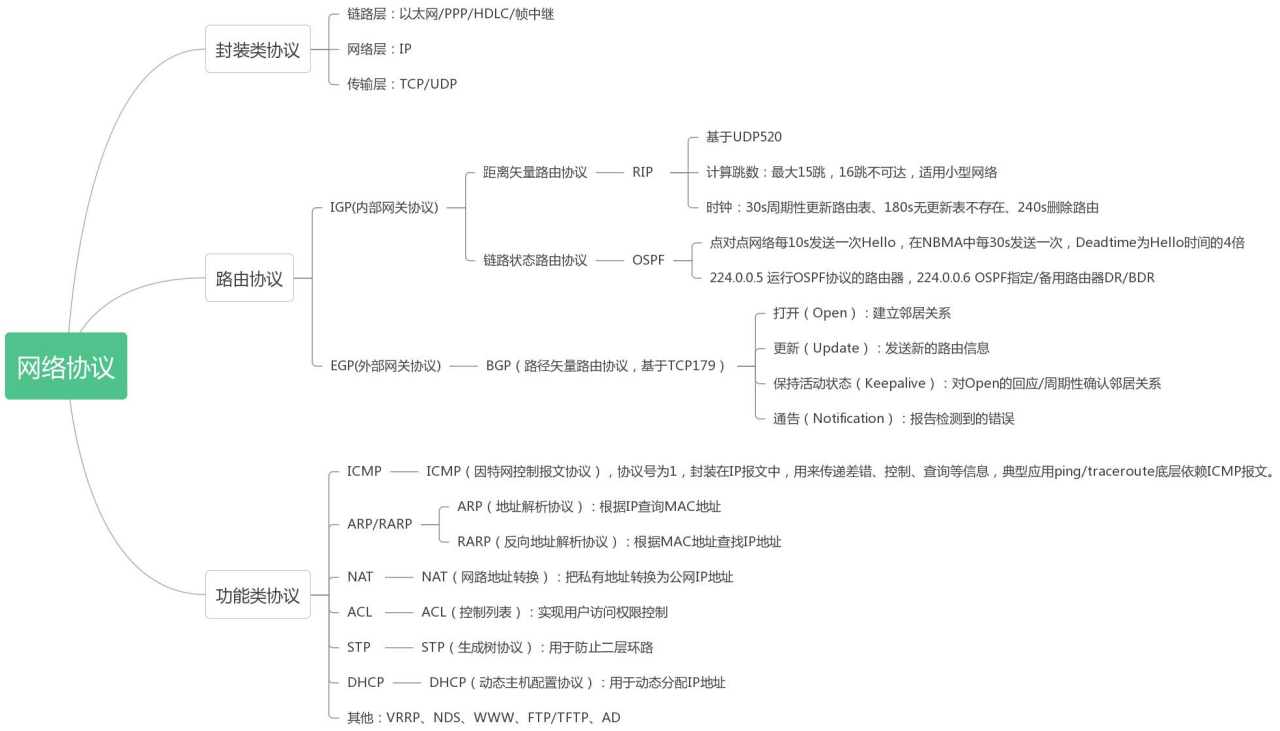
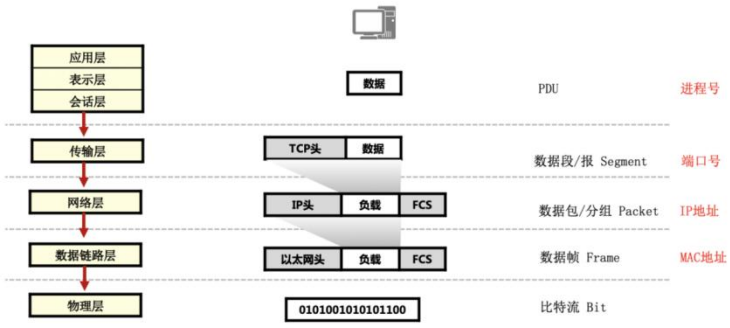
目录

1	9	17	25	128	1000 0000	进制转换：
2	10	18	26	192	1100 0000	二进制转十进制（低转高）：
3	11	19	27	224	1110 0000	110　　$1*2^2+1*2^1+0=6$
4	12	20	28	240	1111 0000	十进制转二进制（高转低）：短除法逆序排序
5	13	21	29	248	1111 1000	
6	14	22	30	252	1111 1100	
7	15	23	31	254	1111 1110	
8	16	24	32	255	1111 1111	



上午选择题

考查内容	分值	重点与备考建议
补充知识点：计算机硬件基础，操作系统软件开发基础，知识产权	10分	涉及内容非常多，建议结合真题看精讲补充视频（别想着拿10分，拿6-8都可以接受）
英文选择填空	5分	平时看到英文缩写，多做笔记，不会的baidu，比如典型协议VLAN、ARP是哪几个单词缩写
第二章：通信基础	3-5分	PCM、E1、海明码（海明不等式）
第三章：广域网	1-2分	帧中继、HDLC
第四章：局域网和城域网	4-5分	CSMA/CD、VLAN、STP、802.1Q
第五章：无线通信网	2-3分	802.11，无线网络安全
第六章：网络互联与互联网	13-16分	重点协议：ARP/RIP/OSPF/BGP/ICMP/TCP
第七章：下一代互联网IPv6	1-2分	IPv6地址格式、过渡技术
第八章：网络安全	5-6分	SSL/PGP、加解密算法、数字签名、数字证书
第九章：操作系统与服务器	10分	常考DNS/DHCP/AD和IIS
第十章：组网技术	3-5分	交换机、路由器、防火墙等组网
第十一章：网络管理	3-5分	SNMP、网络管理常用命令
第十二章：网络规划设计	3-4分	综合布线、网络设计阶段与过程，网络架构



2023.5.26

1. 网络体系结构

1. 物理层：为数据链路层实体提供让立、传输、释放所必须的物理连按，并且捉供透明的比特流传输。

连接方式：全双工或半双工　　传输方式：异步或同步　　数据单位：比特 bit

机械特性	规定接口的外形、大小、引脚数和排列、固定位置。
电气特性	规定接口电缆上各条线路出现的电压范围。
功能特性	指明某条线上出现某一电平的电压表示何种意义。
规程特性	指明各种可能事件出现的顺序。
数据终端设备 DTE	具有一定的数据处理能力和数据收发能力的设备，用于提供或接收数据。公头。常见的 DTE 设备有路由器、PC、终端等。
数据通信设备 DCE	在 DTE 和传输线路之间提供信号变换和编码功能，并负责建立、保持和释放链路的连接。提供时钟。母头。常见的 DCE 设备有 CSU/DSU、NT1、广域网交换机、MODEM 等。

2. 数据链路层：数据链路层将原始的传输线路转变成一条逻辑的传输线路，实现实体间二进制信息块的正确传输，为网络层提供可靠的数据信息。

a. 数据单位：帧，具有流量控制功能。

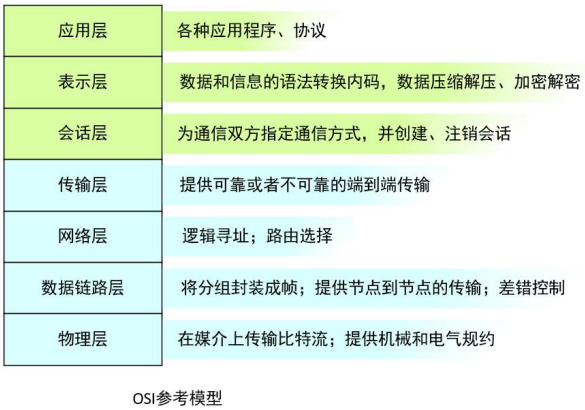
b. 功能：链路连接的建立、拆除和分离；帧定界和帧同步；顺序控制；差错检测、恢复；链路标识、流量/拥塞控制。

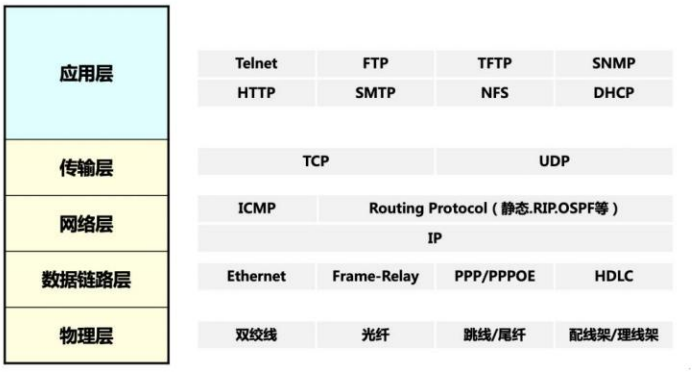
c. 两层：逻辑链路控制 LLC、介质访问控制 MAC。

3. 网络层：网络层控制子网的通信，其主要功能是提供路由选择，即选择到达目的主机的最优路径并沿着该路径传输数据包。

a.具备的功能有：路由选择和中继；激活和终止网络连接；链路复用；差错检测和恢复；流量/拥塞控制等。

4. 传输层：传输层利用实现可靠的端到端的数据传输能实现数据分段、传输和组装，还提供差错控制和流量/拥塞控制等功能。





2. 物理层

2.1 数据通信理论

(1) 信道编码器的作用是将信号转换为合适的形式对传输介质进行数据传输。

(2) 信道解码器将传输介质和传输数据转换为接收信号。

(3) 信源解码器的作用是进行数/模转换（D/A 转换）），即将数字信号或模拟信号转换为文字声音、动画、图像等。

1. 传输速率

码元	在数字通信中常用时间间隔相同的符号来表示一个二进制数字，这样的时间间隔内的信号称为二进制码元。另一种定义是，在使用时间域（时域）的波形表示数字信号时，代表不同离散数值的基本波形就称为码元。
码元速率（波特率)	即单位时间内载波参数（相位、振幅、频率等）变化的次数，单位为波特，常用符号 Baud 表示，简写成 B。
比特率 （信息传输速率、信息速率）	指单位时间内在信道上传送的数据量(即比特数)，单位为比特每秒(bit/s)，简记为 b/s 或 bps。
比特率与波特率关系	比特率=波特率×单个调制状态对应的二进制位数=波特率×$\log_2 N$
带宽	传输过程中信号不会明显减弱的一段频率范围，单位为赫兹(Hz)。 信道带宽 W=最高频率—最低频率
信噪比与分贝	$1dB=10\times\log_{10} S/N$　$30dB=10\times\log_{10} 10^3$
奈奎斯特定理 （无噪声）	最大数据速率 $R=2W\log_2 N = B\log_2 N$ W:带宽，B:波特率=2W，N:码元总的种类数
香农定理 （有噪声）	极限数据速率 C=带宽×$\log_2(1+S/N)$ S:信号功率，N:噪声功率。
误码率	指接收到的错误码元数在总传送码元数中所占的比例。 $P=\frac{\text{错误码元数}}{\text{码元总数}}$
1 字节(B)=8bit　1KB=1024 字节　1MB=1024KB 1GB=1024MB 1TB=1024GB	
信道延迟：电缆信道延迟 200m/us (200km/ms，20 0000km/s)　　卫星信道延迟：270ms	

2. 数据传输方式

按信号类型分类	模拟通信、数字通信
按一次传输的数据位数分类	串行通信、并行通信
按照信号传送的方向与时间的关系分类	单工通信、半双工、全双工
按照数据的同步方分类	同步通信、异步通信 异步通信数据速率=每秒钟传输字符数×（起始位＋终止位＋校验位＋数据位) 异步通信有效数据速率=每秒钟传输字符数×数据位

3. 多路复用

复用技术		特点	应用
时分复用 TDM	同步时分复用	固定时隙的时分复用，即使无数据传输的各子信道轮流按时间独占带宽	E1、Tl,SDH SONET、DDN、PON 下行
	统计时分复用	对同步时分复用进行改进，通过动态地分配时隙来进行数据传输的	ATM
波分复用 WDM		所谓波分复用就是将整个波长频带被划分为若干个波长范围，每路信号占用一个波长范围来进行传输。属于特殊的频分复用	光纤通信
频分复用 FDM		频分复用是指多路信号在频率位置上分开，但同时在一个信道内传输。频分复用信号在频谱上不会重叠，但在时间上是重叠的	宽带有线电视、无线广播、ADSL、无线局域网

4. 调制与编码

（1）编码就是用数字信号承载数字或模拟数据；调制就是用模拟信号承载数字或模拟数据。

（2）调制可以分为基带调制和带通调制。

调制技术	码元种类	比特位	特性
幅移键控（ASK）	2	1	恒定振幅:1，载波关闭:0；抗干扰性差，容易实现
频移键控（FSK）			不同的两个频率分别代表 0 和 1
相移键控（PSK）			不同的两个相位分别代表 0 和 1
QPSK（4PSK）	4	2	+45° 、+135° 、-45° 、-135°分别代表 00、01、10、11
8PSK	8	3	8 个相位分别代表 000、...、111 的 8 个值
DPSK	2	1	0，初始有相位变化；1，初始无相位变化
4QAM	4	2	结合了 ASK 和 PSK 的调制方法

模拟信号调制为模拟信号	调幅（AM）调整载波的振幅； 调频（FM）调整载波的频率； 调相（PM）调整载波的初始相位。
模拟信号调制为数字信号	采样、量化、编码
数字信号调制为模拟信号	幅移键控（ASK）：载波幅度随着基带信号的变化而变化，方式还可称作通-断键控或开关键控。 频移键控（FSK）：载波频率随着基带信号的变化而变化。 相移键控（PSK）：载波相位随着基带信号的变化而变化。PSK 最简单的形式是 BPSK，载波相位有 2 种，分别表示逻辑 0 和 1。4PSK 又称为 QPSK，使用 4 个输出相位表示 2 个输入位；8PSK 使用 8 个输出相位表示 3 个输入位；16PSK 使用 16 个输出相位表示 4 个输入位。 DPSK 称为相对相移键控调制，记作 2DPSK。信息是通过连续信号之间的载波信号的初始相位是否变化来传输的。 正交幅度调制（QAM）：若利用正交载波调制技术传输 ASK 信号，可使频带利用率提高 1 倍。
数字信号调制为数字信号	• 极限编码：极性码正电平 0，负电平 1；单极性码正电平 0，零电平 1；双极性码使用正负电平和零电平共 3 个电平表示信号。 • 归零码（RZ）：正电平→零电平表 0，负电平→零电平表 1。 • 不归零码（NRZ）：遇到 1 时，电平翻转；遇到 0 时，电平不翻转。 • 不归零反向编码（NRZ-I）：遇到 0 时，电平翻转；遇到 1 时，电平不翻转。 • 双向码：负电平→正电平为 0，正电平→负电平为 1。 • 曼彻斯特编码：负电平→正电平为 0，高电平→负电平为 1。编码效率 50% 负电平→正电平为 1，正电平→负电平为 0。 • 差分曼彻斯特编码：有电平变化为 0，无电平变化为 1。 • 4B/5B、8B/10B、8B/6T 编码

编码	效率	应用领域
曼彻斯特编码	50%	以太网
差分曼彻斯特编码		令牌环
4B/5B	80%	FDDI、100Base-TX、100Base-FX
8B/10B		千兆以太网（注:1000base-T 与 100base-Tx 采用 PAM-5 编码）
64/66B	97%	万兆以太网
8B/6T	将 8 位映射为 6 个三进制位	100Base-T4(3 类 UTP)

5. 数据交换方式

数据交换方式		定义	优缺点
电路交换		通信开始之前，主呼叫和被呼叫之间建立连接，之后建立通信，期间独占整个链路，结束通信时释放链路。电路交换是面向连接的	优点：时延小 缺点：链路空闲率高，不能进行差错控制
报文交换		结点把要发送的信息组织成一个报文（数据包），该报文中含有目标结点的地址，完整的报文在网络中一站一站地向前传送。每一个结点接收整个报文并检查目标结点地址，然后根据网络中的拥塞情况在适当的时候转发到下一个结点	优点：不用建立专用通路；可以校验，也可以将一个报文发至多个目的地 缺点：中间节点需要先存储，再转发报文，时间延时较大:中间节点的存储空间也需要较大
分组交换 (确定最大报文长度)	数据报	数据报服务类似于邮政系统的信件投递。每个分组都携带完整的源和目的节点的地址信息，独立地进行传输，每当经过一个态，按一定的路由选择算法选择一条中间节点时都要根据目标地址和网络当前的状最佳的输出线，直至传输到目的节点	优点：不需要建立连接 缺点：每个分组独立选路，不完全走一条路；可靠性差
	虚电路	在虚电路服务方式中，为了进行数据的传输，网络的源主机和目的主机之间先要建立一条逻辑通道，所有报文沿着逻辑通道传输数据。在传输完毕后，还要将这条虚电路释放。虚电路的服务方式是网络层向传输层提供的一种使所有分组按顺序到达目的主机的可靠的数据传送方式。虽然用户感觉到好像占用了一条端到端的物理线路，但实际上并没有真正地占用，即这一条线路不是专用的，所以称之为“虚电路”	优点：相对数据报可以进行流控和差错控制，提高了可靠性，适合远程控制和文件传送 缺点：不如数据报方式灵活
信元交换		信元交换又叫 ATM（异步传输模式)，是一种面向连接的快速分组交换技术，它是通过建立虚电路来进行数据传输的。 信元交换技术是一种快速分组交换技术，它结合了电路交换技术延迟小和分组交换技术灵活的优点。 信元是固定长度的分组，ATM 采用信元交换技术，其信元长度为 53 字节，其中信元头为 5 字节，数据为 48 字节	结合了电路交换技术延迟小和分组交换技术灵活的优点

2.2 数字传输系统

1. 脉冲编码调制 PCM 体制

(1) PCM 数字化过程 3 个步骤：采样、量化和编码。

(2) 采样频率：大于 $2f_{max}$

(3) 解调：把模拟信号转换为数字信号的过程。

名称	总速率	话路组成	每个话音信道的数据速率	使用地区	
T1	1.544Mb/s	30 条语音话路和 2 条控制话路	64kb/s	美国、加拿大、日本、新加坡	时隙 CH0 用作帧同步，时隙 CH16 用来传送信令，El 载波的控制开销占 6.25%。每个时隙传送 8bit（7bit 编码+1bit 信令），共用 256bit。每秒传送 8000 个帧。8000 帧/s，数据速率 64kb/s。
E1	2.048Mb/s	24 条语音话路	64kb/s	中国、欧洲	每个时隙传送 8bit（7bit 编码+1bit 信令），共用 193bit。8000 帧/s，数据速率 64kb/s（8*8000）。
E2=4 个 E1=8.448Mbps；E3=4 个 E2=34.368Mbps；E4=4 个 E3=139.264Mbps；E5=4 个 E4=566.148Mbps					

2. 同步光纤网（SONET）：第 1 级同步传送信号（STS-1），第 1 级光载波（OC-1），第 1 级同步传递模块（STM-1），使用铯原子钟提供时间同步。

光纤级	STS 级	链路速 Mbps	有效载荷 Mbps	负载 Mbps	SDH 对应	常用近似值
OC-1	STS-1	51.840	50.112	1.728	-	
OC-3	STS-3	155.520	150.336	5.184	STM-1	155Mbps
OC-9	STS-9	466.560	451.008	15.552	STM-3	
OC-12	STS-12	622.080	601.344	20.736	STM-4	622Mbps
OC-18	STS-18	933.120	902.016	31.104	STM-6	
OC-24	STS-24	1244.160	1202.688	41.472	STM-8	
OC-36	STS-36	1866.240	1804.032	62.208	STM-13	
OC-48	STS-48	2488.320	2405.376	82.944	STM-16	2.5Gbps
OC-96	STS-96	4976.640	4810.752	165.888	STM-32	
OC-192	STS-192	9953.280	9621.504	331.776	STM-64	10Gbps

3. 同步数字系列（SDH）：提供准同步数字系列（PDH），该方式在 STM-1 中封装 63 个 E1 信道。

2.3 接入技术

1. xDSL：xDSL 技术就是利用电话线中的高频信息传输数据，高频信号损耗大，容易受噪声干扰。

（1）ADSL 虚拟拨号。

（2）ADSL 专线接入。

名称	对称性	上、下行速率 (受距离影响有变化）	极限传输距离	复用技术
ADSL（非对称数字用户线路）	不对称	上行:640~1Mb/s 下行:1 一 8Mb/s	35km	频分复用
VDSL（甚高速数字用户线路）		上行:1.6~2.3Mb/s 下行:12.96 一 52Mb/s	0.9~1.4km	QAM 和 DMT
HDSL（高速数字用户线路）	对称	上行、下行:1.5Mb/s	2.7~3.6km	时分复用
G.SHDSL（对称的高比特数字用户环路）		一对线上、下行可达 192kb/s~2.312Mb/s	3.7~7.1km	

2. HFC（混合光纤一同轴电缆）：HFC 通常由光纤干线、同轴电缆支线和用户配线网络三部分组成，从有线电视台出来的节目信号先变成光信号在干线上传输，到用户区域后把光信号转换成电信号，经分配器分配后通过同轴电缆送到用户。

3. FTTx

（1）FTTx 技术主要用于接入网络光纤化，范围从区域电信机房的局端设备到用户终端设备，局端设备为光线路终端（OLT）、用户端设备为光网络单元（ONU）或光网络终端（ONT）。

• 光纤到交换箱（FTTCab）、光纤到路边（FTTC）、光纤到大楼（FTTB）、光纤到户（FTTH）等。

（2）无源光纤网络（PON）技术：是指 ODN（光配线网）中不含有任何电子器件和电子电源，ODN 全部由光分路器等无源器件组成,不需要贵重的有源电子设备。一个无源光纤网络包括一个安装于中心控制站的 OLT 及一批配套的安装于用户场所的光网络单元 ONU。在 OLT 与 ONU 之间的光配线网包含了光纤和无源分光器/耦合器。

① PON 技术主要有：以太网无源光网络（EPON）和千兆以太网无源光网络（GPON）。

2.4 有线传输介质

1. 常见有线传输介质

同轴电缆	同轴电缆从用途上分，可分为基带同轴电缆和宽带同轴电缆（即网络同轴电缆和视频同轴电缆)。同轴电缆分 50Q2 基带电缆和 75Q 宽带电缆两类。基带电缆又分细同轴电缆和粗同轴电缆，基带电缆仅仅用于数字传输，数据率可达 10Mb/s。
屏蔽双绞线 STP	根据屏蔽方式的不同，屏蔽双绞线可分为两类，即 STP 和 FTP。STP 是指每条线都有各自屏蔽层的屏蔽双绞线，而 FTP 则是采用整体屏蔽的屏蔽双绞线。
非屏蔽双绞线 UTP	（1）双绞线的线序标有标准 568A 和标准 568B。 （2）交叉线是指一端是 568A 标准，另一端是 568B 标准的双绞线；直连线是指两端都是 568A 或 568B 标准的双绞线。 （3）综合布线中对五类线、超五类线、六类线测试的参数有：衰减量、近端串扰、远端串扰、回波损耗、特性阻抗、接线方式。

光纤	（1）光波在光纤中的传播模式与芯线和包层的相对折射率、芯线的直径以及工作波长有关。如果芯线的直径小到光波波长大小，则光纤就成为波导，光在其中无反射地沿直线传播，这种光纤叫单模光纤。 （2）光波在光导纤维中以多种模式传播，不同的传播模式有不同波长的光波和不同的传播和反射路径，这样的光纤叫多模光纤。

单模光纤和多模光纤的特性

	单模光纤	多模光纤
光源	激光二极管	LED
光源波长	1310nm 和 1550nm 两种	850nm 和 1300nm 两种
纤芯直径/包层外径	8.3/125um	50/125um 和 62.5/125um
距离	2~10km	2km
速率	100~10Gb/s	1~10Gb/s
光种类	一种模式的光	不同模式的光

	单模光纤	多模光纤
纤芯和包层直径	纤芯直径 8 或 10um，包层直径为 125um	纤芯直径 50 或 62.5um，包层直径为 125um
光源	光普线较窄的 LED 或 LD 激光器	LED 发光二极管或 LD 激光器
带宽	模态色散小于多模光纤，具有更高的带宽	具有更大的纤芯尺寸，支持多个传输模式，模态色散大于单模光纤，带宽低于单模光纤
护套颜色	黄色	橙色或水绿色
价格	高	低
传输距离	远	近
工作波长	1310nm 或 1550nm	850nm

4. 光纤布线系统的测试指标包括：最大衰减限值、波长窗口参数和回波损耗限值。

2.5 其他知识点

1. RS-232-C：串行通信接口标准，主要用于 DTE 与 DCE 之间的通信接口规范。为 25 针，可简化为 9 针和 15 针。

2. 帧中继：在第二层建立虚电路，用帧方式承载数据业务。在帧中继网上，用户的数据速率可以在一定的范围内变化，从而既可以适应流式业务，又可以适应突发式业务。帧中继提供两种虚电路：交换虚电路和永久虚电路。帧长可变，可以承载各种局域网的数据传输。

3. 异步传输模式（ATM）：异步传输模式（Asynchronous Transfer Mode，ATM）是一项数据传输技术，是实现 B-ISDN 业务的核心技术之一。ATM 是以信元为基础的一种分组交换和复用技术，是一种为了多种业务设计的通用的面向连接的传输模式。ATM 的传送单元是固定长度为 53byte 的 CELL(信元)，其中 5B 为信元头，

用来承载该信元的控制信息;48B 为信元体，用来承载用户要分发的信息。信头部分包含了选择路由用的 VPI(虚通道标识符）/VCI（虚通路标识符）信息，因而它具有分组交换的特点。

固定比特率 CBR	采用固定比特率业务适合于交互式语音和视频流。
可变比特率 VBR	可变比特率业务适合交互式压缩视频信号。
有效比特率 ABR	采用有效比特率业务用于突发通信。
不定比特率 UBR	采用不定比特率业务可用于传送 IP 分组，包括文件传输、电子邮件业务潜在的应用领域。

设备层次	设备名称	工作原理
物理层	中继器、集线器	放大信号，延长传输距离
数据链路层	网桥、交换机	基于目的 MAC 地址转发数据帧
网络层	路由器、三层交换机	基于目的 IP 地址转发数据包
四层以上设备	网关	基于传输层、应用层进行控制

3. 数据链路层

3.1 流量控制和差错控制

1. 流量控制

停等协议	• 工作原理：发送站发一帧，收到应答信号后再发送下一帧，接收站每收到一帧后回送一个应答信号（ACK），表示愿意接收下一帧，如果接收站不应答，发送站必须等待。 • TFA=$2t_p+t_f$　　t_p 路上传送时间（路上跑的时间），tf 发送时间（排队上车的时间）
滑动窗口协议	• 滑动窗口协议主要思想是：允许连续发送多个帧而无须等待应答。 • 如图假设站 S1 和 S2 通过全双工链路连接，S2 维持能容纳 6 个帧的缓冲区（$W_{收}=6$ ） • 这样 S1 就可以连续发送 6 个帧而不必等待应答信号(W 发=6)

2. 差错控制：自动重传 ARQ 协议

停等 ARQ 协议	• 停等 ARQ 协议是停等流控技术和自动请求重发技术的结合。 • 发送站发出一帧后必须等待应答信号，收到肯定应答信号 ACK 后继续发送下一帧；收到否定应答信号 NAK 后重发该帧；若在一定的时间内没有收到应答信号也必须重发。
选择重发 ARQ 协议	重传特定的某一帧　　$W_{发}=W_{收} \le 2^{k-1}$　　k 为帧编号位数
后退 N 帧 ARQ 协议	重传此帧和后续的 N 帧　　$W_{发}=W_{收} \le 2^{k}-1$　　“选上退下”

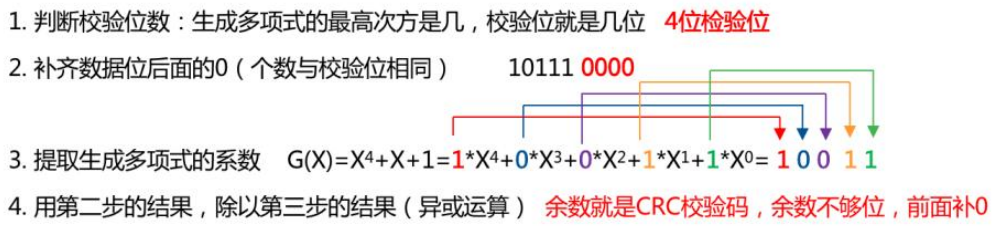
3.2 检错与纠错

1. 一帧包含 m 个数据位（即报文)和 r 个冗余位(校验位)。假设帧的总长度为 n，则有 n=m+r。包含数据和校验位的 n 位单元通常称为 n 位码字。

2. 海明(Hamming)码是通冗余数据位来检测和纠正差错的编码方式。

3. 设海明码校验位为 k，信息位为 m，2^k 个信息，则它们之间的关系应满足 $2^{k-1} \geqslant m+k$。

4. 循环冗余校验码（CRC）自动选择重发：



5. 常见的 CRC 生成多项式。

CRC-16 = $x^6+x^{15}+x^3+1$。用于 FR、X.25、HDLC、PPP 中，用于校验除帧标志位外的全帧。

CRC-32 = $x^{32}+x^{26}+x^{23}+x^{22}+x^{16}+x^{12}+x^{11}+x^{10}+x^8+x^7+x^5+x^4+x^2+x+1$。用于校验以太网(802.3)帧(不含前导和帧起始符)、令牌总线(802.4)帧(不含前导和帧起始符入)、令牌环(802.5)帧(从帧控制字段到 LLC 层数据)、FDDI 帧(从帧控制字段到 INFO)、ATM 全帧、PPP 除帧标志位外的全帧。

3.3 点对点传输

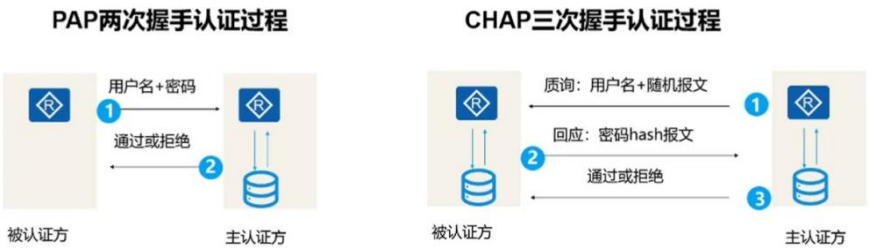
1.点到点协议（PPP）：提供了一种在点到点链路上封装网络层协议信息的标准方法。PPP 包含链路控制协议（LCP）和网络控制协议（NCP）。

PPP 有以下三个主要的组成部分:

- 在串行链路上封装数据报的方法。
- 建立、配置和测试数据链路链接的 LCP 协议。
- 建立和配置不同网络层协议的一组网络控制协议（NCP）。

2. PPP 验证方式：密码验证（PAP）（2 次握手验证）、挑战一握手验证协议（CHAP）（3 次握手验证）。

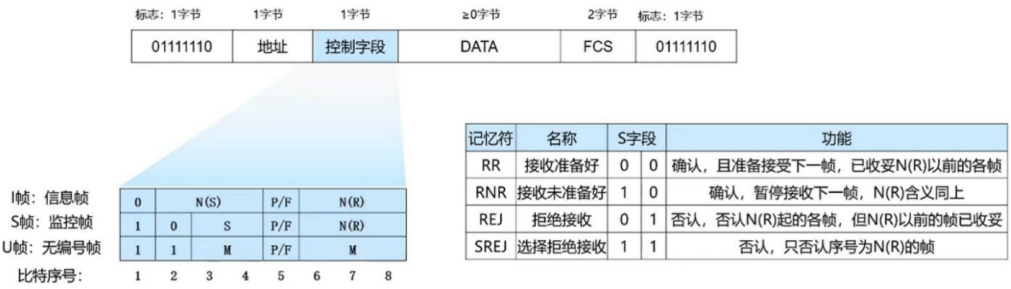
PAP：两次握手验证协议，口令以明文传送，被验证方首先发起请求。
CHAP：三次握手，认证过程不传送认证口令，传送 HMAC 散列值。



3. PPPOE：通过 PPPOE 协议，远端接入设备能够实现对每个接入用户的控制和计费。PPPOE 协议的工作流程包括发现和会话两个阶段，发现阶段是无状态的，目的是获得 PPPOE 终结端（在局端的 ADSL 设备或其他接入设备上）的以太网 MAC 地址，并建立一个唯一的 PPPOEsession-ID。发现阶段结束后就进入标准的 PPP 会话阶段。

3.4 HDLC（高级数据链路控制）

HDLC（高级数据链路控制）是一种面向比特的同步链路控制协议。



记忆符	名称	S字段		功能
RR	接收准备好	0	0	确认，且准备接受下一帧，已收妥N(R)以前的各帧
RNR	接收未准备好	1	0	确认，暂停接收下一帧，N(R)含义同上
REJ	拒绝接收	0	1	否认，否认N(R)起的各帧，但N(R)以前的帧已收妥
SREJ	选择拒绝接收	1	1	否认，只否认序号为N(R)的帧

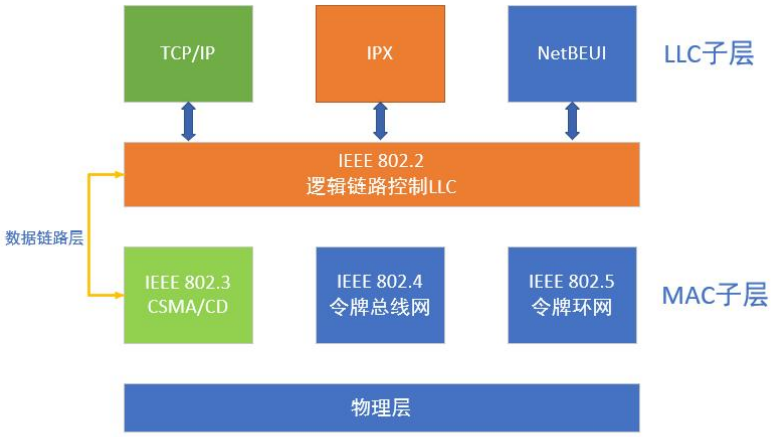
信息帧（I 帧）	第一位为 0，用于承载数据和控制。 N（S）表示发送帧序号，N（R）表示下一个预期要接收帧的序号，N（R）=5，表示下一帧要接收 5 号帧。N（S）和 N（R）均为 3 位二进制编码，可取值 0～7。
监控帧（S 帧）	前两位为 10，监控帧用于差错控制和流量控制。 S 帧控制字段的第三、四位为 S 帧类型编码，共有四种不同编码。
无编号帧（U 帧）	控制字段中不包含编号 N（S）和 N（R），U 帧用于提供对链路的建立、拆除以及多种控制功能求提供不可靠的无连接服务时，它有时也可以承载数据。

3.5 常见广播方式的数据链路层

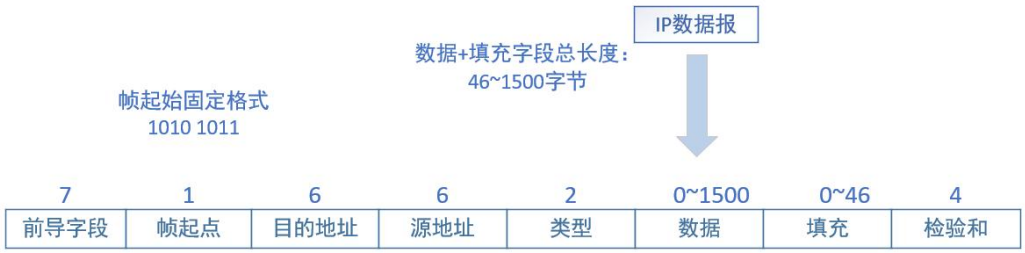
1. 802 标准的数据链路层：①逻辑链路控制（LLC）；②媒体接入控制层（MAC）。

（1）MAC：实现流量控制等功能，包括数据帧的封装/卸装、帧的寻址和识别、帧的接收与发送、链路的管理、帧的差错控制等。MAC 层的主要访问方式有 CSMA/CD、令牌环和令牌总线三种。

• 广播帧形式为 FF.FF.FF.FF.FF.FF，广播是向子网所有端口（含自身端口）发送广播帧；泛洪是向所有端口（除自身端口）发送普通数据帧。



局域网数据链路层结构



MAC帧格式

（2）MAC 地址：前 24 位是厂商编号，由 IEEE 分配给生产以太网网卡的厂家；后 24 位是序列号，由厂家自行分配，用于表示设备地址。全球唯一。

（3）LLC 服务类型

不确认的无连接服务	即数据报服务，适用于点对点通信、广播通信、多播通信（组播通信)。
面向连接服务	即虚电路服务，这种方式特别适合于传送很长的数据文件。
带确认的无连接服务	即可靠的数据报服务，这种方式特别适合于过程控制或自动化工厂环境中的告警信息或控制信号的传输。带确认的无连接服务只用在令牌总线网中。
高速传送服务	专为城域网使用。

2. 载波监听多路访问/冲突检测（CSMA/CD）是一种争用型的介质访问控制协议，其工作原理是:发送数据前先监听信道是否空闲，若空闲，则立即发送数据。在发送数据时，边发送边继续监听。若监听到冲突，则立即停止发送数据，等待一段随机时间再重新尝试。

• 在网络负载较小时，CSMA/CD 协议的通信效率很高;但在网络负载增大时，发送时间增加，发送效率急剧下降。这种网络协议适合传输非实时数据。

• 多路访问：表明多路计算机连接在一根总线上。

• 载波监听（CSMA）：表明发送数据前检测总线中是否有数据发送，如果有，则进入类似退避算法的程序，进而反复进行载波监听工作;如果没有，则依据一定的坚持算法决定如何发送。

• 以太网规定帧间最小间隔为 9.6s，使接收方在接收完数据后清理缓存，做好接收下一帧的准备。

（1）坚持算法

算法	说明	特点
1-持续 CSMA	当信道忙或发生冲突时，要发送帧的站一直持续监听，一旦发现信道有空闲（即在帧间最小间隔时间内没有检测到信道上有信号）便可发送。	有利于抢占信道，减少信道空闲时间；较长的传播延迟和同时监听会导致多次冲突，降低系统性能。
非持续 CSMA	发送方并不持续侦听信道，而是在冲突时等待随机的一段时间 N，再发送。	有更好的信道利用率，减少了冲突的概率；使信道的利用率降低；增加了发送时延。
p-持续 CSMA	发送方按 P 概率发送帧，即信道空闲时（即在帧间最小间隔时间内没有检测到信道上有信号)，发送方不一定发送数据，而是按照 P 概率发送。	P 的取值比较困难，大了会产生冲突，小了会延长等待时间。

（2）冲突检测（CSDMA/CD）：采用“边发送边监听”方式。

• 电磁波在 1km 电缆传播的时延约为 5us.

• 冲突检测最长时间为两倍的总线端到端的传播时延（2r），2r 称为争用期，又称为碰撞窗口。

• 10M 以太网争用期定为 51.2us。对于 10Mb/s 网络，时间 51.2us 可以发送 512bit 数据，即 64 字节。

• 以太网规定 10Mpbs 以太网最小帧长为 64 字节，最大帧长为 1518 字节，最大传输单元(MTU)为 1500 字节。小于 64 字节的都是由于冲突而异常终止的无效帧，接收这类帧时应将其丢弃（千兆以太网和万兆以太网最小帧长为 512 字节)。

• 最小帧长 = 网络速率×2×(最大段长/信号传播速度)

最小帧长：$L_{min}=2R\times d/v$　　R：网络数据速率，d：最大距离，v：传播速度

不冲突：发送时间>正常传送+返回确认时间 L/R >2×d/v 则推出最小帧长公式

• 吞吐率：单位时间实际传送的数据位数。

• 吞吐率=帧长/（传输数据帧所花费的时间+1 帧发送到网络所花费的时间)

=帧长/（网络段长/传播速度+1 帧长/网络数据速率)

• 网络利用率=吞吐率/网络数据速率

（4）退避算法特点：是网络负载越重，可能后退的时间越长，没有对优先级进行定义，不合适突发性业务和流式业务。该算法考虑了网络负载对冲突的影响，在重负载下能有效分解冲突。

（5）二进制指数退避算法：检测到冲突后，马上停止发送数据，并等待随机时间在发送数据。如果连续发生 16 次碰撞后，认为网络繁忙或故障，不再尝试发送。冲突概率：$1/2^n$。 τ = 512 比特时间

3. IEEE 802 系列协议

802体系结构

（1）IEEE 802.1 系列

IEEE 802.1d	生成树协议（STP）
IEEE 802.1P	是交换机与优先级相关的流量处理的协议
IEEE 802.1q	虚拟局域网（VLAN）协议定义了 VLAN 和封装技术，包括 GARP 协议及其源码、GVRP 协议及其源码。
IEEE 802.1s	多生成树协议（MSTP）
IEEE 802.1w	快速生成树协议（RSTP）
IEEE 802.1x	基于端口的访问控制（Port Based Network Access Control）协议起源于 802.11 协议，目的是为了解决无线局域网用户的接入认证问题。

（2）IEEE 802.2 系列：逻辑链路控制（LLC）提供 LAN 和 MAC 子层与高层协议间的一致接口。

（3）IEEE 802.3 系列

IEEE 802.3ab	制定的 1000 Base-T 规格。这是一个传输介质为 4 对 CAT-5 双绞线、100m 内达到以 1 Gb/s 传输数据的标准。
IEEE 802.3u	快速以太网(Fast Ethernet）的最小帧长不变，数据速率提高了 10 倍，所以冲突时槽缩小为 5.12us。以太网的计算冲突时槽的公式为 slot≈2S/0.7C+2tphy。 S 表示网络的跨距（最长传输距离），0.7C 为 0.7 倍光速（信号传播速率），tphy 是发送时延（由于往返需通过站点两次，所以取其时延的两倍值)。
IEEE 802.3z	千兆以太网(Gigabit Ethernet)
IEEE 802.3ae	万兆以太网(10 Gigabit Ethernet)

IEEE 802.4	令牌总线网
IEEE 802.5	令牌环线网
IEEE 802.6	城域网 MAN，定义城域网的媒体访问控制(MAC）子层和物理层规范。
IEEE 802.7	宽带技术咨询组，为其他分委员会提供宽带网络技术的建议和咨询。
IEEE 802.8	光纤技术咨询组，为其他分委员会提供使用有关光纤网络技术的建议和咨询。
IEEE 802.9	集成数据和语音网络（VoIP）定义了综合语音/数据终端访问综合语音/数据局域网（包

	括 IVD LAN、MAN、WAN）的媒体访问控制(MAC)子层和物理层规范。
IEEE 802.10	可互操作局域网安全标准，定义局域网互连安全机制。
IEEE 802.11	无线局域网标准，定义了自由空间媒体的媒体访问控制(MAC)子层和物理层规范。
IEEE 802.12	按需优先定义使用按需优先访问方法的 100Mp/s 以太网标准。
IEEE802.14	有线电视标准。
IEEE 802.15	无线个人局域网（PAN），适用于短程无线通信标准。
IEEE 802.16	宽带无线接入（BWA）标准。

（4）802.3 的传输介质

属性	Ethernet	10Base 5	10Base 2	1Base 5	10Base-T	10Broad 36	10Base-F
拓扑结构	总线型	总线型	总线型	星型	星型	总线型	星型
数据速率 Mbps	10			1	10		
信号类型	基带曼码					宽带 DPSK	基带曼码
最大段长 /m	500		185	250	100	3600	500 或 2000
传输介质	粗同轴电缆			UTP		CATV 电缆	光纤

4. IEEE 802.3 传输介质特性

名称	电缆	最大段长	特点
100Base-T4	4 对 3 类 UTP	100m	3 类双绞线，8B/6T，NRZ 编码
100Base-Tx	2 对 5 类 UTP 或 2 对 STP	100m	100Mb/s 全双工通信，MLT-3 编码
100Base-FX	1 对光纤	2000m	100Mb/s 全双工通信，4B/5B、NRZI 编码
1000Base-Cx	2 对 STP	25m	2 对 STP
1000Base-T	4 对 UTP	100m	4 对 UTP
1000Base-Sx	62.5μm 多模	220m	模式带宽 160MHz*km，波长 850nm
		275m	模式带宽 200MHz*km，波长 850nm
	50μm 多模	500m	模式带宽 400MHz*km，波长 850nm
		550m	模式带宽 500MHz*km，波长 850nm
1000Base-LX	62.5μm 多模	50m	模式带宽 500MHz*km，波长 850nm

	50μm 多模		模式带宽 400MHz*km，波长 850nm
			模式带宽 500MHz*km，波长 850nm
	单模	5000m	波长 1310nm 或 1550nm
10Gbase-S	50μm 多模	300m	波长 850nm
	62.5μm 多模	65m	波长 850nm
10Gbase-L	单模	10km	波长 1310nm
10Gbase-E	单模	40km	波长 1550nm
10Gbase-LX4	单模	10km	波长 1310nm 波分多路复用
	50μm 多模	300m	
	62.5μm 多模		

（5）快速以太网 802.3u 100M

属性	传输介质	特性阻抗	传输距离
100Base-Tx	两对 5 类 UTP	100Ω	100m
	两对 STP	150Ω	100m
100Base-Fx	一对多模光纤 MMF	62.5/125um	2km
	一对单模光纤 SMF	8/125um	40km
100Base-T4	四对 3 类 UTP	100Ω	100m
100Base-T2	两对 3 类 UTP		100m

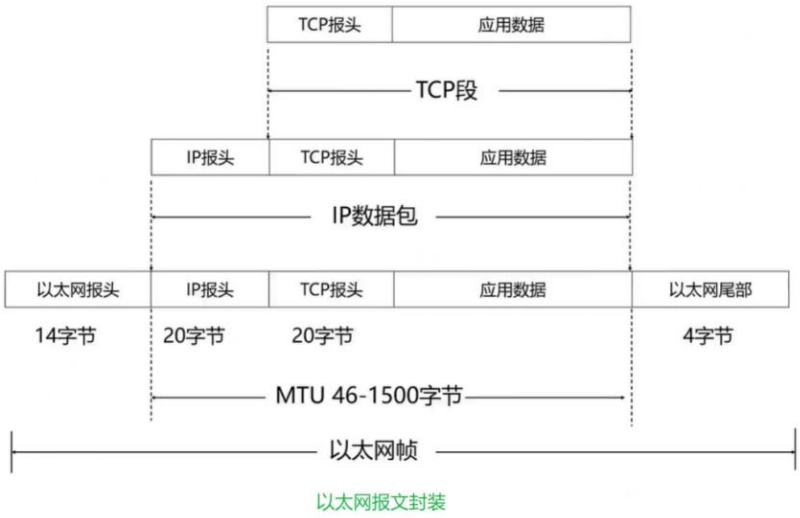
（6）千兆以太网

标准	名称	传输介质	传输距离	特点
IEEE 802.3z	1000Base-CX	两对 STP	25m	屏蔽双绞线，同一房间内设备互联
	1000Base-SX	光纤 （短波 770~860nm）	550m	多模光纤（50，62.5um)
	1000Base-LX	光纤 （长波 1270~1355nm）	5km	单模（10um）或多模光纤（50，62.5um)
IEEE802.3ab	1000Base-T	四对 UTP	100m	5 类非屏蔽双绞线，8B/10B 编码

（7）万兆以太网（802.3ae 10G）

名称	电缆	传输距离	特点
10GBase-S (Short)	50um 多模光纤	300m	850nm 串行
	62.5um 多模光纤	65m	
10GBase-L (Long)	单模光纤	10km	1310nm 串行
10GBase-E (Extended)	单模光纤	40km	1550nm 串行
10GBase-LX4	单模光纤	10km	1310nm 4*2.5Gbps 波分多路复用(WDM)
	50um 多模光纤	300m	
	62.5um 多模光纤		

	802.11	802.11b	802.11a	802.11g	802.11n	802.11ac	802.11ax
标准发布时间	1997	1999		2003	2009	2012	2018
频率范围	2.4GHz	2.4GHz	5.8GHz	2.4GHz	2.4G 5.8G	5.8G	2.4G 5.8G
非重叠信道	3		5	3	3+5	5	8
调制技术	FHSS/DSSS	CCK/DSSS	OFDM	CCK/OFDM	OFDM		
物理发送速率 Mbps	1,2	1,2,5.5,11	6,9,12,18,24,36,48,54		最大可至 600	最大 6900（目前 1300）	9600
实际吞吐	200K	5M	22M	22M	100+M	900M	1G 以上
兼容性	N/A	与 11g 产品可互通	与 11b/g 不能互通	与 11b 产品可互通	向下兼容 802.11a/b/g	向下兼容 802.11a/n	向下兼容 802.11a/n

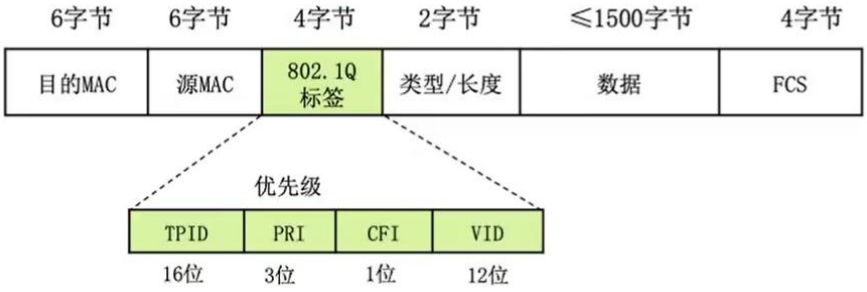


以太网报文封装

7	1	6	6	2	46~1500	4
先导字段	帧开始标志	目的地址	源地址	长度	数据	检验和

IEEE 802.3帧格式

- 前面 7+1 字段用于时钟同步，不算入帧长
- 数据 46-1500 字节，不够至少填充到 46 字节
- 校验位 4 字节，CRC 循环冗余校验 32 位
- 最小帧长 64 字节：6+6+2+46+4=64
- 最大帧长 1518 字节：6+6+2+1500+4=1518



5. 帧中继 RF

- 帧中继在第二层建立虚链路，提供虚链路服务，本地标识 DLCI。
- 基于分组交换的透明传输，可提供面向连接的服务。
- 只做检错和拥塞控制，没有流控和重传机制，开销很少。
- 既可以按需要提供带宽，也可以应对突发的数据传输。　　CIR：承诺速率　　EIR：扩展速率
- 帧长可变，长度可达 1600-4096 字节，可以承载各种局域网的数据帧。
- 可以达到很高的速率，2-45Mbps。
- 不适合对延迟敏感的应用（语音、视频）数据的丢失依赖于运营商对虚电路的配置。
- 不保障可靠的提交。

6. X.25 公共数据网

(1) X.25 分为三个协议层，即物理层、链路层和分组层，分别对应 OSI 模型低三层。
(2) X.25 是一种分组交换技术，面向连接，建立虚链路
(3) X.25 支持差错控制和流量控制，传输速率：64kbps

7. ISDN 和 ATM

- ISDN 综合数字业务网，目的是以数字系统代替模拟电话系统，把音频、视频、数据业务放在一个网上统一传输
- 分为窄带 ISDN 和宽带 ISDN，窄带 ISDN 提供两种用户接口

基本速率 BRI=2B+D=144Kbps

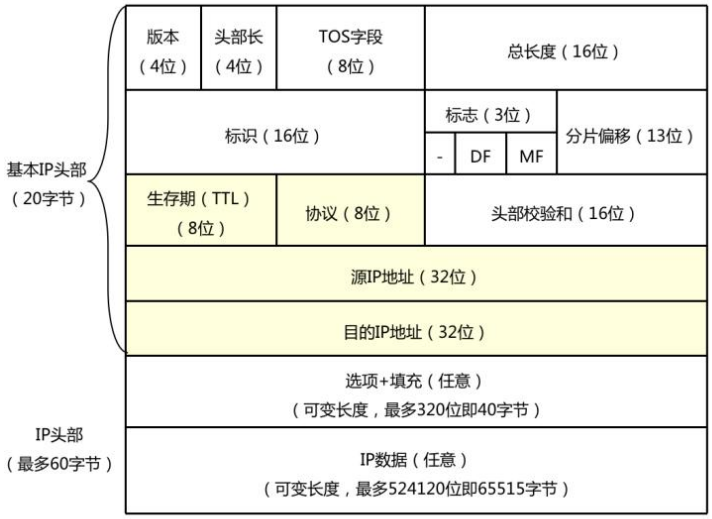
基群速率 PRI=30B+D=2.048M

- 宽带 ISDN，即 ATM，ATM 是信元交换，信元为 53 字节固定长度，ATM 依然是以虚链路提供面向连接的服务 ATM 典型速率为 150M。

4. 网络层

4.1 IP

1. IPv4



IPv4报文格式

（1）头部长度（IHL）：取值 5~15，单位 4 字节。

（2）TOS：为区分服务字段，用区分服务类型，即 QoS 字段。

（3）总长度字段：是 IPv4 数据报的总长度。

（4）标识：标识主机发送的数据报，每次发送+1。

（5）生存期(TTL)：用于设置一个数据包可经过的由器数量的上限。每经过一台路由器便会 -1。

（6）协议字段：包含一个数字，标识数据报有效荷部分的数据类型。最常用的值为 1（ICMP）、6（TCP）和 17（UDP）。

（7）头部校验和：仅计算 IPv4 头部，不检查 IPv4 数据报有效载荷部分的正确性。当 TTL-1 时，头部校验和必须改变。

2. IP 地址分类

A 类地址（大型网络）	0	1.0.0.0~126.255.255.255	子网位 8 位，主机位 24 位
B 类地址（中型网络）	10	128.0.0.0~191.255.255.255	子网位 16 位，主机位 16 位
C 类地址（小型网络）	110	192.0.0.0~223.255.255.255	子网位 24 位，主机位 8 位
D 类地址（组播地址）	1110	224.0.0.0~293.255.255.255	不分网络地址和主机地址
E 类地址（保留地址）	11110	240.0.0.0~247.255.255.255	

地址名称	地址格式	特点	可否作为源地址	可否作为目标地址
有限广播	255.255.255.255 （网络字段和主机字段全 1）	不被路由，会被送到相同物理网络段上的所有主机	否	
直接广播	主机字段全 1，如 192.1.1.255	广播会被路由，并会发送到专门网络上的每台主机	否	是
网络地址	主机位全 0，如 192.168.1.0	表示一个子网	否	否
全 0 地址	0.0.0.0	代表任意主机	是	否
环回地址	127.X.X.X	向自己发送数据	是	是

A 类地址（大型网络）1.0.0.0~126.255.255.255	1. 私有地址：10.x.x.x 2. 保留地址：127.x.x.x
B 类地址（中型网络）128.0.0.0~191.255.255.255	1. 私有地址：172.16.0.0~172.31.255.255 2. 保留地址：169.254.x.x

C 类地址（小型网络）192.0.0.0~223.255.255.255	1. 私有地址：192.168.0.0~192.168.255.255

3. 可变长子网掩码（VLSM）

4. 无类别域间路由（CIDR）

5. 子网范围=[子网地址]～[广播地址]=8.1.64.0～8.1.127.255。

6. 子网能容纳的最大主机数=2 ^{主机位}-2

7. 特殊 IP 地址

(1) 0.0.0.0：计算机的世界里面，没有表示为 0。

(2) 255.255.255.255：受限广播地址，表示 3 层广播的目标地址，在同一个广播域范围内所有主机都会接收这个包，广播域的范围可变，跟子网划分相关。

(3) 169.254.0.0/16：使用 DHCP 自动获取 IP 地址，当 DHCP 服务器发生故障，或响应时间超时，系统会为你分配这样一个地址，不能正常上网。

(4) 127.0.0.0/8 (127.0.0.1-127.255.255.255)：本地环回地址，主要用于测试或网络管理/路由更新，比物理接口稳定。

(5) RFC1918 私有 IP 地址：IPv4 地址空间中有一部分特殊的地址，成为私有 IP 地址，私有 IP 地址不能直接访问公网(Internet)的 IP，只能在本地使用。

A 类：10.0.0.0/8 (10.0.0.1-10.255.255.255)　1 个 A 类地址

B 类：172.16.0.0/12 (172.16.0.1-172.31.255.255)　16 个 B 类地址

C 类：192.168.0.0/16 (192.168.0.1-192.168.255.255)　256 个 C 地址

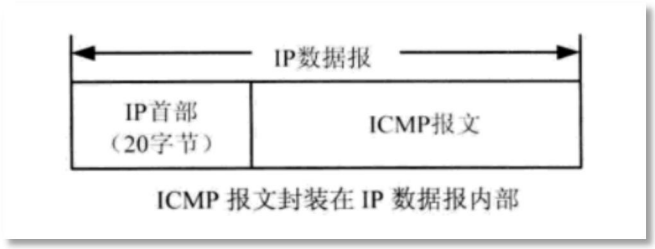
(6) 常见组播地址

224.0.0.1	所有主机	224.0.0.6	DR 和 BDR 的组播接收地址
224.0.0.2	所有路由器	224.0.0.9	RIPv2 组播更新地址
224.0.0.5	所有运行 OSPF 的路由器	224.0.0.18	VRRP 组播地址

4.2 ICMP

1. Internet 控制报文协议（ICMP）：TCP/IP 协议族的一个子协议，是网络层协议，用于 IP 主机和路由器之间传递控制消息。

(1) 控制消息是指网络通不通、主机是否可达、路由是否可用等网络本身的消息。这些控制消息虽然并不传输用户数据，但是对用户数据的传递起着重要的作用。



ICMP 报文封装在 IP 数据报内部

ICMP报文格式

2. ICMP 报文分类

报文种类	类型值	报文类型	报文定义	报文内容
差错报告报文	3	目的不可达	路由器与主机不能交付数据时就向源点发送目的不可达报文	包括网络不可达、主机不可达、协议不可达、端口不可达、需要进行分片却设置了部分片、源路由失败、目的网络未知、目的主机未知、目的网络被禁止、目的主机被禁止、由于服务类型 TOS 网络不可达、由于服务类型 TOS 主机不可达、主机越权、优先权中止生效
	4	源点抑制	由于拥塞而丢弃数据报时就向源点发送抑制报文，降低发送速半	
	5	重定向(改变路由）	路由器将重定向报文发送给主机，优化或改变主机路由	包括网络重定向、主机重定向、对服务类型和网络重定向、对服务类型和主机重定向
	11	时间超时	丢弃 TTL 为 0 的数据，向源点发送时间超时报文	
	12	参数问题	发现数据报首部有不正确字段时丢弃报文，并向源点发送参数问题报文	
询问报文	0	回送应答	收到回送请求报文的主机必须回应源主机回送应答报文	
	8	回送请求		
	13	时间戳请求	请求对方回答当前日期和时间	
	14	时间戳应答	回答当前日期和时间	

3. ICMP 报文应用：Ping 命令(使用回送应答和回送请求报文）、Traceroute 命令(使用时间超时报文和目的不可达报文)。

4.3 ARP 和 RARP

1. 地址解析协议（ARP）：是将 32 位的 IP 地址解析成 48 位的以太网地址。封装在以太网帧中进行发送。

2. 反向地址解析（RARP）：则是将 48 位的以太网地垃解析成 32 位的 IP 地址。

3. ARP 病毒：利用感染主机的方法向网络发送大量虚假的 ARP 报文，主机没有感染 ARP 木马时也有可能导致网络访问不稳定。ARP 病毒还能在局域网内产生大量的广播包，造成广播风暴。

4. ARP 病毒解决方法：
   (1) 接入交换机端口绑定固定的 MAC 地址。
   (2) 查看接入交换机的端口异常(一个端口短时间出现多个 MAC 地址)。

(3) 安装 ARP 防火墙。

(4) 使用 arp-d 命令清除 ARP 缓存。

(5) 使用“arp-s 网关 IP 地址/网关 MAC 地址”命令设置静态绑定。

(6) 安装杀毒软件。

(7) 给各类终端系统打补丁。

(8) 交换机启用 ARP 病毒防治功能等。

4.4 IPv6

1. IPv6

IPv6头部默认40字节

- 版本（4 位）：用 0110 指示 IPv6
- 通信类型（8 位）：用于区分不同的 IP 分组，相当于 IPv4 中服务类型字段（实际不用)
- 流标记（20 位）：标识某些需要特别处理的分组（实际不用)
- 负载长度（16 位）：表示除了 IPv6 固定头部 40 个字节之外的负载长度，扩展头包含在负载长度之中
- 下一头部（8 位）：指明下一个头部类型，可能是 IPv6 扩展头部或高层协议的头部
- 跳数限制（8 位）：用于检测路由循环，类似 TTL
- 源地址(128 位)：发送节点的地址
- 目标地址(128 位)：接收节点的地址

2. IPv6 书写规则

(1) 任何一个 16 位段中起始的 0 不必写出来。只有起始的 0 才能被忽略，末尾的 0 不能忽略。

(2) 任何由全 0 组成的 1 个或多个 16 位段的单个连续字符串都可以用一个双冒号“**::**”来表示。双冒号只能用一次。

3. 单播地址

（1）全球单播地址	001
（2）链路本地单播地址	1111111010（FE80::/10）
（3）地区本地单播地址	1111111011（FE8C::/10）
（4）任意播地址	
（5）组播地址	

地址类型	高位数字（二进制）	高位数字(十六进制)
未指定	00...0	::/128
环回地址	00...1	::1/128
多播地址	1111 1111	FF00::/8
链路本地单播地址	11 1111 1010	FE80::/10
地区本地单播地址（有争议）	11 1111 1011	FEC0::/10
全球单播地址（当前分配的）	001	2xxx::/4 或者 3xxx::/4
剩下作为未来全球单播地址分配		

4. IPv4 过渡 IPv6 技术

（1）隧道技术：解决 IPv6 节点之间通过 IPv4 网络进行通信。（手工隧道、GRE 隧道）

（2）双栈技术：同时运行 IPv4 和 IPv6。

（3）翻译技术：解决纯 IPv6 节点与纯 IPv4 节点之间通进行通信。

（4）NAT-PT 技术（网络地址转换与协议转换）（NAT64 技术）

（5）ISATAP 技术（站内自动隧道寻址协议）

4.5 NAT

1. 网络地址转换（NAT）：将数据报文中的 IP 地址替换成另一个 IP 地址，一般是私有地址转换为公有地址来实现访问公网的目的。

2. 基本 NAT 分为：静态 NAT 和动态 NAT。

3. 网络地址端口转换（NAPT）：允许多个内部地址映射到同一个公有地址上，也可称之为多对一地址转换或地址复用。NAPT 将内部的所有地址映射到一个外部 IP 地址(也可以是少数外部 IP 地址)，这样做的好处是隐藏了内部网络的 IP 配置、节省了资源。

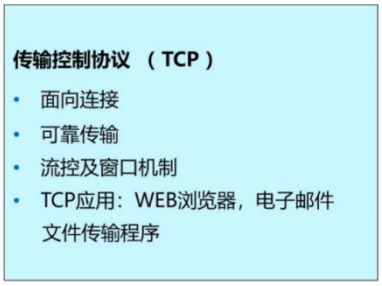
层次	协议封装	协议号	协议名称	备注
网络层	基于 IP 协议	1	ICMP	Internet 控制报文协议
		2	IGMP	Internet 组管理协议
		6	TCP	传输控制协议
		17	UDP	用户数据报协议
		41	IPv6	互联网协议第 6 版
		47	GRE	通用路由封装协议
		50	ESP	封装安全载荷协议
		51	AH	身份验证标头
		89	OSPF	224.0.0.1 - 在本地子网的所有主机 224.0.0.2 - 在本地了网的所有路由器 224.0.0.5 - 运行 OSPF 协议的路由器 224.0.0.6 - OSPF 指定/备用指定路由器 DR/BDR
		112	VRRP	虚拟路由器冗余协议

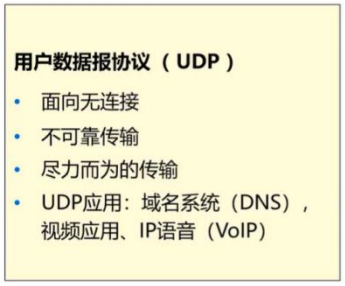
5. 传输层

5.1 TCP

1. 网络服务方式：面向连接服务、无连接服务。
2. TCP（传输控制协议）：是一种可靠的、面向连接的字节流服务。
3. TCP 三种机制

①使用序号对数据报进行标记	这种方式便于 TCP 接收服务在向高层传递数据之前调整失序的数据包。
②TCP 使用确认、校验和定时器系统提供可靠性。	当接收者按照顺序识别出数据报未能到达或发生错误时，接收者将通知发送者； 当接收者在特定时间没有发送确认信息时，那么发送者就会认为发送的数据包并没有到达接收方，这时发送者就会考虑重传数据。
③TCP 使用窗口机制调整数据流量	窗口机制可以减少因接收方缓冲区满而造成丢失数据报文的可能性。

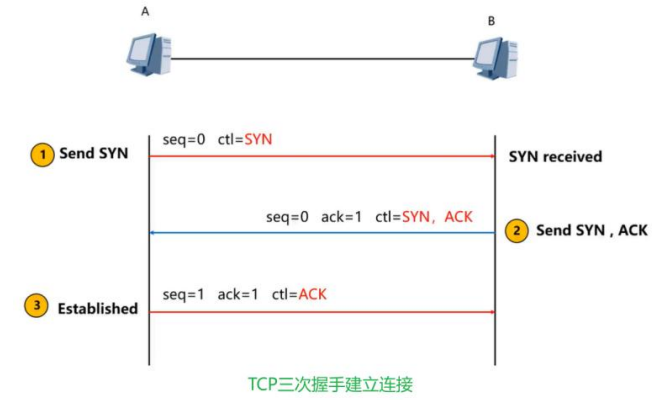




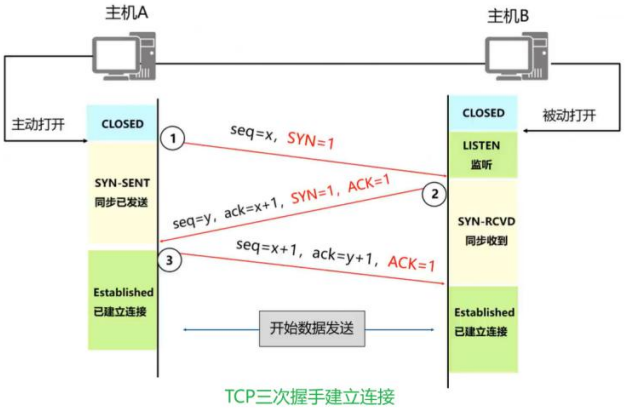
4. TCP 报文首部格式

URG：紧急
ACK：确认
PSH：推送
RST：复位
YSN：同步
FIN：终止

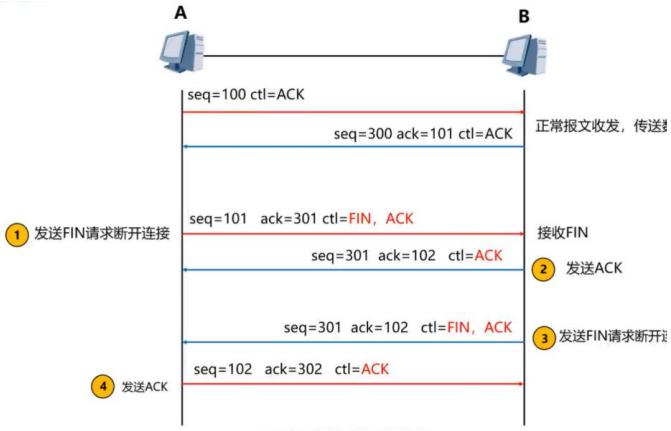
5. TCP 建立连接和释放连接



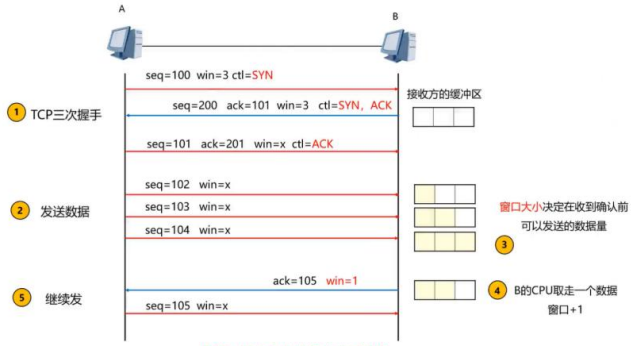
TCP三次握手建立连接



TCP三次握手建立连接



TCP四次挥手断开连接



TCP 可变大小的滑动窗口机制

TCP慢开始和拥塞避免算法的实现

TCP拥塞控制

5.2 UDP

1. UDP（用户数据报协议）：是一种不可靠的、无连接的数据报服务。源主机在传送数据前不需要和目标主机建立连接。UDP 比 TCP 更加高效。

2. 端口种类：系统端口（0~1023）、登记端口（1024~49151）、客户端使用端口（49152~65535）。

143	IMAP	交互式邮件存取协议

层次	协议封装	协议号	协议名称	协议号	备注
传输层	基于 TCP 协议	6	FTP	20	文件传输协议（数据连接端口）
				21	文件传输协议（控制连接端口）
			SSH	22	安全登陆
			Telnet	23	远程登陆
			SMTP	25	电子邮件传输协议
			HTTP	80	www 超文本传输协议
			POP3	110	邮局协议
			BGP	179	边界网关协议
			HTTPS	443	基于 TLS/SSL 的网页浏览端口
			RDP	3389	远程桌面
	基于UDP协议	17	DNS	53	域名服务
			DHCP	67	服务器接收请求的端口
				68	客户机接收回应的端口
			TFTP	69	简单文件传输协议
			SNMP	161	简单网络管理协议（网管向设备轮询）
				162	简单网络管理协议（设备发送陷阱）
			IKE	500	IPSec 中密钥协商协议
			RIP	520	RIPv1 使用广播更新 RIPv2 组播更新地址 224.0.0.9 RIPng 组播更新地址 FF02::9

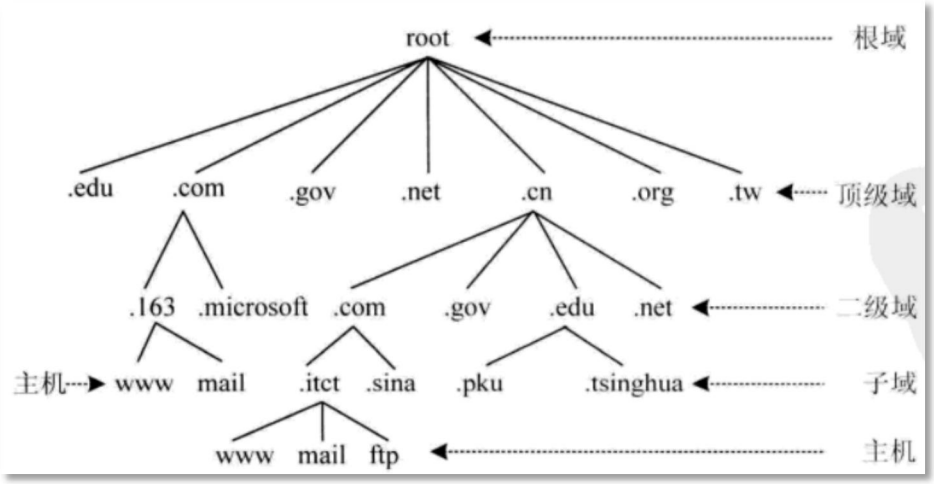
6. 应用层

6.1 DNS

1. DNS(域名系统)：主机名解析为 IP 地址的系统。

   完整表达：主机.…三级域名.二级域名．顶级域名

   注意：域名的每个部分不超过 63 个字符，整个域名不超过 255 个字符。顶级域名后的“.”号表示根域，通常可以不用写。



域名名称	作用	域名名称	作用
.com	商业机构	.org	非盈利组织
.edu	教育机构	.biz	商业
.gov	政府部门	.info	网络信息服务组织
.int	国际组织	.pro	会计、律师和医生
.mil	美国军事部门	.name	个人
.net	网络组织，现可任何人注册	.museum	博物馆
国家代码	国家（如 cn 代表中国）	.coop	商业合作团体
		.acro	航空工业

2. 按域名空间层次划分的服务器

名称	定义	作用
根域名服务器	最高层次域名服务器，该服务器保存了全球所有顶级域名服务器的 IP 地址和域名。全球有 100 多个	本地域名无法解析域名时，直接向根域名服务器请求

顶级域名服务器	管理本级域名（如.cn）上注册的所有二级域名	可以解析本级域名下的二级域名的 IP 地址；提交下一步所寻域名服务器地址
权限域名服务器	一个域可以分为多个区，每一个区都设置服务器，即权限服务器	该区域管理主机的域名和 IP 地址的映射、解析
本地域名服务器	主机发出的 DNS 查询报文最初送到的服务器	查询本地域名和 IP 地址的映射、解析。向上级域名服务器进行域名查询

3. 按作用划分的域名服务器

名称	定义	作用
主域名服务器	维护本区所有域名信息，信息存于磁盘文件和数据库中	提供本区域名解析，区内域名信息的权威。具有域名数据库。一个域有且只有一个主域名服务器。
辅域名服务器	主域名服务器的备份服务器提供域名解析服务，信息存于磁盘文件和数据库中	主域名服务器备份，可进行域名解析的负载均衡。具有域名数据库。
缓存域名服务器	向其他域名服务器进行域名查询，将查询结果保存在缓存中的域名服务器	改善网络中 DNS 服务器的性能，减少反复查询相同域名的时间，提高解析速度，节约出口带宽。获取解析结果耗时最短，没有域名数据库
转发域名服务器	负责非本地和缓存中无法查到的域名。接收域名查询请求，首先查询自身缓存，如果找不到对应的，则转发到指定的域名服务器查询	负责域名转发，由于转发域名服务器同样可以有缓存，因此可以减少流量和查询次数。具有域名数据库。

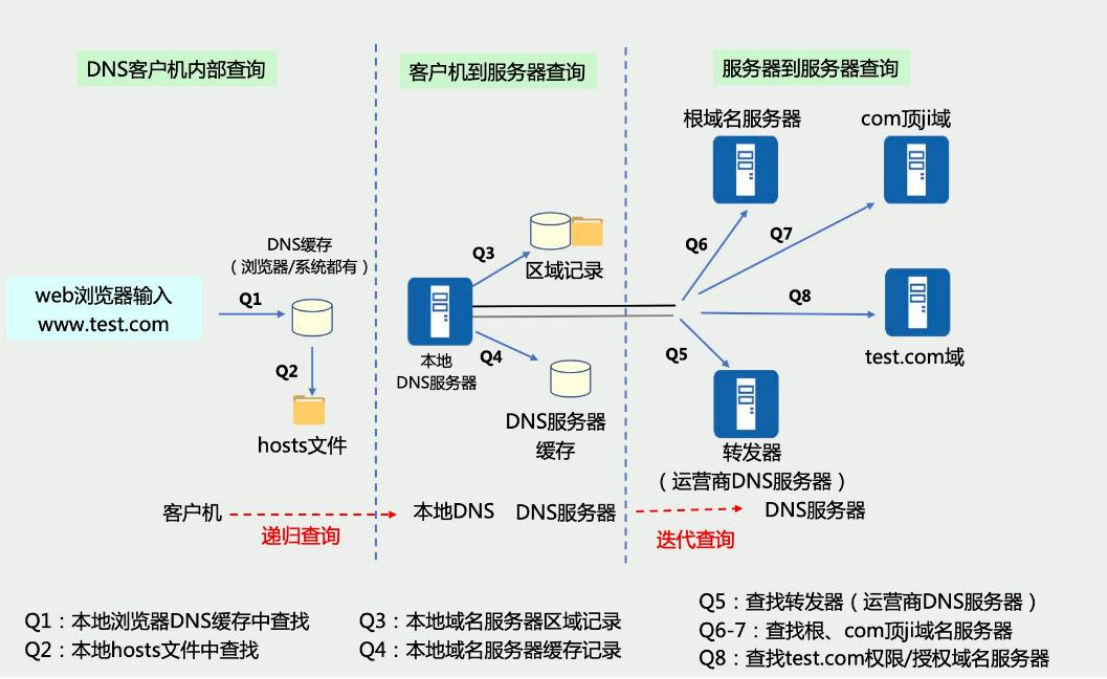
4. 资源记录

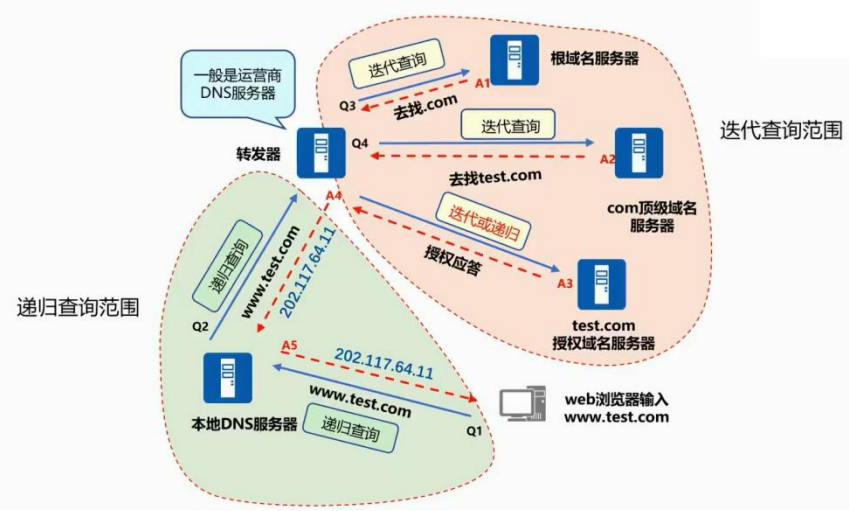
A	将 DNS 域名映射到 IPv4 的 32 位地址中	host1.itct.com.cn.INA202.0.0.10
AAAA	将 DNS 域名映射到 IPv4 的 128 位地址中	ipv6_host2.itct.com.cn.INAAAA 2002:0:1:2:3:4:567:89ab
CNAME	规范名资源记录，允许多个名称对应同一主机	aliasname.itct.com.cn.CNAME truename.itct.com.cn

MX	邮件交换器资源记录，其后的数字首选参数值（0～65535 指明与其他邮件交换服务器有关的邮件交换服务器的优先级。较低的数值被授予较高的优先级	example.itct.com.cn.MX 10 mailserver1.itct.com.cn
NS	域名服务器记录，指明该域名由哪台服务器来解析	example.itct.com.cn.IN NS nameserver1.itct.com.cn.
PTR	指针，用于将一个 IP 地址映射为一个主机名	202.0.0.10.in-addr.arpa.PTR host.itct.com.cn

记录类型	说明	备注
SOA	SOA 叫起始授权机构记录， SOA 记录用于在众多 NS 记录中哪一台是主服务器。	SOA 记录还设置一些数据版本和更新以及过期时间的信息。
A	把主机名解析为 IP 地址	www.test.com →1.1.1.1
指针 PTR	反向查询，把 IP 地址解析为主机名	1.1.1.1 →www.test.com
名字服务器 NS	为一个域指定授权域名服务器， 该域的所有子域也被委派给这个服务器	比如某个区域由 ns1.domain.com 进行解析
邮件服务器 MX	指明区域的邮件服务器及优先级	建立电子邮箱服务，需要 MX 记录将指向邮件服务器地址。
别名 CNAME	指定主机名的别名把主机名解析为另一个主机名	www.test.com 别名为 webserver12.test.com

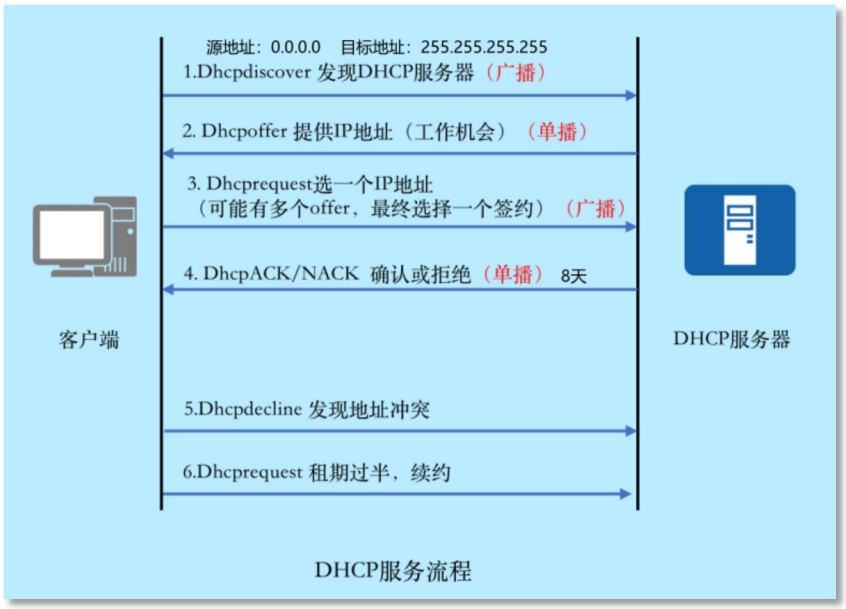
5. 域名解析方法：递归查询、迭代查询。





6.2 DHCP

1.



6.3 WWW 和 HTTP

1.WWW：万维网（WWW），是一个规模巨大、可以互联的资料空间。WWW 的核心由三个主要标准构成：URL、HTTP（超文本传送协议）、HTML（超文本标记语言）。

- URL：<协议>:/<主机>:<端口>/<路径>
- 常见 HTTP 请求报文

方法	意义	方法	意义
GET	请求读取 URL 标识的信息	DELETE	删除 URL 所指定的资源
HEAD	请求读取 URL 标识的信息的首部	OPTION	请求一些参数信息
POST	把消息（如注释）加载到指定网页上，没有 Read 方法	TRACE	进行环回测试

PUT	指明 URL 创建或修改资源，俗称的上传资源	CONNECT	用于代理服务器

6.4 Email

1. 电邮地址格式：用户名@域名
2. 常见的电子邮件协议：简单邮件传输协议（SMTP）、邮局协议（POP）、Internet 邮件访问协议（IMAP）。
3. PGP：邮件加密软件，PGP 采用了 RSA 和传统加密的杂合算法、数字签名的邮件文摘算法和加密前压缩等手段，功能强大、加解密快且开源。

6.5 FTP

1. FTP（文件传输协议）：TCP 协议，20 端口为数据连接，21 端口控制连接。
2. FTP 工作方式：主动式（PORT）、被动式（PASV）。【相对于服务器是否首先发起数据连接】

6.6 SNMP

1. OSI 网络管理：性能管理、配置管理、故障管理、安全管理、计费管理。
2. 公共管理信息服务/协议（CMIS/CMIP）：是 OSI 提供的网络管理协议簇。CMIS 定义了每个网络组成部件提供的网络管理服务，CMIP 则是实现 CIMS 服务的协议。
3. 代理与监视器两种通信方式：轮询和事件报告。
4. 网络管理系统组成：管理站、代理、管理信息库、网络管理协议。

管理站	是位于网络系统主干或者靠近主干的工作站，是网络管理系统的核心，负责管理代理和管理信息库，定期查询代理信息，确定独立的网络设备和网络状态是否正常。
代理	又称为管理代理，位于被管理设备内部。负责收集被管理设备的各种信息和响应管理站的命令或请求，并将其传输到 MIB 数据库中。 代理所在地设备可以是网管交换机、服务器、网桥、路由器、网关及任何合法节点的计算机。
管理信息库 MIB	相当于一个虚拟数据库，提供有关被管理网络各类系统和设备的信息，属于分布式数据库。
网络管理协议	用于管理站和代理之间传递、交互信息。常见的网管协议有 SNMP 和 CMIS/CMIP。 网管站通过 SNMP 向被管设备的网络管理代理发出各种请求报文，代理则接收这些请求后完成相应的操作，可以把自身信息主动通知给网管站。

5. SNMP（简单网络管理协议）：是在应用层上进行网络设备间通信的管理协议，可以进行网络状态监视、网络参数设定、网络流量统计与分析、发现网络故障等。

SNMP 基于 UDP 协议，是一组标准，由 SNMP 协议、管理信息库(MIB)和管理信息结构(SMI)组成。

（1）SNMP PUD：SNMP 规定了 5 个重要的协议数据单元 PDU，也称为 SNMP 报文。SNMP 报文可以分为从管理站到代理的 SNMP 报文和从代理到管理站的 SNMP 报文（SNMP 报文建议不超过 484 个字节）。

（2）SNMP 协议实体发送请求和应答报文的默认端口号是 161，SNMP 代理发送陷阱报文（Trap）的默认端口号是 162。

操作编号	分类	名称	用途
0	网管找客户端（领导找下属）	get-request	查询一个或多个变量的值
1		get-next-request	在 MIB 树上检索下一个变量
2		set-request	多一个或多个变量的值进行设置
3	客户端反馈（下属向领导汇报）	get-response	对 get/set 报文做出相应
4		Trap（162）	向管理进程报告代理发生的事件

从管理站到代理的 SNMP 报文		从代理到管理站的 SNMP 报文
从一个数据项取数据	把值存储到一个数据项	
Get-Request（从代理进程处提取一个或多个数据项）	Set-Request（设置代理进程的一个或多个数据项）	Get-Response（这个操作是代理进程作为对 Get-Request、Get-Next-Request、Set-Request 的响应）
Get-Next-Request（从代理进程处提取一个或多个数据项的下一个数据项）		Trap（代理进程主动发出的报文，通知管理进程有某些事件发生）

版本	特点
SNMPv1	易于实现、使用团体名认证（属于同一团体的管理站和被管理站才能互相作用）
SNMPv2	可以实现分布和集中两种方式的管理；增加管理站之间的信息交换；改进管理信息机构（可以一次性取大量数据)；增加多协议支持；引入了信息模块的概念（模块有 MIB 模块、MIB 的依从性声明模块、代理能力说明模块）
SNMPv3	模块化设计，提供安全的支持，基于用户的安全模型

版本	问题
SNMPv1	• SNMP 网络管理中，管理站和代理站之间可以是一对多关系，也可以是多对一关系 RFC1157 规定 • SNMP 基本认知和控制机制，通过团体名验证实现 • 团体名 Community 明文传输，不安全
SNMPv2	• SNMPv2 增加定义了 GetBulk 和 inform 两个新协议操作

	• GetBulk：快速获取大块数据 • Inform：允许一个 NMS 向另一个 NMS 发送 Trap 信息/接收响应消息
SNMPv3	• SNMPv3 重新定义了网络管理框架和安全机制。 • 重新定义网络管理框架：将前两版中的管理站和代理统一叫做 SNMP 实体(entity) • 安全机制：认证和加密传输 　• 时间序列模块，提供重放攻击防护 　• 认证模块：完整性和数据源认证，使用 SHA 或 MD5 　• 加密模块：防止内容泄露，使用 DES 算法

（3） SNMPv3 安全分类：主要安全威胁、次要安全威胁。

主要安全威胁	有两种:修改信息、假冒。 • 修改信息是指擅自修改 SNMP 报文，篡改管理操作伪造管理对象。 • 假冒就是冒充用户标识。
次要安全威胁	有两种:修改报文流、消息泄露。 • 修改报文流可能出现乱序、延长、重放的威胁。 • 消息泄露则可能造成 SNMP 之间的信息被窃听。
两种服务不被保护或者无法保护	拒绝服务、通信分析。

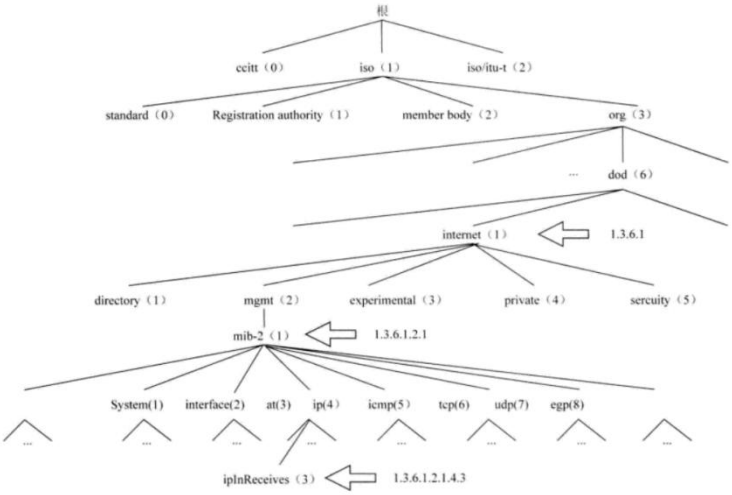
（4） SNMP 轮询监控：支持的设备数 $X=\frac{\text{轮询周期 N}}{\text{单个设备轮询时间 T}}$

6. 管理信息库（MIB）：MIB 指定主机和路由器等被管设备需要保存的数据项和可以对这些数据项进行的操作。

类别（标号)	描述	类别（标号)	描述
system (1)	主机、路由器操作系统	icmp (5)	ICMP 信息
interface (2)	网络接口信息	tcp(6)	TCP 信息
Address translation(3)	地址转换（已经废弃多年）	udp (7)	UDP 信息
ip (4)	IP 信息	egp (8)	EGP 信息

7. 管理信息结构（SMI）：SMI 定义了命名管理对象和定义对象类型（包括范围和长度）的通用规则，以及把对象和对象的值进行编码的规则。

SMI 的功能：命名被管理对象、存储被管对象的数据类型、编码管理数据。



6.7 RMON（远程监控协议）

1.RMON：用于监视网络通信情况的设备叫网络监视器（Monitor）或网络分析器(Analyzer)、探测器（Probe）等。【监测流量 vs 监测设备】

• RMON 定义了管理信息库 RMON　MIB-II（流量信息），与 SNMP MIB（设备信息）RMON 目标：监视子网范围内通信，从而减少管理站和被管理系统之间的通信负载。

RMON（MIB-II子树)

- **statistics(1)：以太子网的统计信息**
- **history(2)：子网的周期性统计信息**
- **alarm(3)：用于定义取样间隔和报警门限**
- **host(4)：关于一个主机的通信统计数据**
- **hostTopN(5)；某种参数最大的N台主机的统计数据**
- **matrix(6);一对地址之间的通信统计数据**
- **filter(7)：对分组进行过滤的信息**
- **capture(8)：捕获特殊分组的信息**
- **event(9)：定义网络事件的信息**
- **tokenRing(10)：关于令牌环网的配置和统计信息**

6.8 其他协议

1. Telnet：TCP/IP 终端仿真协议（Telnet）是一种基于 TCP 的虚拟终端通讯协议，端口号为 23。Telnet 采用客户端/服务器的工作方式，采用网络虚拟终端（NVT）实现客户端和服务器的数据传输，可以实现远程登录、远程管理交换机和路由器。

2. 代理服务器（Proxy Server）：处于客户端和需要访问网络之间，客户向网络发送信息和接收信息均通过代理服务器转发而实现。

• 代理服务器的优点有：共享 IP 地址、缓存功能提高访问速度信息转发、过滤和禁止某些通信，提升上网效率、隐藏内部网络细节以提高安全性、监控用户行为避免来自 Internet 上病毒的入侵、提高访问某些网站的速度、突破对某些网站的访问限制。

3. 安全外壳协议（SSH）：是目前较可靠、专为远程登录会话和其他网络服务提供安全性的协议。

4. VoIP：就是将模拟声音信号数字化，通过数据报在 IP 数据网络上做实时传递。

•VoIP 最大的优势是能广泛地采用 Internet 和全球 IP 互连的环境，提供比传统业务更多、更好的服务。

7. 网络安全

7.1 安全设计、原则与审计

1. 网络安全设计基本原则

（1）充分、全面、完整地对系统的安全漏洞和安全威胁等各类因素进行分析、评估和检测是设计网络安全系统的必要前提条件。

（2）强调安全防护、监测和应急恢复。要求在网络发生被攻击的情况下，必须尽快恢复网络信息中心的服务，减少损失。

（3）网络安全的“木桶原则”强调对信息均衡、全面地进行保护。木桶的最大容积取决于最短的一块木板，因此系统安全性取决于最薄弱模块的安全性。

（4）良好的等级划分是实现网络安全的保障。

（5）网络安全应以不影响系统的正常运行和合法用户的操作活动为前提。

（6）考虑安全问题应考虑安全与保密系统的设计要与网络设计相结合，同时要兼顾性能价格的平衡。

网络安全设计原则还有易操作性原则、动态发展原则、技术与管理相结合原则。

2. 网络安全体系设计

分类	层次	手段
物理环境安全	物理层安全	线路安全（备份、管理)、设备安全（备份、备件、抗干扰)、机房安全（温度、湿度、电源、烟监控、除尘设施、防盗、防雷）
操作系统安全	系统层安全	网络操作系统自身安全（系统漏洞补丁、访问控制、身份认证)、系统安全正确配置、防范病毒、防范木马、数据库容灾
网络安全	网络层安全	基于网络层的资源访问控制、基于网络层的身份验证、路由安全性
应用安全	应用层安全	各类应用软件和数据的安全（如数据库容灾）
管理安全	网络管理层安全	建立安全管理制度、加强人员管理

3. 安全审计

（1)控制目标	企业根据具体的计算机应用、结合单位实际制定出的安全控制要求。
（2)安全漏洞	系统的安全薄弱环节，容易被干扰或破坏的地方。
（3)控制措施	企业为实现其安全控制目标所制定的安全控制技术、配置方法及各种规范制度。
（4)控制测试	将企业的各种安全控制措施与预定的安全标准进行一致性比较，确定各项控制措施是否存在、是否得到执行、对漏洞的防范是否有效，评价企业安全措施的可依赖程度。

4. 信息安全五要素

（1）机密性	保证信息不泄露给未经授权的进程或实体，只供授权者使用。

（2）完整性	信息只能被得到允许的人修改，并且能够被判别该信息是否已被篡改过。同时一个系统也应该按其原来规定的功能运行，不被非授权者操纵。
（3）可用性	只有授权者才可以在需要时访问该数据，而非授权者应被拒绝访问数据。
（4）可控性	可控制数据流向和行为。
（5）可审查性	出现问题有据可循。
另外，有人将五要素进行了扩展，增加了可鉴别性和不可抵赖性。	
可鉴别性	网络应对用户、进程、系统和信息等实体进行身份鉴别。
不可抵赖性	数据的发送方与接收方都无法对数据传输的事实进行抵赖。

7.2 可靠性

1. 系统可靠性概念

平均无故障时间（MTTF）	MTTF 指系统无故障运行的平均时间,取所有从系统开始正常运行到发生故障之间的时间段的平均值。
平均修复时间（MTTR）	MTTR 指系统从发生故障到维修结束之间的时间段的平均值
平均失效间隔（MTBF）	MTBF 指系统两次故障发生时间之间的时间段的平均值。
关系	平均失效间隔：MTBF=∑(T2+T3+T1)/N 平均无故障时间：MTTF=∑T1/N 平均修复时间：MTTR=∑(T2+T3)/N 三者之间的关系：MTBF=MTTF+MTTR
失效率	单位时间内失效元件和元件总数的比率，用 λ 表示。 MTBF=1/λ

2. 系统可靠性

串联系统	由 n 个子系统串联而成，一个子系统失效，则整个系统失效。
并联系统	由 n 个子系统并联而成，n 个系统互为冗余，只要有一个系统正常，则整个系统正常。
模冗余系统	由 n 个系统和一个表决器组成，通常表决器是视为永远不会坏的，超过 n+1 个系统多数相同结果的输出作为系统输出。

7.3 网络安全威胁

1. 安全攻击类型

类型	定义	攻击的安全要素
中断	攻击计算机或网络系统，使得其资源变得不可用或不能用	可用性
窃取	访问未授权的资源	机密性
篡改	截获并修改资源内容	完整性
伪造	伪造信息	真实性

计算机病毒	是一段附着在其他程序上的、可以自我繁殖的、有一定的破坏能力的程序代码。复制后的程序仍然具有感染和破坏的功能。
蠕虫	是一段可以借助程序自行传播的程序或代码。
木马	是利用计算机程序漏洞侵入后窃取信息的程序，这个程序往往伪装成善意的、无危害的程序。
僵尸网络（Botnet)	是指采用一种或多种传播手段使大量主机感染 bot 程序（僵尸程序)，从而在控制者和被感染主机之间所形成的一个可以一对多控制的网络。
拒绝服务(DOS)	利用大量合法的请求占用大量网络资源，以达到瘫痪网络的目的。
分布式拒绝服务攻击（DDOS)	很多 DOS 攻击源一起攻击某台服务器就形成了 DDOS 攻击。 常见防范 DOS 和 DDOS 的方式有根据 IP 地址对数据包进行过滤、为系统访问提供更高级别的身份认证、使用工具软件检测不正常的高流量，由于这种攻击并不在被攻击端植入病毒，因此安装防病毒软件无效。
垃圾邮件	未经用户许可就强行发送到用户邮箱中的任何电子邮件。

前缀	含义	解释	例子
Boot	引导区病毒	通过感染磁盘引导扇区进行传播的病毒	Boot.WYx
DosCom	DOS 病毒	只通过 DOS 操作系统进行复制和传播的病毒	DosCom.Virus.Dir2.2048 (DirII 病毒）
Worm	蠕虫病毒	通过网络或漏洞进行自主传播，向外发送带毒邮件或通过即时通讯工具（QQ、MSN）发送带毒文件	Worm.Sasser（震荡波）
Trojan	木马	木马通常伪装成有用的程序诱骗用户主动激活，或利用系统漏洞侵入用户电脑。计	Trojan.Win32.PGPCoder.a（文件加密机)、Trojan.QQPsw

		算机感染特洛伊木马后的典型现象是有未知程序试图建立网络连接	
Backdoor	后门	通过网络或者系统漏洞入侵电脑并隐藏起来，方便黑客远程控制	Backdoor.Huigezi.ik(灰鸽子变种 IK)、Backdoor.IRCBot
Win32、PE、Win95、W32、w95	文件型病毒或系统病毒	感染可执行文件（如.exe、.com)、.dll 文件的病毒。若与其他前缀连用，则表示病毒的运行 平台	Win32.CIH Backdoor.Win32.PcClient.al，表示运行在 32 位.Windows 平台上的后门
Macro	宏病毒	宏语言编写，感染办公软件（如 Word、Excel)，并且能通过宏自我复制的程序	Macro.Melissa、Macro.Word、Macro.Word.Apr30
Script	脚本病毒	使用脚本语言编写，通过网页传播、感染、破坏或调用特殊指令下载并运行病毒、木马文件	Script.RedLof（红色结束符)、Vbs.valentin(情人节)
Harm	恶意程序	直接对被攻击主机进行破坏	Harm.Delfile（删除文件)、Harm.formatC.f（格式化 C 盘）
Joke	恶作剧程序	不会对计算机和文件产生破坏，但可能会给用户带来恐慌和麻烦，如做控制鼠标	Joke.CrayMourse（疯狂鼠标）
Hack	黑客病毒	通过网络或漏洞进入系统并隐藏起来，木马负责入侵用户计算机，黑客通过木马进行远程控制。	游戏木马 Trojan.Lmir.PSW60
Binder	捆绑机病毒	将特定程序捆绑下载	下载大礼包或某些软件捆绑病毒

- SQL 注入攻击：select，create user
- 跨站脚本攻击 XSS：script
- 木马：c&c、trojan/troy
- 一句话木马(用于攻击网页)：

  php 的一句话木马：<?php @eval($_POST['pass']);?>.

  asp 的一句话是：<%eval request ("pass")%>

  aspx 的一句话是：<%@Page Language="Jscript"%><%eval(Request.Item["pass"],"unsafe");%

2. 病毒四个阶段：潜伏阶段（震网病毒）、繁殖阶段（勒索病毒）、触发阶段（震网病毒）、执行阶段。

7.4 加密算法与信息摘要

1. 常见对称加密算法

共享密钥加密算法/对称加密算法：加密和解密密钥也一样

公钥加密算法/非对称加密算法：加密和解密密钥不一样

算法	解释	特点
DES	Data Encryption Standard，数据加密标准，分组加密算法 采用移位+替换，速度快，密钥易产生。	分组长度 64 位，密钥长度 64 位，有效密钥长度是 56 位
3DES	三重 DES (TDEA)，使用 DES 对明文进行“加密-解密-加密”操作。 • 加密：K1 加密→K2 解密→K3 加密 • 解密：K3 解密→K2 加密→K1 解密 一般，K1 和 K3 是相同的密钥。	密钥长度 112 位
IDEA	International Data Encryption Algorithm，国际数据加密算法，分组加密算法。设计思想:混合使用来自不同代数群中的运算。	明文和密文分组都是 64 位，密钥长度为 128 位，用于 PGP
AES	Advanced Encryption Standard，高级加密标准。 可以通过硬件实现，速度快，像 3DES 一样安全。	分组长度 128 位，支持 128，192 和 256 位三种密钥长度
RC4/5	流加密算法，用于 WIFI，用于 SSL 协议。加密速度快，可达到 DES 的 10 倍。	分组和密钥长度都可变

2. 非对称加密：RSA、ECC（椭圆曲线加密算法）、DH 算法、DSA 算法。
3. 信息完整性验证算法

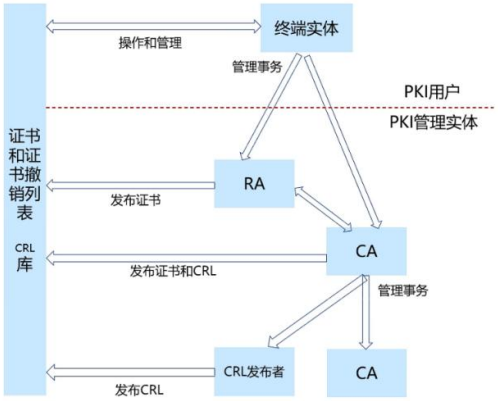
MD5	对任意长度报文进行运算，先把报文按 512 位分组，最后得到 128 位报文摘要。
SHA-1	也是对 512 位长的数据块进行复杂运行，最终产生 160 位散列值， 比 MD5 更安全，计算比 MD5 慢。

7.5 数字签名与数字证书

1. 数字签名：是用于确认发送者身份和消息完整性的一个加密消息摘要，具有如下特点：
   - 使用用户私钥进行签名
   - 接收者能够核实发送者
   - 发送者事后不能抵赖对报文的签名接收者不能伪造对报文的签名
2. 数字证书：包含用户的公钥及 CA 私钥的签名。X.509 格式（国际电信联盟（ITU-T）制定）

7.6 密钥分配

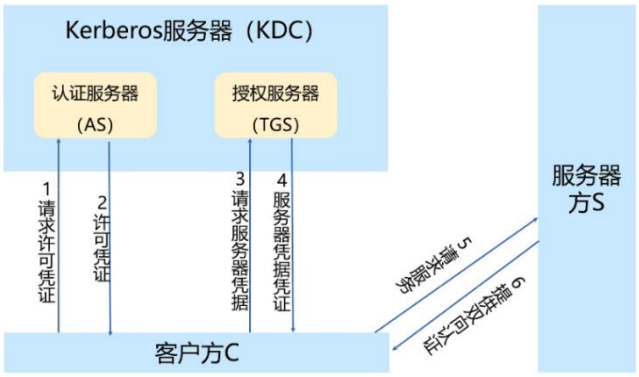
1. 公钥分配



PKI体系结构

用户/终端实体	指将要向认证中心申请数字证书的客户，可以是个人，也可以是集团或团体、某政府机构等。
注册机构 RA	注册机构提供用户和 CA 之间的一个接口，它获取并认证用户的身份，向 CA 提出证书请求。它主要完成收集用户信息和确认用户身份的功能。注册机构并不给用户签发证书，而只是对用户进行资格审查。较小的机构，可以由 CA 兼任 RA 的工作。
证书颁发机构 CA	负责给用户颁发证书。
证书发布系统	负责证书发放，如可以通过用户自己或是通过目录服务。
CRL 库	证书吊销列表，存放过期或者无效证书。

2. 对称密钥分配



Kerberos体系结构

验证服务器 AS	AS 就是一个密钥分配中心(KDC)。同时负责用户的 AS 注册、分配账号和密码，负责确认用户并发布用户和 TGS 之间的会话密钥。
票据授予服务器 TGS	TGS 是发行服务器方的票据，提供用户和服务器之间的会话密钥。Kerberos 把用户验证和票据发行分开了。虽然 AS 只用对用户本身的 ID 验证一次，但为了获得不同的真实服务器票据，用户需要多次联系 TGS.

3. SET 协议：安全电子交易(Secure Electronic Transaction，SET)。它采用公钥密码体制和 X.509 数字证书标准，主要用于保障网上购物信息的安全性。

7.7 SSL、HTTPS

1. SSL：安全套接层（SSL）协议，是一个安全传输、保证数据完整的安全协议，之后的传输层安全（TTLS）是 SSL 的非专有版本。SSL 处于应用层和传输层之间。SSL 主要包括 SSL 记录协议、SSL 握手协议、SSL 告警协议、SSL 修改密文协议等。

<table>
<tr><td>SSL 握手协议</td><td>SSL 修改密文协议</td><td>SSL 告警协议</td><td>HTTP</td></tr>
<tr><td colspan="4">SSL 记录协议</td></tr>
<tr><td colspan="4">TCP</td></tr>
<tr><td colspan="4">IP</td></tr>
</table>

2. HTTPS：安全超文本传输协议（HTTPS)，是 HTTP 的安全版。使用 SSL 来对信息内容进行加密，使用 TCP 的 443 端口发送和接收报文。其使用语法与 HTTP 类似，使用“HTTPS://+ URL”形式。

3. S-HTTP：安全超文本传输协议(S-HTTP)，是一种面向安全信息通信的协议，是 EIT 公司结合 HTTP 而设计的一种消息安全通信协议。S-HTTP 可提供通信保密、身份识别、可信赖的信息传输服务及数字签名等。

	SSL	S-HTTP
工作层次	传输层和应用层之间	应用层
处理对象	数据流	应用数据
基于消息的抗抵赖性证明	不可以	可以
加密算法	RC4	可以协商加密算法（如 RSA、DSA、DES)

7.8 Radius

1. 远程用户拨号认证系统（RADIUS）：是目前最广泛的授权、计费和认证协议。

7.9 VPN

1. VPN 技术：虚拟专用网络（VPN）是在公用网络上建立专用网络的技术。由于整个 VPN 网络中的任意两个节点之间的连接并没有传统专网所需的端到端的物理链路，而是架构在公用网络服务商所提供的网络平台，所以称之为虚拟网。

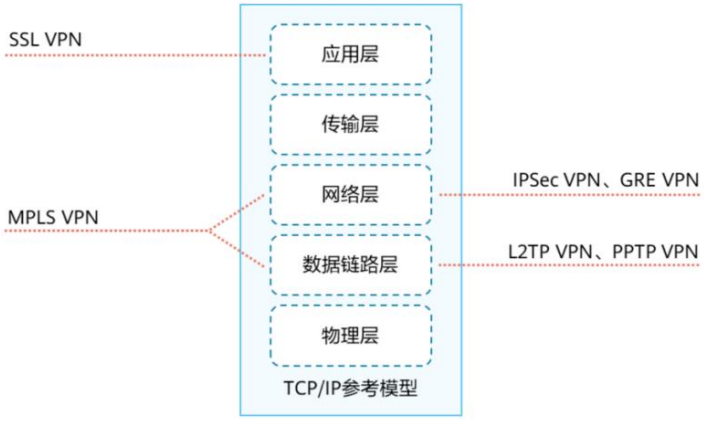
实现 VPN 的关键技术主要有隧道技术、加/解密技术、密钥管理技术和身份认证技术。

2. VPN 隧道技术：实现 VPN 的最关键部分是在公网上建立虚信道，而建立虚信道是利用隧道技术实现的，IP 隧道的建立可以在链路层和网络层。

VPN 主要隧道协议有 PPTP、L2TP、IPsec、SSL VPN、TLS VPN。

点到点隧道技术 PPTP	第 2 层隧道协议。是一种用于让远程用户拨号连接到本地的 ISP,是通过因特网安全访问内网资源的技术。它能将 PPP 帧封装成 IP 数据包，以便能够在基于 IP 的互联网上进行传输。PPTP 使用 TCP 连接创建、维护、终止隧道，并使用 GRE（通用路由封装）将 PPP 帧封装成隧道数据。被封装后的 PPP 帧的有效载荷可以被加密、压缩或同时被加

	密与压缩。
L2TP 协议	第 2 层隧道协议。思科研发。是 PPTP 与 L2F（第二层转发）的一种综合。
IPSec 协议	第 3 层隧道协议。在隧道外面再封装，保证了隧道在传输过程中的安全。
SSL VPN TLS VPN	第 4 层隧道协议。两类 VPN 使用了 SSL 和 TLS 技术，在传输层实现 VPN 的技术。由于 SSL 需要对传输数据加密，因此 SSL VPN 的速度比 IPSec VPN 慢。SSL VPN 配置简单。



3. IPSec：Internet 协议安全性（IPSec）是通过对 IP 协议的分组进行加密和认证来保护 IP 协议的网络传输协议族（一些相互关联的协议的集合)。IPSec 工作在 TCP/IP 协议栈的网络层，为 TCP/IP 通信提供访问控制机密性、数据源验证、抗重放、数据完整性等多种安全服务。

IPSec 协议	功能	代表协议
认证头 AH	数据完整性和源认证	MD5、SHA
封装安全负荷 ESP	数据加密	DES、3DES、AES
Internet 密钥交换协议 IKE	密钥生成和分发	DH

IPSec 应用场景：点到点、端到端、端到点。

IPSec 工作模式：传输模式、隧道模式。

4. MPLS：多协议标记交换（MPLS），2.5 层协议，是核心路由器利用含有边缘路由器在 IP 分组内提供的前向信息的标签（Label）或标记（Tag）实现网络层交换的一种交换方式。MPLS 技术主要是为了提高路由器转发速率而提出的，其核心思想是利用标签交换取代复杂的路由运算和路由交换。该技术实现的核心就是把 IP 数据报封装在 MPLS 数据包中。MPLS 将 IP 地址映射为简单、固定长度的标签，这和 IP 中的包转发、包交换不同。

MPLS 流程	当分组进入 MPLS 网络时，由边缘路由器（LER）划分为不同的转发等价类(FEC)并打上不同标记，该标记定长且包含了目标地址、源地址、传输层端口号、服务质量、带宽、延长等信息。分类建立，分组被转发到标记交换通路（LSP)中，由标签交换路由器（LSR）

	根据标记作转发。在出口 LER 上去除标记，使用 P 路由机制将分组向目的地转发。
MPLS VPN	MPLS VPN 承载平台由 P 路由器、PE 路由器和 CE 路由器组成。 • P 路由器是核心网路由器，在运营商网络中，只负责依据 MPLS 标签完成数据包的高速转发，只维护到 PE 路由器的路由信息,而不维护 VPN 相关的路由信息。P 路由器是不连接任何 CE 路由器的骨干网路由设备，相当于标签交换路由器（LSR)。 • PE 路由器是边缘路由器，负责待传送数据包的 MPLS 标签的生成和去除，还负责发起根据路由建立交换标签的动作，相当于标签边缘路由器（LER)。PE 路由器连接 CE 路由器和 P 路由器，是最重要的网络节点。用户的流量通过 PE 路由器流入用户网络，或者通过 PE 路由器流到 MPLS 骨干网。 • CE 路由器是用户边缘设备，是直接与电信运营商相连的用户端路由器，该设备上不存在任何带有标签的数据包。CE 路由器通过连接一个或多个 PE 路由器为用户提供服务接入。CE 路由器通常是一台 P 路由器，它与连接的 PE 路由器建立邻接关系。

7.10 网络隔离与入侵检测

1. 网络隔离

第一代隔离技术	完全的隔离
第二代隔离技术	硬件卡隔离
第三代隔离技术	数据传播隔离
第四代隔离技术	空气开关隔离
第五隔离技术	安全通道隔离

2. 网络隔离技术：防火墙、多重安全网关（统一威胁管理 UTM）、VLAN 划分、人工策略。

(1) UMT 的功能有：ACL、防入侵、防病毒、内容过滤、流量整形、防 DOS。

3. 入侵检测：包括两个步骤：信息收集和数据分析。可以旁路部署在 DMZ 中。入侵检测就是收集这些数据并分析数据找到痕迹。

（1）入侵检测系统(IDS)分类

- 按信息来源分：HIDS、NIDS、DIDS（主机/网络/分布式)
- 按响应方式分：实时检测和非实时检测
- 按数据分析技术和处理方式分；异常检测、误用检测和混合检测
  - 异常检测：建立并不断更新和维护系统正常行为的轮廓，定义报警阈值，超过阈值则报警能够检测从未出现的攻击，但误报率高。
  - 误用检测：对已知的入侵行为特征进行提取，形成入侵模式库，匹配则进行报警已知入检测准确率高，对于未知入侵检测准确率低，高度依赖特征库专家系统和模式匹配。

（2）入侵检测信息来源

① 操作系统审计记录/操作系统日志

② 网络数据：核心交换机镜像，服务器接入交换机镜像

（3）分析方法：1.模式匹配；2.统计分析；3.数据完整性分析。

（4）检测方法：1.模式匹配法；2.专家系统法；3.基于状态转移分析的检测法。

4. 入侵防御系统（IPS）：是一种抢先的网络安全检测和防御系统，能检测出攻击并积极响应。
   - IPS 不仅具有入侵检测系统检测攻击行为的能力，而且具有拦截攻击并阻断攻击的功能。
   - IPS 不是 IDS 和防火墙功能的简单组合，IPS 在攻击响应上采取的是主动的全面深层次的防御。
   - IPS 能检测入侵，并能主动防御，IDS 只能检测记录日志，发出警报

国产加密算法

算法名称	算法特征描述
SM1	对称加密，分组长度和密钥长度都为 128 比特
SM2	非对称加密，用于公钥加密算法、密钥交换协议、数字签名算法（椭圆曲线问题）
SM3	杂凑算法（哈希），分组 512 位，输出杂凑值长度为 256 位
SM4	对称加密，分组长度和密钥长度都为 128 比特
SM9	标识密码算法，支持公钥加密、密钥交换、数字签名等安全功能

等级保护

【等保一级】“自主保护级”，信息系统受到破坏后，会对公民、法人和其他组织权益造成损害，但不损害国家安全、社会秩序和公共利益。

【等保二级】“审计安全保护级”，信息系统受到破坏后，会对公民、法人和其他组织的合法权益产生严重损害，或者对社会秩序和公共利益造成损害，但不损害国家安全。

【等保三级】“强制安全保护级”，信息系统受到破坏后，会对社会秩序和公共利益造成严重损害，或者对国家安全造成损害。

【等保四级】“结构化保护级”，信息系统受到破坏后，会对社会秩序和公共利益造成特别严重损害，或者对国家安全造成严重损坏。

【等保五级】“访问验证保护级”，信息系统受到破坏后，会对国家安全造成特别严重损害。

8. 无线基础 WLAN

8.1 无线局域网

1. IEEE802.11 工作模式：基础设施网络、自主网络。

（1）服务集：最小构件（基本服务集 BSS），一个基本服务集覆盖的区域为基本服务区。一个 AP 可成基本服务集中的基站。一个服务集通过接入 AP 连接到分配系统（DS），然后再连接一个基本服务集，构成扩展服务集（ESS）。安装 AP 需要给 AP 分配一个不超 32 字节的服务集标识（SSID）和一个信道。

（2）ISM：工业、科学和医疗频段。2.4GHz 无线频段分为 13 个信道（1、6、11 互不重叠、干扰）。

（3）802.11 物理层：跳频（FHSS）、红外技术（IR）、直接序列扩频（DSSS）、正交频分复用技术（OFDM）、高速直接序列扩频（HR-DSSS）。

2. 802.11 系列标准

标准	运行频段	主要技术	数据速率
802.11	2.400~2.483GHz	DBPSK、DQPSK	1Mb/s 和 2Mb/s
802.11a	5.150~5.350GHz、5.725~5.850GHz， 与 802.11b/g 互不兼容	OFDM 调制技术	54Mb/s
802.11b	2.400~2.483GHz，与 802.11a 互不兼容	CCK 技术	11Mb/s
802.11g	2.400~2.483GHz	OFDM 调制技术	54Mb/s
802.11n	支持双频段，兼容 802.11b 802.11a 两种标准	MIMO（多进多出）与 OFDM 技术	300~600Mb/s

3. IEEE 802.11MAC 层协议

（1）采用载波侦听多路访问/冲突避免协议（CSMA/CA），不采用 CSMA/CD 的原因有：

①无线网络中，接收信号的强度往往远小于发送信号，因此要实现碰撞的花费过大；

②隐蔽站(隐蔽终端问题)，并非所有站都能听到对方。

（2）CSMA/CA 的 MAC 层分为 DCF 和 PCF 两层。

①分布协调功能(DCF)。DCF 没有中心控制，通过争用信道获取信道信息发送权，用于支持突发式通信。

②点协调功能(PCF)。PCF 选择接入 AP 集中控制 BSS，支持多媒体应用。

（3）802.11 的各类帧间隔

类别	定义	长度	优先级	适用范围
SIFS	短帧间间隔	最短	最高	适用 ACK.CTS 帧、过长.MAC 帧后分片数据帧
PIFS	点协调帧间间隔	适中 (SIFS+1 个时隙时间)	中	使用点协调 PCF 方式时
DIFS	分布协调功能 帧间间隔	最长 (SIFS+2 个时隙时间)	低	使用分布式协调 DCP 方式时

8.2 无线局域网安全

1. 有线等效保密（WEP）协议：是对在两台设备间无线传输的数据进行加密的方式，用以防止非法用户窃听或侵入无线网络。加密和解密使用同样的算法和密钥。WEP 采用的是 RC4 算法，使用 40 位或 64 位密钥，2003 年被淘汰。

2. IEEE 802.11i WPA

简写	全称	特点
TKIP	临时秘钥完整性协议	使用 WEP 机制的 RC4 加密，可通过升级硬件或驱动方式来实现
CCMP	计数器模式密码块链消息完整码协议	使用 AES 加密和 CCM 认证，该算法对硬件要求较高，需要更换硬件
WRAP	无线增强认证协议	使用 AES 加密和 OCB 加密

（1）SSID 访问控制：隐藏 SSID，让不知道的人搜索不到。

（2）物理地址过滤：在无线路由器设置 MAC 地址黑白名单。

（3）WEP 认证和加密：PSK 预共享密钥认证，RC4 加密。

（4）WPA（802.11i 草案）认证：802.1x 加密：RC4（增强）+TKIP（临时密钥完整协议），动态改变密钥）完整性认证和防重放攻击。

（5）WPA2（802.11i）：针对 WPA 的优化，加密协议：基于 AES 的 CCMP。

8.3 3G

1. 3G 标准：CDMA2000、WCDMA、TD-SCDMA。

- CDMA2000（码分多址）：中国电信主导，下载 3.1Mbit/s，上行 1.8Mbits/s。
- WCDMA（宽带码分多址）：中国联通主导，支持 384Kb/s~2Mb/s 数据传输速率。
- TD-SCDMA（时分同步的码分多址）：中国移动主导，网络速度可达 384kb/s。

运营商	2G	3G	4G	5G	备注
中国移动	GSM	TD-SCDMA	TD-LTE	SA（独立组网） NSA（非独立组网）	CDMA（码分多址） TD（时分复用） FDD（频分复用）
中国联通		WCDMA	TD-LTE FDD-LTE		
中国电信	CDMA	CDMA2000			

2. 5G 三大核心：增强型移动宽带（eMBB）、超高可靠低延时（uRLL）、海量机器类终端通信（mMTC）。

频带名称	波段名称	频率范围	波长范围	频带名称	波段名称	频率范围	波长范围
极低频 ELF	极长波	3Hz-30Hz	0-10000km	高频 HF	短波	3-30MHz	100-10m
超低频 SLF	超长波	30Hz-300Hz	10000-1000km	甚高频 VHF	米波	30-300MHz	10-1m
特低频 ULF	特长波	300Hz-3kHz	1000-100km	特高频 UHF	分米波	300-3000MHz	100-10cm
甚低频 VLF	甚长波	3-30kHz	100-10km	超高频 SHF	厘米波	3-30GHz	10-1cm
低频 LF	长波	30-300kHz	10-1km	极高频 EHF	毫米波	30-300GHz	10-1mm
中频 MF	中波	300k-3MHz	1000-100m	至高频	丝米波	300-3000GHz	1-0.1mm

9. 存储技术

9.1 RAID（独立磁盘冗余阵列）

RAID 级别	RAID0	RAID1	RAID5	RAID6	RAID10
可靠性	最低	高	较高	高	
冗余类型	无	镜像冗余	校验冗余		镜像冗余
空间利用率	100%	50%	(N-1)/N	(N-2)/N	50%
性能	最高	最低	较高		高
允许坏盘数量	0	N/2	1	2	N/2
至少盘数	2		3	4	

RAID 级别	RAID 0	RAID 1	RAID 3	RAID 5/6	RAID 10
应用场景	迅速读写，安全性要求不高，如图形工作站等	随机数据写入安全性要求高，如服务器、数据库存储领域	连续数据传输，安全性要求高，如视频编辑、大型数据库等	随机数据传输，安全性要求高，如金融、数据库、存储等	数据量大，安全性要求高，如银行、金融等领域

9.2 NAS 和 SAN

1. 网络附属存储（NAS）
2. 存储区域网络及其协议（SAN）：FC SAN、IP SAN。

	DAS	NAS	FC-SAN	IP-SAN
传输类型	SCSI、FC、SAS	IP	FC	IP
数据类型	块级	文件级	块级	块级
典型应用	任何	文件服务器	数据库应用	视频监控
优点	易于理解 兼容性好	易于安装 成本低	高扩展性、高性能 高可用性	高扩展性 成本低
缺点	难管理，扩展性有限 存储空间利用率不高	性能较低 对某些应用不适合	较昂贵，配置复杂 互操作性问题	性能较低

3. 主流硬盘类型

	SATA	SAS	NL-SAS	SSD
主流转速（RPM)	7,200	15,000/10,000	7200	NA
串行/并行	串行			
主流容量	1T/2T/4T/6T	1T/2T/4T/6T	2T/3T/4T	300G/600G/960G
MTBF（h）	1.200,000	1,600,000	1,200,000	2,000,000
备注	由 ATA 硬盘发展而来采用串行方式传轮，SATA 2.0 支 300MB/s,SATA3.D 实现 600MB/s 最高数据传输率.	SAS 专为满足高性能企业需求而设计，并且兼 SATA 硬盘。能够提 3.0Gbits 的传输率，规划到 12.0Gbit/s	带有 SAS 接口的“企业级 SATA 驱动器”。适用于在一个此盘阵列系统中实现分级存储，简化了磁盘阵，列系统的设计	固态硬盘（Solid State Disk）用固态电子存储芯片阵列而制成的硬盘，由控制单元和存储单元（FLASH 芯片、DRAM 芯片）组成。固态硬盘的接口规范和定义，功能及使用方法上与普通硬盘的完全相同，在产品外形和尺寸上也完全与普予硬盘—致

接口	IDE	SATA	SCSI	SAS	FC
接口类型	并行	串行	并行	串行	
主流接口速率	100MB/S 133MB/S	300MB/S 600MB/S	320MB/S	3Gb/S 6GB/S 12GBb/S	2Gb/S、4Gb/S 8Gb/S、16Gb/S
主流容量	总线	1T/2T/4T/6T/10T	总线	1T/2T/4T/6T	点对点、环路、交换式
双工	半双工	半双工	半双工	全双工	全双工
最大连接设备数	2	1 or 15 with port multiplier	16	16256	127-loop 1600 万 fabric
线缆长度	0.4m	1m	12m	6m	30m(铜轴电缆) 10km(光纤)
应用	普通 PC 机	低端工作站	中高端工作站		高端工作站

10. 网络规划与设计

10.1 网络生命周期

1. 网络生命周期五阶段：需求规范、通信规范、逻辑网络设计、物理网络设计、实施阶段。

（1）需求规范阶段	进行网络需求分析。
（2）通信规范阶段	进行网络体系分析。
（3）逻辑网络设计阶段	确定逻辑的网络结构。
（4）物理网络设计阶段	确定物理的网络结构。
（5）实施阶段	进网络设备安装、调试及网络运行时的维护工作。

10.2 网络需求分析

功能需求	用户和用户业务具体需要的功能。
应用需求	用户需要的应用类型、地点和网络带宽的需求;对延迟的需求;吞吐量需求。
计算机设备需求	主要是了解各类 PC 机、服务器、工作站、存储等设备以及运行操作系统的需求。
网络需求	网络拓扑结构需求、网络管理需求、资源管理需求、网络可扩展的需求。
安全需求	可靠性需求、可用性需求、完整性需求、一致性需求。

10.3 通信规范

1. 通信规范分析任务：就是通过分析网络通信模式和网络的流量特点，发现网络的关键点和瓶颈，为逻辑网络设计工作提供有意义的参考和模型依据，从而避免了设计的盲目性。

（1）通信模式分析	1.对通信模式进行分析，确定现有网络中的网络通信模式。 2.通信模式：对等通信模式、客户机/服务器（CIS）通信模式、浏览器/服务器通信模式、分布式计算通信模式。
（2）通信边界分析	确定局域网通信边界（广播域、冲突域)，确定广域网通信边界（自治区域、路由算法区域和局域网交界)，虚拟专用网络通信边界。
（3）通信流分布分析	通信流分布分析有时需要汇总所有单个信息流量的大小。

2. 80/20 规则：对于一个网段内部总的通信流量，80%的流量流转在网段内部，而剩下的 20%则是网段外部流量。这个规则适用于内部交流较多而外部访问较少的网络。

3. 20/80 规则：对于一个网段内部总的通信流量，20%的流量流转在网段内部，而剩下的 80%则是网段外部流量。这个规则适用于外部联系较多而内部联系较小的网络，可以较大限度地满足用户的远程联网需求，这个规则适用的网络允许存在具有特殊外部应用的网段。

10.4 逻辑网络设计

1. 逻辑网络设计：就是根据需求分析，依据用户分布、特点、数量和应用需求等形成符合的逻辑网络结构，大致得出网络互联特性及设备分布，但不涉及具体设备和信息点的确定。

2. 分层化网络设计模型

接入层	1. 作用是允许终端用户连接到网络，因此接入层交换机具有低成本和高端口密度特性。 2. 其他功能：用户接入与认证、二三层交换、QOS、MAC 地址过滤。
汇聚层	1. 是多台接入层交换机的汇聚点，它必须能够处理来自接入层设备的所有通信流量，并提供到核心层的上行链路，因此汇聚层交换机与接入层交换机比较需要更高的性能、更少的接口和更高的交换速率。 2. 其他功能：访问列表控制、VLAN 间的路由选择执行、分组过滤、组播管理、QoS、负载均衡、快速收敛等。
核心层	1. 功能主要是实现骨干网络之间的优化传输，骨干层设计任务的重点通常是冗余能力、可靠性和高速的传输。网络核心层将数据分组从一个区域高速地转发到另一个区域，快速转发和收敛是其主要功能。对核心层的设计及网络设备的要求十分严格。 2. 其他功能：链路聚合、IP 路由配置管理、IP 组播、静态 VLAN、生成树、设置陷阱和报警、服务器群的高速连接等。

3. 网络设计原则

（1）考虑设备先进性，但不一定必须采用最先进的设备，需要考虑合理性。

（2）网络系统设计应该采用开放的标准和技术。

（3）网络设计考虑近期目标和远期目标，要考虑其扩展性，为将来扩展考虑。

（4）结合实际情况进行设计考虑。例如在进行金融业务系统的网络设计时，应该优先考虑高可用性原则；在进行小型企业的网络设计时，应该优先考虑经济性原则。

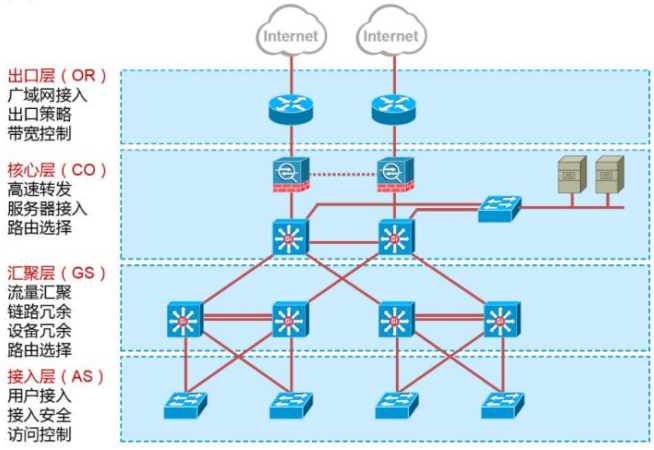
10.5 物理网络设计

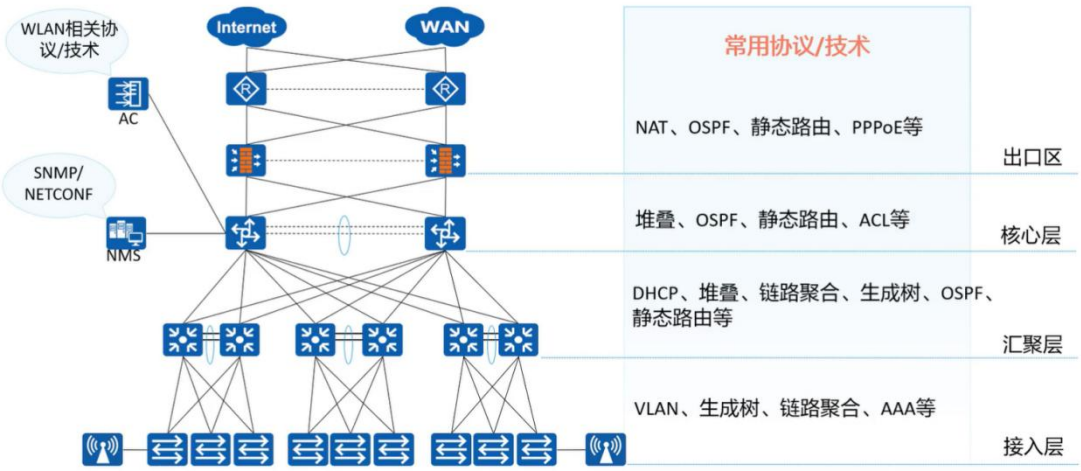
1. 设备选择原则

层次	设备选用原则
接入层	● 提供多种固定端口数量搭配供组网选择，可堆叠、易扩展； ● 在满足技术性能要求的基础上，最好价格便宜、使用方便、即插即用、配置简单； ● 支持二层交换和高带宽链路； ● 支持 ACL 和安全接入； ● 具备一定的网络服务质量、控制能力及端到端的 QoS 可选； ● 支持三层交换、远程管理和 SNMP
汇聚层	● 提供多种固定端口数量搭配供组网选择，可堆叠、易扩展； ● 在满足技术性能要求的基础上，最好价格便宜、使用方便、即插即用、配置简单； ● 支持 IP 路由，提供高带宽链路，保证高速数据转发； ● 具备一定的网络服务质量、控制能力及端到端的 QoS； ● 提供负载均衡的自动冗余链路、远程管理和 SNMP

核心层	● 数据的高速交换、高稳定性； ● 保证设备的正常运行和管理； ● 支持提供数据负载均衡和自动冗余链路、VLAN 定义与下发、生成树

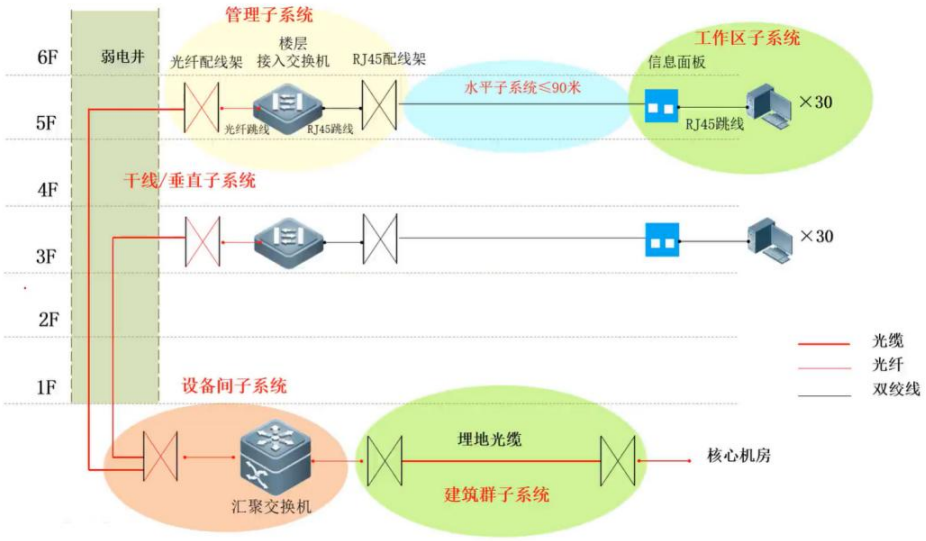
交换机连接方式	优势	劣势
堆叠（前提）	（1）逻辑上把多台设备虚拟成一台设备，简化运维，方便管理。 （2）一台物理设备故障，其他设备可以接管转发、控制平台，避免了单点故障。 （3）跨设备的链路聚合，物理上的无环网络，无需再部署 STP。 （4）链路聚合中的链路全部有效使用，链路利用率 100%。	（1）堆叠都是私有协议，不支持跨厂商设备堆叠。 （2）需要单独购买堆叠线缆。(现在最新的用光纤也能实现堆叠) （3）存在一定资源浪费，特别高端设备，如果 2 台核心都配置双引擎，堆叠后只有 1 个引擎工作。 （4）如果堆叠系统升级或重启，一般会有 20~60s 的业务中断。 （5）可靠性风险：控制层面统一后，相当于把鸡蛋放在一个篮子里，如果整个逻辑设备的控制平面出现问题（比如说路由表被人攻击破坏），就有可能导致整机瘫痪，影响的范围大。
级联（前提）	• 延长网络的距离。 • 可跨设备级联。	• 编码/解码过程，延时较长。 • 必须同时占用两个端口。 • 用户将损失性能/价格比。 • 多个设备的级联会产生级联瓶颈。
集群（目的）	• 软件实现。 •将多台互相连接的交换机作为一台逻辑设备进行管理。 •可以管理若干台其它交换机，只需要占用一个 IP 地址（仅命令交换机需要） •多台交换机协同工作，大大降低管理强度	• 厂家通过私有协议来实现集群。 • 跨设备集群存在技术局限性。





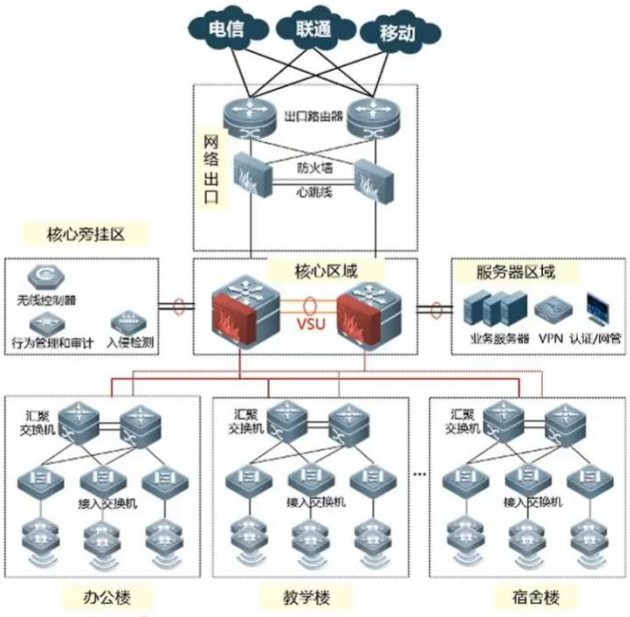
2. 综合布线

（1）干线子系统	是各水平子系统（各楼层）设备之间的互联系统。
（2）水平子系统	是各个楼层配线间中的配线架到工作区信息插座之间所安装的线缆
（3）工作区子系统	是由终端设备连接到信息插座的连线组成的，包括连接线和适配器。工作区子系统中信息插座的安装位置距离地面的高度为 30~50cm；如果信息插座到网卡之间使用无屏蔽双绞线，布线距离最大为 10m。
（4）设备间子系统	位置处于设备间，并且集中安装了许多大型设备（主要是服务器、管理终端）的子系统。
（5）管理子系统	该系统由互相连接、交叉连接和配线架、信息插座式配线架及相关跳线组成。
（6）建筑群子系统	将一个建筑物中的电缆、光缆和无线延伸到建筑群的另外一些建筑物中的通信设备和装置上。建筑群之间往往采用单模光纤进行连接。
注意：在测试线路的主要指标中，近端串扰是指一对相邻的另一对线通过电磁感应所产生的偶合信号衰减是由于集肤效应、绝缘损耗、阻抗不匹配、连接电阻等因素造成信号沿链路传输时的损失。	



技术措施层次	需求项目	需求项目	需求项目	需求项目
机房及物理线路安全	机房安全	计算机通信线路安全	骨干线路冗余防护	设备防雷
网络安全	安全区域划分	安全区域级别	区域内部安全策略	区域边界安全策略
	路由设备安全	网闸	防火墙	入侵检测系统
	抗 DDOS	VPN	流量管理	网络监控与审计
	网络监控与审计	访问控制		
系统安全	身份认证	账号管理	主机系统配置管理	漏洞发现与补丁管理
	内核加固	病毒防护	桌面安全管理	系统备份与恢复
	系统监控与审计	访问控制		
应用安全	数据库安全	邮件服务安全	Web 服务安全	系统应用定制安全

认方式	认证设备 NAC	应用场景	特点
802.1x	交换机	校园网、企业	安全性高，一般需要 PC 安装客户端
PPPoE	BRAS/BAS	家庭宽带、校园网	实现简单，可以共享上网
IPoE		机顶盒这类哑终端	也可以 IPoE+Web portal 网页认证（用得少)
portal	认证网关（服务器)	商超、公共场所	安全性低，便捷性高
MAC 认证	认证服务器	打印机等哑终端	一般入网第一次进行认证，后续即放行
其他认证：短信认证、微信认证用于访客，哑终端也可以不认证。			

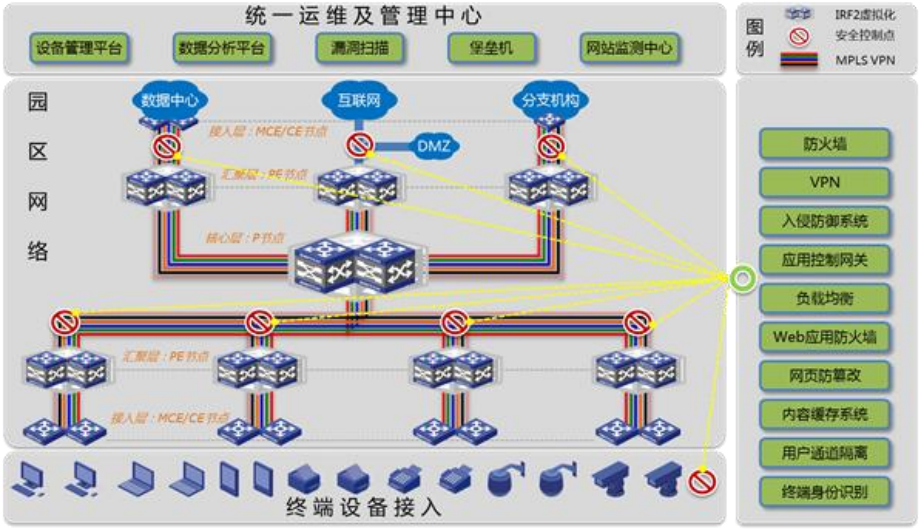


园区网技术设备

设备	部署方式	功能	关键字
交换机	三层架构	二层交换机实现互连，三层交换机具有路由功能	VLAN/逻辑隔离
路由器	网络出口	NAT、路由选路	出口
防火墙	串行	区域隔离，访问控制	访问控制
IPS		入侵行为检测并阻断	阻断
IDS	旁路	入侵行为检测不阻断	旁路
WAF	串行	保障 Web 应用安全	Web
上网行为管理		用户上网行为进行控制	行为管理
无线控制器	旁路	实现用户漫游，AP 统一管理	漫游
FC 交换机	串行	实现存储互联网，服务器双链路连接，一般一条为 FC，另一条为以太网	服务器双链路

专用故障排查工具

- 欧姆表、数字万用表及电缆测试器：利用这些参数可以检测电缆的物理连通性。
  测试并报告电缆状况，其中包括近端串音、信号衰减及噪音。
- 时域反射计与光时域反射计
  时域反射器（TDR）：能够快速定位金属线缆中的短路、断路、阻抗等问题。
  光时域反射器（OTDR）：精确测量光纤的长度、断裂位置、信号衰减等。
- 网络监测器：分析统计网络状态
- 网络分析仪：科来



11. 计算机硬件

11.1 CPU 体系结构

11.2 1.CPU

CPU	运算器	算术逻辑单元 ALU	用于进行各种算术逻辑运算。
		通用寄存器	用来存放操作数、中间结果和各种地址信息的一系列存储单元。
		数据暂存器	用来暂存从主存储器读出的数据，这个数据不能存放在通用寄存器中，否则会破坏其原有的内容。
		程序状态寄存器 PSW	用于保留与算术逻辑运算指令或测试指令的结果对应的各种状态信息。移位器在 ALU 输出端用暂存器来存放运算结果，具有对运算结果进行移位运算的功能。
	控制器	程序计数器 PC	用于指出下条指令在主存中的存放地址，CPU 根据 PC 的内容去主存处取得指令。。
		指令寄存器 IR	用于保存当前正在执行的这条指令的代码。
		地址寄存器 AR	用于存放 CPU 当前访问的内存单元地址。
		数据寄存器 DR	用于暂存从内存储器中读出或写入的指令或数据。
		指令译码器	用于对获取的指令进行译码，产生该指令操作所需要的一系列微操作信号，以控制计算机各部件完成该指令。

2. 指令组成：操作码、地址码。
   (1) 操作码：说明指令的操作性质及功能；地址码：说明操作数的地址。
   (2) 一条指令必须有一个操作码，但有可能包含几个地址码。

3. 指令执行过程：取指令、取操作数、执行操作。

取指周期	地址由 PC 给出，取出指令后，PC 内容自动递增。取操作数周期期间要解决的是计算操作数地址并取出操作数。
执行周期	执行周期的主要任务是完成由指令操作码规定的动作，包括传送结果及记录状态信息。执行过程中要保留状态信息，尤其是条件码要保存在 PSW 中。若程序出现转移，则在执行周期内还要决定转移地址的问题。因此，执行周期的操作对不同指令也不相同。
指令周期	将一条指令从取出到执行完成所需要的时间称为指令周期。

它们之间的关系	一个指令周期可以划分为一个或多个总线周期，根据指令的不同，需要的总线周期也不同；而一个总线周期又可分为几个时钟周期，通常是 4 个时钟周期，有些计算机可能不同。
	总线数据传输率=时钟频率/每个总线包含的时钟周期×每个总线周期传送的字节数

4. CPU 系统指令：复杂指令集（CISC）、精简指令集（RISC）。

指令区别：

(1) 指令系统的指令数目。

(2) 编程的便利性。

(3) 寻址方式。

(4) 指令长度。

(5) 控制器复杂性。

指令系绕类型	指 令	寻址方式	实现方式
CISC（复杂）	数量多，使用频率差别大，可变长格式	支持多种方式	
RISC（精简）	数量少，使用频率接近，定长格式	支持方式少	硬布线逻辑控制为主

5. CPU 的主要性能指标：主频、位和字长、缓存。

11.3 流水线技术

1. 流水线：是一种将指令分解为多个小的步骤，并让几条不同指令的各个操作步骤重叠，从而实现几条指令并行处理以加速程序运行速度的技术。

2. 流水线性能指标

吞吐率	吞吐率指的是计算机中的流水线在单位时间内可以处理的任务或执行指令的个数。 吞吐率：$TP=\frac{N}{T}$　　N：指令条数　　T：执行完 N 条指令时间
加速比	加速比是指某一流水线采用串行模式的工作速度与采用流水线模式的工作速度的比值。加速比数值越大，说明这条流水线的工作安排方式越好。
效率	效率是指流水线中各个部件的利用率。

11.4 内存结构与寻址

1. 内存储器类型

随机存取存储器（RAM）	1.随机存取：是指 CPU 可以对存储器中的数据随机地存取，与信息所处的物理位置无关。RAM 具有读写方便、灵活的特点，但断电后信息全部丢失，常用于主存和高速缓存中。 2.分类：DRAM、SRAM。 • DRAM 的信息会随时间的延长而逐渐消失，因此需要定时对其进行刷新来维持信息不丢失。

	• SRAM 在不断电的情况下，信息能够一直保持而不丢失，也不需要刷新。
只读存储器（ROM）	随机存取方式的存储器，信息是固定在存储器内的，只可读出，不能修改，读取的速度比 RAM 慢。
顺序存取存储器（SAM）	SAM 只能按某种顺序存取，存取时间的长短与信息在存储体上的物理位置相关，只能用平均存取时间作为存取速度的指标。磁带机就是 SAM 的一种。
直接存取存储器（DAM）	DAM 的存取时间与信息所在的物理位置有关，相对 SAM 来说，DAM 的存取时间更短。
相联存储器（CAM）	CAM 是一种基于数据内容进行访问的存储设备。

存取方式	读/写装置	数据块标志	访问特性	代表
顺序存取	共享读/写装置	无	特定线性顺序	磁带
直接存取		数据分块，每块一个唯一标志	可直接移到特定数据块	
随机存叹	每个可寻址单元专有读/写装置	每个可寻址单元均有一个唯一地址	随时访问任何一个存储单元	主存储器
相联存取（属随机存取）			根据内容而非地址来选择读写点	Cache

2. 主存储器类型

(1) 主存储器一般由地址寄存器、数据寄存器、存储体、控制线路和地址译码电路等部分组成。

RAM（随机存储器）	可读/写，只能暂存数据，断电后数据丢失。
SRAM（静态随机存储器）	在不断电时信息能够一直保持，读写速度快，生产成本高，多用于容量较小的高速缓冲存储器。
DRAM（动态随机存储器）	需要定时刷新以维持信息不丢失，读写速度较慢，集成度高，生产成本低，多用于容量较大的主存储器。
ROM（只读存储器）	出厂前用掩膜技术写入，常用于存放 BIOS 和微程序控制。
PROM（可编程 ROM）	只能够一次写入，需用特殊电子设备进行写入。
EPROM（可擦除的 PROM）	用某种方法可擦去信息，可写入多次。
E2PROM（电可擦除 EPROM）	可以写入，但速度慢。
闪速存储器(Flash Memory)	其特性介于 EPROM 与 E2PROM 之间。但不能进行字节级别的删除操作。
CAM（相联存储器）	CAM 是一种特殊的存储器，是一种基于数据内容进行访问的存储设备。其速度比基于地址进行读写的方式要快。

3. 存储介质读写速度由快到慢是：寄存器、Cache、内存、硬盘、光盘。

4. 高速缓存：在计算机存储系统的层次结构中,介于中央处理器和主存储器之间的高速小容量存储器和主存储器一起构成一级的存储器。高速缓冲存储器和主存储器之间信息的调度和传送是由硬件自动完成的。当 CPU 存取主存储器时，硬件首先自动对存取地址进行译码，以便检查主存中的数据是否在高速缓存中：

若要存取的主存储器单元的数据已在高速存储器中，则称为命中，硬件就将存取主存储器的地址映射为高速存储器的地址并执行存取操作；

若该单元不在高速存储器中，则称为脱靶，硬件将执行存取主存储器操作,并自动将该单元所在的主存储器单元调入高速存储器中的空闲存储单元中。

5. Cache（高速缓冲存储器）：高速缓冲存储器是位于主存与 CPU 之间的一级存储器，由静态存储芯片(SRAM)组成，容量比较小但速度比主存高得多，接近于 CPU 的速度。但其成本更高，因此 Cache 的容量要比内存小得多。Cache 存储了频繁访问内存的数据。

直接映射	• 是一种多对一的映射关系，但一个主存块只能够复制到 Cache 的一个特定位置上去。 • Cache 的行号 i 和主存的块号 j 有函数关系：i= j % m(其中 m 为 Cache 总行数)
全相联映射	• 将主存中任一主存块能映射到 Cache 中任意行（主存块的容量等于 Cache 行容量)。根据主存地址不能直接提取 Cache 页号，而是需要将主存块标记与 Cache 各页的标记逐个比较，直到找到标记符合的页（访问 Cache 命中），或者全部比较完后仍无符合的标记（访问 Cache 失败)。 • 主存块标记与 Cache 各页的标记逐个比较，所以这种映射方式速度很慢，失掉了高速缓存的作用，这是全相联映射方式的最大缺点。如果让主页标记与各 Cache 标记同时比较，则成本太高。
组相联映射	• 是前两种方式的折中方案。它将 Cache 中的块再分成组，各组之间是直接映像，而组内各块之间则是全相联映像。 • 主存地址=区号+组号+组内块号+块内地址号

6. 命中率：$L=M\times(1-H)+N\times H$　M：直接访问主存的时间　N：访问高速缓存的时间　L：CPU 访问内存的平均时间　H：命中率

7. 内存地址编址：内存容量=最高地址-最低地址+1

11.5 数表示和计算

1. 定点整数：指机器数的小数点位置固定在机器数的最低位之后。
2. 定点小数：指机器数的小数点位置固定在符号位之后，有效数值部分在最高位之前。
3. 定点数表示：原码、补码、反码、移码。

原码	用真实的二进制值直接表示数值的编码就叫原码。
反码	正整数的反码就是其本身；而负整数的反码则通过对其绝对值按位求反来取得。基本规律是：除符号位外的其余各位逐位取反就得到反码。反码表示的数和原码相同且一一对应
补码	正数的补码与原码一样；负数的补码是对其原码（除符号位外）按各位取反，并在末位补加 1 而得到的
移码	叫增码，是符号位取反的补码，一般用做浮点数的阶码表示，因此只用于整数。目的是保证浮点数的机器零为全零。移码和补码仅仅是符号位相反

编码方式	数值	表示方法
原码	+1 -1	0 0000001 1 0000001
反码	+1 -1	0 0000001 1 1111110
补码	+1 -1	0 0000001 1 1111111
移码	+1 -1	1 0000001 0 1111111

十进制数字	原码	反码	补码	移码
+0	0 0000000	0 0000000	0 0000000（正数原反补码相同)	1 0000000
-0	1 0000000	11111111	0 0000000 负数补码是反码+1，即 1 00000000，高位溢出 -128 的补码是 10000000	1 0000000

原码、反码，正负零不一样，补码、移码正负零一样。多出一位，可以表示-128

11.6 总线与中断

1. 总线(Bus)：是连接计算机有关部件的一组信号线，是计算机中用来传送信息的公共通道。
2. 总线分类：内部总线、系统总线。

传输信号种类分：

数据总线 DB	一般情况下是双向总线，用于各个部件之间的数据传输。
地址总线 AB	单向总线，是微处理器或其他主设备发出的地址信号线。
控制总线 CB	处理器与存储器或接口等之间控制信号。

按数据的传送格式	并行接口、串行接口
按主机访问 I/O 设备的控制方式	程序查询接口、中断接口、DMA 接口以及通道控制器、I/O 处理机等。
按时序控制方式	同步接口、异步接口。
I/O 端口的寻址	独立的 I/O 寻址方式（独立编址) 存储器映像 I/O 寻址方式(统一编址)

3. 数据传输控制方法：程序控制方式、中断方式、直接存储区存取（DMA）等。

(1) DMA 方式：是指在传输数据时将从一个地址空间复制到另一个地址空间的过程中，只要 CPU 初始化这个传输动作，传输动作的具体操作由 DMA 控制器来实行和完成,这个过程中不需要 CPU 参与，数据传送完毕后再把信息反馈给 CPU，这样就极大地减轻了 CPU 的负担，节省系统资源，提高 I/O 系统处理数据的能力，并减少 CPU 的周期浪费。

12. 计算机软件

12.1 操作系统

1. 操作系统运行状态：就绪态、运行态、阻塞态。

2. 并发：是指一定时间内物理机器上有两个或两个以上的程序同时处于开始运行却尚未结束的状态，并且次序并不是事先确定的。

3. 并行：严格意义上的回时执行在多处理机系统中才可能实现。

4. PV 原语实现进程的同步：进程同步时的信号量只与制约进程和被制约进程有关，同步的信号量成为私有信号量。利用 PV 原语实现进程同步的方法是：首先判断进程间的关系是否为同步，若是，则为各并发进程设置各自的私有信号量，并为私有信号量赋初值，然后利用 PV 原语和私有信号量来规定各个进程的执行顺序。可以通过消费者和生产者进程之间的同步来说明。

5. 进程之间的互斥是进程间竞争共享资源的使用权，这种竞争没有固定的先后顺序关系；
   而进程同步涉及共享资源的并发进程之间有一种必然的依赖关系。

12.2 软件开发

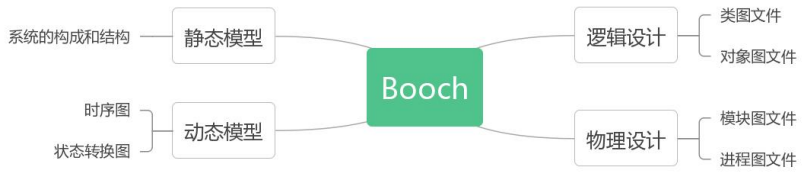
1. 结构化程序设计：是以模块功能和详细处理过程设计为主的一种传统的程序设计思想，采用自顶向下、逐步求精的方式进行。任何程序都可以由顺序、选择、循环三种基本结构构成。高内聚低耦合。

2. 面向对象概念

对象	任何事物
类	类可以看作是对象的模板。类是对一组有相同数据和相同操作的对象的定义，一个类所包含的方法和数据描述是一组对象的共同属性和行为。
消息和方法	对象之间进行通信的机制叫做消息。

3. 面向对象的特征：继承性、多态性、封装性。

4. 面向对象方法：Booch 方法、Coad 方法、OMT 方法等。

Booch 方法	 1）类图：描述类与类之间的关系。 2）对象图：描述实例和对象间传递消息。 3）模块图：描述构件。 4）进程图：描述进程分配处理器的情况。 5）时序图：描述对象图中不同对象之间的动态交互关系。 6）状态图：描述一个类的状态变化。
Coad 方法	分为两部分：面向对象分析（OOA）、面向对象设计（OOD）。

5. 软件规模度量：代码行、功能点分析法、德尔菲法、构造性成本模型。

6. UML：用例图、类图、序列图、状态图、活动图、组件图、部署图。

7. 软件开发模型：瀑布模型、快速原型模型、增量模型、螺旋模型、喷泉模型、混合模型。
• 瀑布模型六阶段：定制计划、需求分析、软件设计、程序编写、软件测试、运行维护。

8. CMM 模型：能力成熟度模型。CMM 分为五个等级：一级为初始级；二级为可重复级；三级为已定义级；四级为已管理级；五级为优化级。

9. 软件测试：单元测试、集成测试、系统测试、验收测试、回归测试。

(1) 验收测试三种策略：正式验收、非正式验收、α测试、β测试。

(2) 白盒测试：又称结构测试或逻辑驱动测试。利用白盒测试法对软件进行动态测试时，主要是测试软件产品的内部结构和处理过程，而不关注软件产品的功能。白盒测试法中对测试的覆盖标准主要有：逻辑覆盖、循环覆盖和基本路径测试。白盒测试的主要方法有逻辑驱动、基路测试等，通常用于软件验证。

(3) 黑盒测试：又称功能测试或数据驱动测试。

	别名	测试阶段	测试对象	测试人员	测试依据	测试方法
单元测试(UT)	模块测试 组件测试	在编码之后进行，来检验代码的正确性	模块、类、函数和对象也可能是更小的单元 （如:一行代码，一个单词）0	由白盒测试工程师或开发人员	依据代码、详细设计文档来进行测试	白盒测试
集成测试(IT)	组装测试 联合测试	单元测试之后，检验模块间接口的正确性	模块间的接口	白盒测试工程师或开发人员	单元测试的文档、概要设计文档	黑盒测试+白盒测试(灰盒测试)
系统测试(ST)	--	集成测试之后	整个系统（软件、硬件）	黑盒测试工程师	需求规格说明书	黑盒测试
验收测试	交付测试	系统测试通过后	整个系统（包括：软件、硬件）	最终用户或需求方	用户需求、验收标准	

10. 备份方式：正常备份、增量备份、差异备份、每日备份、副本备份。

备份策略	完全备份	增量备份	差异备份	
空间使用	最多	最少	少于完全备份	使用空间：完全备份>差异备份>增量备份
备份速度	最慢	最快	快于完全备份	备份速度：增量备份>差异备份>完全备份
恢复速度	最快	最慢	快于增量备份	恢复速度：完全备份>差异备份>增量备份

12.3 项目管理基础

1. 计划审评技术（PERT）:是由关国海军捉出的利用网络分析制定计划及对计划予以评价的技术。

2. 关键路径：关键路径法（CPM），在一个项目中，只有项目网络中最长的或耗时最多的活动完成之后，项目才能结束，这条最长的活动路线就叫关键路径，组成关键路径的活动称为关键活动。CPM 是通过寻找项目过程中活动序列的进度安排的最少总时差来预测项目工期的一种网络分析方法。基本工作原理是：给每个最小任务单元计算工期、定义最早开始和结束日期、最迟开始和结束日期、按照活动的关系形成顺序的网络逻辑图，找出其中最长的路径，即为关键路径。

3. 关键路径法的时间计算：正推法、逆推法。

4. 甘特图：它直观地表明任务计划在什么时候进行，及实际进展与计划要求的对比；也可以表示子任务之间的并行和串行关系。

12.4 软件知识产权知识

1. 知识产权期限保护

客体类型	权利类型	保护期限
公民作品	署名权、修改权、保护作品完整权	没有限制
	发表权、使用权和获得报酬权	作者终生及其死亡后的 50 年(第 50 年的 12 月 31 日)
单位作品	发表权、使用权和获得报酬权	50 年(首次发表后的第 50 年的 12 月 31 日)，若其间未发表，不保护
公民软件产品	署名权、修改权	没有限制
	分表权、复制权、发行权、出租权、信息网络传播权、翻译权、使用许可权、获得报酬权、转让权	作者终生及其死亡后的 50 年(第 50 年的 12 月 31 日)。对于合作开发的,则以最后死亡的作者为准
单位软件产品	反表权、复制权、发行权、出租权、信息网络传播权、翻译权、使用许可权、获得报酬权、转让权	著作权的保护期为 50 年(首次发表后的第 50 年的 12 月 31 日)，若 50 年内未发表的不予保护
注册商标		有效期为 10 年(若注册人死亡或倒闭 1 年后,未转移则可注销，期满后 6 个月内必须续注)
发明专利权		保护期为 20 年(从申请日开始)
实用新型		保护期为 10 年(从申请日开始)
外观设计专利权		保护期为 15 年(从申请日开始)

2. 识产权归属

情况说明		判断说明	归属
作品	职务作品	利用单位的物质技术条件进行创作，并由单位承担责任的	除署名权外其他著作权归单位
		有合同约定，其著作权属于单位	除署名权外其他著作权归单位
		其他	作者拥有著作权，单位有权在业务范围内优先使用
软件	职务作品	属于本职工作中明确规定的开发目标	单位亨有著作权
		属于从事本职工作活动的结果	单位亨有著作权
		使用了单位资金、专用设备、未公开的信息等物质、技术条件并由单位或组织承担责任的软件	单位亨有著作权

	委托创作	有合同约定,著作权归委托方	委托方
		合同中未约定著作权归属	创作方
	合作开发	只进行组织、提供咨询意见、物质条件或者进行其他辅助工作	不享有著作权
		共同创作的	共同享有，按人头比例。成果可分割的，可分开申请
商标		谁先申请谁拥有(除知名商标的非法抢注) 同时申请,则根据谁先使用(需提供证据) 无法提供证据协商归属,无效时使用抽签(但不可不确定)	
专利		谁先申请谁拥有，如果双方同一天申请，则双方协商，协商不成，均不予受理(同时驳回双方的专利申请）	

13. Windows

13.1 域与活动目录

13.2 用户与组

1. 用户账号：Administrator 账户、Guest 账户、IUSR_机器名、IWAM_机器名。
2. 组账号

Administrator 组	对服务器有完全控制权限，可以为用户指派用户权利和访问控制权限。
Guest 组	成员拥有一个在登录时创建的临时配置文件，注销时将删除该配置文件。“来宾账号”(默认为禁用）也是 Guests 组的默认成员。
Power Use 组	成员可以创建本地组，并在已创建的本地组中添加或删除用户，还可以在 Power Users 组、Users 组和 Guests 组中添加或删除用户。
Users 组	成员可以运行应用程序，但是不能修改操作系统的设置。
Backup Operators 组	该组成员不管是否具有访问该计算机文件的权限，都可以运行系统的备份工具，对这些文件和文件夹进行备份和还原。
Network Configuration Operators 组	该组成员可以在客户端执行一般的网络设置任务(如更改 IP 地址)，但是不能设置网络服务器。
Everyone 组	任何用户都属于这个组，因此当 GUEST 被启用时，改组的权限设置必须严格限制。
Interactive 组	任何本地登录的用户都属于这个组。
System 组	该组拥有系统中最高的权限，系统和系统级服务的运行都是依靠 System 赋予的权限，从任务管理器中可以看到很多进程是由 System 开启的。System 组只有一个用户（即 System)。

13.3 文件系统与分区管理

1.windows 文件分区文件系统：FAT16、FAT32、NTFS。其中的 FAT16 和 FAT32 均是文件配置表（FAT）方式的文件系统。

13.4 网络配置

ipconfig	用于显示计算机中网络适配器的 IP 地址、子网掩码及默认网关等信息。
tracert	检查数据包路由路径。
Pathping	要跟踪路径并为路径中的每个路由器和链路提供网络延迟和数据包丢失等相关信息。
ARP	根据目的计算机的 IP 地址获得对应的 MAC 地址。
route	主要用于手动配置静态路由并显示路由信息表。
netstat	netstat 是一个监控 TCP/IP 网络的工具，它可以显示路由表、实际的网络连接、每一个网络接

	口设备的状态信息，以及与 IP、TCP、UDP 和 ICMP 等协议相关的统计数据。一般用于检验本机各端口的网络连接情况。
nslookup	一个用于查询 Internet 域名信息或诊断 DNS 服务器问题的工具。
FTP	

分类	选项	用途	分类	选项	用途
ipconfig	/all	显示 IP、掩码、网关等详细信息	arp	-a	显示当前 ARP 缓存表
	/renew	更新 DHCP 配置，重新获 IP		-d	删除某条 ARP 缓存
	/release	释放 DHCP 获得的 IP 地址			arp-d 10.1.10.118
	/flushdns	清除 DNS 缓存信息		-s	静态绑定 ARP
	/displaydns	显示 DNS 缓存信息			arp-s 10.1.1.1 00-aa-00-62-c6-09
ping	-t	持续 ping，直到 Ctrl+C 中断	netstat		显示 TCP 连接，侦听的端口及统计信息
	-a	将 lP 解析为主机名		-n	显示活动的 TCP 连接
	-n Conunt	设置 ping 包的个数		-r	显示 lP 路由表，与 route print 一样
traceroute tracert	无	跟踪网络传输路径 原理：递增 TTL 字段的 ICMP 回送错误报文	route	print	显示路由表
pathping		结合了 ping 和 tracert 功能，可以显示通信线路上每个子网的延时和丢包率		add	添加静态路由，重启不在
				-p	与 add 联合使用，重启路由还在
nslookup	功能	用于显示 DNS 查询信息，诊断，故障排查			
		nslookup www.baidu.com Server:61.139.2.69 Address:61.139.2.69#53 Non-authoritative answer: www.baidu.com canonical name = www.a.shifen.com. Name:www.a.shifen.com Address:14.215.177.38 Name:www.a.shifen.com Address:14.215.177.39	交互式解析： Set type=mx：查询本地域的邮件交换器记录 Server NAME：指定由哪个 DNS 服务器进行解析		

13.5 系统管理命令

1. MMC（微软管理控制台）
2. regedit（注册表编辑器）
3. IIS 认证方式
   （1）集成的 Windows 身份验证。
   （2）Windows 域服务器的摘要式身份验证。
   （3）基本身份验证（以明文形式发送密码)。

14. Linux

14.1 分区与文件管理

1. 分区管理：系统分配了 1~16 的序列号码，主分区和扩展分区最多 4 个。
2. 两个专门分区：：Linux SWAP 分区、Linux Native 分区。
3. Linux 常见分区格式：ext、ext2、ext3、iso9660、NFS、HPFS。
4. 文件管理：根目录‘/’
5. Linux 主要目录及其作用

/bin	存放着最经常使用的命令（二进制文件）。
/boot	存放的是启动 Linux 时使用的一些核心文件，包括一些连接文件以及镜像文件。
/dev	存放的是 Linux 的外部设备，在 Linux 中访问设备的方式和访问文件的方式是相同的。
/etc	存放所有的系统管理所需要的配置文件和子目录。
/home	用户的主目录。
/lib	存放着系统最基本的动态连接共享库。
/var	被修改的目录放在这个目录下。包括各种日志文件。
/tmp	存放一些临时文件。
/mnt	挂载点，让用户临时挂载别的文件系统。
/opt	给主机额外安装软件所摆放的目录。默认空。
/root	系统管理员目录。
/srv	存放一些服务启动之后需要提取的数据。
/usr	用户的很多应用程序和文件都放在这个目录下。
/sbin	存放的是系统管理员使用的系统管理程序。

14.2 系统启动过程

（1）引导加载程序 GRUB/LILO。（POST 加电自检）
（2）加载内核。
（3）执行 init 进程。
（4）通过 /etc/inittab 文件进行初始化。
（5）执行 /bin/login。

14.3 系统运行级别：一共 7 个级别

0：系统停机状态，系统默认运行级别不能设为 0，否则不能正常启动。
1：单用户工作状态，root 权限，用于系统维护，禁止远程登录。
2：多用户状态(没有 NFS)。
3：完全的多用户状态(有 NFS)，登录后进入控制台命令行模式。

4：系统未使用，保留。

5：X11 控制台，登录后进入图形 GUI 模式。

6：系统正常关闭并重启，默认运行级别不能设为 6，否则不能正常启动。

14.4 守护进程

（1）dhcpd：动态主机控制协议（Dynamic Host Control Protocol，DHCP)的服务守护进程。

（2）Crond：crond 是 UNIX 下的一个传统程序，该程序周期性地运行用户调度的任务。比起传统的 UNIX 版本，Linux 版本添加了不少属性，而且更安全,配置更简单。类似于 Windows 中的计划任务。

（3）Httpd：Web 服务器 Apache 守护进程，可用来提供 HTML 文件及 CGI 动态内容服务。

（4）iptables：iptables 防火墙守护进程。

（5）named：DNS (BIND)服务器守护进程。

（6）Pppoe：ADSL 连接守护进程。

（7）Sendmail：邮件服务器 sendmail 守护进程。

（8）Smb：Samba 文件共享/打印服务守护进程。

（9）Snmpd：简单网络管理守护进程。

（10）Squid：代理服务器 squid 守护进程。

（11）Sshd：SSH 服务器守护进程。Secure Shell Protocol 可以实现安全地远程管理主机。

14.5 常见配置

1. ifcfg-ethx 配置文件：用于存放系统 eth 接口的 IP 配置信息。
2. /etc/sysconfig/network 配置文件：用于存放系统基本的网络信息。
3. /etc/hostname：系统主机名文件
4. /etc/hosts：包含 IP 地址和主机名之间的映射，还包含主机别名

   127.0.0.1 pc1 localhost　　#127.0.0.1 是 IP 地址，pc1 是主机名，localhost 是别名 192.168.0.2 pc2
5. /etc/host.conf：　指定客户机域名解析顺序，该文件内容：order hosts，bind
6. /etc/resolv.conf：指定客户机域名搜索顺序和 DNS 服务器地址：

   Seach test.edu.cn

   nameserver 114.114.114.114　　#首选 DNS 服务器

   nameserver 8.8.8.8　　#备用 DNS 服务器

14.6 常用命令

1. Linux 系统管理命令：ls、“>”(输入出重定向和管道命令)、“|”（管道命令）、chmod、cd、mkdir 和 rmdir、cp、rm、mv、cat、pwd、ln、grep、mount、rpm、ps、kill、chkconfig、passwd、useradd、groupadd。
2. 网络配置命令：ifconfig、ifdown 和 ifup、route、traceroute、iptables。

cat	用来在屏幕上滚动显示文件的内容，cat 命令也可以同时查看多个文件的内容，还可以用来合并文件　　格式 cat [-选项]fileName [filename2] ...[fileNameN]
more	如果文本文件比较长，一屏显示不完，这时可以使用 more 命令将文件内容分屏显示。
less	less 命令的功能与 more 命令很相似，也是按页显示文件，不同的是 less 命令在显示文件时允许用户既可以向前或向后翻阅文件。

	按 B 键向前翻页显示；按 P 键向后翻页显示;输入百分比显示指定位置；按 Q 键退出显示。
cp	文件复制命令。 cp[-选项] - a：整个目录复制。它保留链接、文件属性，并递归地复制子目录。 -f：删除已经存在的目标文件且不提示。
mv	文件移动命令
rm	文件删除命令。 rm[-选项] -f：忽略不存在的文件，从不给出提示。 -r：指示 rm 将参数中列出的全部目录和子目录均递归地删除。最大的笑话：删库跑路 rm -rf /*
mkdir	创建目录命令
rmdir	删除目录命令
cd	改变目录命令
pwd	显示当前目录命令
ls	列目录命令
chmod	文件访问权限命令。chmod g+rw test.txt
ln	文件链接命令。ln 命令的功能是在文件之间创建链接。

14.7 配置命令

1. DNS 配置

（1）配置文件：named.conf

（2）正向区域配置文件：/huanu.net.db

- A 记录：用于指明一个域名对应的 IP 地址。
- CNAME 记录（别名记录）：可以将多个不同名称指向同一个服务器。在创建别名记录之前必须要先创建 A 记录。
- MX 记录：用于指明邮件服务器的 IP 地址。

（3）反向域名解析文件：/hunau.net.rev

2. DHCP 配置：DHCP 是动态主机配置协议，用于向计算机自动提供 IP 地址、子网掩码和默认路由等基本配置信息。

（1）配置文件：/etc/dhcpd.conf

（2）dhcpd.leases 配置文件：是 DHCP 服务器自动创建和维护的，不需要管理员参与配。

3. FTP 配置

(1) 配置文件：vsftpd.conf

(2) vsftpd.ftpusers 配置：用来记录“不允许”登录到 FTP 服务器的用户，通常是系统默认用户。

(3) vsftpd/user_list 文件与 vsftpd/ftpusers 文件的作用类似。

(4) FTP 服务管理

停止：/etc/init.d/vsftpd stop

启动：/etc/init.d/vsftpd start

重启：/etc/init.d/vsftpd restart

4. Web 服务器：用 Apache

(1) 配置文件：/etc/httpd.conf

(2) Apache 支持虚拟主机：基于 IP、基于名字。

(3) Apache 的管理

启动：/etc/rc.d/init.d/httpd start

停止：/etc/rc.d/init.d/httpd stop

重启：service httpd restart

15. 交换机基础

15.1 交换机概念

1. 交换机：交换机(Switch)是一种信号转发的设备，可以为交换机自身的任意两端口间提供独立的电信号通路。

2. 交换机分类

管理	网管交换机（智能机）、非网管交换机(傻瓜交换机)。
工作层次	2 层交换机、3 层交换机、4 层交换机。
网络拓扑结构	接入层交换机、汇聚层交换机、核心层交换机。
交换方式	直通式交换、存储转换式交换、无碎片转发交换（接收到 64 字节后转发）。

交换机类别	交换依据
2 层交换机	MAC 地址
3 层交换机	IP 地址
4 层交换机	TCP/UDP 端口
帧中继交换机	虚电路号(DLCI)
ATM 交换机	虚电路标识 VPI 和 VCI

冲突域	1.冲突域是物理层的概念，是指会发生物理碰撞的域。 2.单纯复制信号的集线器和中继器是不能隔离冲突域的。 3.使用第 2 层技术的设备能分割 CSMA/CD 的设备，可以隔离冲突域。 4.网桥、交换机、路由器能隔离冲突域。
广播域	1.广播域是数据链路层的概念，是能接收同一广播报文的节点集合。 2.隔离广播域需要使用第 3 层设备，路由器、3 层交换机都能隔离广播域。

吞吐量	1.吞吐量是单位时间内网络中通过数据包的数量。 2.吞吐量(Mp/s）=万兆端口数量×14.88 Mp/s+千兆端口数量×1.488 Mp/s+百兆端口数量×0.1488 Mp/s。
背板带宽	1.带宽是交换机接口处理器或接口卡和数据总线间所能吞吐的最大数据量。 2.全双工计算 背板带宽(Mb/s）=万兆端口数量×10000Mp/s×2+千兆端口数量×1000Mb/s×2+百兆端口数量×100Mb/s×2+其他端口×端口速率×2

3. 交换机端口：光纤端口、以太网端口、GBIC、SFP、万兆模块。

光纤端口	100Base-FX 光纤端口，速率为 100Mb/s，接多模光纤。 1000Base-SX 光纤端口，速率为 1000Mb/s，接多模光纤。
以太网端口	100Base-TX 以太网端口，速率为 100Mb/s，接双绞线。1000Base-T 以太网端口，速率为 1000Mb/s，接双绞线。
GBIC	1. 是将千兆位电信号转换为光信号的接口器件，是千兆以太网连接标准。GBIC 在设计上可以为热插拔使用。目前 GBIC 基本被 SFP 取代。只要使用 GBIC 模块，就能连接双绞线、单模光纤、多模光纤的介质。还可以作为级联模块，用于交换机的级联和堆叠。 1000Base-T GBIC 模块，接超五类和六类双绞线。 1000Base-SX GBIC 模块，接多模光纤。 1000Base-LX/LH GBIC 模块，接单模光纤。 1000Base-ZX GBIC 模块，接长波光纤，适合长距离传输，可达 100km。
SFP	1. 是 GBIC 的替代和升级版本，是小型的、新的千兆接口标准。 2. 还有 10GBase-KX4（并行方式）和 10GBase-KR(串行方式)，用于背板。
万兆模块	

万兆模块

模块名称	连接介质	可传输距离
10GBase-Cx4	Cx4 铜缆（属于屏蔽双绞线)	15m
10GBase-SR	多模光纤	200m~300m，传输距离为 300m，则需要使用 50um 的优化多模（OM3）
10GBase-LX4	单模、多模光纤	多模 300m，单模 10km
10GBase-LR	单模光纤	2~10km，可达 25km
10GBase-LRM	多模光纤	使用 OM3 可达 260m
10GBase-ER	单模光纤	2~40km
10GBase-ZR	单模光纤	80km
10GBase-T	屏蔽或非屏蔽双绞线	100m

15.2 交换机工作原理

2 层交换机	2 层交换机识别数据中的 MAC 地址和转发数据到端口的功能，便于硬件实现使用 ASIC 芯片可以实现高速数据查询和转发。
3 层交换机	网络层交换机。

15.3 交换机配置

1. 路由器连接方式

（1）基于 Console 口的命令行接口（CLI）配置方式。

（2）通过 Web 界面配置。

（3）通过 Cisco Works、CAN、SDM 等软件配置。

2. CLI 转换方式

模式	访问方法	提示符	退出方法
用户模式	登录交换机之后	switch>	logout 或 quit
特权模式	在用户模式 switch>下，输入 enable（简写 en）命令	switch#	disable
全局配置模式	在特权模式 switch#下，输入 config(简写 con)命令	switch(config)#	exit 或者 Ctrl+Z
VLAN 配置模式 (VTP 透明模式下，可创建 ID>1005 的 VLAN)	在全局模式 switch（config）#下，输入 vlan vlan-id 命令，vlan-id 表示 vlan 号	Switch(config-vlan)#	(1) exit 退回到 switch (config）#; (2)Ctrl+Z 或者 end 退回到 switch#
VLAN 配置 (配置 ID 1～1005 的 VLAN)	在特权模式 switch#下，输入 Vlan database 命令	Switch(vlan)#	exit 退回到 switch#
接口配置模式	在特权模式 switch#下，输入 interface 命令	Switch(config-if)#	(1) exit 退回到 switch (config）#; (2)Ctrl+Z 或者 end 退回到 switch#
Line 接口配置模式	在特权模式 switch#下，输入 link console0 命令	Switch(config-line)#	(1) exit 退回到 switch (config)#: (2)Ctrl+Z 或者 end 退回到 switch#

3. 交换机基础配置

15.4 端口配置

1. 基本端口配置

堆叠交换机的接口标识	堆叠成员号/模块号/接口号。Gigabitethernet3/0/23 表示交换机堆叠成员 3 的端口 4 的 10/100/1000Mb/s 网口，简写为 gi3/0/23。
非堆叠交换机的接口标识	模块号/接口号，如 fa0/1。配置接口后，可通过 show interface 命令查看接口状态.

2. 端口工作模式

Access 模式	用于与计算机相连，只能运行设置一个 VLAN。Access 丢弃其他 VLAN 数据。
Trunk 模式	用于交换机之间的连接，把数据打上各类 VLAN 标签，带有标签的数据被转发到另一个交换机的 Trunk 口。
Hybrid 模式	用于交换机之间连接或者计算机连接，属于多个 VLAN，可以发送和接收多个 VLAN 的报文.
QinQ	双层标签，一般用于运营商城域网

3. 常见接口类型

接口类型	接口配置名称	简写
10/100Mb/s 网口	fastethernet	fa
10/100/1000Mb/s 网口	gigabitethernet	gi
10000Mb/s 以太网	10 gigabitethernet	te
SFP 模块千兆网口	SFP	SFP

15.5 VLAN、VTP

1. 虚拟局域网（VLAN)：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数据交换技术。有助于控制流量、减少设备投资、简化网络管理、提高网络的安全性。

2. VLAN 划分
   （1）基于端口
   （2）基于 MAC 地址
   （3）基于网络层上层协议
   （4）基于 IP 组播
   （5）基于策略

3. VLAN 配置：VLAN 配置模式、VLAN 数据库配置模式。

4. VLAN 作用：控制网络流量、提高网络安全性、灵活的网络管理。

5. VLAN 数据帧

VLAN数据帧

太网帧形式	• 有标记帧(Tagged 帧)：IEEE 802.1Q 协议规定，在以太网数据帧的目的 MAC 地址和源 MAC 地址字段之后、协议类型字段之前加入 4 个字节的 VLAN 标签（又称 VLAN Tag，简称 Tag)的数据帧。 • 无标记帧（Untagged 帧）：原始的、未加入 4 字节 VLAN 标签的数据帧。
TPID	• 2 字节，Tag Protocol ldentifier（标签协议标识符），表示数据帧类型。 • 取值为 0x8100 时表示 IEEE 802.1Q 的 VLAN 数据帧。如果不支持 802.1Q 的设备收到这样的帧，会将其丢弃。
PRI	• 3 bit，Priority，表示数据帧的优先级，用于 QoS。 • 取值范围为 0~7，值越大优先级越高。当网络阻塞时，交换机优先发送优先级高的数据帧。
CFI	• 1 bit，Canonical Format Indicator(标准格式指示位)，表示 MAC 地址在不同的传输介质中是否以标准格式进行封装，用于兼容以太网和令牌环网。 • CFI 取值为 0 表示 MAC 地址以标准格式进行封装，为 1 表示以非标准格式封装。 • 在以太网中，CFI 的值为 0。
VID	• 12 bit，VLAN ID，表示该数据帧所属 VLAN 的编号。 • VLAN ID 取值范围是 0~4095。由于 0 和 4095 为协议保留取值，所以 VLANID 的有效取值范围是 1~4094。 •交换机利用 VLAN 标签中的 VID 来识别数据帧所属的 VLAN，广播帧只在同一 VLAN 内转发，这就将广播域限制在一个 VLAN 内。
带 VLAN 标签的数据帧	• 数据帧的 Length/Type = 0x8100。

6. VTP：VLAN 中继协议又称虚拟局域网干道协议，是一种消息协议，协议，用于在 VTP 域内同步 VLAN 信息（VLAN 的添加、删除和重命名)。可以系统地增加、删除、改变 VLAN 信息，并同时更新全网交换机，而无须一台一台地配置。VTP 是通过 ISL 帧或 Cisco 专有 DTP 帧来保持 VLAN 一致性的。

7. VTP 域：又称为 VLAN 管理域，是由若干相互联系的、相同 VTP 域名的交换机组成的。

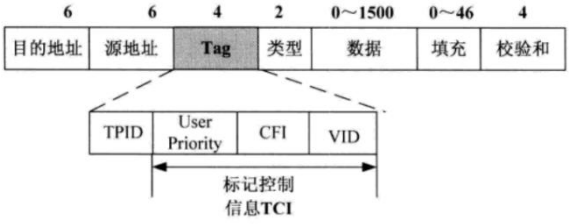
8. VTP 模式

Server（服务器）模式	生成 VTP 消息（包含 VLAN ID、VLAN 名称)，学习并转发相同域名 VTP 消息，创建、删除、更改 VLAN。交换机的默认工作模式就是服务器模式。
Client（客户端）模式	请求 VTP 消息，学习并转发相同域名的 VTP 消息，不可以创建、删除、更改 VLAN。局域网中所有的汇聚交换机和接入交换机建议配置为 Client 模式。
Transparent（透明)模式	不加入到 VTP 中,不产生 VTP 消息,不学习 VTP 消息,可以转发 VTP 消息，可以添加、删除和更改 VLAN，但只在本地有效。

9. VTP 通告：VTP 域中的交换机通过组播地址并使用中继端口发送通告。VTP 通告被相邻的交换机接收并更新它们的 VTP 和 VLAN 配置。VTP 通告包含 VLAN ID (ISL 和 802.1Q)、VTP 域名、VTP 配置版本号、VLAN 配置（包括每个 VLAN 的 MTU 大小）及帧格式。

10. VTP 修剪：通过减少不必要的广播、多播等提高网络带宽。

11. VTP 协议：IEEE 802.1q 和 ISL

<table>
<tr><td>IEEE 802.1q</td><td>俗称 dot1q。
 

IEEE802.1q 格式
<table>
<tr><th>字段</th><th>长度/位</th><th>意义</th></tr>
<tr><td>TPID</td><td>16</td><td>标记协议标识符(TPID)，设定为 0x8100,表示该帧包含 802.1q 标记</td></tr>
<tr><td>Priority</td><td>3</td><td>提供 8 个优先级（由 802.1q 定义）。当有多个帧等待发送时，按优先级发送数据包</td></tr>
<tr><td>CFI</td><td>1</td><td>规范格式指示(CFI)，0 表示以太网，1 表示 FDDI 和令牌环网。这一位在以太网与 FDDI 和令牌环网交换数据帧时使用</td></tr>
<tr><td>VID</td><td>12</td><td>VLAN 标识符(0-4095)，其中 VID 0 用于识别优先级，VID 4095 保留未用，所以最多可配置 1-4094 个 VLAN</td></tr>
</table></td></tr>
<tr><td>ISL</td><td>思科私有协议，只能在快速和千兆以太网连接中使用。Trunk 采用 ISL 格式时，VLAN ID 的最大值为 1023。</td></tr>
</table>

12. VTP 配置

15.6 STP

1. 生成树协议（STP）：是一种链路管理协议，为网络提供路径冗余，同时防止产生环路。交换机之间使用网桥协议数据单元（BPDU）来交换 STP 信息。BPDU 包含了实现 STP 必要的根网桥 ID、根路径成本、发送网桥 ID、端口 ID 等信息，具有配置 BPDU 和通告拓扑变化的功能。

BPDU的报文格式

字节	字段	描述
2	PID	协议ID，对于STP而言，该字段的值总为0
1	PVI	协议版本ID，对于STP而言，该字段的值总为0
1	BPDU Type	指示本BPDU的类型，若值为0x00，则表示本报文为配置BPDU；若值为0x80，则为TCN BPDU
1	Flags	标志，STP只使用了该字段的最高及最低两个比特位，最低位是TC（Topology Change，拓扑变更）标志，最高位是TCA（Topology Change Acknowledgment，拓扑变更确认）标志
8	Root ID	根网桥的桥ID
4	RPC	根路径开销，到达根桥的STP Cost
8	Bridge ID	BPDU发送桥的ID
2	Port ID	BPDU发送网桥的接口ID（优先级+接口号）
2	Message Age	消息寿命，从根网桥发出BPDU之后的秒数，每经过一个网桥都加1，所以它本质上是到达根桥的跳数
2	Max Age	最大寿命，当一段时间未收到任何BPDU，生存期到达最大寿命时，网桥认为该接口连接的链路发生故障。默认20s
2	Hello Time	根网桥连续发送的BPDU之间的时间间隔，默认2s
2	Forward Delay	转发延迟，在侦听和学习状态所停留的时间间隔，默认15s

2. STP 作用

（1）逻辑上断开环路，防止广播风暴的产生。

（2）当线路出现故障，断开的接口被激活，恢复通信，起备份线路的作用。

（3）形成一个最佳的树形拓扑。

3. STP 交换机接口状态：阻塞状态到侦听状态需要 20 秒，侦听状态到学习状态需要 15 秒，学习状态到转发状态需要 15 秒。

状态	用途
阻塞（Blocking）	接收 BPDU、不转发帧
侦听（Listening）	接收 BPDU、不转发帧、接收网管消息
学习（Learning）	接收 BPDU、不转发帧、接收网管消息、把终端站点位置信息添加到地址数据库（构建网桥表）
转发（Forwarding）	发送和接收用户数据、接收 BPDU、接收网管消息、把终端站点位置信息添加到地址数据库
禁用（Disable）	端口处于 shutdown 状态，不转发 BPDU 和数据帧

4. STP 工作原理：STP 首先选举根网桥（Root Bridge)，然后选择根端口（Root Ports)，最后选择指定端口(Designated Ports)。

选择根网桥	每台交换机都有一个唯一的网桥 ID(BID)，最小 BID 值的交换机为根交换机。其中 BID，是由 2 字节网桥优先级字段和 6 字节 MAC 地址字段组成。
选择根端口	选择根网桥后，其他的非根网桥选择一个距离根桥最近的端口为根端口。依据： （1）交换机中到根桥总路径成本最低的端口。 （2）直连的网桥 ID 最小的端口。 （3）直连的邻居端口 D 最小的端口。
选择指定端口	每个网段选择一个指定端口，根桥端口均为指定端口。依据： （1）到根路径成本最低。 （2）端口所在的网桥的 ID 值较小。 （3）端口 ID 值较小。

5. STP 配置：默认的交换机优先级为 32768，STP 端口的优先级默认为 128。

- BID（桥 ID）：用于标识一台交换机，由 16 位的优先级+48 位的 MAC 地址组成；优先级范围：0-65535，默认为 32768。
- PID（端口 ID）：用于标识交换机的一个接口，由 8 位优先级+8 位端口编号组成；优先级范围：0-255，默认为 128。
- 路径开销：用于衡量交换机之间路径的优劣，越低越好。

6. Trunk 端口负载均衡：通过设置 STP 端口优先级或路径成本两种方式实现 Trunk 的负载均衡。

（1）设置 STP 端口优先级实现。

（2）设置 STP 路径成本优先级实现。

7. 端口汇聚：STP 只能在设备间保证一条活动链路，而其他链路将处于备用闲置状态。端口汇聚多个物理链路，组成一个逻辑链路，成倍地提高设备间带宽。

15.7 HSRP（VRRP）

1. 热备份路由协议（HSRP）：可以配置一个交换机群集。HSRP 允许两台或多台交换机使用同一个虚拟的 MAC 地址和 P 地址，看起来多台交换机就像是一台大交换机，其实这台大交换机并不存在，只是多台互为备份的交换机。
2. VRRP（网关冗余）
3. GVRP（GARP VLAN Registration Protocol），称为 VLAN 注册协议。支持 VLAN 范围 1-4094。

• GVRP 的计时器

定时器类型	需要 GARP 动态注册的 VLAN 数量(N)			
	N<=500	500<N<=1000	1000<N<=1500	N>1500
Hold 定时器	100 厘秒（1 秒）	200 厘秒（2 秒）	800 厘秒（8 秒）	1000 厘秒（10 秒）
Join 定时器	600 厘秒（6 秒）	1200 厘秒（12 秒）	4000 厘秒（40 秒）	60O0 厘秒（1 分）
Leave 定时器	3000 厘秒（30 秒）	6000 厘秒（1 分）	20000 厘秒（3 分 20 秒）	30000 厘秒（5 分）
LeaveAll 定时器	12000 厘秒（2 分）	24000 厘秒（4 分）	30000 厘秒（5 分）	32765 厘秒（5 分 27.65 秒）

参数	缺省值
GVRP 功能	全局和接口的 GVRP 功能都处于关闭状态
GVRP 接口注册模式	normal
Hold 定时器	10 厘秒
Join 定时器	20 厘秒
Leave 定时器	60 厘秒
LeaveAll 定时器	1000 厘秒

16. 路由器基础

16.1 路由器概念

1. 路由器：路由器（Router）是连接网络中各类局域网和广域网的设备，它会根据信道的情况自动选择和设定路由，以最佳路径按前后顺序发送信号的设备。路由就是指通过相互连接的网络把信息从源地点移动到目标地点的活动。

2. 路由器基本功能：连接各类网络；隔离子网和广播，抑制广播风暴；路由；转发；网络安全；实现网络地址转换，把私有地址转换为共有地址。

3. 路由器分类

性能	高性能路由器、中端路由器、低端路由器
结构	模块结构路由器、非模块结构路由器
网络位置	核心路由器、分发路由器、接入路由器

4. 路由器组成：多种内存，ROM 存储引导软件，Flash 用来存储 IOS，RAM 是主存（存储当前运行配置，掉电消失），NVRAM 保存启动配置（备份配置，掉电不消失）。

16.2 路由器原理

1. 路由器原理：路由器的主要功能是进行路由处理和包转发。

2. 松散源路由(Loose Source Route)

松散源路由只给出 IP 数据报必须经过源站指定的路由器，并不给出一条完备的路径，没有直连的路由器之间的路由需要有寻址功能的软件支撑。

3. 严格源路由（Strict Source Route)

严格源路由选项 P 数据报要经过路径上的每一个路由器,相邻路由器之间不得有中间路由器，并且所经过路由器的顺序不可更改。

16.3 端口种类

RJ45	8 针的模块化插孔或插头。
高速同步串口 Serial	用于连接 DDN、帧中继(Frame Relay)、X.25、PSTN（模拟电话线路)等网络。
ISDN BRI	通过 ISDN 线路实现路由器与 Internet 或其他网络的远程连接。ISDN BRI 端口采用 RJ-45 标准，与 ISDN NTI 的连接使用 RJ-45 to RJ-45 直通线。
异步串口 async	适合 Modem 间的连接，实现 PSTN 的拨号接入。
Console 口	通过超级终端配置设备。
AUX 端口	外观与 RJ45 端口，内部电路不同，实现功能不同。通过 AUX 端口与 Modem 进行连接时必须借助 RJ-45 to DB9 或 RJ-45 to DB25 适配器进行转换。
E1/T1 端口	用于连接运行商网络。
光纤接口	用于连接光纤，提供于千兆速率。

16.4 路由器基础配置

4. 路由器连接方式

（4）基于 Console 口的命令行接口（CLI）配置方式。

（5）通过 Web 界面配置。

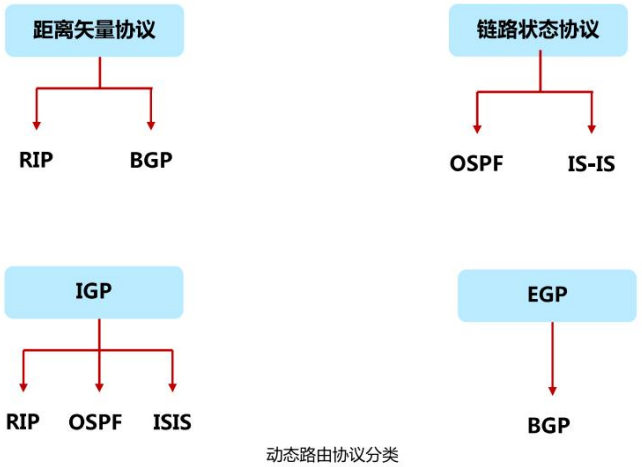
（6）通过 Cisco Works、CAN、SDM 等软件配置。

5. CLI 转换方式

模式	访问方法	提示符	退出方法
用户模式	登录路由器之后	router>	logout 或 quit
特权模式	在用户模式 router>下，输入 enable（简写 en）命令	router#	disable
全局配置模式	在特权模式 router#下，输入 config（简写 con）命令	router (config）#	exit 或者 Ctrl+Z
接口配置模式	在全局模式 router (config) #下，输入带有指定接口的 interface 命令	router (config-if)#	(1) exit 退回到 router (config）#; (2)Ctrl+Z 或者 end 退回到 router#
路由器配置模式	在全局模式 router (config) #下，输入 rip、ospf 等	router (config-router）#	(1) exit 退回到 router (config）#; (2)Ctrl+Z 或者 end 退回到 router#
Line 接口配置模式	在特权模式 router#下，输入 link console 0 命令	router (config-line）#	(1) exit 退回到 router (config）#; (2)Ctrl+Z 或者 end 退回到 routerl

6. 静态路由表：固定路由表，不会随网络的改变而改变。
7. 动态路由表：是路由器根据网络系统的运行情况自动调整的路由表。

路由协议或路由种类	相应路由的优先级
DIRECT	0
OSPF	10
IS-IS	15
STATIC	60
RIP	100
OSPF AS E	150
OSPF NSSA	
IBGP	255
EBGP	



动态路由协议分类

Destination/Mask	Proto	Pre	Cost	Flags	NextHop	Interface
192.168.12.0/24	Direct	0	0	D	192.168.12.1	GigabitEthernet0/0/0
192.168.12.1/32	Direct	0	0	D	127.0.0.1	GigabitEthernet0/0/0
192.168.13.1/32	Direct	0	0	D	127.0.0.1	GigabitEthernet0/0/1
127.0.0.0/8	Direct	0	0	D	127.0.0.1	InLoopBack0
2.2.2.0/24	RIP	100	1	D	192.168.12.2	GigabitEthernet0/0/0

路由前缀　协议　优先级　开销　标志位　下一跳　出接口

8. 路由器基本配置

16.5 RIP

1. 路由信息协议（RIP）：距离矢量路由协议，算法为动态路由算法。基于 UDP，端口号为 520。

RIPv1 报文基于广播，RIPv2 基于组播(组播地址 224.0.0.9)。RIP 路由的更新周期为 30 秒，如果路由器 180 秒没有回应，则标志路由不可达，如果 240 秒内没有回应，则删除路由表信息。（华为 300 秒）

RIP 协议的最大跳数为 15 条，16 条表示不可达，直连网络跳数为 0.每经过一个节点跳数增 1。

RIP 分为 RIPv1、RIPv2 和 RIPng 三个版本，其中 RIPv2 相对 RIPvl 的改进点有：使用组播而不是广播来传播路由更新报文；RIPv2 属于无类协议，支持可变长子网掩码（VLSM）和无类别域间路由(CIDR)；采用了触发更新机制来加速路由收敛;支持认证,使用经过散列的口令字来限制更新信息的传播。RIPng 协议支持 IPv6。

RIPv1	RIPv2
有类，不携带子网掩码	无类，携带子网掩码
广播更新	组播更新（224.0.0.9)
周期性更新(30s)	触发更新
不支持 VLSM、CIDR	支持 VLSM、CIDR
不提供认证	提供明文和 MD5 认证

2. 路由收敛：网络设备的路由表与网络拓扑结构保持一致。
   （1）水平分割
   （2）路由中毒
   （3）反向中毒
   （4）抑制定时器
   （5）触发更新
3. RIP 配置

16.6 OSPF

1. OSPF（开放式最短路径优先）：采用 SPF 算法（Dijkstra），内部网关协议（IGP），用于在单一自治系统（AS）内决策路由。基于 IP，组播方式传播。使用链路状态广播（LSA）传送给某区域内所有路由器。路由器之间交互的是链路状态信息，而不是直接交互路由。不能自动汇总。能汇总区域间路由和外部路由。

   224.0.0.5 全部路由器　　224.0.0.6 指定路由器

2. 五类报文

Hello	用于发现邻居，保证邻居之间 keeplive。默认报文发送间隔 10 秒，默认无效时间间隔为发送间隔的四倍。组播地址：224.0.0.5 Hello 包应该包含：源路由器的 RID、源路由器的 Area ID、源路由器接口的掩码、源路由器接口的认证类型和认证信息、源路由器接口的 Hello 包发送的时间间隔、源路由器接口的无效时间间隔、优先级、DR/BDR 接口 IP 地址、五个标记位、源路由器的所有邻居的 RID。
DD 或 DBD	
LSR（请求）	请求一个或多个 LSA，通告邻接路由器提供 LSA 的详细信息给发送路由器。
LSU（更新）	包含 LSA 的详细信息，一般用来响应 LSR 消息。
LSAck（应答）	用来确认已收到 LSU 消息。

3. DR/BDR 的作用是减少网络通信量、负责为整个网络生成 LSA、减少链路状态数据库的大小。

OSPF 网络类型	特点	数据传输方式
点到点网络 (Point-to-Point）	有效邻居总是可以形成邻居关系	组播地址为 224.0.0.5，该地址称为 AllSPFRouters
点到多点网络 (Point-to-Multicast）	不选举 DR/BDR，可看作是多个 Point-to-Point 链路的集合	单播（Unicast)
广播型网络 (Broadcast)	选举 DR/BDR，所有路由器和 BR/BDR 交换信息。DR/BDR 不能被抢占。广播型网络有：以太网、Token Ring 和 FDDI	DR、BDR 组播到 224.0.0.5；DR/BDR 侦听 224.0.0.6，该地址称为 AllDRouters
非广播型 (NBMA)	没有广播，需手动指定邻居，Hello 消息单播。NBMA 网络有 X.25、Frame Relay 和 ATM	单播
虚链接 (Virtual Link)	虚链路一旦建立，就不再发送 Hello 消息。应用：通过一个非 Area 0 连接到 Area 0；一个非 Area 0 连接 Area 0 的两个分段骨干区域	单播

4. OSPF 工作流

(1) 启动 OSPF 进程的接口，发送 Hello 消息。

(2) 交换 Hello 消息建立邻居关系。

(3) 每台路由器对所有邻居发送 LSA。

(4) 路由器接收邻居发过来的 LSA 并保存在 LSDB 中，发送一个 LSAcopy 给其他邻居。

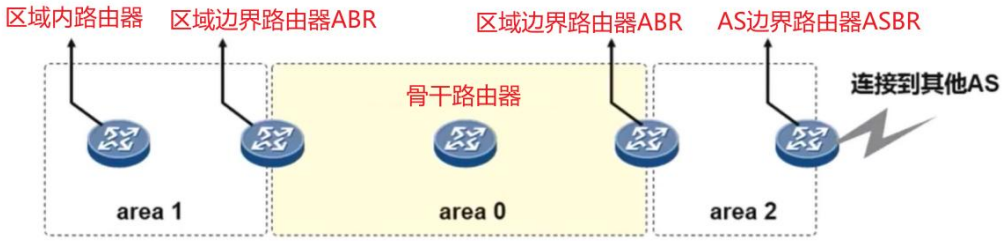
(5) LSA 泛洪扩散到整个区域，区域内所有路由器都会形成相同的 LSDB。

(6) 当所有路由器的 LSDB 完全相同时，每台路由器将以自身为根，使用最短路径算法算出到达每个目的地的最短路径。

(7) 每台路由器通过最短路径构建出自己的路由表，包含区域内路由（最优)、区域间路由、E1 外部路由和 E2 外部路由。

5. 概念

AS	自治系统（AS）是指使用同一个内部路由协议的一组网络。 公用 AS（1～64511）需要向 IANA 申请，私有 AS（64512～65535）。
IGP	内部网关协议（IGP）在同一个自治系统内交换路由信息。IGP 的主要目的是发现和计算自治域内的路由信息。 IGP 使用的路由协议有 RIP、OSPF、IS-IS、EIGRP、IGRP。
EGP	外部网关协议（EGP）是一种连接不同自治系统的相邻路由器之间交换路由信息的协议。 EGP 使用的路由协议有 BGP。
链路状态路由协议	运行距离矢量路由协议的路由器会将所有它知道的路由信息与邻居共享，当然只是与直连邻居共享。运行链路状态路由协议的路由器只将它所直连的链路状态与邻居共享。
区域 Area	OSPF 是分层路由协议，每个 AS 中，网络被分为不同的区域，每个区域拥有特定的标识符。 每个 OSPF 区域中必须包含 Area 0,



- 区域内路由器 Internal Router
- 区域边界路由器ABR Area Border Router
- 骨干路由器 Backbone Router
- AS边界路由器ASBR AS Boundary Router

	距离矢量路由协议	链路状态路由协议
发布路由触发条件	周期性发布路由信息	网络扑拓变化发布路由信息
发布路由信息的路由器	所有路由器	指定路由器(Designated Router，DR)
发布方式	广播	组播
应答方式	不要求应答	要求应答
支持协议	RIP、IGRP、BGP(增强型距离矢量路由协议）	OSPF、IS-IS

6. OSPF 配置

16.7 BGP

1. BGP：边界网关协议，一种增强的距离矢量由协议。

2. 特点：

（1）不用周期性发送路由信息。

（2）路由变化，发送增量路由（变化了的路由信息)。

（3）周期性发送 Keepalive 报文效验 TCP 的连通性。

3. 对等体：在 BGP 中，两个路由器之间的相邻连接称为对等体连接，两个路由器互为对等体。

4. BGP 消息

Open 报文	建立邻居关系。
Keepalive 报	保持活动状态，周期性确认邻居关系，对 open 报文回应。
Update 报文	发送新的路由信息。
Notification 报文	报告检测到的错误。

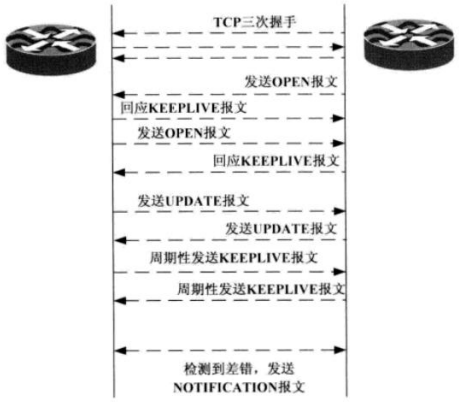


图 22-4 BGP 报文工作流程

5. BGP 基本配置

16.8 IGRP 和 EIGRP

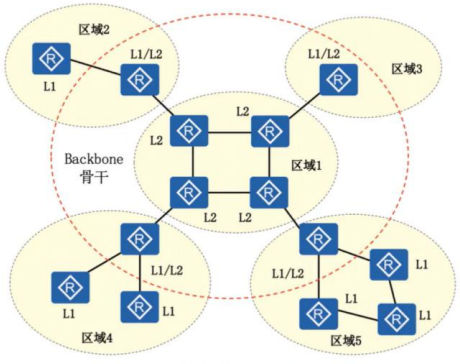
1. IGRP：思科路由协议，距离矢量路由协议，更新周期 90 秒。
2. EIGRP：思科路由协议：平衡混合路由选择协议，不定期更新。

16.9 IS-IS（中间系统到中间系统）

1. IS-IS：内部网关协议。电信运营商普遍采用的内部路由网关协议。分级的链路状态路由协议。运行在链路层。IS-IS 具有层次性，分为两层 Level-1 和 Level-2。

• Level-1(L1)是普通区域(Area)，Level-2(L2)是骨干区(Backbone)。

• 骨干区 Backbone 是连续的 Level-2 路由器的集合，由所有的 L2(含 L1/L2)路由器组成，L1 和 L2 运行相同的 SPF 算法，一个路由器可能同时参与 L1 和 L2。



IS-IS区域结构图

16.10 IPv6

1. IPv6 基本配置
2. 支持 IPv6 的协议：BGP4+、RIPng、OSPFv3。
3. VLAN 配置
4. IPv6-over-IPv4 GRE 隧道
   （1）GRE（通用路由封装协议）
   （2）IPv6-over-IPv4 隧道（6 to 4 隧道）
   （3）ISATAP 隧道（站内自动隧道寻址协议）

GRE	第三层隧道协议，隧道是一个虚拟的点对点的连接，这个接口提供了一条通路，使封装的数据报能够在这个通路上传输，并且在一个隧道的两端分别对数据报进行封装和解封。 GRE 通常和 IPSec 联合使用。
IPv6-over-IPv4	IPv6-over-IPv4 隧道是将 IPv6 报文封装在 IPv4 报文中发送，封装后，报文穿越 IPv4 网络，目的 IPv6 路由器将封装数据包解封装。
ISATAP 隧道	站内自动隧道寻址协议（ISATAP）是一种站点内部的 IPv6 网络将 IPv4 网络视为一个非广播型多路访问(NBMA）链路层的 IPv6 隧道技术，即将 IPv4 网络当作 IPv6 的虚拟链路层。

16.11 NAT

1. 静态 NAT：将合法 IP 地址和内部 IP 地址进行绑定，这种绑定的好处就是外网可以访问内网主机，内网可以访问外网。
   (1) 配置内部端口
   (2) 配置外部端口
   (3) 内外网地址建立一一对应关系

2. 动态 NAT：内部私有 IP 地址动态地转换为合法址池内的 IP 地址，但是对应关系不固定。
   (1) 配置内部端口
   (2) 配置外部端口
   (3) 定义合法 IP 地址
   (4) 定义访问列表（ACL）
   (5) 关联 ACL，并进行地址转换（全局模式下）

3. 网络地址端口转换
   (1) 配置内部端口
   (2) 配置外部端口
   (3) 定义复用的合法 IP 地址
   (4) 定义访问列表（ACL）
   (5) 关联 ACL，并进行地址转换（全局模式下）

17. 配置

17.1 防火墙

1.防火墙：包过滤防火墙、代理服务器式防火墙、基于状态检测的防火墙。

2.防火墙区域结构：内网、外网、DMZ 区。

17.2 ACL

1. 标准访问控制列表：基于 IP 地址，列表取值为 1~99，分析数据包的源地址决定允许或拒绝数据报通过。

2. 扩展访问列表：

分类	编号范围	参数
基本 ACL	2000-2999	源 IP 地址等。
高级 ACL	3000-3999	源 IP 地址、目的 IP 地址、源端口、目的端口等。
二层 ACL	4000-4999	源 MAC 地址、目的 MAC 地址、以太帧协议类型等。

17.3 防火墙配置

1. 防火墙 4 类命令模式

模式	访问方法	提示符
用户模式	登录防火墙之后	Firewall>
特权模式	在用户模式 Firewall >下，输入 enable 命令	Firewall#
全局配置模式	在特权模式 Firewall #下，输入 configure terminal 命令	Firewall(config)#
监视模式模式	防火墙开机或重启过程中按住 Esc 键，可更新操作系统映像文件恢复口令	monitor>

17.4 IPSec VPN

1. IPSec 协议组成：加密、摘要、对称密钥交换、安全协议四个部分。
2. SA 约定：安全参数索引、IP 目的地址、安全协议（AH 或 ESP）3 个部分。

3. 使用 IKE SA 分为两个阶段

构建 IKE SA（第一阶段）	（1）参数协商 • 加密算法：DES、3DES、AES 等。 • 摘要算法：MD5 或 SHA1 • 身份认证方法：预置共享密钥认证或 Kerberos 方式认证 • Diffie-Hellman 密钥交换算法：DH1、DH2、DH5、DH14、DH15、DH16 • 生存时间：<86400 秒 （2）交换密钥 （3）双方身份认证 （4）双方身份认证
构建 IPSec SA (第二阶段）	（1）参数协商 • 加密算法：DES、3DES • 摘要算法：MD5 或 SHA1 • 安全协议：AH 或 ESP • 封装模式：传输模式或隧道模式 （2）创建、配笠加密映射集并应用，构建 IPSec SA

17.5 IPSec VPN 配置

（1）启动 IKE（ISAKMP/IKE）配置

（2）配置 IKE 策略

（3）配置 IKE 身份认证（RSA 签名方式、随机 RSA 加密、预共享密钥三种方式）

（4）检测 IKE 配置

（5）配置 IPSec SA 变换集

（6）创建 ACL，对 IPSec 进行控制

（7）创建加密映射集合

（8）应用加密映射集

（9）检测命令

Router (config) # show crypto ipsec transform-set　　#显示 IPSec 变换集

Router (config) # show crypto map　　#显示 crypto maps

Router (config) # show crypto ipsec sa　　#显示 IPSec SA 的状态

1. 配置 IPsec VPN 要点（2022.11）

（1）配置 ACL，匹配感兴趣的流量，即需要 IPSec 保护的数据流。

（2）配置 IPSec 安全提议，定义 IPSec 的保护方法。

（3）配置 IKE 对等体，定义对等体间 IKE 协商时的属性。

（4）配置安全策略，并引用 ACL、安全提议和 IKE 对等体，确定对何种数据流采取何种保护方法。

（5）在接口上应用安全策略，保护相应流量。