}B$。

（2）存储周期：连续启动两次独立的存储器操作所需最小时间。存储周期一般是ns级，即10^{-9}s

（3）存取时间：从启动一次存储到完成所需要的时间

（4）存储器带宽：每秒钟能访问的位数，记作

$B_m=1s/$存储器周期×每个周期可访问的字节数

假设有一个存储器存储容量为$M\times N$位，若使用$m\times n(m\le M,n\le N)$的芯片，则需要$(M/m)\times(N/n)$个存储芯片 ★★

相关联存储器：一种**按内容寻址**的存储器。**原理**是把数据或数据某一部分作为关键字，将关键字与存储器中每一个单元进行比较，找出存储器中所有与关键字相同的数据

Cache：又称高速缓存存储器，是为解决与主存之间的速度匹配问题而设立。

命中率：在Cache中访问到信息的概率。程序执行过程中分别对Cache的访问次数为N_1和对主存的访问次数为N_2，则Cache命中率为H $H=N_1/(N_1+N_2)$ ★

平均存取时间：可以用Cache和主存的访问周期T_1、T_2和命中率H来表示，即：$T=H\times T_1+(1-H)T_2$。★★

地址映像：当CPU访问内存时，用的是访问主存的地址，由该**地址变为Cache的地址**称为地址变换，**变换由硬件来实现**，已达到快速访问的目的。地址映像的方式有：全相联方式、直接方式和组相联方式

1.3.4 流水线技术：将一个操作分为多个可独立处理的子操作（如取指令、译码、取操作数、执行），每个子操作在一个专门的硬件站上执行，这样一个操作需要流水线上多个站的处理才能完成。

流水线周期：操作时间最长的一个。记为 Δt ★★

吞吐率： $p = 1/\Delta t$

流水线建立时间： $T = n \times \Delta t = \sum_{i}^{n} \Delta t_i$

执行 m 条指令的时间为： $T = n \times \Delta t + (m-1) \times \Delta t = (n+m-1)\Delta t$

$$T = \sum_{i=1}^{n} \Delta t_i + (m-1) \times \Delta t$$

1.3.5 I/O 接口的分类：

（1）按数据传输格式：并行和串行

（2）按主机访问 I/O 的方式：程序查询接口、中断接口、DMA 接口

（3）按时序控制：同步和异步

程序查询接口：CPU 通过执行程序查询外设状态，判断是否有数据传输

中断接口：CPU 暂停当前正在执行的程序，转去处理这些事件，当处理结束后再继续原来执行的程序。

DMA 接口：采用一个**专门的控制器**来控制内存与外设之间的数据交流，**无需 CPU 介入。**

通道控制方式：CPU 只需发出 I／O 指令，通道完成相应的 I／O 操作，并在操作结束时向 CPU 发出中断信号；同时一个通道还能控制多台外设。

通道的特点：通道分担了 CPU 对输入输出操作的控制；减少了外设对 CPU 请求中断的次数；提高了 CPU 的运行效率；实现了 CPU 与外设之间的并行执行。

1.3.6 总线系统：一般可分为芯片内总线、元件级总线、内总线和外总线。

一个 32K×32 位的主存储器，其地址线和数据线的总和为 47 根。

32K×32位的存储器，其数据线需要32根；32K是其容量大小，根据2的n次幂=32×1024可以计算出：n=15。于是至少需要15根地址线，所以，所需的地址和数据线总和为47。

内总线又称**系统总线**，分为**数据总线**、**地址总线**和**控制总线**；常见系统总线标准：

ISA 总线：数据线 16 位，地址线 24 位，频率为 8Mhz

EISA 总线：是 ISA 总线扩展，数据线 32 位，频率为 8Mhz。

PCI 总线：目前微型机所采用的总线标准，总线的工作与处理机的工作是并行的，总线上的设备是即插即用的。该总线频率为 33.3Mhz。PCI-2 带宽为

64 位，频率为 66.6Mhz

外总线又称**通信总线**，可直接与外设相连或与其它计算机相连。常见的标准有：

串行总线接口 RS232：是数据终端设备 DTE 与数字通信设备 DCE 之间数据交换的接口。用于 modem、键盘及其它终端之间传输数据。

SCSI 总线：是一种并行总线，广泛用于连接硬盘、光盘等。

通用串行总线 USB：提供电源，即插即用。USB1.1 传输速率为 12M；USB2.0 传输速率为 480M，其中 1.5M 用于鼠标键盘等外设；USB3.0 传输速率为 5G。

IEEE1394：由 6 条信号线组成，可连接设备多，速度快支持即插即用。

1.3.6 指令系统

指令由操作码和操作数（地址码）组成。指令长度分为固定长度和可变长度两种。

寻址方式：

立即寻址：指令的地址码字段给出的不是操作数的地址而是操作数本身。其特点是访问一次存储器就可同时取出指令和操作数。

直接寻址（寄存器寻址）：指令的地址码字段给出操作数所在存储单元地址（寄存器号）。

变址寻址：操作数的地址由某个变址寄存器的内容和位移量相加

间接寻址：操作数的地址是主存中的存储单元的内容

相对寻址：操作数的地址由指令寄存器的内容与位移量相加

复杂指令计算机 CISC：

特点：

（1）指令采用可变长指令格式，指令系统丰富，使用频率差别大，处理特殊任务效率高。

（2）支持更多的数据类型和寻址方式。

（3）指令系统对应的控制信号复杂，大多采用微程序控制方式。

（4）高级语言实现简单，效率高

简单指令计算机 RISC

特点：

（1）采取定长指令格式，精简指令数量，使用频率接近。

（2）采用寄存器操作，寻址方式少。

（3）大部分指令都采用硬联控制实现。

（4）优化编译程序来支持高级程序语言，需要较大的存储空间

1.4 操作系统：

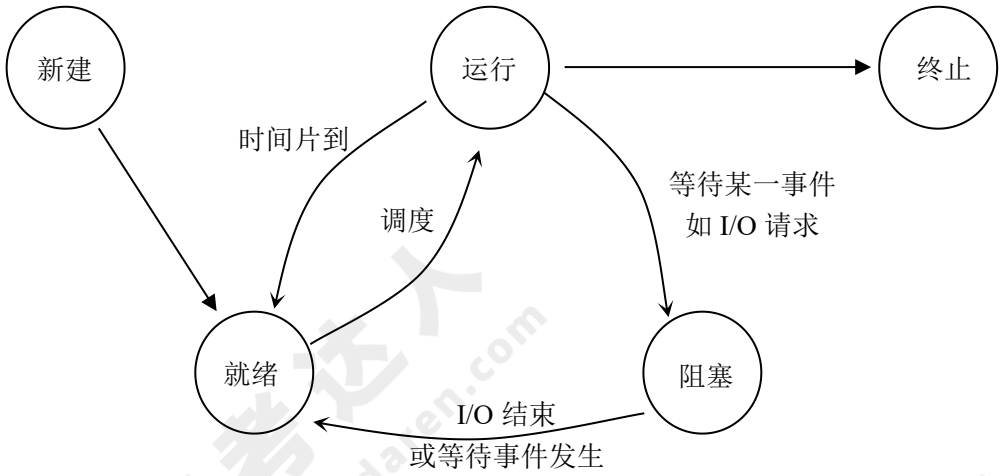
操作系统是计算机系统中的系统软件，它有效的**组织和管理系统中的软硬件资源**，合理的组织计算机系统的工作流程，控制程序执行，并为用户提供**良好的工作环境和友好的接口**。

操作系统主要有**并发性、共享性、虚拟性**和**不确定性** 4 个特征。

操作系统功能如下：**进程管理、存储管理、设备管理、文件管理和作业管理**

软件分为**系统软件**和**应用软件**。常见的**系统软件**有：**操作系统、语言处理程序、连接程序、诊断程序和数据库管理系统**。操作系统是系统软件最核心的部分。**应用软件**是为**某一个专门的应用目的而开发的软件**，如科学计算、工程设计、事物处理、数据处理、过程控制、文字和表格处理软件、辅助设计和实时处理软件等。

进程是程序的一次执行，它是动态的有生命期的并且需要处理机来执行。是操作系统并行工作的基本单位，也是**核心调度及资源分配**的**最小单位**。



线程是比进程更小的**能够独立运行**的基本单位，是**处理器分配**的**最小单位**。

同步：是进程间直接制约的问题

互斥：是进程间间接制约的问题

PV 操作：是实现进程同步与互斥的常用方法；P 操作表示申请一个资源，V 操作表示释放一个资源。

某个系统中有 R 个资源，现有有 m 个进程互斥，每个进程需要 n 个资源，则系统不发生死锁所需要资源数 $m\times(n-1)+1\le R$ **个。** ★★

死锁避免的经典算法为银行家算法，这种算法会增加系统开销。

分页存储：

分页地址由**页号**和**页内地址**组成

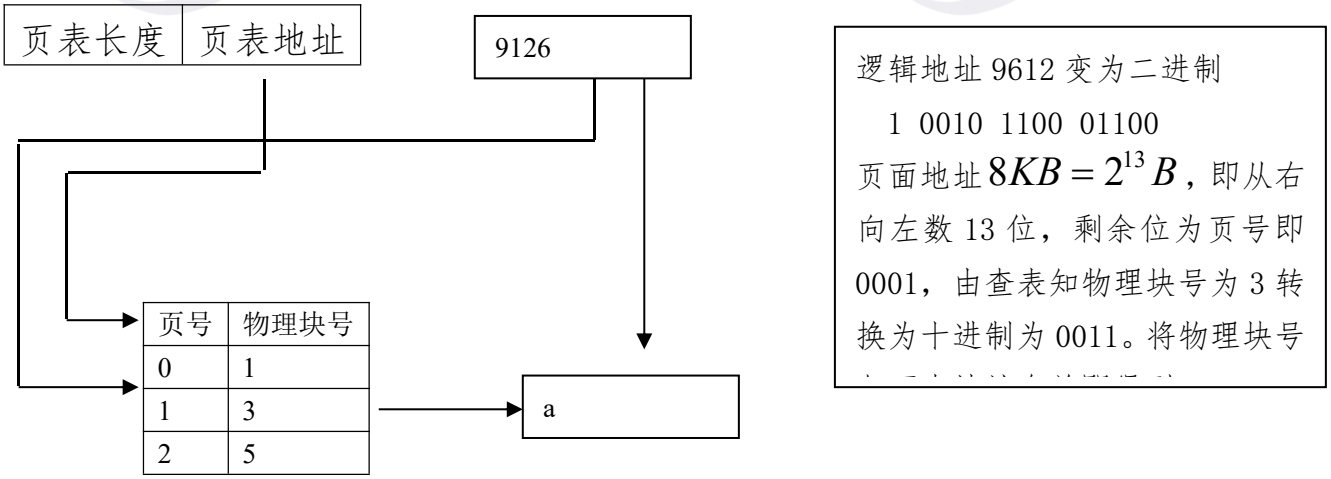
地址变换：进程在执行过程中通过查找页表，可以找到对应的物理块号。**页表**的作用是**实现页号到物理块号的地址映射**

页式存储的优点：利用率高、碎片效，分配管理简单

缺点：增加系统开销，可能产生抖动现象

例：

页式存储系统的地址由页号和业内地址两部分组成，地址变换过程如下，假设页面地址为 8KB，十进制逻辑地址 9612 经地址变换后的物理地址 a 是



逻辑地址 9612 变为二进制

1 0010 1100 01100

页面地址 $8KB = 2^{13}B$，即从右向左数 13 位，剩余位为页号即 0001，由查表知物理块号为 3 转换为十进制为 0011。将物理块号

段式存储：由段号和段内地址组成

进程在执行过程中，通过查段表来找到每个段所对应的内存区，因此段表实现了逻辑段到内存区的映射。段表由页号、段长和基址组成。**物理地址=基址+位移量**

页式存储的优点：多道程序共享内存，各段程序修改互不影响

缺点：内存利用率低，内存浪费大

虚拟存储器：利用大量的外存来扩展内存，产生一个比有限的实际内存空间大得多的，逻辑的虚拟内存空间。

磁盘管理

磁盘：每个磁道存储容量是相同的，位密度是不同的。

磁道数=(外半径-内半径)×道密度×记录面数，注意硬盘的第一面和最后一面是保护用，要减掉。如 3 个双面盘片的记录面数位 3×2-2=4

非格式化容量=位密度×π×最内圈直径×总磁道数

格式化容量=每道扇区数×扇区容量×总磁道数

平均数据传输速率=每道扇区数×扇区容量×盘片转数

存取时间=寻道时间+等待时间。寻道时间指磁头移动到磁道所需时间；等待时间为等待读写的扇区到磁头下方所需时间

读取磁盘数据时间包括 3 个部分：寻道时间+找扇区时间（旋转延迟时间）+传播时间

1.5 系统开发与运行基础：

软件生命周期：指软件产品从计划到软件交付使用，直到最终退出为止的过程。包括**计划阶段、分析阶段、实现阶段、测试阶段**和**运行维护**阶段。

软件开发模型：瀑布模型、螺旋模型、喷泉模型、原型化模型、演化模型

瀑布模型：严格遵循软件生命周期各阶段的固定顺序，一个阶段完成再进入另一阶段，适用于结构化开发方法。

维护阶段

瀑布模型：软件计划、需求分析、软件设计、程序编码、软件测试、运行维护

瀑布模型的优点： 定义阶段 开发阶段

1、为项目提供按阶段划分的检查点。

2、当前阶段完成后，只需关注后续阶段

3、可在迭代模型中应用瀑布模型

4、适用于大规模系统项目

缺点：

1、各阶段划分完全固定，阶段之间产生大量文档，增加了工作量。

2、用户直到工程末期才能见到开发成果，增加了开发风险。

3、不适应用户需求变化。

原型化模型：开发人员对用户提出问题进行总结，就主要需求达成一致意见，开发一个原型并运行，然后对原型进行反复修改，使之完善。衡量原型化模型开发人员能力标准是快速获取需求能力

优点：用户需求清楚，降低开发风险与成本,用户参与决策，减少项目管理，要求完整的生命周期

缺点：不适用大型系统，系统难于维护。

演化模型：根据用户需求，快速分析构造该软件的一个初始版本，称之为原型，根据用户在使用原型过程中提出的建议改进原型，获得原型的新版本，重复这一过程，使用户最终获得满意的软件产品。

螺旋模型：将瀑布模型和原型模型结合，强调了其它模型所忽略的风险分析，适合大型复杂系统

优点：支持用户需求的动态变化，降低风险。

缺点：增加开发成本

喷泉模型：主要用于描述面向对象的开发过程，核心的特点是迭代。所有开发活动没有明显边界，允许各种开发活动交叉进行。

软件开发方法：

结构化方法：用系统工程的思想和工程化的方法，按用户至上的原则，结构化、模块化、自顶向下的对系统进行分析和设计的方法。**结构化开发方法是面向数据流的开发方法。**

优点：从系统整体出发，强调整体优化的条件下，自上而下的分析和设计；遵循用户至上原则；严格区分系统开发的阶段性；每个阶段的成果作为下一阶段的依据，便于系统开发的管理与控制；文档规范化，按照工程标准建立规范化的文档资料。

缺点：开发周期长，难于适应环境变化；

数据流图：用于描述数据流从输入到输出的变化流程，由加工、数据流、文件和外部实体构成。

概要设计：主要设计软件的结构、确定系统由那些模块组成，以及每个模块之间关系。

详细设计：确定应该如何实现具体所要求的系统，得出对目标系统的精确描述。

Jackson 是面向数据结构的开发方法。

面向对象的方法：从客观事物中构造软件系统，运用了对象、类、继承、封装、聚合、消息传递和多态等概念描述软件系统。

面向对象的软件开发方法有：**Booch 方法、coad 方法 jocobson 方法，对象建模技术 OTM 等**

统一建模语言 UML 是面向对象软件的标准化建模语言。它的词汇表中包含了 3 种构造块，即**事物、关系和图。**

事物是对模型中最具代表性的成分的抽象

关系把事物结合在一起，包括依赖、关联、泛化和实现。泛化关系是一种一般/特殊关系，利用这种关系子类可以共享父类的结构与行为。

图聚集了相关事务，包括类图、对象图用例图等。

需求分析

任务：确定软件系统的功能需求；分析软件系统的数据要求；导出系统逻辑模型；修正项目开发计划。

工作：需求获取；需求分析与综合；编写需求规格说明书；需求评审。

需求分类：功能需求；非功能需求；设计约束。

需求工具：数据流图 DFD、数据字典、判定表、判定树

软件设计：

模块设计原则：高内聚，低耦合

软件测试：

目的：尽可能多的发现软件产品的错误和缺陷。

测试方法：

白盒测试：需要**了解程序内部结构**，测试用例是根据程序内部逻辑来设计。白盒测试用于软件的**单元测试**。

黑盒测试：对软件已经实现的**功能是否满足需求**进行测试和验证。黑盒测试不关心内部逻辑结构，只根据程序的功能说明来设计测试用例。黑盒测试用于**软件的功能测试**。

灰盒测试：关注**输出对于输入的正确性**，同时也**关注内部**表现，但不像白盒那样详细完整。

测试的步骤：单元测试、集成测试、确认测试、系统测试

项目管理：范围管理，时间管理，成本管理，质量管理，人力资源管理，沟通管理，风险管理，采购管理，整体管理

时间管理

甘特图：用水平线段表示任务的工作阶段；线段的起点和终点对应任务的开始和完成；线段的长度表示完成任务所需时间。

优点：清晰的描述每个任务从何时开始到何时结束以及各任务之间的并行性。

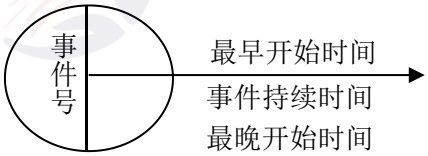
缺点：不能反映任务之间的依赖关系，难以确定任务关键所在，也不能反映任务中有潜力部分。

PERT：是一个有向图，途中用有向弧表示任务，可以标上任务完成所需时间；图中的节点表示流入节点的任务结束，并开始流出节点任务，把这些节点称为事件。事件本身不消耗时间和资源，它仅表示某个时间点。

Pert 图不仅给出了任务开始时间、结束时间和完成任务所需时间，还给出了任务之间关系，以及如期完成整个工程的关键路径。但不能反映任务之间的并行关系。

最晚开始时间取最小，最早开始时间取最大。

关键路径上的最早开始时间和最晚开始时间的点是相等的。



人力资源管理：需要综合考虑系统规模、技术复杂度、项目计划、成本和进度等因素。

风险管理：风险具有**不确定性**和**损失**两大特性

分类:项目风险，技术风险，商业风险

风险曝光度：风险的概率乘以风险可能造成的损失。

软件成熟度模型 CMM：分为 5 个等级，初始级、可重复级、定义级、管理级和优化级，每一级都为下一级提供基础。

• 初始级：软件过程的特点是无秩序的，有时甚至是混乱的。软件过程定义几乎处于无章法和步骤可循的状态，软件产品所取得的成功往往依赖于极个别人的努力和机遇。

• 可重复级：已建立了基本的项目管理过程，可用于对成本、进度和功能特性进行跟踪。对类似的应用项目，有章可循并能重复以往所取得的成功。

• 已定义级：用于管理的和工程的软件过程均已文档化、标准化，并形成了整个软件组织的标准软件过程。全部项目均采用与实际情况相吻合的、适当修改后的标准软件过程来进行操作。

• 已管理级：软件过程和产品质量有详细的度量标准。软件过程和产品质量得到了定量的认识和控制。

• 优化级：通过对来自过程、新概念和新技术等方面的各种有用信息的定量分析，能够不断地、持续地对促进过程进行改进。

除第一级外，每一级都设定了一组目标，如果达到了这组目标，则表明达到了这个成熟级别，自然可以向下一级别迈进。CMM 体系不主张跨级别的进化。因为从第二级开始，每一个低级别的实现均是高级别实现的基础。

文档的编制在开过过程中占有突出地位。文档作为检查项目进度和设计质量的依据；是设计人员在一定阶段的工作成果和结束标识；有助于提高设计效率。

知识产权

著作权：作者对其创作的作品享有的人身权和财产权

自软件开发完成之日起，保护期为 50 年，期满后，除人身权外其他权利终止。

人身权包括：署名权、发表权、修改权和保护作品完整权

财产权包括：发行权、出租权、展览权、表演权和信息网络传播权

合理使用是指可不经著作权人许可，也无需支付报酬，使用其作品。

著作权归属

1、职务开发软件著作权归单位。包括：本职工作明确的开发目标或从事本职工作活动的结果。

2、利用单位资金、专用设备、未公开的信息等物质技术条件，并由单位承担责任的软件，著作权归单位。

3、合作开发软件著作权一般为共同所有，如果有软件著作权协议，按协议确定著作

权归属。

4、委托开发的软件，著作权归属由委托人和受托人通过合同约定，如果未明确，著作权归属受托人。

5、接受任务开发的软件，著作权归属在合同中明确约定的一方，未明确的，属于软件开发单位。

6、只进行组织、提供咨询意见、物质条件或其他辅助工作不享有著作权。

侵权判定：

1、中国公民、法人和组织的作品，不论发表是否发表均享有著作权。

2、开发软件所用思想、处理过程、操作方法及数学概念不受保护。

3、法规、决定、命令、立法文件、官方译文、新闻和通用数表不受保护。

以下属于合理使用：

1、个人学习、研究或欣赏，适当引用不构成侵权。

2、为介绍、评论某一作品或说明某一问题，在作品中适当引用他人已发表的作品。

3、公开演讲内容、免费表演他人作品、不够成侵权

4、用户教学或科学研究不构成侵权

5、将汉语译成少数民族语言作品或盲文出版不构成侵权

专利权：由国务院相关部门授予的，对发明创造者在规定的时间内享有的独占使用权。**发明专利的保护时限为自申请日起 20 年，实用新型专利和外观设计专利为自申请日起 10 年**

两个以上申请人分别对同样的发明创造申请专利，专利权授予**最先申请的人。**同时申请专利，在收到国务院专利行政部门通知后，**自行协商确定申请人，协商不成的均予以驳回。**

同样的发明创造，只能授予一项专利。

强制实施许可：法律规定不经专利权人许可而实施专利权人之专利的不构成侵权

专利权归属：

下列情况专利权归属单位：

1、履行本单位交付的本职工作外的任务所作出的发明。

2、离职、退休或调动工作 1 年后与原单位相关的发明

3、职务发明创造

4、利用本单位的物质技术条件完成发明创造，其专利权依据合同约定。

商标法

商标注册年限为 10 年，注册人死亡或倒闭 1 年未转移可以注销，期满后 6 个月内可以续注。

商标谁先申请谁拥有，但知名商标非法抢注的除外。

同时申请，谁先使用谁拥有（需提供证据）

无法提供证据、协商归属无效时抽签确定（但不可不确定）

公民作品保护期限：作者终身及死后 50 年，合作的作品，以最后一名作者死亡为准。

标准是对重复性事物和概念所做的统一规定。它以科学、技术和实践经验的综合成果为基础，经有关方面协商一致，由主管机构批准，以特定形式发布，作为共同遵守的准则和依据。

我国家标准的有效期一般为 5 年

标准编号

国际标准代号：标准代号+专业类号+顺序号+年代号

我国标准代号：标准代号+标准发布顺序号+标准发布年号

强制性标准代号 GB

推荐性标准代号 GB/T

指导性标准代号 GB/Z

实物标准代号 GSB

行业标准代号：汉语拼音大写字母

地方标准代号：由 DB 加省级行政区代码前两位

企业标准代号：由 Q/XXX 加企业代号组成

国际标准：IEC　ISO　ITU

国家标准：ANSI　GB

行业标准：IEEE

商业秘密：不为公众所知，具有经济利益和实用性，并且已采取了保密措施的技术信息和经营信息。