

【软考达人】

软考资料免费获取

- 1、最新软考题库
- 2、软考备考资料
- 3、考前压轴题



微信扫一扫，立马获取



6W+ 免费题库



免费备考资料

PC版题库: ruankaodaren.com

目录

第1章	计算机系统知识	4
1.1	硬件知识	错误！未定义书签。
1.1.1	计算机结构	错误！未定义书签。
1.1.1.1	计算机组成（运算器、控制器、存储器、原码、反码、补码）	4
1.1.1.2	指令系统（指令、寻址方式、CSIC、RISC）	6
1.1.1.3	多处理器（耦合系统、阵列处理机、双机系统、同步）	8
1.1.2	存储器	9
1.1.2.1	存储介质	9
1.1.3	输入输出（I/O）系统	10
1.2	操作系统	10
第2章	系统开发和运行基础	11
2.1	软件分类	11
2.2	软件生存周期	11
2.3	软件开发模型	11
2.4	软件测试	12
2.5	软件项目管理	12
第3章	网络技术	12
3.1	网络体系结构	12
3.1.1	网络分类	12
3.2	参考模型	13
3.3	数据通信	14
3.3.1	传输介质	14
3.3.2	编码和传输	15
3.4	传输技术	15
3.5	差错控制技术	16
第4章	局域网与城域网	16
4.1	IEEE802 项目体系结构	16
4.2	802.3 和以太网	16
4.3	802.11 无线局域网	17
4.4	网桥	17
4.5	虚拟局域网 VLAN	18

第5章	广域网与接入网	18
第6章	TCP/IP 协议族	19
6.1	概述	19
6.2	网络层协议	20
6.2.1	ARP 地址解析协议	20
6.2.2	RARP 反向地址解析协议	20
6.3	IP 协议	21
6.3.1	进制转换的基础知识	21
6.3.2	IP 地址	22
6.3.3	关于 IP 的计算	23
6.3.4	IP 协议	25
6.3.5	ICMP	26
6.4	传输层协议	27
6.4.1	UDP 协议	27
6.4.2	TCP 协议	27
6.5	应用层协议	错误! 未定义书签。
第7章	交换和路由	29
7.1	交换机	30
7.1.1	交换机工作原理	30
7.1.2	交换机交换方式	30
7.1.2.1	交换机配置	30
7.2	路由	31
7.2.1	路由基础	31
7.2.2	常见路由协议	32
7.2.2.1	路由信息协议 RIP	32
7.2.2.2	内部网关路由协议 IGRP/EIGRP	33
7.2.2.3	开放式最短路径优先协议 OSPF	33
7.3	路由交换配置案例	33
7.3.1	综合案例	33
7.3.2	OSPF 的基本配置	38
第8章	网络操作系统 NOS	39
8.1	Windows 操作系统	39

8.1.1	域	39
8.1.2	活动目录的组成	39
8.2	Linux 系统	40
8.2.1	Linux 磁盘管理	40
8.2.2	文件系统	40
8.2.3	常用命令及常见配置文件格式	40
8.2.4	文件类型与权限	41
第9章	应用层协议及网络服务实现	42
9.1	DNS	42
9.1.1	基础知识	42
9.1.2	LINUX 实现 DNS	43
9.1.3	Windows 实现 DNS	44
9.2	DHCP 动态主机配置协议	44
9.2.1	DHCP 基础知识	44
9.2.2	LINUX 下 DHCP 配置	45
9.2.3	windows 下配置 DHCP	46
9.3	电子邮件	46
9.4	文件传输协议 FTP	47

计算机系统知识

计算机组成（运算器、控制器、存储器、原码、反码、补码）

■ 运算器

算术逻辑单元（ALU）、累加器、状态寄存器、通用寄存器等组成。算术逻辑运算单元（ALU）

的基本功能为加、减、乘、除四则运算，与、或、非、异或等逻辑操作，以及移位、求补等操作。计算机运行时，运算器的操作和操作种类由控制器决定。运算器处理的数据来自存储器；处理后的结果数据通常送回存储器，或暂时寄存在运算器中。与 Control Unit 共同组成了 CPU 的核心部分。

■ 控制器

是整个 CPU 的指挥控制中心，由指令寄存器 IR(Instruction Register)、程序计数器 PC(Program Counter)

和操作控制器 OC(Operation Controller)三个部件组成，对协调整个电脑有序工作极为重要。

■ 存储器

根据存储器在计算机系统中所起的作用，可分为主存储器、辅助存储器、高速缓冲存储器、控制存储器等。为了解决对存储器要求容量大，速度快，成本低三者之间的矛盾，目前通常采用多级存储器体系结构，即使用高速缓冲存储器、主存储器和外存储器。

名称简称用途特点

高速缓冲存储器 Cache 高速存取指令和数据 存取速度快，但存储容量小

主存储器 内存 存放计算机运行期间的大量程序和数据 存取速度较快，存储容量不大

外存储器 外存 存放系统程序和大型数据文件及数据库 存储容量大，位成本低

高速缓存是为了解决高速设备和低速设备相连，提高访问速度

■ I/O 部件

输入设备 向计算机输入数据和信息的设备。是计算机与用户或其他设备通信的桥梁。

输出设备（Output Device）是人与计算机交互的一种部件，用于数据的输出。

■ 原码、补码、反码

计算机储存有符号的整数时，是用该整数的补码进行储存的，0 的原码、补码都是 0，正数的原码、补码可以特殊理解为相同，负数的补码是它的反码加 1。

【考试要点】：计算，例如给予一个数值算补码和反码

■ 历年考题及解析

- 在计算机中，最适合进行数字加减运算的数字编码是（1），最适合表示浮点数阶码的数字

编码是 (2)

(1)A. 原码 B. 反码 C 补码 D. 移码

(2)A. 原码 B. 反码 C 补码 D. 移码

● (1) 不属于计算机控制器中的部件。

(1) A. 指令寄存器 IR B. 程序计数器 PC

C. 算术逻辑单元 ALU D. 程序状态字寄存器 PSW

试题解析：ALU 属于运算器，不属于控制器。答案：C

● 在 CPU 与主存之间设置高速缓冲存储器 Cache，其目的是为了 (2) 。

(2) A. 扩大主存的存储容量 B. 提高 CPU 对主存的访问效率

C. 既扩大主存容量又提高存取速度 D. 提高外存储器的速度

试题解析：Cache 是不具有扩大主存容量功能的，更不可能提高外存的访问速度。但 Cache 的访问速度是在 CPU 和内存之间，可以提高 CPU 对内存的访问效率。

答案：B

● 计算机在进行浮点数的相加（减）运算之前先进行对阶操作，若 x 的阶码大于 y 的阶码，则应将 (2) 。

(2) A. x 的阶码缩小至与 y 的阶码相同，且使 x 的尾数部分进行算术左移。

B. x 的阶码缩小至与 y 的阶码相同，且使 x 的尾数部分进行算术右移。

C. y 的阶码扩大至与 x 的阶码相同，且使 y 的尾数部分进行算术左移。

D. y 的阶码扩大至与 x 的阶码相同，且使 y 的尾数部分进行算术右移。

试题解析：为了减少误差（保持精度），要将阶码值小的数的尾数右移。

答案：D

● 在 CPU 中，(3) 可用于传送和暂存用户数据，为 ALU 执行算术逻辑运算提供工作区。

(3) A. 程序计数器 B. 累加寄存器 C. 程序状态寄存器 D. 地址寄存器

试题解析：

为了保证程序(在操作系统中理解为进程)能够连续地执行下去，CPU 必须具有某些手段来确定下一条指令的地址。而程序计数器正是起到这种作用，所以通常又称为指令计数器。在程序开始执行前，必须将它的起始地址，即程序的一条指令所在的内存单元地址送入 PC，因此程序计数器(PC)的内容即是从内存提取的第一条指令的地址。当执行指令时，CPU 将自动修改 PC 的内容，即每执行一条指令 PC 增加一个量，这个量等于指令所含的字节数，以便使其保持的总是将要执行的下一条指令的地址。

状态寄存器：用来标识协处理器中指令执行情况的，它相当于 CPU 中的标志位寄存器。

累加寄存器：主要用来保存操作数和运算结果等信息，从而节省读取操作数所需占用总线时间和访问存储器的时间。

地址寄存器：可作为存储器指针。

答案：B

● 关于在 I/O 设备与主机间交换数据的叙述，(4) 是错误的。

(4) A. 中断方式下，CPU 需要执行程序来实现数据传送任务。

B. 中断方式和 DMA 方式下，CPU 与 I/O 设备都可同步工作。

C. 中断方式和 DMA 方式中，快速 I/O 设备更适合采用中断方式传递数据。

D. 若同时接到 DMA 请求和中断请求，CPU 优先响应 DMA 请求。

试题解析：快速 I/O 设备处理的数据量比较大，更适合采用 DMA 方式传递数据。答案：C

● Cache 用于存放主存数据的部分拷贝，主存单元地址与 Cache 单元地址之间的转换方式由 (5) 完成。

(5) A. 硬件 B. 软件 C. 用户 D. 程序员

试题解析：当然是硬件啦。答案：A

● (1) 是指按内容访问的存储器。

(1) A. 虚拟存储器 B. 相联存储器
C. 高速缓存 (Cache) D. 随机访问存储器

试题解析：

相联存储器 (associative memory) 也称为按内容访问存储器 (content addressed memory)，是一种不根据地址而是根据存储内容来进行存取的存储器。

参考答案：B

● 处理机主要由处理器、存储器和总线组成。总线包括 (2) 。

(2) A. 数据总线、地址总线、控制总线 B. 并行总线、串行总线、逻辑总线
C. 单工总线、双工总线、外部总线 D. 逻辑总线、物理总线、内部总线

● 计算机中常采用原码、反码、补码和移码表示数据，其中， ± 0 编码相同的是 (3) 。

(3) A. 原码和补码 B. 反码和补码 C. 补码和移码 D. 原码和移码

参考答案：C

指令系统 (指令、寻址方式、CSIC、RISC)

■ 指令

告诉计算机从事某一特殊运算的代码 数据传送指令、算术运算指令、位运算指令、程序流程控制指令、串操作指令、处理器控制指令。

指令周期是执行一条指令所需要的时间，一般由若干个机器周期组成，是从取指令、分析指令到执行完所需的全部时间。

CPU 从内存取出一条指令并执行这条指令的时间总和。 指令不同，所需的机器周期数也不同。对于一些简单的单字节指令，在取指令周期中，指令取出到指令寄存器后，立即译码执行，不再需要其它的机器周期。对于一些比较复杂的指令，例如转移指令、乘法指令，则需要两个或者两个以上的机器周期。 从指令的执行速度看，单字节和双字节指令一般为单机器周期和双机器周期，三字节指令都是双机器周期，只有乘、除指令占用 4 个机器周期。在编程时要注意选用具有同样功能而机器指令步骤的并行。

指令流水线：将指令流的处理过程划分为取指、译码、计算操作数地址、取操作数、执行指令、写操作数等几个并行处理的过程段。这就是指令 6 级流水时序。在这个流水线中，处理器有六个操作部件，同时对这六条指令进行加工，加快了程序的执行速度。目前，几乎所有的高性能计算机都采用了指令流水线。周期数少的指令。

例如：一个指令分为三个步骤，取指 4T，分析 3T，执行 5T。则指令周期为 5T【取时间值最长的】，串

行运行 100 条指令的时间是 $100 \times (4+3+5)T=1200T$ ，并行执行 100 条指令的时间是 $99 \times 5T + (4+3+5)T=507T$

[考试要点]：指令周期运算时常考的重点

■ 寻址方式

寻址方式就是寻找操作数或操作数地址的方式。8086 提供了与操作数有关和与 I/O 端口地址有关的两类寻址方式。与操作数有关的寻址方式有七种，分别是立即寻址，寄存器寻址，直接

寻址，寄存器间接寻址，寄存器相对寻址，基址加变址寻址，相对基址加变址寻址；与 I/O 端口有关的寻址方式有直接端口寻址和间接端口寻址方式。

[考试要点]：前些年经常考，主要是寄存器寻址

■ CISC 复杂指令集和 RISC 精简指令集

RISC 具有简单高效的特色。对不常用的功能，常通过组合指令来完成。RISC 机器更适用于专用机；而 CISC 机器则更适用于通用机。

[考试要点]：考察 CSIC 和 RISC 的差异

■ 历年试题及分析

- 某指令流水线由 5 段组成，第 1、3、5 段所需时间为 Δt ，第 2、4 段所需时间分别为 $3\Delta t$ 、 $2\Delta t$ ，那么连续输入 n 条指令时的吞吐率（单位时间内执行的指令个数）

TP 为（4）。

试题解析：

TP=指令总数÷执行这些指令所需要的总时间。

执行这些指令所需要的总时间= $(\Delta t + 3\Delta t + \Delta t + 2\Delta t + \Delta t) + 3(n-1)\Delta t$

参考答案：B

- 现有四级指令流水线，分别完成取指、取作的时间依次为取、运算、传送结果四步操作。若完成上述操 $9ns$ 、 $10ns$ 、 $6ns$ 、 $8ns$ 。则流水线的操作周期应设计为（2） ns 。

（2）A. 6 B. 8 C. 9 D. 10

试题解析：取最大的那个微指令时间作为流水线操作周期。答案：D

- 若每一条指令都可以分解为取指、分析和执行三步。已知取指时间 t 取指= $4\Delta t$ ，分析时间 t 分析= $3\Delta t$ ，执行时间 t 执行= $5\Delta t$ 。如果按串行方式执行完 100 条指令需要（2） Δt 。

如果按照流水方式执行，执行完 100 条指令需要（3） Δt 。

（2）A. 1190 B. 1195 C. 1200 D. 1205

（3）A. 504 B. 507 C. 508 D. 510

试题解析：

串行执行时，总执行时间= $100 \times (t_{\text{取指}} + t_{\text{分析}} + t_{\text{执行}}) = 100 \times 12\Delta t = 1200\Delta t$ 。

流水执行的情况可以参看下图：

连续两条指令的执行时间差为 $t_{\text{执行}} = 5\Delta t$ ，

因此 100 条指令的总执行时间= $(t_{\text{取指}} + t_{\text{分析}} + t_{\text{执行}}) + 99 \times t_{\text{执行}} = 507\Delta t$ 。

答案：（2）C （3）B

- 若内存地址区间为 $4000H \sim 43FFH$ ，每个存储单位可存储 16 位二进制数，该内存区域由 4 片存储器芯片构成，则构成该内存所用的存储器芯片的容量是（4）。

（4）A. $512 \times 16\text{bit}$ B. $256 \times 8\text{bit}$ C. $256 \times 16\text{bit}$ D. $1024 \times 8\text{bit}$

试题解析：

总存储单位= $(43FFH - 4000H + 1H) = 400H = 1024$ （H 代表 16 进制）

每个存储器芯片的容量为： $1024 \times 16 / 4 = 4096$ 。

由于每个存储单位可存储 16 位二进制数，所以可以采用 $256 \times 16\text{bit}$ 或者 $512 \times 8\text{bit}$ 的芯片。最好是前者，这样系统控制比较简单。

答案：C

- 下面的描述中，（3）不是 RISC 设计应遵循的设计原则。

- (3) A. 指令条数应少一些
B. 寻址方式尽可能少
C. 采用变长指令，功能复杂的指令长度长而简单指令长度短
D. 设计尽可能多的通用寄存器

试题解析：

CISC 的特点是多采用变长指令，而 RISC 刚好相反。

答案：C

- 若内存按字节编址，用存储容量为 32K X 8 比特的存储器芯片构成地址编号 A0000H 至 DFFFFH 的内存空间，则至少需要 (1) 片。

(1) A. 4 B. 6 C. 8 D. 10

试题解析：

$DFFFFH - A0000H = 3FFFFH < 2^{18}$, $32K = 2^{15}$, 则至少需要芯片为 $2^{18} / 2^{15} = 8$ 。

答案：C

- 高速缓存 Cache 与主存间采用全相联的地址映像方式，高速缓存的容量为 4MB，分为 4 块，每块 1MB，主存容量为 256MB，若主存读写时间为 30ns，高速缓存的读写时间为 3ns，平均读写时间为 3.27ns，则该高速缓存的命中率为 (1) %。若地址更换表如下所示，则主存地址为 888888H 时，高速缓存地址为 (2) H。

地址更换表

0 38H

1 88H

2 59H

3 67H

(1) A. 90 B. 95 C. 97 D. 99

(2) A. 488888 B. 388888 C. 288888 D. 188888

试题解析：

设该高速缓存的命中率为 x ，则 $3x + 30 \times (1 - x) = 3.27$ ，解得 $x = 99\%$ 。

主存容量为 256MB，每块 1MB，则主存可以分为 $256 / 1 = 256 = 2^8$ 块，即块号为 8 位，

则主存地址的高 8 位是 88H，对应地址更换表，高速缓存地址为 188888H。

答案：(1) D (2) D

多处理器（耦合系统、阵列处理机、双机系统、同步）

■ SMP

对称多处理" (Symmetrical Multi-Processing) 又叫 SMP，是指在一个计算机上汇集了一组处理器(多 CPU)，各 CPU 之间共享内存子系统以及总线结构。相当于任何任务都平均分配到每个 CPU 执行，对于单一任务计算较为有利

非对称多处理器

每个处理器处理不同的任务，如整数运算由特定处理器处理，浮点元素按由专用处理器处理，

分工明确，适合于多种任务计算

【考试要点】：对称和 SMP 的简单区别

■ 计算机体系结构分类

SISD——单指令流单数据流

SIMD——单指令流多数据流

MISD——多指令流单数据流

MIMD——多指令流多数据流

此处考试一般都比较简单，只要记住 S 单 I 指令 M 多 D 数据即可

■ 耦合系统

紧耦合系统：通过共享主存来实现处理机间通信，处理机相互间关系紧密

松耦合系统：通过消息传递方式实现处理机间的相互通信，每个处理机是有一个独立性较强的计算模块组成

■ 双机系统

双机主从模式：一台为工作机，另外一台为备份机，正常状态工作机工作，备份机监视工作机状态，工作机故障，备份机接替工作，工作机正常后，人工或者自动的方式切换到工作机工作模式

双机互备模式：都为工作机负载，互相监视状态

存储器

存储介质

■ 存储分类

根据存储器在计算机系统中所起的作用，可分为主存储器、辅助存储器、高速缓冲存储器、控制存储器等。为了解决对存储器要求容量大，速度快，成本低三者之间的矛盾，目前通常采用多级存储器体系结构，即使用高速缓冲存储器、主存储器和外存储器。

名称简称用途特点

高速缓冲存储器 Cache 高速存取指令和数据 存取速度快，但存储容量小

主存储器 内存 存放计算机运行期间的大量程序和数据 存取速度较快，存储容量不大

外存储器 外存 存放系统程序和大型数据文件及数据库 存储容量大，位成本低

高速缓存是为了解决高速设备和低速设备相连，提高访问速度

按照存取方式分类，可分为 RAM（随机存储器，断电数据丢失，如内存）、ROM（只读存储器，

有一特例 xPROM 是可擦写只读）、SAM（串行访问存储器，如磁带）

【考试要点】：暂无

■ 存储容量

1B（Byte、字节）=8bit（位）

1KB=2¹⁰ 字节=1024 字节

1MB=1024KB

1GB=1024MB

1TB=1024GB

PB EB ZB YB NB DB 是后面的单位，知道就行

■ 高速缓存

地址映像直接看题就行，不在此赘述

例如，计算机中有一级、二级缓存，假设算法命中率为 80%，CPU 从外存调取数据的几率是
(1-80%)(1-80%)=4%

■ 磁盘阵列存储器

RAID0 级别：无容错能力，效率为单磁盘的 N 倍，利用率 100%

RAID1 级别：有容错能力，效率无提高，利用率 50%

RAID5 级别：有容错能力，效率略小于单磁盘的 N 倍，利用率 N-1/N

RAID6 级别：有容错能力，效率略小于单磁盘的 N 倍，利用率 N-2/N

输入输出 (I/O) 系统

■ 输入输出控制系统

中央处理程序控制方式，其中的中断方式是使 CPU 和外设并行工作，效率很高

直接存储器存取方式 DMA，这种方式 CPU 并未干预

输入输出处理及控制方式，

■ 常见接口

SCSI，可连接 7 个外设，支持热插拔（带点插拔）

并行端口，双向多位数据同时传送

通用接口总线

RS-232，也叫串行口，比并行口的传输距离远，DB-9 和 DB-25 都是串行口

USB，可连接 127 个设备，支持热插拔，USB1.1 为 1.5Mb/s，USB2.0 为 480Mb/s，USB3.0 为 5Gb/s

IEEE1394，串行口的一种，也叫火线

操作系统

■ RAS

通过 RAS 来衡量计算机系统

R，可靠性，一定时间内正常运行的概率

A、可用性=平均无故障时间 MTBF / (平均无故障时间 MTBF + 平均故障修复时间 MTTR)

S、可维修性

例如：两部件的可靠性分别是 R_1 和 R_2 ，串行和并行方式的总体可靠性分别是 $R_1 \cdot R_2$ 和 $1 - (1 - R_1)(1 - R_2)$

系统开发和运行基础

软件分类

系统软件，如操作系统

支撑软件，如开发工具

应用软件，如 office

实时处理软件，一般是工业软件

软件生存周期

■ 软件定义

问题定义，落实问题的性质、工程目标和规模，明白要解决什么问题

可行性研究，估计系统的成本和效益

需求分析，明确系统必须具备哪些功能，用数据字典和简要算法描述系统逻辑性

■ 软件开发

概要设计，确立总体结构和模块关系，定义模块之间的接口，设计全局数据结构，制定综合测试计划

详细设计，设计模块内的细节，如算法、数据结构和接口信息

编码和单元测试，使用程序设计语言实现模块内功能并测试该模块
综合测试

软件开发模型

瀑布模型，自顶到下的线性模型，开发后期的测试阶段才能发现问题，增加了开发的风险

快速原型模型，

增量模型，先开发核心模块，其他构件逐步附加

螺旋模型，适合于大型复杂项目

喷泉模型，面向对象的典型开发模型

结构化设计、面向对象设计

耦合度：做到高内聚（模块内）低耦合（模块间）是一个较科学的做法

程序控制的三种结构，顺序、选择、循环

面向对象方法（OO）=对象+类+继承+通过消息的通信

对象是具有特殊属性（数据）和行为方式（方法）的实体

类是具有相同属性和行为的一个或多个对象的描述

实例是类所描述的一个具体的对象

统一建模语言 UML，是一种图示建模语言，UML 表示法包括事务、关系和图三种构造块

软件测试

人工测试，也叫代码审查，可调编码错和逻辑错

机器测试——白盒测试，要完全理解程序结构和处理过程，测试逻辑路径，也称为结构测试，逻辑覆

盖是白盒测试的常用方法

机器测试——黑盒测试，测试程序的输入输出，也叫功能测试，黑盒白盒互为补充

软件调试技术一般有蛮干法、原因排除法（对分查找法、归纳法、演绎法）、回溯法

软件项目管理

软件编码规模=(最大规模+4 最可能的规模+最小规模)/6

■ 进度安排工具

关键日期表

甘特图能直观表明每个任务的计划进度和当前进度

网络图，PERT 和 CPM 都采用网络图，网络图找工期要找最长路径

软件过程能力评估，ISO9000:2000 和 CMM（软件成熟度模型），CMM 五个级别，级别三为已定义级，CMM5（5 级别）达到优化级

网络技术

网络体系结构

■ 网络计算模型

主机终端模型

对等模型

客户端/服务器模型即 C/S 即 Client/Server 模型，网络应用服务如 DNS、DHCP 一般都是 C/S 模型，属于胖客户端模型

浏览器/服务器模型即 B/S 即 Browser/Server 模型，属于瘦客户端模型

网络分类

■ 按拓扑结构划分

网络拓扑（物理拓扑指的是网络中所有计算机和通信设备、通信媒体之间的物理连接方式，逻辑拓扑指的是网络中数据逻辑性工作的方式）

总线型拓扑：耗材少，成本小，冲突多

星型拓扑：耗材多，过于依赖中间节点，便于管理

环型拓扑：单点坏网络瘫痪

树型拓扑：星型拓扑的扩展，层次化便于管理

网型拓扑：可靠性高、实现均衡负载、选路成本高

■ 按范围划分

LAN MAN WAN 等比较好记，但是大家应该结合 VLAN，WLAN 记忆

■ 协议分层

协议分层的目标是降低网络系统设计的复杂度，提高网络传输的适应性和灵活性

在同一层次中能够完成相同功能的元素成为对等实体

对等实体之间的通信必须使用相同的通信规则称之为协议

协议的构成：语法、语义、时序，语法规定了数据包的格式，语义定义如何处理，时序可忽略

■ 服务访问点 SAP

SAP 是上层调用下层服务的接口，是服务的唯一标识，比如 IP 包头的协议类型

参考模型

■ OSI 参考模型

国际标准化组织 ISO 颁布开放互联参考模型 OSI/RM，对应我国国标 9387（GB9387）

共 7 层，从下向上依次是

物理层：为数据通信提供传输介质及互连设备，传输数据单元称为比特流

数据链路层：传输的数据单元称为数据帧 Frame

网络层：使用逻辑地址进行选址，比如 IP 路由

传输层：实现端到端的流量控制

会话层：建立在传输层连接的基础上，例如远程登陆的会话管理

表示层：通信系统之间数据的表示方式，如 ASCII 码，能实现加解密，压缩解压缩如 JPEG

应用层：提供方便的接口和运行程序

■ TCP/IP 参考模型

网络接口层：对应 OSI 的物理层和数据链路层

网际层：对应 OSI 的网络层

传输层：对应 OSI 的传输层

应用层：对应 OSI 的应用层，表示层，会话层

OSI 和 TCP/IP 的比较：TCP/IP 现有协议后有模型，OSI 具有通用性

协议结构图

应用层	HTTP	FTP	SMTP	POP	TELNET	DNS	TFTP	SNMP
传输层	TCP						UDP	
网络层	ICMP		IGMP					
	IP							
					ARP		RARP	
接口层	802.x	PPP		Frame-Relay			X25	

注意：基本上没有见过的协议在应用层（我会在后面介绍其他常见的协议）

DNS 在下层默认使用 UDP，当 DNS 数据量大于 512 字节时和进行区域复制的时候使用 TCP

数据通信

■ 通信基本概念

发送信号端为信源，接收端为信宿，通信线路为信道，信道传输信号，信号有连续变化的模拟信号和离散的数字信号两种

模拟信号有三个要素，振幅、周期、相位

■ 数据通信理论

傅里叶分析：考的比较少

奈奎斯特定理：考虑的是无噪声信道，最大数据传输率 $=2H$ ，如信道带宽为 3KHZ，码元率为 4，则速率 $=2 \times 3000\text{HZ} \times \log_2(4) = 12\text{Kb/s}$

香农公式：考虑噪声的信道，信噪比 $\text{dB} = 10\log_{10}(\text{信号功率 } S / \text{噪声功率 } N)$ ，最大数据传输率 $=\text{带宽 } H \times \log_2(1 + S/N)$ ，例如给定条件带宽为 3KHZ，信噪比为 30dB，因为 $30\text{dB} = 10\log_{10}(S/N)$ ，得到 $S/N = 1000$ ，则最大数据传输率 $= 3000\text{HZ} \times \log_2(1 + 1000) = 30\text{Kb/s}$

大家最容易出现人为考虑噪声后怎么传输速度比没考虑噪声速度快，这是因为条件不同造成的

传输介质

■ 有线介质

同轴电缆：宽带同轴特性阻抗 75 欧姆，用于模拟信号传输如有线电视，采用频分多路复用 FDM，宽缆接口 AUI，细缆接口 BNC-T

双绞线，屏蔽双绞线 STP 和非屏蔽双绞线 UTP 中五类线带宽 100MHZ，速度一般 100Mbps，5 类线由四组线绕合而成，其中 1、2、3、6 可用，其他可不连接，有些设备的上连线路需要线路另一端 $1 \leftrightarrow 3$ 、 $2 \leftrightarrow 6$ 对调。抗干扰能力较弱，接口名称为 RJ-X

光纤，光源可以是发光二极管 LED（一般用在多模光纤中）和注入型激光二极管（ILD 一般用在单模光纤）

单模光纤线芯细，成本高，性能和传输距离优于多模光纤

■ 无线介质

无线电，低频善穿透障碍，高频善绕过障碍（利用电离层折射）

微波，按照直线传播，不能曲线传输需使用中继塔

卫星，和微波相同，三颗卫星可以提供全球通信服务，在 1GHZ 以上

红外线，不能穿透障碍物

编码和传输

■ 数字-数字编码

单极性码，正电压表示 1，另外一种状态表示 0

极性编码，正电压和负电压表示

非归零电平编码 NRZ-L，正电平表示 1，负电平表示 0

非归零反相编码 NRZ-I，信号电平的一次反转代表 1，电平没变化代表 0

归零码 RZ，有正电平、负电平、零电平，正电平代表 1，负电平表示 0

双相位编码

曼彻斯特编码，负电平到正电平的跳变代表 1，反之代表 0，反之亦可

差分曼彻斯特编码，比特开始位置没电平跳变表示 1，有电平跳转表示 0

双极性编码，零电平代表 0，正负电平表示 1，连续的 1 必须跳转

数字-模拟编码

幅移键控 ASK，容易受噪声干扰

频移键控 FSK，容易受到介质带宽的影响

相移键控 PSK，例如 8 相位则依次可以发送 3 比特= $\log_2(8)$

正交幅调 QAM，是 ASK 和 PSK 结合

传输技术

■ 多路复用技术

频分多路复用 FDM：带宽利用率高，CATV 使用 FDM

时分多路复用 TDM：统计时分多路复用效率高于同步时分多路复用，例如 10 个 9.6Kb/s 信道时分多路复用，每信道利

用率 70%，控制开销 5%，则复用带宽为 $10 \times 9.6 \times 70\% / (1-5\%)$

波分多路复用 WDM，光纤通信技术中使用

差错控制技术

误码率为错误的码值/传输的码值，常见的有检错码如奇偶校验码和 CRC 码和纠错码如海明码
奇偶校验码很少考

海明码：编码规则，插入数据的 1、2、4、8、16 位置，需要插入码元数 K，原数据码数+K<=2^K，右边的位置是第一位，

校验时从 n 位开始，选择 n 位，跳过 n 位，选择 n 位，所有选择的位加起来应该是偶数个 1。

CRC 码，循环冗余校验码，CRC 通过模 2 运算，相当于异或运算，多项式如 X^4+X^2+1 ，数据是 100011011，则用

1000110110000 和 10101 取模（数据后加 4 个 0，因为多项式最高次为 4，多项式的二进制 10101）常见多项式有

CRC-32: $G(X)=X^{32}+X^{26}+X^{23}$

CRC-CCITT: $G(X)=X^{16}+X^{12}+X^5$

CRC-16: $G(X)=X^{16}+X^{15}+X^2$

磁盘驱动器用 CRC-16，以太网使用 CRC-32

局域网与城域网

IEEE802 项目体系结构

数据链路层	以太网	802.2 逻辑链路控制						LLC 子层
物理层		<u>802.3CSMA/CD</u>	802.4 令牌总线	802.5 令牌环	FDDI	<u>802.11 无线局域网</u>	802.15 无线个人网	MAC 子层

使用相同的 LLC，802.1 定义了体系结构与传输介质无关的部分集中在 LLC 子层

MAC 子层负责数据帧的封装与解封装、帧的校验

802.3 和以太网

■ 以太网工作原理

以太网采用 CSMA/CD 【带冲突检测的载波侦听多路访问】，规则是 先听后发、边听边发、冲突停止、随机延迟后重发

CSMA 三种类型

非减持 CSMA：有冲突随机延迟时间到再监听，媒体利用率低

1-坚持 CSMA：只要媒体空闲，站点就立即发送，冲突不可避免，以太网采用的方式

P-坚持 CSMA：是非坚持和 1 型坚持的折中

■ 以太网帧格式

物理层		数据链路层				
前导码	帧界定	目标 MAC	源 MAC	类型/长度	数据	帧校验
7 字节	1 字节	6 字节	6 字节	2 字节	46-1500 字节	4 字节

MAC 地址是物理地址，由 48bit 组成，前 24 位表示厂商信息，后 24 位表示产品 ID，第 8 位为 0 表示单播地址，第 8 位为 1 表示组播地址，表示方便采用十六进制表示。

如，0000 0000 0100 0100 0100 0100 0100 0100 0100 0100 1111 写为 00-44-44-44-44-F，这是单播地址，第八位为 0，通过十六进制判断是否单播可判断十六进制表示的第 2 位如果为偶数就是单播，奇数为组播。十六进制最大值为 F

类型/长度为上层协议的 SAP

数据最小为 46 字节，源和目标 MAC+类型+帧校验+数据>=64 字节，小于 64 字节称之为碎片交换机通常会丢弃碎片，

数据最大为 MTU【最大传输单元】，路径 MTU 是数据经过完整路径中 MTU 最小为依据

帧校验只有检错没有纠错能力，采用 CRC-32

以太网都采用相同的帧格式，由于速度变快，网络跨度变短

802.11 无线局域网

802.11 采用 CSMA/CA

■ 802.11 工作标准

802.11 使用 2.4GHZ 频段，速度为 1Mbps 或 2Mbps

802.11a 使用 5GHZ 频段，使用 OFDM 调制，支持 54Mbps

802.11b 使用 2.4GHZ 频段，速度为 11Mbps，支持 WEP 对等加密

802.11g 使用 2.4GHZ 频段，使用 CKK 和 OFDM 调制，支持 54Mbps

■ 无线网络的拓扑

对等网络

Ad-hoc

网桥

网桥用于连接不通的局域网，实现帧格式的转换

网桥分为透明网桥和源路由网桥：透明网桥是由网桥自己决定路由选择，源路由网桥认为每个帧的源节点知道目的节点是否在同一网段，能获取最佳路径

交换机是一个多接口的网桥

使用交换机可以分割冲突域，但是不能分割广播域

虚拟局域网 VLAN

■ VLAN 优点

切割广播域，减少广播提高网络性能

不通 VLAN 在不同广播域，增加网络安全
使网络易于维护，更具逻辑性

■ VLAN 划分

根据端口划分：静态 VLAN

根据 MAC 地址划分，动态 VLAN，需要一台 VMPS 服务器

根据网络层地址或协议划分，动态 VLAN

根据 IP 组播地址划分，动态 VLAN，可以跨网段

根据策略划分，动态 VLAN

■ VLAN 封装模式

802.1Q：在以太网帧的源 MAC 和类型长度中增加 4 字节的 VLAN 标记，是通用格式

ISL：在以太网帧前增加 26 字节的 VLAN 标记，CISCO 专有

■ VLAN 编号

VLAN 1 默认存在，不能删除，所有端口默认都出在 VLAN 1 中

VLAN 1002 - 1005 预留给令牌网络

ISL 模式下最大 VLAN 编号为 1023

广域网与接入网

■ 数据链路层协议

HDLC 高级数据链路控制，帧格式由 6 个字段组成，所有帧以 01111110 表示开始和结束也叫 F 标识

SLIP 串行线路 IP 协议

PPP 点对点协议，PPP 提供 PAP2 次握手和 CHAP3 次握手两种协议进行验证

■ 接入网方式

PSTN 公共交换电话网，使用 RS-232 标准接口连接 DTE 和 modem，使用 PPP 协议

X.25 采用面向连接的虚电路通信，支持永久虚电路 PVC 和交换虚电路 SVC

帧中继网 Frame Relay，提供面向连接的数据链路层通信，支持 PVC 和 SVC

■ 电信数字通信系统

数字数据网 DDN，提供 PVC

T1 载波传输速率为 1.536Mb/s，使用 TDM 由 24 个 DS0 复用组成，T2=4T1 T3=6T2 T4=7T3

E1 载波传输速率为 2.048Mb/s，使用 TDM 由 32 个信道复用，0 和 16 信道用于控制，E4=4E3=16E2=64E1

■ SONET 和 SDH

SONET 同步光纤网络使用 OC 描述数据速率，OC-1 为 51.84Mb/s OC-3=155.520Mb/s

SDN 同步数字序列使用 STM 描述数据速率，STM-1=OC-3，采用双向环网络，拥有自愈功能

■ 综合业务数字网 ISDN

宽带综合业务数字网 B-ISDN，使用组播，基于 ATM

窄带综合业务数字网 N-ISDN，2B+D 通道，B 通道 64Kbps，D 通道 16Kbps

■ ATM 异步传输模式

ATM 传输的基本载体为信元，信元由 5 个字节信头和 48 字节信息字段组成，共 53 字节

ATM 协议结构，历年考的不多，后期补充

■ xDSL 用户数字线路

对称用户数字线路指上传下载速度相同的，除下面写的三种，其他的都是对称

非对称用户数字线路指上传下载速度不同，如 ADSL，G-lite，VDSL

其中 VDSL 速度最快

ADSL 使用 频分多路复用 FDM，所以在客户端存在分离器，远端存在 POTS 分离器和 DSLAM【接入 internet】

■ HFC 混合光纤同轴电缆网

主干线路采用光纤，接入采用同轴电缆，使用 CATV 传输，信道复用使用 FDM 频分多路复用，需要使用 Cable Modem 电缆调制解调器调制信号

TCP/IP 协议族

概述

ARPA 是 TCP/IP 的前身，NSF 是 TCP/IP 的骨干组成

先有协议后形成模型

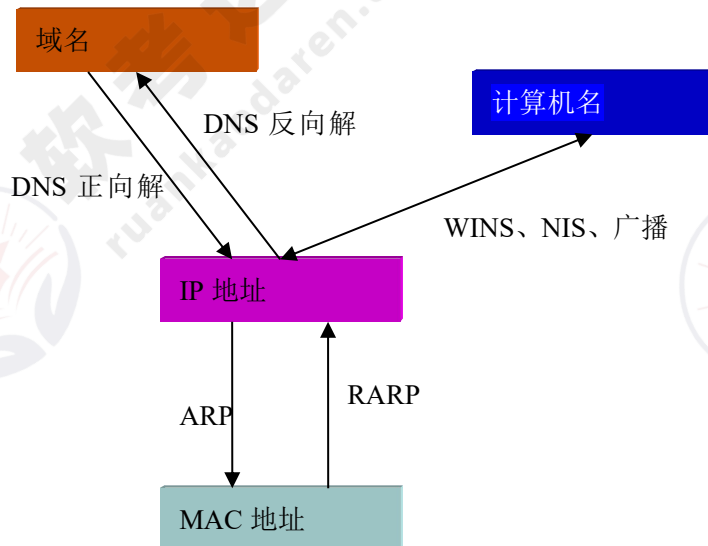
协议分层图参看前面

网络层协议

ARP 地址解析协议

处于网络层偏下层，实现 IP 地址和 MAC 地址的转换

计算机中名字和地址转换图



■ ARP 工作原理

首先发送端主机检查自己的 ARP 缓存列表中是否有接收端主机信息，这个列表的生存周期为 300S，如没有则广播发送 ARP request 【包内包含发送端主机 IP 和 MAC 和接收端主机 IP】，接收端主机返回 ARP response 单播并将发送端主机的 IP 和 MAC 映射关系缓存，ARP 病毒利用计算机根据 ARP Response 更新缓存的工作机制传播，中病毒计算机发送伪装的 ARP Response 包【如 IP 是网关地址，而 MAC 则为中病毒主机或者全 1 的广播地址】。

■ ARP 缓存操作

C:\>arp -a 查看本机缓存列表

C:\>arp -d 删除缓存列表

C:\>arp -s IP 地址 MAC 地址 绑定静态的 IP 和 MAC 映射，静态绑定优先级高于动态

RARP 反向地址解析协议

RARP 用于将物理地址解析为逻辑地址

主要用于无盘工作站启动中

IP 协议

■ 网络层功能

定义了 IP 地址
定义了 IP 包格式
实现了路径选择

进制转换的基础知识

二进制：0 和 1 表示

八进制：0、1、2、3、4、5、6、7 表示

十进制：0、1、2、3、4、5、6、7、8、9 表示

十六进制：0、1、2、3、4、5、6、7、8、9、A、B、C、D、E、F 【A 为 10、B 为 11、C 为 12、D 为 13、E 为 14、F 为 15】表示

■ 二进制换十进制

一个 1, N 个 0 为 2^N

N 个 1 为 2^N-1

如：10010111 $=2^7+2^4+2^3-1 = 151$

10000000 2^7 128

+10000 $+2^4$ 16

+111 $+2^3-1$ 7

■ 十进制转二进制

记住几个特殊值，即 $2^0=1$, $2^1=2$, $2^2=4$, $2^3=8$, $2^4=16$, $2^5=32$, $2^6=64$, $2^7=128$, $2^8=256$, $2^9=512$, $2^{10}=1024$,

所有的十进制数字都拆解为 2 的 N 次方相加即可

如：163= $128+32+2+1=10000000+100000+10+1=10100011$

拆解计算： $2^{12}=2^{10}*2^2=1024*4=4096$

■ 二进制、八进制、十进制、十六进制的关系

一个八进制位占三个二进制位，一个十六进制位占四个二进制位

如一个十进制数 135 分别转换为二进制、八进制、十六进制

135 十进制 (135)₁₀

=128+4+2+1

=10000111

=010 000 111

=2 0 7

=1000 0111

=8 7

二进制

从右向左每 3 位表示一个八进制位，不够 3 位补 0

八进制数位 (207)₈

从右向左每 4 位表示一个十六进制位，不够 4 位补 0

(87)₁₆

IP 地址

IP 是层次化的逻辑地址，MAC 是无层次化

IP 地址=网络地址 NetID+主机地址 HostID

网络地址相同的两台主机在一个物理网络可直接通信，网络地址不同的两台主机需通过路由器转发通信

IP 地址是 32 位地址，采用点分十进制方式表示，每位为用 “.” 分割

■ IPV4 地址分类

类别	第一个字节范围	第一字节	第二字节	第三字节	第四字节	默认子网掩码
A 类	1-126	0xxxxxxx				255.0.0.0
B 类	128-191	10xxxxxx				255.255.0.0
C 类	192-223	110xxxxxx				255.255.255.0
D 类	224-239	1110xxxxx	组播地址			
E 类	240-255	1111xxxxx	保留用于实验			IPV6 前身

灰色部分为网络地址部分，橘色部分为主机地址部分，每字节用十进制表示最大为 255

■ 子网掩码

用于标识网络地址和主机地址

对应的网络地址部分用 1 表示，对应的主机地址部分用 0 表示

IP 十进制表示	130	3	5	8
IP 二进制表示	10000010	00000011	00000101	00001000
子网掩码二进制	11111111	11111111	00000000	00000000
子网掩码十进制	255	255	0	0
说明	第一字节处于 128-191，属于 B 类地址，默认网络地址为前两个字节，用灰色部分表示，橘色部分表示主机地址			

■ 特殊 IPV4 地址

名称	地址范围	备注
本网络	0.0.0.0	能作为源地址，不能作为目标地址
有限/受限广播地址	255.255.255.255	本物理网络内全广播，只能作为目标地址
网络地址	网络地址+全 0 主机地址	如 130.3.0.0
直接广播地址	网络地址+全 1 主机地址	本逻辑网段广播，只能作为目标地址，如 130.3.255.255

回环地址	127.x.x.x	本机 TCP/IP 测试
私有地址	10.x.x.x	
	172.16.x.x-172.31.x.x	
	169.254.x.x	微软系统中，当主机自动获取 IP 失败后选择此 IP
	192.168.x.x	
网络地址和广播地址不用在节点上，只是一种表示方法		

关于 IP 的计算

VLSM：可变长子网掩码，将网络 ID 延长达到把大的网络切割为小的网络，也叫切割子网，用以提高地址的利用率

■ VLSM 均等划分

如，给定一个地址，平均划分为 5 个子网，求出每个子网范围，每个子网的网络地址、广播地址、可用主机个数、子网掩码

步骤	表示	划分规则	备注
1	IP 十进制	196.129.17.0/24 或 196.129.17.0/255.255.255.0	给定一个网络地址，默认子网掩码为 24 位长即 255.255.255.0
2	二进制	11000100.10000001.00001001.00000000	
3		需延长 K 位， $2^K \geq 5$ ，则 K 取值为 3，即延长 3 位，延长的 3 位有如下 8 种组合，任意用其中 5 种即可	
4		11000100.10000001.00001001.00000000 前三字节可忽略，最后一字节的范围是 00000000-00011111 子网掩码：11100000 其中 00000000 为本子网网络地址【主机 ID 全为 0】 其中 00011111 为本子网广播地址【主机 ID 全为 1】	有效范围： 196.129.17.1-196.129.17.30 子网掩码：255.255.255.224 网络地址：196.129.17.0 广播地址：196.129.17.31
		11000100.10000001.00001001.00100000 前三字节可忽略，最后一字节的范围是 00100000-00111111 子网掩码：11100000 其中 00100000 为本子网网络地址【主机 ID 全为 0】 其中 00111111 为本子网广播地址【主机 ID 全为 1】	有效范围： 196.129.17.33-196.129.17.62 子网掩码：255.255.255.224 网络地址：196.129.17.32 广播地址：196.129.17.63
	同上	11000100.10000001.00001001.01000000	196.129.17.65-196.129.17.94
		11000100.10000001.00001001.01100000	196.129.17.97-196.129.17.126
		11000100.10000001.00001001.10000000	196.129.17.129-196.129.17.158

		11000100.10000001.00001001.10100000	196.129.17.161-196.129.17.190
		11000100.10000001.00001001.11000000	196.129.17.193-196.129.17.222
		11000100.10000001.00001001.11100000	196.129.17.225-196.129.17.254
5	总结	<p><u>延长 K 位，可切割出 2^K 个子网，每个子网可用主机个数为 $2^{(32-\text{原始掩码长度}-K)-2}$，</u></p> <p><u>此例中为 $2^{(32-24-3)-2}=30$【减去 2 是因为每个子网都有一个网段地址和广播地址】</u></p>	

■ VLSM 不均等划分

不均等划分建议先满足大子网，再划小子网

如：给定 196.129.17.0/24 网段，需要划分给 A 部门为 100 台主机，B 部门 60 台主机，C 部门 30 台主机，D 部门 25 台主机。

步骤	划分规则	结果
1、A 部门 100 台主机，主机 ID 应满足 $2^M - 2 \geq 100$ ，M 取值为 7，则主机 ID 留 7 位即可，因为子网掩码延长到第四个字节，前三个字节忽略	第四个字节为 00000000 后七位为主机地址 00000000 有效范围 00000001 至 01111110 子网掩码 10000000 网络地址 00000000 广播地址 01111111	196.129.17.1 196.129.17.126 255.255.255.128 196.129.17.0 196.129.17.127
2、B 部门 60 台主机，主机 ID 应满足 $2^M - 2 \geq 60$ ，M 取值为 6，则主机 ID 留 6 位即可，划分 A 时延长的 1 位网络 ID 用 0 表示，则此处得用 1 开头，需延长 2 位做为网络 ID	第四个字节为 10000000 后六位为主机地址 10000000 有效范围 10000001 至 10111110 子网掩码 11000000 网络地址 10000000 广播地址 10111111	0 开头已经被 A 部门用完 196.129.17.129 196.129.17.190 255.255.255.192 196.129.17.128 196.129.17.191
3、C 部门 30 台主机，主机 ID 应满足 $2^M - 2 \geq 30$ ，M 取值为 5，则主机 ID 留 5 位即可，划分 B 时延长的 2 位网络 ID 用 10 表示，则此处得用 11 开头，需延长 3 位做为网络 ID	第四个字节为 11000000 后五位为主机地址 11000000 有效范围 11000001 至 11011110 子网掩码 11100000 网络地址 11000000 广播地址 11011111	10 开头已经被 B 部门用完 196.129.17.193 196.129.17.222 255.255.255.224 196.129.17.192 196.129.17.223
4、D 部门 25 台主机，主机 ID 应满足 $2^M - 2 \geq 25$ ，M 取值为 5，则主机 ID	第四个字节为 11100000 后五位为主机地址 11100000 有效范围 11100001 至 11111110	110 开头已经被 B 部门用完 196.129.17.225 196.129.17.254

留 5 位即可，划分 C	子网掩码	11100000	255.255.255.224
时延长的 3 位网络 ID	网络地址	11100000	196.129.17.224
用 110 表示，则此处	广播地址	11111111	196.129.17.255
得用 111 开头，需延			
长 3 位做为网络 ID			

由以上知识引申：如一个点到点的网络，为了避免 IP 资源浪费，应该采用的子网掩码长度为？点到点网络需要两个主

机 IP 即可，即一个网段 2 个 IP， $2^{\text{主机 ID 数 } M-2} \geq 2$ 即可，则 M 为 2，留 2 位主机 ID，则网络 ID 为 30 位，子网掩码为 255.255.255.11111100 即 255.255.255.252

■ CIDR

无类域间路由或者叫路由汇聚

通过缩短子网掩码长度达到将小网络合并为大的超网

汇聚思路：将给出的十进制 IP 段转换为二进制表示，找相同部分即可

如：177.7.97.0/24 177.7.99.0/24 177.7.104.0/24 177.7.112.0/24 汇聚后的地址为？

前 2 个字节完全相同，可以忽略，将第三个字节转换为二进制

97=64+32+1 =01100001

99=64+32+2+1 =01100011

104=64+32+8 =01101000

112=64+32+8+4 =01101100

相同的部分用蓝色标识，蓝色部分即为网络 ID 部分，则汇聚后的网络地址为

177.7.01100000.0/255.255.11100000.0 即 177.7.96.0/27

■ IPV6 地址

128 位地址，用每 16 位冒号分隔表示，0000：0000：00C6：0000：0000：0000：F000：3433/64

压缩写法，一组或多组为 0 时将多个 0 压缩为双冒号：：，只能压缩一段，一组前为 0 时可省略

以上 IP 可写为 0：0：C6：：F000：3433/64

IPV6 首部 40 字节

■ IPV6 三种地址类型

单播地址（Unicast）：其中 0：0：0：0：0：0：0：1 表示回环地址，做本机测试

多播地址（Multicast）：以 1111 1111 开始的即 FF 开头

任意播地址（Anycast）：

IP 协议

■ IP 协议特点

不可靠

非面向连接尽最大努力投递，当 IP 包中生存周期 TTL 为 0 时丢弃数据包

■ IP 数据报格式【每行 32 位】

0-3	4-7	8-11	12-15	16-19	20-23	24-27	28-31	
版本： IPV4 0100 IPV6 0110	<u>首部长度：</u> <u>以 4 字节</u> <u>为单位</u> 最大值 1111，则 <u>首部最大</u> <u>为</u> <u>15*4=60</u> <u>字节，默</u> <u>认 20 字</u> <u>节</u>	服务类型： 对上层提出的服务质量		IP 数据报总长度：以字节为单位，最大值 1111111111111111=2^16-1=65535 <u>所以一个 IP 数据报最大为 65535 字节</u>			<u>默认区报</u> <u>头为选项</u> <u>之前的 5</u> <u>行即 20 字</u> <u>节，选项最</u> <u>多 为</u> <u>60-20=40</u> <u>字节</u>	
标识：IP 重组需要				标志：		片偏移：		
<u>生存周期 TTL：每过</u> <u>一路由器减 1，TTL</u> <u>为 0 时路由器丢弃</u>		<u>协议号：提供上层</u> <u>SAP，6 表示 TCP，</u> <u>17 表示 UDP</u>		头校验和： <u>采用 CRC-16</u>				
源 IP 地址								
目的 IP 地址								
选项						填充域		
数据								
								数据区

ICMP

■ ICMP

因特网控制信息协议

Ping 命令使用 ICMP 协议位于网络层偏上，封装在 IP 中

■ ICMP 报文分为三类：

差错报文：【目标不可达（3）、超时（11）、参数出错（12）】控制报文：【源抑制（4 当路由器因拥塞丢掉数据包时）、重定向（5 动态选择最佳路由）】

请求/应答报文：【回应请求/应答（0/8 如使用 ping 命令时）、路由器请求/通告请求/应答（10/9 初始化路由表）、时间戳请求/应答（13/14 计算往返时间同步时钟）、地址掩码请求/应答（17/18 区分网段）】

传输层协议

传输层负责端到端传输

■ 端口

端口是上层分用的 SAP，用以区分不同应用

端口分为保留端口【也叫知名端口，端口号小于 1024】和动态端口【也叫用户端口，端口号是 1024-65535】

插口 Socket=IP+端口

UDP 协议

用户数据报协议

■ UDP 协议特点

不可靠【协议分层中，下层不可靠可靠性由上层协议保证】

非面向连接【无须建立连接效率高】

UDP 协议包头 8 个字节，校验和字段可选

■ UDP 知名端口

端口号	服务名	备注
<u>53</u>	<u>DNS</u>	<u>默认 DNS 均使用 UDP，当大于 512 和区域复制时使用 TCP</u>
67/68	BOOTP/DHCP	引导协议
<u>69</u>	<u>TFTP</u>	<u>简单文件传输协议，每包 512 字节，结尾加 1 字节结束标记</u>
<u>161</u>	<u>SNMP</u>	<u>简单网络管理协议</u>
<u>162</u>	<u>SNMP-TRAP</u>	<u>简单网络管理协议陷阱-自陷协议</u>
4000	QQ	QQ 客户端，每开一 QQ 端口号+1
8000	QQ	QQ 服务器端

TCP 协议

传输控制协议

■ TCP 协议特点

可靠的

面向连接的

全双工数据流

■ TCP 协议数据段结构

0-3	4-9	10-15					16-28	29-31	段头
源端口号						目的端口号			
<u>序列号</u>									
<u>确认序号</u>									
<u>TCP 段头</u>	保留	U	<u>A</u>	P	<u>R</u>	<u>S</u>	<u>F</u>	窗口大小	
<u>长度, 4 字</u>		R	<u>C</u>	S	<u>S</u>	<u>Y</u>	<u>I</u>		
<u>节为单位, _</u>		G	<u>K</u>	H	<u>T</u>	<u>N</u>	<u>N</u>		
<u>默认 20 字</u>									
<u>节</u>									
校验和						紧急指针			
选项								填充	
数据									

序号累计递增，第一次发送数据序号为 100，则第二个数据序号为 101

确认序号为对对方发送数据的确认，当 ACK 为 1 时确认序号才有用，确认序号是对方发送数据的序号+1

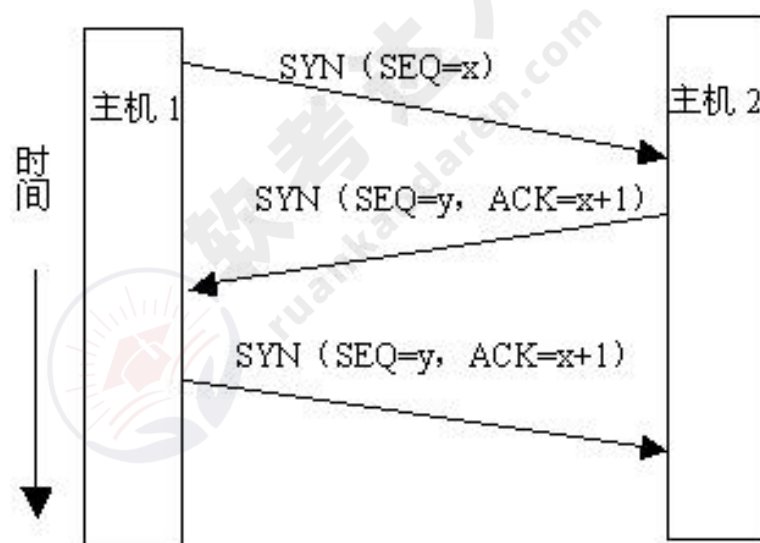
ACK: 当 ACK 为 1 时说明数据段是确认对方

RST: 当 RST 为 1 时重新建立连接

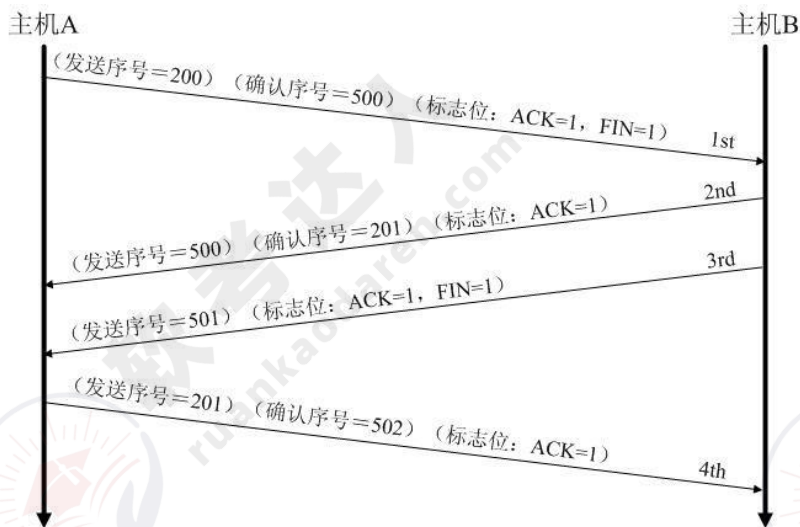
SYN: 同步, SYN 为 1 时建立连接

FIN: FIN 为 1 时断开连接

■ TCP 建立连接的三次握手



■ TCP 断开连接的四次握手



TCP 使用滑动窗口实现流量控制

■ TCP 知名端口

端口号	服务名	备注
<u>20</u>	<u>FTP-DATA</u>	<u>FTP 数据连接</u>
<u>21</u>	<u>FTP</u>	<u>FTP 控制连接</u>
23	TELNET	远程登录
<u>25</u>	<u>SMTP</u>	<u>发送邮件</u>
<u>53</u>	<u>DNS</u>	<u>大于 512 和区域复制时使用 TCP</u>
<u>80</u>	<u>HTTP</u>	
<u>443</u>	<u>HTTPS</u>	<u>HTTP+SSL 安全 HTTP 协议</u>
<u>110</u>	<u>POP3</u>	<u>邮局协议, 接收邮件</u>
143	IMAP	协同 接收邮件
3128 8080	HTTP 代理	

交换和路由

■ 集线器 HUB

物理层连接设备, 共享带宽, 集线器连接的所有节点在一个冲突域中

网络设备里的操作系统称之为 IOS,

■ 网络设备的连接方式

CON: 通过 console 口连接 (DB-9 转 RJ-45), 使用仿真终端操作, 速率 9600bps

telnet: 远程登录, telnet 明文传输, 不安全

TFTP: 上传下载配置信息

SNMP:

VPN:

SSH: 远程登录, 密文传输, 安全

交换机

交换机工作原理

交换机工作于数据链路层, 使用 ASIC 芯片转发数据, 速度快

交换机上连接的设备独享带宽, 交换机上每个端口都是一个独立的冲突域【交换机分隔冲突域】

根据端口和 MAC 映射表对照数据帧的目的 MAC 地址转发数据、端口 MAC 地址映射表的形成是自动学习的过程, 自动

学习是根据源 MAC 地址学习, 若端口 MAC 地址映射表中不存在数据帧所对应的条目, 则向除数据进入端口之外的所有端

口广播, 端口 MAC 地址映射表生存周期为 300S

查看端口地址映射表的命令 SW1#show mac-address-table

交换机交换方式

静态交换和动态交换【动态交换是一帧一连接】

存储转发交换【支持不同速度端口之间的转换】

切入交换【也叫直接交换, 稳定网络中工作效率高】

碎片丢弃交换【检查帧是否够 64 字节, 小于 64 字节作为碎片丢弃】

全双工交换【发送和接受数据帧同时进行, 不受 CSMA/CD 约束】

交换机配置

■ 交换机的模式及模式间转换

提示符	当前模式	命令
hostname>	用户模式	输入 enable 进入特权模式
hostname#	特权模式	输入 config terminal 进入全局配置模式
hostname(config)#	全局配置模式	输入 interface f0/1 进入接口模式
hostname(config-if)#	接口配置模式	输入 exit 命令回到上一模式
hostname(config)#	全局配置模式	输入 end 命令回到特权模式
hostname#	特权模式	输入 vlan database 进入 VLAN 配置模式

hostname(VLAN)# hostname#	VLAN 配置模式 特权模式	输入 end 命令回到特权模式 输入 setup 命令进入设置配置模式
------------------------------	-------------------	--

■ VLAN 线路模式

Access 模式：接入模式，一条线路承载一个 VLAN 通信

TRUNK 模式：干道模式，一条线路承载多个 VLAN 通信

■ VTP

VTP：VLAN 干道协议，简化 VLAN 操作

VTP 三种模式：服务器 SERVER 模式可以配置 VLAN 参数、透明 TRANSFER 模式只传递服务器的 VLAN 参数但不学习、

客户端 CLIENT 模式学习服务器的 VLAN 参数，默认情况下所有交换机在透明模式下。

■ STP

生成树协议，进行均衡负载，将不同 VLAN 的通信分配到不同的 TRUNK 链路上，同时避免网络环路

默认情况下，VLAN 在 TRUNK 端口上的权值【port-priority】为 128，数字越小优先级越高，默认情况下交换机 STP 路径值【cost】为 19，数字越大优先级越低

■ STP 步骤

选择根桥，选择桥 ID 最小的【桥优先级+桥 MAC 地址，默认桥优先级都是 32768，所以 MAC 越小优先级越高】

选根端口，在非根桥交换机上选根端口，首选依据是 cost 值，cost 相同比较端口，端口越小优先级越高

路由

路由基础

路由选择是网络层功能，所以路由器工作于网络层，也称之为网关

路由器根据 IP 数据报中的目的 IP 地址对应路由器中的路由表进行寻径

数据通过网络传输时，源 MAC 和目的 MAC 会改变但 IP 不会改变

■ 路由表

路由匹配顺序是从子网掩码最长匹配，如单机路由高于网段路由高于默认路由

■ 路由类型

直连路由：端口设置 IP 并且处于激活状态时形成直连路由，用 C 表示

静态路由：非直连网段手工设置路由条目，用 S 表示

默认路由：静态路由的特例，一般用在末梢网络，优先级最低，用 S*表示

动态路由：路由协议根据网络变换动态修改路由表的信息，分为两种【RIP 是距离矢量路由协议 (D-V)的典型代表，

OSPF 是链路状态协议 (L-S)的典型代表】，其中 RIP 用 R 表示，OSPF 用 O 表示

■ 路由选择算法

距离矢量 D-V，每一路由器只清楚到达目的节点需转发的下一站地址，收敛速度慢

链路状态 L-S，每一个路由器都保存一份最新的整个网络的拓扑结构图，采用 Dijkstra 算法计算最短路径，收敛速度快

■ 路由中的基本概念

AS：自制系统，是互联网互联的宏观单位，共享相同的路由选择策略，AS 内部使用内部网关协议 IGP 传递路由信息，AS 之间通过外部网关协议 EGP 传递路由信息

RIP、OSPF、IGRP、IS-IS 都是内部网关协议 IGP

EGP、BGP、IDRP 都是外部网关协议 EGP

常见路由协议

路由信息协议 RIP

RIP 使用 UDP 的 520 端口

RIP 只使用跳数作为唯一衡量标准，如到达目的地有多条相同跳数线路，则实现均衡负载，默认支持 4 线，最多 6 线

RIP 中直连网络跳数为 0，最大 15 跳，16 跳代表不可达

RIP 每 30S 发送向邻接路由器发送路由信息（即更新周期），每条路由生存周期 180S，生存周期到未收到更新设置为 16 跳不可达

RIP 采用水平分割防止路由环路，即从邻居接收到的路由信息不会反向传递给邻居

RIPv1 采用广播传播路由信息，不支持 VLSM/CIDR，RIPv2 使用 224.0.0.9 组播地址传播路由信息，支持 VLSM/CIDR

使用广播更新路由，不支持 VLSM/CIDR

EIGRP, 组播更新路由, 支持 VLSM/CIDR, 每 5 秒发送更新信息, 采用 DUAL 算法

开放式最短路径优先协议 OSPF

支持 VLSM/CIDR, 使用组播 224.0.0.6 发送路由信息, 使用链路状态通告 LSA 在路由器间共享链路状态和路由信息
路由更新周期为 10S

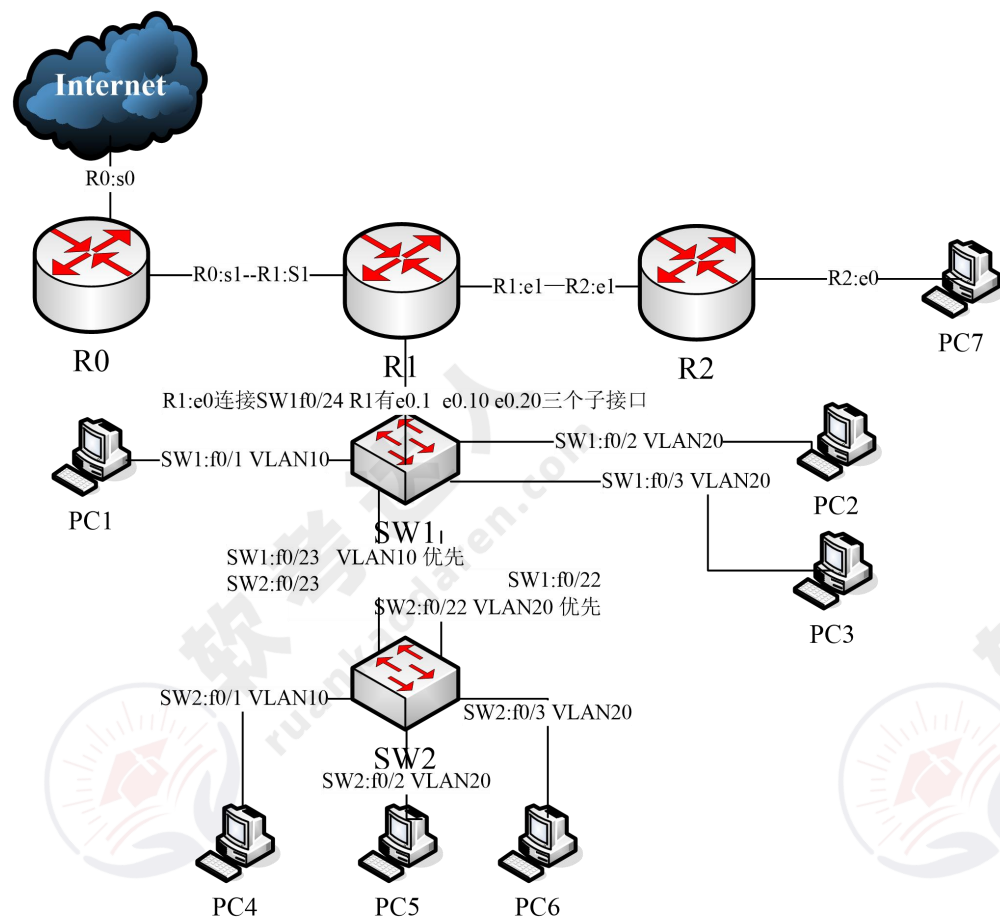
区域：AREA0 是 OSPF 的主干区域，所有区域都需要连入 AREA0，区域间路由信息交换也要通过 AREA0

DR: 指定路由器, DR 是一个区域中 ID 最高的路由器 (路由器 ID 是用于识别路由器的 IP 地址, 需手工配置, **不配置则默认为路由器回送地址中最高的 IP 地址**)

BDR: 备份指定路由器, DR 崩溃时替代

路由交换配置案例

综合案例



具体配置参数

设备名	接口	IP/子网掩码/所归属的VLAN	说明
R0	S0	202.9.9.1/29	连接 internet
	S1	172.16.10.1/30	30 位子网掩码，提高了网络地址利用率
R1	S1	172.16.10.2/30	同上
	E0.1	192.168.1.1/24	子接口，用于实现单臂路由，实现 VLAN 间通信
	E0.10	192.168.10.1/24	子接口，用于实现单臂路由，实现 VLAN 间通信
	E0.20	192.168.20.1/24	子接口，用于实现单臂路由，实现 VLAN 间通信
	E1	172.16.20.1/30	30 位子网掩码，提高了网络地址利用率
R2	E1	172.16.20.2/30	30 位子网掩码，提高了网络地址利用率
	E0	172.16.30.1/24	是 PC7 的网关
SW1	F0/1	VLAN10	Access 模式
	F0/2	VLAN20	Access 模式
	F0/3	VLAN20	Access 模式
	F0/22	TRUNK 线路	实现 SW1 和 SW2 的 STP
	F0/23	TRUNK 线路	实现 SW1 和 SW2 的 STP
	F0/24	TRUNK 线路	实现单臂路由，需要一条线路承载多个 VLAN
SW2	F0/1	VLAN10	Access 模式
	F0/2	VLAN20	Access 模式
	F0/3	VLAN20	Access 模式
	F0/22	TRUNK 线路	实现 SW1 和 SW2 的 STP
	F0/23	TRUNK 线路	实现 SW1 和 SW2 的 STP
PC1		192.168.10.11/24	网关指向 R1 的 E0.10 子接口地址 192.168.10.1
PC2		192.168.20.22/24	网关指向 R1 的 E0.20 子接口地址 192.168.20.1
PC3		192.168.20.33/24	网关指向 R1 的 E0.20 子接口地址 192.168.20.1
PC4		192.168.10.44/24	网关指向 R1 的 E0.10 子接口地址 192.168.10.1
PC5		192.168.20.55/24	网关指向 R1 的 E0.20 子接口地址 192.168.20.1
PC6		192.168.20.66/24	网关指向 R1 的 E0.20 子接口地址 192.168.20.1
PC7		172.16.30.2/24	网关指向 R2 的 E0 接口地址 172.16.30.1
此实验包括，交换机路由器基本配置，VLAN 配置，远程管理配置，VTP 配置，STP 配置，静态路由配置，RIPV2 配置			

R0 的配置：在此例中，特意将 R0 设置为静态路由模式，建议还是记命令全称，简写熟悉后再用，下一跳地址都采用下一路由器接口 IP 地址，其它表示方法很少用到

命令	描述
Router> enable	使用 enable 命令从用户模式转至特权模式
Router# configterminal	进入全局配置模式
Router(config)#hostname R0	设置设备名称为 R0

R0(config)#enable password 123	设置明文口令为 123
R0(config)#enable secret abc	设置密文口令为 abc，若设置 secret 则 password 失效
R0(config)#interface s0	进入 s0 接口模式
R0(config-if)#ip address 202.9.9.1 255.255.255.248	设置 s0 接口 IP 地址，注意子网掩码
R0(config-if)#no shutdown	激活端口
R0(config-if)#int s1	进入 s1 接口模式，可简写
R0(config-if)#ip address 172.16.10.1 255.255.255.252	设置 s1 接口 IP 地址，注意子网掩码
R0(config-if)#no shut	激活端口，可简写
R0(config-if)#exit	退到上一模式，此例退到全局配置模式
R0(config)#ip routing	启用 IP 路由
R0(config)# ip route 172.16.0.0 255.255.0.0 172.16.10.2	添加到 172.16.0.0/16 的静态路由，注意此处用到了路由汇总，格式为 ip route 目标网段 目标网段掩码 下一跳地址 此例中下一跳地址应该是 R1 路由器的 s1 接口 IP
R0(config)# ip route 192.168.0.0 255.255.0.0 172.16.10.2	添加到 192.168.0.0/16 网段静态路由，也使用了路由汇总。此例中下一跳应该是 R1 路由器的 s1 接口 IP
R0(config)# ip route 0.0.0.0 0.0.0.0 s0	添加默认路由【优先级最低】，其它所有的数据包从本路由器的 s0 口扔出去【下一跳可以是本路由器出口接口名】
R0(config)#ip classless	启用默认路由
R0(config)#end	直接退到特权模式
R0#show running-config	查看 RAM 中的运行配置
R0#copy running-config startup-config	将 RAM 中的配置保存到 NVRAM 启动配置文件中，等同于 write 命令 简写 R0#copy run startup

R1 的配置，R1 和 R2 采用 RIP 实现，因为使用了 VLSM，所以需要使使用 RIPV2，并且使用了 172.16.x.x 下的 10、20、30 子网段，所以需要关闭自动汇总功能	
命令	描述
Router> enable	进入特权模式
Router# configt	进入全局配置模式
Router(config)#hostname R1	设置设备名为 R1
R1(config)#int s1	进入 s1 接口模式
R1(config-if)# ip address 172.16.10.2 255.255.255.252	配置 s1 接口的 ip 地址为 172.16.10.2 子网掩码为 255.255.255.252
R1(config-if)#no shut	激活接口
R1(config-if)#int e1	进入 e1 接口模式
R1(config-if)#	配置 e1 接口的 ip 地址为 172.16.20.1 子网掩

ip address 172.16.20.1 255.255.255.252	码为 255.255.255.252
R1(config-if)#no shut	激活接口
R1(config-if)#int e0	进入 e0 接口模式
R1(config-if)#no shut	激活接口
R1(config-if)#int e0.1	进入 e0.1 子接口模式
R1(config-subif)# ip address 192.168.1.1 255.255.255.0	配置子接口 IP, 这个子接口的 IP 属于 VLAN1 的 IP 段, 父接口激活后子接口激活命令可以省略
R1(config-subif)#encapsulation dot1q vlan 1	在 e0.1 子接口启用 802.1Q 封装, 封装 vlan1
R1(config-if)#int e0.10	进入 e0.10 子接口模式
R1(config-subif)# ip address 192.168.10.1 255.255.255.0	配置子接口 IP, 这个子接口的 IP 属于 VLAN10 的 IP 段, 父接口激活后子接口激活命令可以省略
R1(config-subif)#encapsulation dot1q vlan 10	在 e0.10 子接口启用 802.1Q 封装, 封装 vlan10
R1(config-if)#int e0.20	进入 e0.20 子接口模式
R1(config-subif)# ip address 192.168.20.1 255.255.255.0	配置子接口 IP, 这个子接口的 IP 属于 VLAN20 的 IP 段, 父接口激活后子接口激活命令可以省略
R1(config-subif)#encapsulation dot1q vlan 20	在 e0.20 子接口启用 802.1Q 封装, 封装 vlan20
R1(config-subif)#exit	退到上一层
R1(config)#ip routing	启用 IP 路由功能
R1(config)#router rip	启用 RIP 动态路由协议
R1(config-router)#version 2	使用 RIP V2 版本
R1(config-router)#no auto-summary	关闭路由自动汇总功能
R1(config-router)#network 172.16.10.0	宣告直连网段 172.16.10.0
R1(config-router)#network 172.16.20.0	宣告直连网段 172.16.20.0
R1(config-router)#network 192.168.1.0	宣告直连网段 192.168.1.0
R1(config-router)#network 192.168.10.0	宣告直连网段 192.168.10.0
R1(config-router)#network 192.168.20.0	宣告直连网段 192.168.20.0

R2 的配置:	
命令	描述
R2(config)#interface e1	进入 e1 接口模式
R2(config-if)#ip address 172.16.20.2 255.255.255.252	设置 e1 接口 IP 地址, 注意子网掩码
R2(config-if)#no shutdown	激活端口
R2(config-if)#int e0	进入 e0 接口模式, 可简写
R2(config-if)#ip address 172.16.30.1 255.255.255.0	设置 e0 接口 IP 地址
R2(config-if)#no shut	激活端口, 可简写
R2(config-if)#exit	退到上一模式
R2(config)#ip routing	启动 IP 路由
R2(config)#router rip	启用 RIP 动态路由协议

R2(config-router)#version 2	使用 RIP V2 版本
R2(config-router)#no auto-summary	关闭路由自动汇总功能
R2(config-router)#network 172.16.20.0	宣告直连网段 172.16.20.0
R2(config-router)# network 172.16.30.0	宣告直连网段 172.16.30.0

SW1 的配置： 重复命令省略	
命令	描述
SW1(config)#interface vlan 1	进入 VLAN1 接口模式
SW1(config)#ip address 192.168.1.2 255.255.255.0	给 VLAN1 设置 IP，交换机设置 IP 目的是为了 实现远程管理
SW1(config)#ip default-gateway 192.168.1.1	设置默认网关，设置默认网关的目的是实现 跨网段远程管理，此例中 PC1-7 可以远程登 录到每个设备
SW1(config)exit	退至上一模式
SW1#vlan database	进入 vlan 配置模式
SW1(VLAN)#vlan 10 name V10	添加 VLAN，编号为 10 名字为 V10，name V10 可省略
SW1(VLAN)#vlan 20 name V20	添加 VLAN，编号为 20 名字为 V20
SW1(VLAN)#vtp server	设置本交换机为 VTP 服务器模式
SW1(VLAN)#vtp domain enpass	设置 VTP 的域为 enpass
SW1(VLAN)#vtp password 123456	设置 VTP 密码为 123456
SW1(VLAN)#vtp pruning	启用 VTP 修剪功能
SW1(VLAN)#exit	退至上一模式
SW1#config terminal	进入全局配置模式
SW1(config)#interface f0/1	进入 f0/1 接口模式
SW1(config-if)#Switchport mode access	设置 f0/1 为 access 接入线路模式 或将 f0/1 设置为静态 VLAN 模式
SW1(config-if)#Switchport access vlan 10	将端口 f0/1 分配给 vlan 10 或使 f0/1 端口可识别 vlan 10 封装
SW1(config)#interface range f0/2 - 3	进入接口模式，注意多端口的写法，range 表 示范围 2-3 的“-”前后各有一个空格
SW1(config-if)#Switchport mode access	设置端口为 access 接入线路模式
SW1(config-if)#Switchport access vlan 20	将端口分配给 vlan 20
SW1(config)#interface f0/24	进入接口模式
SW1(config-if)#Switchport mode trunk	设置端口为 trunk 干道模式
SW1(config-if)#Switchport trunk encapsulation dot1q	使用 802.1Q 协议封装 trunk 另外一种 cisco 特有的封装协议为 ISL
SW1(config-if)#Switchport trunk allowed vlan all	允许所有的 VLAN 通过 trunk
SW1(config)#interface f0/22	进入接口模式
SW1(config-if)#Switchport mode trunk	设置端口为 trunk 干道模式
SW1(config-if)#Switchport trunk encapsulation	使用 802.1Q 协议封装 trunk

dot1q	另外一种 cisco 特有的封装协议为 ISL
SW1(config-if)#Switchport trunk allowed vlan all	允许所有的 VLAN 通过 trunk
SW1(config-if)#spanning-tree vlan 10 port-priority 10	Vlan10 对于 f0/22 端口权值为 10, 默认为 128, 数字越小优先级越高, 意即 vlan10 通过 f0/22 口传输 也可以使用 SW1(config-if)#spanning-tree vlan 20 cost 40 即 VLAN20 对于 f0/22 端口的 STP 路径成本为 40, 默认为 19, 数字越小越优先, 意即阻止 VLAN20 通过 f0/22 口传输
SW1(config)#interface f0/23	进入接口模式
SW1(config-if)#Switchport mode trunk	设置端口为 trunk 干道模式
SW1(config-if)#Switchport trunk encapsulation dot1q	使用 802.1Q 协议封装 trunk 另外一种 cisco 特有的封装协议为 ISL
SW1(config-if)#Switchport trunk allowed vlan all	允许所有的 VLAN 通过 trunk
SW1(config-if)#spanning-tree vlan 20 port-priority 10	Vlan20 对于 f0/23 端口权值为 10, 默认为 128, 数字越小优先级越高, 意即 vlan20 通过 f0/23 口传输 也可以使用 SW1(config-if)#spanning-tree vlan 10 cost 40 即 VLAN10 对于 f0/22 端口的 STP 路径成本为 40, 默认为 19, 数字越小越优先, 意即阻止 VLAN10 通过 f0/22 口传输

SW2 的配置:	
命令	描述
SW2(config)#interface vlan 1	进入 VLAN1 接口模式
SW2(config)#ip address 192.168.1.3 255.255.255.0	给 VLAN1 设置 IP, 交换机设置 IP 目的为了实现远程管理
SW2(config)#ip default-gateway 192.168.1.1	设置默认网关, 设置默认网关的目的是实现跨网段远程管理, 此例中 PC1-7 可以远程登录到每个设备
SW2(config)#vlan database	进入 vlan 配置模式或者 vlan 数据库模式
SW2(VLAN)#vtp client	设置 vtp 为客户端模式
SW2(VLAN)#vtp domain enpass	所属的 vtp 域为 enpass
SW2(VLAN)#vtp password 123456	Vtp 域的密码是 123456

OSPF 的基本配置

Router(config)#router ospf 1

进入 ospf 配置子模式, 指定 ospf 进程号为 1

Router(config-router)#network 192.168.8.0 0.0.0.255 area 0 指定与该路由器直接相连的网络，注意子网掩码是原掩码的反码，area 0 指所在的区域号

网络操作系统 NOS

■ 网络通信的系统功能调用

Socket 套接字，unix 称之为 socket，windows 称之为 winsock，套接字由协议、IP、端口号组成

RPC 远程过程调用

■ 文件系统

VFAT 虚拟文件分配表，FAT32 单个文件最大尺寸 4GB

NTFS

EXT3

DFS 分布式文件系统

NFS 网络文件系统

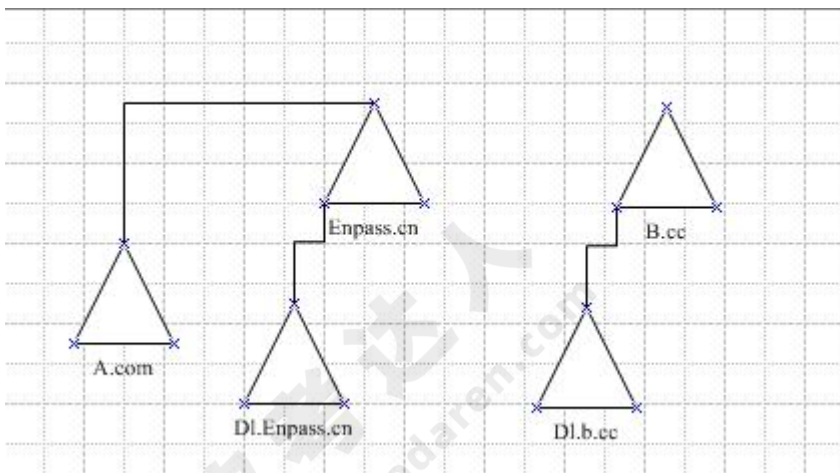
Windows 操作系统

域

域 domain 是 windows 网络操作系统的逻辑组织单元，是活动目录 AD 最核心的管理单位和复制单位，域是网络系统的安全性边界，域采用集中式管理，而工作组是对等网模式，采用松散管理

Windows 有 4 中域结构：单一域模型、主域模型、多主域模型、完全信任模型

活动目录的组成



如上图：一共两个林，其中 enpass.cn 为左侧林的根域，b.cc 为右侧林的根域，dl.enpass.cn 是 enpass.cn 的子域【因为共用相同的域结构部分】，a.com 是左侧域林中的一个域树。

■ 信任关系

林内信任：自动、可传递、双向

外部信任——林间信任，两个林中的非根域信任，如 a.com 和 dl.b.cc 信任：手动、不可传递、单向

根域信任——林信任，两个林的根域信任，如 enpass.cn 和 b.cc 信任：手动、可传递、单向/双向

■ 操作主机角色

操作主机角色有 5 种，其中域架构主机和域命名主机只存在于林的根域，基础结构主机、RID 主机和 PDC 仿真主机每个

域都存在，操作主机可占用，2003 域结构中，域控制器之间的关系都是平等的

常用命令

命令	解释	命令	解释
Cmd	进入命令行模式	Mmc	打开微软管理控制台
Gpedit	组策略编辑器	Regedit	注册表编辑器

Linux 系统

Linux 是开源的类 UNIX 系统

遵守 GUN 的 GPL 协议

Linux 系统是指使用了 linux 内核的系统

内核版本，2【主版本号】.6【此版本号，奇数为测试版，偶数为稳定版】.24

Linux 中 init 进程是一切进程的父进程，PID 永远为 1

Linux 磁盘管理

	主分区	扩展分区			说明
		逻辑驱动器	逻辑驱动器	逻辑驱动器	主分区≤4
Windows 表示	C:	D:	E:	F:	扩展分区≤1
Linux 表示 IDE	/dev/hda1	/dev/hda5	/dev/hda6	/dev/hda7	主+扩展≤4
Linux 表示 SCSI	/dev/sda1	/dev/sda1	/dev/sda1	/dev/sda1	

如 hda5 中 hd 代表是 IDE 接口硬盘，若是 sd 代表 SCSI 接口硬盘，a 代表第一块硬盘，5 代表第一个逻辑驱动器，linux 把 1、2、3、4 留给主分区

文件系统

<u>/bin</u>	<u>执行程序 and 命令</u>	<u>/sbin</u>	<u>用于系统管理的命令</u>
/boot	系统启动文件，包括内核	<u>/proc</u>	<u>内存进程信息，关机小时，无需备份</u>
<u>/etc</u>	<u>配置文件</u>	/dev	设备
/home	普通用户主目录	<u>/root</u>	<u>超级用户 root 主目录</u>

Linux 采用 EXT 文件系统，SWAP 为交换分区，一般为内存的 2 倍大小

常用命令及常见配置文件格式

■ Linux 命令格式

[root@enpass /home]#命令字 【选项】 【参数】

其中，root 表示当前登录用户，enpass 表示主机名称，/home 表示当前所在目录，#表示当前用户是超级用户，如果是普通用

户用\$提示符

如 ls -la -color=no /home，选项中“-”代表短选项，可分开写，“--”代表长选项，不能分开写即可写为 ls -l -a -color=no /home

■ 常用配置文件

/etc/passwd	储存用户信息，所有用户可读，不安全
<u>/etc/shadow</u>	<u>影子密码，存储用户加密后的密码，密文，只 root 可读，安全</u>
/etc/group	储存组信息
/etc/fstab	文件系统挂在表
<u>/etc/inittab</u>	<u>系统引导配置文件，共有 7 个级别，0 关机 1 单用户 3 字符界面多用户 5 图形界面多用户 6 重启</u>

■ 常用命令

Ls	列出目录列表	Cat	查看合并文件
<u>More</u>	<u>分屏查看</u>	Chown	更改文件属主和属组
<u>Chmod</u>	<u>修改文件权限</u>	<u>Pwd</u>	<u>获取当前所在目录路径</u>

文件类型与权限

-rwxrw-r-- 3 zhangsan CW filename

第一个位置“-”表示文件类型，“-”表示普通文件，“d”表示目录，“b”表示块设备如磁盘，“C”表示字符设备如键盘

后续 3 位“rwx”表示该文件的属主权限，该文件属主为 zhangsan，拥有 r 读 w 写 x 执行，八进制表示法则中，读 r

用 4、写 w 用 2、执行 x 用 1，所以属主权限也可以在命令中用 4+2+1=7 代表

后续 3 位“rw-”表示该文件的属组权限，该文件属组为 CW，八进制表示为 读 4+写 2=6

后续 3 为“-r-”表示其他用户权限，八进制表示为 读 4=4

如，现修改文件属主为 wangzhanf，属组为 enpass，权限变更为 rwxr----

-rwxrw-r-- 3 zhangsan CW filename

[root@enpass /home]#chown wangzhanf:enpass filename

-rwxrw-r-- 3 wangzhanf enpass filename

[root@enpass /home]#chmod 740 filename 或者 chmod u=rwx,g=r filename

-rwxr--r-- 3 wangzhanf enpass filename

其中 u 代表属主，g 代表属组，a 代表所有，o 代表其他用户，赋权可以使用“+/-”的相对赋权或者“=”的绝对赋权

应用层协议及网络服务实现

DNS

基础知识

DNS 是一种 C/S 模式 服务

Hosts 文件：静态的域名和 IP 的映射关系

Dns 域名解析系统是一个 层次化、分布式的数据库，避免了它的前身 hosts 文件的线性检索速度慢的缺点

DNS 正向：由域名解析 IP

DNS 反向：由 IP 解析域名，如防垃圾邮件应用中

DNS 默认使用 UDP53 端口，当数据量大于 512 字节或者区域复制时使用 TCP 的 53 端口

DNS 层次化的第一级是 根域，用 “.” 表示，第二级为 顶级域 【com、mil（国防）】

使用 DNS 轮询可以实现简单的均衡负载【即一个域名对应多个主机 IP】，缺陷是 DNS 和主机无互动，主机宕机，DNS 继续解析到宕机的主机上，造成客户不能访问

■ 域名解析两种类型

递归解析：客户和本地 DNS 之间，或者 DNS 转发器 常用 递归解析

反复解析：也叫迭代解析，DNS 服务器之间 常用 迭代解析

■ 域名解析过程

1、查看本机缓存是否有记录【ipconfig /displaydns 查看 DNS 缓存 ipconfig /flushdns 清除 DNS 缓存】

2、查看本机 hosts 文件

3、查询本地 DNS 服务器缓存

4、是否是本地 DNS 的区域，若不是本地 DNS 向根域 DNS 查询，根域 DNS 返回一个推荐地址，反复迭代至得到结果

5、本地 DNS 缓存记录信息，并将结果返回给客户端

■ DNS 记录类型

A IPV4 主机记录

AAAA IPV6 主机记录

CNAME 别名

NS 定义 DNS 服务器

SOA 定义权威 DNS 服务器

MX 邮件交换记录，必须指向主机

PTR 反向指针

LINUX 实现 DNS

LINUX 下使用 BIND 实现 DNS

BIND 的守护进程名为 named

BIND 的配置文件为 /etc/named.conf

区域文件储存在 工作目录/var/named 中

■ 主配置文件样例

Directory "/var/named" ; //定义工作目录，所有区域文件放在这个目录里

forwarders {202.96.69.38 202.96.64.68}; //定义转发器

zone "." {

type hint; //该类型为根提示，共有三种类型 master slave hint

file "named.root"; //区域文件的名字

};

zone "enpass.cn" IN { //enpass.cn 区的正向解析

type master; //区域类型为 主要区域，如果是辅助区域则为 slave

file "enpass.cn.zone";

};

zone "0.22.222.222.in-addr.arpa" IN { //enpass.cn 区的反向解析，是 IP 地址段的前 3 个字节逆序写

type master;

file "enpass.cn.rev";

};

■ 正向区域文件样例

前部分一般不考，忽略【例如这个文件是 enpass.cn.zone】

IN NS ns.enpass.cn. //本域的 DNS 信息由 ns.enpass.cn. 这台主机维护

ns IN A 222.22.2.3 //定义一条主机记录

www IN CNAME //定义一条别名记录

@ IN MX 10 ns //定义邮件交换记录，数字越小优先级越高，@代表本域，MX 必须指向一条主机记录

■ 反向区域样例

前部分一般不考，忽略【例如这个文件是 enpass.cn.rev】

3 IN PTR ns.enpass.cn. //222.22.2.3 对应的主机名是 ns.enpass.cn, 定义一条反向指针记录

■ 客户端配置

LINUX 中配置指定 DNS 的配置文件的 /etc/resolv.conf

search enpass.cn //设定默认搜索域，也可以用 domain enpass.cn 定义

nameserver 10.0.0.1 //首选 DNS 服务器 IP

nameserver 11.22.33.44 //辅助 DNS 服务器 IP，最多三个

DNS 测试

Nslookup 有两种方式：交互式和直接方式

直接方式：nslookup 域名

交互方式：nslookup，在上下文提示中操作

Server IP 地址 //指定 DNS 服务器作为测试服务器

Set type=【A MX CNAME PTR ALL】//设置查询类型

Windows 实现 DNS

Windows 实现主要是看图说话，在历年试题解析中解释

DHCP 动态主机配置协议

DHCP 基础知识

DHCP 作用：集中管理和自动分配 IP 网络地址等参数

DHCP 必须分配 IP 和子网掩码，网关、DNS 等属于选项

选项优先级【保留选项>作用域选项>服务器选项】

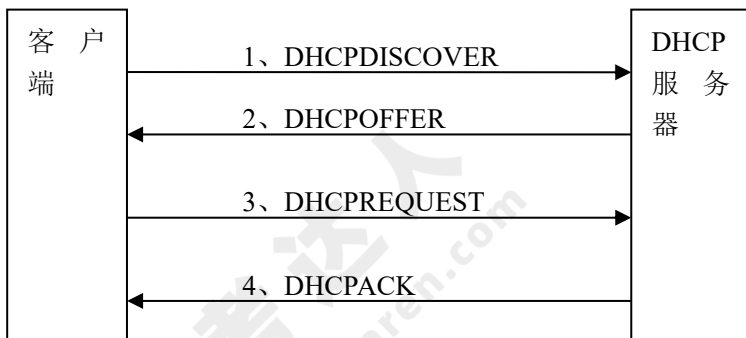
选项影响范围【服务器选项>作用域选项>保留选项】

保留：给指定 MAC 地址分配固定 IP 地址

DHCP 是典型的 C/S 模式

DHCP 服务器使用 UDP67 端口，客户端使用 UDP68 端口

■ DHCP 工作过程



系统不同实现不同，

1、2、3、4 全部都是广播包

■ 租约更新

手动更新：`ipconfig /release`【释放现有】 `ipconfig /renew`【重新获取】

自动更新：客户端到达最大租约的 50% 时间时，发送 DHCPREQUEST 单播包 申请续约，若续约不成功，则在最大租约时间的 87.5% 时向全网发送 DHCPDISCOVER 广播包，若无其他任何服务器，在 到达最大租约时间时丢弃 IP 配置参数

LINUX 下 DHCP 配置

DHCP 的守护进程名为 dhcpd

主配置文件为/etc/dhcpd.conf

跨网段提供 DHCP 服务需使用 DHCP 中继代理 dhcp-relay

租约文件是/var/state/dhcp/dhcp.lease

■ Dhcpd.conf 配置案例

`ddns-update-style ad-hoc;`

`option domain-name "enpass.cn";`

`option domain-name-servers 202.96.69.38,202.96.64.68;` //在配置文件根下的 option 选项影响整个服务器，此条指定客户端获取的 DNS 地址

`default-lease-time 36000;` //默认租约时间，秒为单位

`max-lease-time 360000;` //最大租约时间

`subnet 192.168.1.0 netmask 255.255.255.0 {` //定义作用域

`range 192.168.1.0.10 192.168.1. 90;` //定义地址池

`range 192.168.1.0.100 192.168.1.0.200;`

`option routers 192.168.1.0.1;` //出现在作用域中的 option 选项只影响本作用域

`host manager {` //定义保留，根据 MAC 地址分配固定的 IP 地址


```
hardware Ethernet 00:11:22:33:44:55;
```

```
fixed-address 192.168.1.20;
```

```
}//保留定义结束
```

```
}//作用域定义结束
```

```
subnet 192.168.2.0 netmask 255.255.255.0 { //定义作用域
```

```
range 192.168.2.0.10 192.168.2. 90; //定义地址池
```

```
option netmask 255.255.255.0;
```

```
option routers 192.168.2. 1; //出现在作用域中的 option 选项只影响本作用域
```

```
}//作用域定义结束
```

■ 客户端网卡配置文件 /etc/sysconfig/network-scripts/ifcfg-eth0 【记住文件位置】

```
DEVICE=eth0 //接口名称
```

```
BOOTPROTO=none //静态配置，若该值为“dhcp”则为动态获得，另外 static 也是表示静态 ip 地址
```

```
BROADCAST=192.168.10.255 //广播地址，通过 IP 地址和子网掩码自动计算得到，可省略
```

```
HWADDR=00:13:D3:27:9F:80 //物理地址，可省略
```

```
IPADDR=192.168.10.238 //设置 IP 地址，若设置 BOOTPROTO=dhcp 此行可省略
```

```
NETMASK=255.255.255.0 //设置子网掩码，若设置 BOOTPROTO=dhcp 此行可省略
```

```
NETWORK=192.168.10.0 // 设置网络地址，可通过 IP 地址和子网掩码自动计算得到，可省略
```

```
ONBOOT=yes //开机时自动加载
```

```
GATEWAY=192.168.10.1 //设置默认网关
```

■ 网卡的控制

```
ifdown eth0 关闭网络
```

```
ifconfig eth0 down
```

```
关闭网络
```

```
ifup eth0 开启网络
```

```
ifconfig eth0 up
```

```
开启网络
```

windows 下配置 DHCP

windows 安装 DHCP 需要授权

作用域红色向上箭头表示未激活，需激活后才能工作，激活后变为绿色向下箭头

电子邮件

■ 电子邮件协议

RFC822:7 位 ASCII 码纯文本邮件定义

SMTP：使用 TCP25 端口的发送电子邮件 协议

POP3：使用 TCP110 端口的接收电子邮件 协议

IMAP4：使用 TCP143 端口的协同接收电子邮件 协议

MIME：可以传输 多媒体邮件

■ 电子邮件系统组成

邮件传输代理 MTA【exchange 和 sendmail 等】+ 邮件投递代理 MDA【devecot 等】+ 邮件用户代理 MUA【outlook 和 foxmail 等】组成了 C/S 模式 的邮件系统

MTA 和 DNS 的 MX 记录结合实现邮件跨域传送

文件传输协议 FTP