

【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](http://ruankaodaren.com)

一、可靠度(可用性)计算机

串联  $R=R_1 \times R_2$  对应失效率：入  $1+入2$  并联  $R=1-(1-R_1)(1-R_2)$

二、香农定理（有噪声）数据速率：

在一条带宽为  $W$  (HZ)，信噪比为  $S/N$  的有噪声极限数据速率

$V_{max}=W \log_2(1+S/N)$  单位 (b/s)

分贝与信噪比的关系为： $dB=10\lg 10S/N$   $dB$  的单位分贝

例：设信道带宽为 4kHz，信噪比为 30dB，

按照香农定理，信道的最大数据传输速率约等于？

解：1，例出香农定理算式： $V_{max}=W\log_2(1+S/N)$

2，例出信噪比关系： $dB=10\lg 10S/N$

3，计算  $30dB=10\lg 10S/N$  则  $S/N=1000$

4， $V_{max}=4KHz \log_2(1+1000)=4000 \times 10 = 40kb/s$

注意：此处单位换算  $1 kb/S=1000b/s$

三、奈奎斯特定理（无噪声）

若信道带宽为  $W$  (HZ)，则最大码元速率（波特率） $B=2W$  (baud)

由奈奎斯特定理可得： $V_{max}=B \log_2 N=2 w \log_2 N$  单位 (b/s)

例：设信道带宽为 3400Hz，调制为 4 种不同的码元，

根据 Nyquist 定理，理想信道的数据速率为？

解：1，根据题意例出奈奎斯特定理算式： $V_{max}=2 W \log_2 N$

2，直接套入数字： $V_{max}=2 \times 3400 \times \log_2(2^2)$  (2 次方)

3， $V_{max}=2 \times 3400 \times 2=13600b/S=13.6kb/s$

注意：此处出现单位换算一次， $13600b/s=13.6kb/2$

例 1：设信道采用 2DPSK 调制，码元速率为 300 波特，

则最大数据速率为解： $V_{max}=B \log_2 N=300 \times 1=300b/s$

例 2：在异步通信中，每个字符包含 1 位起始位，7 位数据位，

1 位奇偶校验位和两位终止位，若每秒传送 100 个字符，

采用 4DPSK 调制，则码元速率为？有效数据速率为？

解：1，根据题意计算数据速率为  $(1+7+1+2) \times 100=1100b/s$

2，由奈奎斯特定理得出， $1100b/S=B \times \log_2 4$

3， $B=1100/2=550baud$

4，有效数据速率，即单位时间内传输的数据位，即  $7 \times 100=700b/S$

四、PCM 计算问题

PCM 主要经过 3 个过程：采样，量化和编码。 $f=1/T \geq 2f_{max}$

$f$  为采样频率， $T$  为采样周期， $f_{max}$  为信号的最高频率。

例：设信道带宽为 3400HZ，采用 PCM 编码，采样周期为  $125 \mu s$ ，

每个样本量化为 128 个等级，则信道的数据速率为？

解： $f=1/S=1/125us=8000Hz$   $8000Hz > 3400Hz \times 2$   $128=2$  的 7 次方

则：数据速率= $8000Hz \times 7=56000b/S=56kb/s$

八、Cache：又称高速缓存存储器

命中率：访问信息的概率

假如执行过程中对 Cache 的访问次数为  $N_1$  和对主存访问为  $N_2$ ，则 Cache 命中率为  $H$

$=N_1 / (N_1+N_2)$

平均存取时间：可用 Cache 和主存的访问周期  $T_1$ 、 $T_2$  和命中率  $H$  表示

即： $T=H \times T_1 + (1-H) T_2$

九、最小帧长计算，先求往时间，再用时间\*数据速率

例如：一个运行 CSMA/CD 协议的以太网，数据

速率为  $1Gb/s$ ，网段长  $1km$ ，信号速率为  $20000km/s$ ，

则最小帧长是多少？

单程传播时间为  $1km/20000=5us$ ，往返要  $10us$ ，最小帧为  $1Gb/s \times 10us=10000bit$

七、流水线计算

流水线周期值等于最慢的那个指令周期（最大值）

流水线执行时间=首条指令的全部时间+（指令总数-1）\*周期值

流水线吞吐率=任务数/完成时间

流水线加速比=不采用流水线的执行时间/采用流水线的执行时间

流水线的总时间=（指令总数+2）\*周期值

例：若每一条指令为取指、分析和执行。已知取指时间  $a$ ，分析时间  $b$ ，

执行时间  $c$ （最大）。按串行方式执行完 100 条指令需要 多少时间？

按照流水方式执行，执行完 100 条指令需要多少时间。

流水线周期为  $C$ ，即最大值。

100 条指令的串行方式时间是  $(a+b+c) \times 100$

100 条指令的流水方式时间是  $(a+b+c) + c \times 99$

流水线吞吐率为  $100 / (a+b+c) + c \times 99$

五、数据传输延迟

总延迟  $T=发送延迟 T_1+传输延迟 T_2$

注意：电信号在电缆上传播的速度为光速的  $2/3$ ，即  $20wkm/s$

卫星传送信号的延迟恒定为  $270ms$  与地面距离无关

例：在相隔  $2000km$  的两地间通过电缆以  $4800b/s$  的速率传送

$3000$  比特长的数据包，从开始发生到接收数据需要的时间是？

如果用  $50Kb/s$  的卫星信道传送，则需要的时间是？

对于电缆：传输延迟  $T_1=2000km / (20km/ms)=10ms$

发送延迟  $T_2=3000b / (4800b/s)=625ms$

$T=T_1+T_2=625ms+10ms=635ms$

对于卫星：

传输延迟  $T_1=270ms$  发送延迟  $T_2=3000 b / (50kb/s)=60ms$

$T=T_1+T_2=270ms+60ms=330ms$

注意：卫星传输数据时与地面相隔距离无关。

六、求芯片数计算必考

假设有一个存储器存储容量为  $M \times N$  位，若使用  $m \times n$  的芯片，则需要  $(M/m) \times (N/n)$  个存储芯片（注：单位要换成一致）

● 若内存地址区间为  $4000H \sim 43FFFH$ ，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

总存储单位=  $(43FFFH - 4000H + 1H) = 400H = 1024$  ( $H$  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  $256 \times 16bit$

7、应用层 处理网络应用 6、表示层 数据表示，数据压缩

5、会话层 互联主机通信 4、传输层 端到端应答，分组排序，流量控制

3、网络层 分组传输和路由选择 2、链路层 传送以帧为单位的信息

1、物理层 二进制数据传送

应用层	HTTP、FTP、telnet、SMTP	SNMP、DNS、DHCP
	POP、DNS	TFTP
传输层	TCP	UDP
网络层	IP、ICMP、ARP、RARP	
通信子网层	电话网，局域网，无线网	

二、特殊 IP 地址

私网地址

$10.0.0.0 \sim 10.255.255.255$  (1 个)  $172.16.0.0 \sim 172.31.255.255$  (16 个)

$192.168.0.0 \sim 192.168.255.255$  (256 个)

$127.0.0.1$  是 IPv4 的回环地址，用于回路测试

$169.254.0.0 \sim 169.254.255.255$  是自动专用 IP 地址，

在网络故障找不到 DHCP 或 DHCP 服务器失效时使用

IPv6 中  $0.0.0.0.0.0.0.0.0$  表示不确定地址，不分配给任何节点

$0.0.0.0.0.0.0.0.1$  是 IPv6 回环地址，向自身发送 IPv6 分组

全球单播  $001$ 、多播地址  $11111111$ 、单播  $11111010$

三、常见协议端口

TCP 数据 20 控制 21 、 Telnet 23 、 smtp 25 、 TFTP 69 、 DNS 53 (TCP

和 UDP 都可调用) 、 HTML 80 、 SNMP 161、DHCP 67、68 、 pop3 110

https/ssl 443、SQL services 118 、 SQL server 156

四、IEEE802.3ae 10Gb/s 以太网

IEEE802.3ab/z 1000Mb/s 以太网 IEEE802.3au 100Mb/s 以太网

IEEE 802.3au

100BASE-TX 5 类非屏蔽双绞线 2 对跳线 距离 100m

100BASE-FX 62.5/125 多模光纤 2 对用于收发 距离 400m

100BASE-T4 3 类非屏蔽双绞线 4 对用于收发 距离 100m

多模与单模区别：多模使用发光二极管，单模使用激光二极管。

多模允许多束光纤穿过，单模比多模采用的波长短。

单模只允许一束光线穿过，单模传输频带宽，多模传输频带窄。

EE802. 11	标准	速度	技术
802. 11	2.4GHZ，ISM 频段	1mb/s，2mb/s	扩频通信技术
802. 11b	2.4GHZ，ISM 频段	11mb/s	Cck 技术
802. 11a	5GHZ，U-NII 频段	54mb/s	OFDM 调制技术
802. 11g	2.4GHZ，ISM 频段	54mb/s	OFDM 调制技术
802. 11n	智能无线技术	300—600mb/s	MIMO 与 OFDM 术

五、E1、E3、T1、T3

E1 由 32 个子信道组成， 30 个传送话音数据，2 个子信道

CH0 和 CH16 用于传送控制命令，该基本帧的传送时间为  $125us$ 。

在 E1 中，每个子信道的数据速率是 **64Kb/s**，E1 控制开销占 **6.25%**

E1 信道的数据速率是 **2.048Mb/s**

T1 每个信道的数据速率为 **64kb/s**，T1 总数据速率是 **1.544Mb/s**

E3 数据速率是 **34.368Mb/s**， T3 数据速率为 **44.736Mb/s**

六、关键路径

哪个路径中值最大，就为关键路径。

最早开始时间：从头往后算，有两个取大的

最晚开始时间：从后往前算，减去所用时间，两个取小的

节点推迟时间：两个路径相减+1

七、不发生死锁的资源数 R

**M 个进程，每个进程要 N 个资源，不发生死锁；公式：M\*（N-1）+1**

八、CSMA/CD(载波监听多路访问/冲突检测)：

CSMA/CD 采用二进制后退算法，保证系统的稳定性，有效分解冲突。

CSMA/CD，不适用于所有 802.3 以太网，在 10 千兆位忽略了 CSMA/CD。

非坚持：忙等待再侦听；不忙立即发送；减少冲突，信道利用率低：

I 坚持：忙继续侦听；不忙立即发送；提高信道利用率，增大冲突：

p 坚持：线路忙继续侦听；不忙时，根据 p 概率进行发送，

另外的  $1-p$  概率为继续侦听；有效平衡，但复杂：

**CSMA/CA：不带有冲突**

CSMA/CA 协议适用于突发性业务。

各个发送站在两次帧间间隔（IFS）之间进行竞争发送。

九、路由协议

RIP 每 30 秒，IGRP 每 90 秒，发布路由更新。

OSPF 不论是否网络拓扑发生改变，每 10 秒发送一次 hello 数据包，

OSPF 如果 40 秒没有收到 hello 分组，就认为对方不存在。

IGRP 内部网关路由协议，是一种动态距离向量路由协议，由思科设计

使用组合用户配置尺度，包括带宽，延迟，可靠性和最大传输单元 (MTU)。

IGRP 协议的路由度量一般情况下可以简化为跳步数。

默认 IGRP 每隔 90 秒发送一次路由更新广播，在 3 个更新周期 (270 秒)，

没有从路由中的第一个路由器接收到更新，则宣布路由不可访问。

IGRP 配置为：

Router(config)#router igrp 10

Router(config)-router)#network 192.168.20.0

IGRP 不支持可变长子网掩码

十二、计算机组成

程序计数器 (PC)：用于存储指令的地址，程序员可以访问

指令寄存器 (IR)：用于暂存内存中取出的，正在运行的指令。

程序员不能访问，操作和地址码都存入 IR 中。

算术逻辑单元 (ALU)：用于  $+-*/$  等运算

累加寄存器 (AC)：用来保存操作数和运算结果等信息



## 十一、进程



1 表示进程被选中，2 时间片用完  
3 等待某个事件 4 等待的事件已获得

## 十、交换机

交换机三种方式：存储转发交换，直通交换，碎片过滤式交换。

STP：生成树协议，STP 要求每个网桥分配一个唯一的标识（BID），BID 通常由优先级（2 bytes）和网桥 MAC 地址（6bytes）构成。交换机优先级以 4096 为块大小递增或递减，默认值为 32768。规则：选择较优先级小的交换机，优先级相同时最小的 MAC 为根交换机。IEEE802.1d 协议，就是生成树协议，所有网桥有 5 种状态功能。

1. 监听：识别根桥，可区分根端口，指定端口，不能学习接收帧的地址。
2. 学习：MAC 端口能够学习接收帧的 MAC 地址，但不转发。
3. 转发：MAC 端口可以学习接收帧地址，并可以转发口。
4. 禁用：MAC 端口不参与生成树算法。
5. 阻塞：不转发器，不学习 VTP（VLAN 中继协议）交换机的运行模式分 3 种：
  1. 服务器模式（server）：可以创建添加删除和修改 VLAN 配置并从中继端口发出 VTP 组播帧，把配置信息分发到所有交换机。
  2. 客户机模式：不允许创建修改删除 VLAN，但可监听并修改自己的 VLAN。
  3. 透明模式：可进行 VLAN 配置，但信息不传播至其他交换机。

## 十五、IP 协议相关

全 0 为本机地址，全 1 广播地址，其它为本机地址

## 1. IP 头部固定长 20 个字节

ARP 协议（报文封装在以太网帧中传送）网络层协议，由 IP 找 MAC。  
RARP（反向地址解析）由 MAC 找 IP  
ICMP 报文控制协议（报文封装在 IP 数据部分传送）属于网络层协议

## 2. BGP 边界网关协议，三张表：邻居表、BGP 转发表、路由表

BGP 四种报文：

Open 报文：用于建立邻居关系  
Update 报文：用于发送新的路由信息  
Keepalive：对 open 的应答和周期性的确认邻居关系  
通告报文：用于报告检测到的错误

## 3. DHCP 动态主机配置协议

服务过程：工作在 UDP 应用层，采用 C/S 模式，服务器使用 UDP 端口 67，客户端使用 UDP 端口 68  
当租约 50%时，重新发送数据包，当 87.5%时，停止租约。

## 4. RIP 距离向量路由协议（rip 基于 Bellman-Ford 算法）

RIP 通过广播方式周期性（30s）的通告路由表，最大跳数为 15 跳。

RIP 有两个版本分别为 RIPv1 和 RIPv2。区别在：

- (1) RIPv1 不支持可变长度子网掩码（VLSM），而 RIPv2 支持 VLSM；
- (2) RIPv2 支持明文和 MD5 密文认证；
- (3) RIPv1 采用广播方式，RIPv2 采用组播方式，组播地址 224.0.0.9；
- (4) RIPv2 采用触发更新方式来加速路由收敛。
- (5) RIPv2 采用水平分割方法来消除路由循环。
- (6) RIPv2 支持路由汇总 CIDR

## 5. IGRP 是动态距离矢量路由协议，由 cisco 公司设计，每 90s 更新广播，

270s 没有收到更新，则认为路由不可访问，630s 后清除该路由。

IGRP 采用带宽、延迟、可靠性和负载作为度量标准，

度量最小的做最佳路径，不支持 VLSM 和不连续子网。

基本配置命令

```
Router igrp 109 //109 自治系统号
Network network-number //发布直连网段
Bandwidth 带宽 单位为 Kbps
Clock rate 时钟
```

EIGRP 是 cisco 在 IGRP 基础上的一种新的改进型协议，其度量值有：

带宽、延迟、可靠性、负载、最大传输单元。支持 VLSM 和 CIDR

## 7. 常见路由协议管理距离

RIP 管理距离 120，IGRP 为 100，EIGRP 为 90，OSPF 为 110，直连网络为 0

## 6. OSPF 开放式最短路径优先协议，是一种链路状态路由协议

OSPF 原理与配置命令（ospf 基于 Dijkstra 算法）

OSPF 主要优点

- (1) OSPF 没有跳数限制。
- (2) OSPF 支持 VLSM 和 CIDR
- (3) OSPF 采用触发更新，收敛速度快

三张表：邻居表 拓扑表 路由表

OSPF 网络划分为两个逻辑的级别：骨干区域记为 area0，非骨干区域

在 OSPF 中，定时发出 Hello 分组与特定的邻居进行联系，

默认情况下 40s 没收到该分组就认为对方不存在了。

TCP 进行流量控制的方法是采用可变大小的滑动窗口协议

## 7. RIP 支持 CIDR 和 VLSM，最大跳为 15，广播时间为 30s 更新

IGRP 不支持 CIDR、VLSM，90s 更新，270s 没收到，认为不可达，630s 清除路由。EIGRP 支持 CIDR/VLSM，度量值有：带宽、延迟、可靠性、负载、最大传输单元

OSPF 无跳数限制，支持 CIDR 和 VLSM，定时发 hello 与邻居进行联系，

40s 没收到认为对方不存在。区域号 1—65535，用的是反掩码。

EIGRP :network 192.168.1.0 0.0.0.255

OSPF :network 192.168.1.0 0.0.0.255 area 0

ISIS: network 49.0001.1111.1111.1111.00

RIP V2: network 192.168.1.0

BGP: neighbor 192.168.1.1 remote-as 64512

network 192.168.1.0 mask 255.255.255.0

ACL : access-list 10 permit 192.168.1.0 0.0.0.255

注：EIGRP，OSPF，ACL 后面要接子网反掩码

## 十四、数据编码

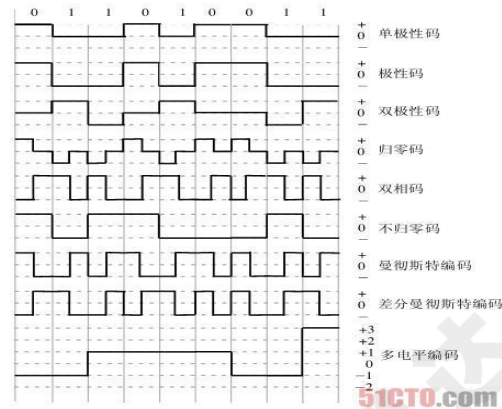


图2-3 常用编码方案

## 7. ISDN 综合业务数字网

ISDN 包括基本速率接口（2B+D）B 的速率 64kps，D 为 16dps

主要速率接口（30B+D）B 和 D 的速率是 64kps

## 十六、网络设备

中断器：工作物理层，起放大比特流作用

网桥：工作链路层，按要求选择 MAC 地址

路由器：工作网络层，路由选择，数据分组，计费

网关：工作高层，执行不同的协议，将不同协议转换。

## 十七、数据加密

DES：速度快，适用于加密大量数据场合。密钥长度 56

三重 DES：使用两个密钥，执行三次 DES 算法，强度更高，长度 112/168

IDEA：国际加密算法，长度 128 位密钥。

AES 支持 128、192 和 256 三种密钥长度。速度快，安全级别高。

加密密钥公开称为公钥，解密密钥隐藏在个体中称为私钥。

私钥带个人特性，可以解决数据的签名验证问题。

公钥用于加密和认证，私钥用于解密和签名

## 十八、报文摘要（MD）

报文摘要采用哈希算法，方法有 MD5 和 SHA

使用最广的方法 MD5，MD5 为 64 位，SHA 为 160 位

## 十九、网络管理

管理功能分为：管理站和代理两部分

网络管理系统分为：集中式、分布式、分层式

集成式：适合小型网络，分布式：适合大型网络。

网络管理功能：计费、安全、性能、配置、故障管理

计费、性能、故障属于监视，安全和配置属于控制功能。

## 十三、软件开发模型

瀑布模型，自顶到下的线性模型，后期测试阶段才能发现问题，增加了开发的风险，不适合开发需求不明确的情况。

V 模型：强调测试贯穿于整个过程中。

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

## 二十、IEEE802 标准

IEEE802.1d 生成树协议、w 快速生成树协议

x 基于端口访问，增加了安全性

IEEE802.1q 虚拟局域网

IEEE802.1A 局域网体系结构

E802.2 逻辑链路控制协议 802.3 CSMA/CD 与物理层规范

802.3u 快速以太网 802.3z 千兆以太网

802.3ae 万兆以太网 802.4 令牌总线标准 taken bus

802.5 令牌环标准 taken ring

802.10 局域网安全机制 802.11 无线局域网标准

数据链路层分为两个子层：

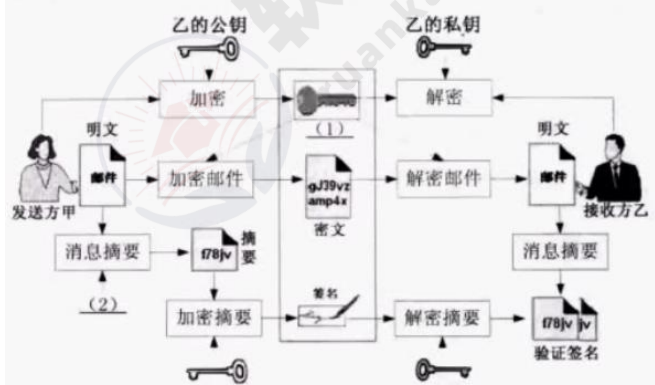
目的是将与硬件相关和与硬件无关的部分分开。

逻辑链路控制子层（LLC） 介质访问控制（MAC）：

IPSEC 封装在 IP 中传输

VPN 主要隧道协议有：PPTP (2)，L2TP (2)、IPsec (3)、SSLVPN\TSLVPN (4)

私钥用来签名和解密，公钥用来认证和加密的，具体可以看下图



1：会话密钥，2：MD5 3：甲的私钥 4：甲的公钥

第一条是认证和加密，第三条是签名和解密，

交换机的基本配置：

## 1、配置 enable 口令和主机名

```
Switch>          用户执行模式提示符
Switch>enable    进入特权模式
Switch#          特权模式提示符
Switch#config terminal 进入配置模式
Switch(config)# 配置模式提示符
Switch(config)#enable password cisco
Switch(config)#enable secret cisco
Switch(config)#hostname C2950
C2950(config)#end 退回到特权模式
```

## 2、配置交换机 IP 地址、默认网关、域名、域名服务器

```
C2950(config)#ip address 192.168.1.1 255.255.255.0
C2950(config)#ip default-gateway 192.168.1.254
C2950(config)#ip domain-name cisco.com 设置域名
C2950(config)#ip domain-server 200.0.0.1 设置域名服务器
```

## 3、设置交换机的端口属性

```
C2950(config)#interface fastethernet0/1 进入接口 0/1 的配置模式
C2950(config-if)# speed ? 查看 speed 命令的子命令
C2950(config-if)#speed 100 设置该端口速率为 100Mbps
C2950(config-if)#dplex ? 查看 dplex 命令的子命令
C2950(config-if)#dplex full 设置端口为全双工
C2950(config-if)#description TO_PC1 设置端口描述为 TO_PC1
C2950(config-if)#end (或 ^Z) 返回特权模式
C2950#show interface fastethernet0/1
C2950#show interface fastethernet0/1 status
```

## 4、配置和查看 MAC 地址表

```
C2950(config)#mac-address-table ?
查看 mac-address-table 的子命令
C2950(config)#mac-address-table aging-time 100
超时时间为 100s
C2950(config)#mac-address-table permanent
0000.0c01.bbcc f0/3 加入永久地址
C2950(config)#mac-address-table restricted static
0000.0c02.bbcc f0/6 f0/7 加入静态地址
C2950(config)#end
C2950#show mac-address-table 查看整个 MAC 地址表
C2950#clear mac-address-table restricted static
清除限制性地址
```

## 5、配置 VTP 协议 (VLAN Trunking Protocol)

配置 2950A 交换机为服务器模式

```
Switch>enable Switch#config terminal
Switch(config)#hostname 2950A 修改主机名为 2950A
2950A(config)#end
2950A#vlan dataBase 进入 VLAN 配置子模式
2950A(vlan)#vtp ? 查看和 VTP 配合使用的命令
2950A(vlan)#vtp server 为 Server 模式
Setting device to VTP SERVER mode
2950A(vlan)#vtp domain vtpserver 设置域名
Changing VTP domain name from NULL to vtpserver
2950A(vlan)#vtp pruning 启动修剪模式
2950A(vlan)#exit 退出 VLAN 配置模式
配置 2950B 为客户端模式，则他会从服务器
(2950A) 那里学习到 VTP 的其他信息
2950B(vlan)#vtp client
Setting device to VTP CLIENT mode
```

## 5、配置 VLAN Trunk 端口

```
Switch#config
Switch(config)#interface f0/24 进入端口 24 配置模式
Switch(config-if)#switchport mode trunk 设置当前端口为 Trunk 模式
Switch(config-if)#switchport trunk allowed vlan all
Switch(config-if)#exit
Switch(config)#exit
```

## 6、创建 VLAN

```
2950A#vlan dataBase
2950A(vlan)#vlan 2 创建一个 VLAN2
VLAN2 added:
Name:VLAN0002 系统自动命名
2950A(vlan)#vlan 3 name vlan3 建一个 VLAN3, 并命名为 vlan3
```

## 7、将端口加入到某个 VLAN 中

```
Switch#config terminal
Switch(config)#interface f0/9 进入端口 9 的配置模式
Switch(config-if)#switchport mode access
设置端口为静态 VLAN 访问模式
Switch(config-if)#switchport access vlan2
把端口 9 分配给相信的 VLAN2
Switch(config-if)#exit
Switch(config)#interface f0/10
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan3
Switch(config-if)#exit
Switch(config)#exit
```

## 8、配置 STP 权值

```
Switch1#config terminal
Switch1(config)#interface f0/23
Trunk1
Switch1(config-if)#spanning-tree vlan 1 port-priority 10
将 VLAN1、2 的端口权值设置为 10
Switch1(config-if)#exit
Switch1(config)#interface f0/24
Trunk2
Switch1(config-if)#spanning-tree vlan 3 port-priority 10
将 VLAN3、4、5 的端口权值设置为 10
Switch1(config-if)#end
Switch1#copy running-config start-config 保存配置文件
```

## 9、配置 STP 路径值的负载均衡

```
Switch1#config terminal
Switch1(config)#interface f0/23
Trunk1
Switch1(config)#spanning-tree vlan 3 cost 30
设置 VLAN3、4、5 生成树路径值为 30
Switch1(config-if)#exit
Switch1(config)#interface
f0/24
Trunk2
Switch1(config-if)#spanning-tree vlan 1 cost 30
设置 VLAN1、2 生成树路径值为 30
Switch1(config-if)#end
```

## 路由器基本配置

## 1、配置以太网

```
Router>enable 进入特权执行模式
Router#config t 进入全局配置模式
Router(config)#interface fastethernet0/1
Router(config-if)#ip address 192.168.1.11 255.255.255.0
Router(config-if)#no shutdown 激活接口
Router(config-if)#end 退回到特权模式
Router#show running-config 查看配置结果
```

## 2、配置终端服务器，设置两个路由器的主机名

Term\_Server#

```
Term_Server#router1 访问主机表中的 router1 路由器
Trying router1(10.1.1.1,2001)...Open
Router>enable
Router#config t
Router(config)#hostname router1 设置路由器 1 的主机名
Router1(config)#end
Router1#
Term_Server#
Term_Server#router2
Trying router2(10.1.1.1,2002)...Open
Router>enable
Router#config t
用 ctrl+shift+6 松开后按 6
Term_Server#show sessions 查看终端服务器的会话
Term_Server#disconnect2 断开会话 2
Term_Server#show line 1 查看线路 1 的状态
Term_Server#clear line 2 清除线路 2
```

## 3、配置静态路由

(1) IPv4 静态路由设置  
路由器 R1: E0(10.1.1.1/24) E1(192.168.1.1/24)  
路由器 R2: E0(10.1.1.2/24)  
路由器 R3  
R1#ping 10.1.1.2 (R1 上 ping R2, 结果连通)  
R1#ping 192.168.1.3 (R1 上 ping R3, 结果连通)  
从 R2 路由器 ping 路由器 R1 的 E1 接口  
R2#ping 192.168.1.1 (ping R1 的 E1 接口, 结果不连通)  
R2#show ip route (查看路由表)  
发现路由表中显示只有直接相连的网段 10.1.1.0/24 在其路由表内,  
标志为 C 表示连接(Connected)。为此, 可以在 R2 路由表中加入静态路由。

```
R2#config t
R2(config)#ip route 192.168.1.0 255.255.255.0 10.1.1.1
// (加入静态路由)
R2#(config)#end
这条静态路由由信息表示从该路由器出发往
192.168.1.0 255.255.255.0 网段的数据包其
下一跳点(Next Hop)的地址是 10.1.1.1(即通过 R1 的 E0 接口地址)。
再从 R2 ping R1 的 E1 接口, 发现可以 ping 通了。
注意: 在有些路由器上默认情况是不启动 IP 路由的,
这时可以用 ip routing 和 no ip routing 来启动和关闭 IP 路由。
```

## (2) IPv6 静态路由设置

R1: E0(2005::1/64) S0(2007::1/64)

PC1: IP 2005:CCCC::2/64 网关 2005:CCCC::1  
PC2: IP 2004:CCCC::2/64 网关 2004:CCCC::1

R1 相关配置如下。

```
Router#
Router#configure terminal
Router(config)#hostname R1
R1(config)#ipv6 unicast-routing (开启 IPv6 单播路由)
R1(config)#interface f0/0
R1(config-if)#ipv6 address 2005:CCCC::1/64 (设置 E0 口 IPv6 地址)
R1(config-if)#no shut
R1(config-if)#exit
R1(config)#interface Serial0/2/0
R1(config-if)#ipv6 address 2007:CCCC::1/64 (设置 S0 口 IPv6 地址)
R1(config-if)#clock rate 128000 (配置 S0 口时钟频率)
R1(config-if)#exit
R1(config)#ipv6 route 2004:CCCC::/64 Serial0/2/0 设置 IPv6 静态地址)
```

R2 相关配置如下。

```
Router#
Router#configure terminal
Router(config)#hostname R2
R2(config)#ipv6 unicast-routing (开启 IPv6 单播路由)
R2(config)#interface f0/0
R2(config-if)#ipv6 address 2004:CCCC::1/64 (设置 E0 口 IPv6 地址)
R2(config-if)#no shut
R2(config-if)#exit
R2(config)#interface Serial0/2/0
R2(config-if)#ipv6 address 2007:CCCC::2/64 (设置 S0 口 IPv6 地址)
R2(config-if)#clock rate 128000 (配置 S0 口时钟频率)
R2(config-if)#exit
R2(config)#ipv6 route 2005:CCCC::/64 Serial0/2/0 (设置 IPv6 静态路由)
```

## 五、配置路由协议

RIP 相关命令

命令	功能
router rip	指定使用 RIP 协议
version{1 2}	指定 RIP 版本
network network	指定与该路由器相连的网络
show ip route	查看路由表信息
show ip route rip	查看 RIP 协议路由信息

```
R1#config t
R1(config)#no logging console
// (不在控制台接口显示 log 提示信息)
R1(config)#interface fastethernet0/1
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface serial 0
R1(config-if)#ip address 192.168.65.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface serial 1
R1(config-if)#ip address 192.168.67.1 255.255.255.0
R1(config-if)#no shutdown
用 show ip route 命令查看路由表信息
```

配置路由器 R1

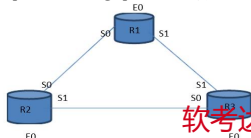
```
R1(config)#ip routing (允许路由选择协议)
R1(config)#router rip (进入 rip 协议配置子模式)
R1(config-router)#network 192.168.1.0 (声明网络 192.168.1.0/24)
R1(config-router)#network 192.168.65.0
R1(config-router)#network 192.168.67.0
R1(config-router)#version 2 (设置 RIP 协议版本 2)
R1(config-router)#exit
类似配置路由器 R2、R3
R2(config-router)#network 192.168.3.0
R2(config-router)#network 192.168.65.0
R2(config-router)#network 192.168.69.0
R3(config-router)#network 192.168.5.0
R3(config-router)#network 192.168.67.0
R3(config-router)#network 192.168.69.0
```

## 2. 配置 IGRP 协议

内部网关路由协议 (Interior Gateway Routing Protocol, IGRP) 是一种动态距离向量路由协议, 它不支持 VLSM 和不连续的子网。默认情况下, IGRP 每 90s 发送一次路由更新广播, 在 3 个更新周期内 (即 270s) 没有从路由表中的一个路由器接收到更新, 则宣布路由不可用。在 7 个更新周期 (即 360s) 后, IOS 软件从路由表中清除路由。

IGRP 相关命令

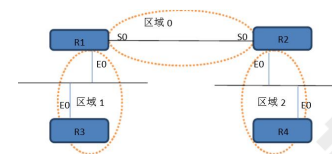
命令	功能
router igrp autonomous-system	指定使用 IGRP 协议
network network	指定与该路由器相连的网络
show ip route	查看路由表信息
show ip route igrp	查看 IGRP 协议路由信息



图中各接口 IP 地址分配如下。

## 3. 配置 OSPF 协议

router ospf process-id 指定使用 OSPF 协议  
network address wildcard-mask area area-id  
//指定与该路由器相连的网络  
show ip route 查看路由表信息  
show ip route ospf 查看 OSPF 协议路由信息  
注: 1. OSPF 路由进程 process-id 需要指定范围在 1-65535 之间。  
3. wildcard-mask 是子网掩码的反码, 网络区域 ID area-id 是在 0-4294967295 内的十进制数, 也可以带有 IP 地址格式的 x.x.x.x。当网络区域 ID 为 0 时为主干域。不同网络区域的路由器通过主干域学习路由信息。按照设计图所示的网络拓扑结构图来配置 OSPF 协议。



R1	E0	192.1.0.129/26
R1	S0	192.200.10.5/30
R2	E0	192.1.0.65/26
R2	S0	192.200.10.6/30
R3	E0	192.1.0.130/26
R4	E0	192.1.0.66/26

```
R1:
interface Ethernet 0
ip address 192.1.0.129 255.255.255.192
Interface serial 0
ip address 192.200.10.5 255.255.255.252
router ospf 100
network 192.200.10.4 0.0.0.3 area 0
network 192.1.0.128 0.0.0.63 area 1
R2:
```

```
interface Ethernet 0
ip address 192.1.0.65 255.255.255.192
interface serial 0
ip address 192.200.10.6 255.255.255.252
router ospf 200
network 192.200.10.4 0.0.0.3 area 0
network 192.1.0.64 0.0.0.63 area 2
R3:
```

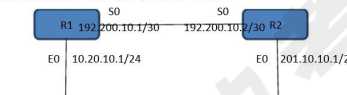
```
interface ethernet 0
ip address 192.1.0.130 255.255.255.192
router ospf 300
network 192.1.0.128 0.0.0.63 area 1
R4:
```

```
interface Ethernet 0
ip address 192.1.0.66 255.255.255.192
router ospf 400
network 192.1.0.64 0.0.0.63 area 1
用以下命令来调试或查看配置信息和路由信息。
debug ip ospf events
debug ip ospf packet
show ip ospf
show ip ospf database
show ip ospf interface
show ip ospf neighbor
show ip route
```

## 4. 配置 EIGRP 协议

EIGRP 是增强型 IGRP 协议, 是最典型的平衡混合路由选择协议, 它使用一种扩散更新算法, 实现了很高的路由性能。

参照所示网络拓扑图, 配置 EIGRP 协议使全网连通。



如同配置其他网络路由协议一样, 首先根据拓扑结构图配置各接口, 接下来在 EIGRP 协议配置模式下, 使用 network 命令来声明网段。与 RIP 和 IGRP 协议不同的是, EIGRP 协议的网段声明中, 如果是主网地址 (即 A、B、C 类的主网, 没划分子网的网络), 只需输入此网络地址; 如果是子网的话, 则必须在网络地址后面写入反掩码。

配置中使用 no auto-summary 命令关闭了 EIGRP 协议的路由自动汇总功能, 默认的配置是自动汇总生效。在处理 VLSM 尤其是存在不连续子网的网络中, 通常都需要关闭该功能。

下面给出各路由器的配置清单, 只列出其重要的配置信息。

```
R1#show running-config
Interface Serial0
Ip address 192.200.10.1 255.255.255.252
Interface Ethernet0
Ip address 10.20.10.1 255.255.255.255
router eigrp 200
network 192.200.10.0 0.0.0.3
network 10.20.10.0 0.0.0.255
no auto-summary
```

```
R2#show running-config
Interface Serial0
```

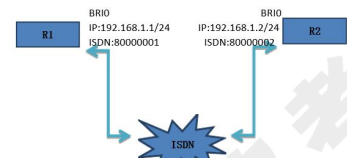


```
Ip address 192.200.10.2 255.255.255.0
Interface Ethernet0
Ip address 201.10.10.1 255.255.255.255
router eigrp 200
network 192.200.10.0 0.0.0.3
network 201.10.10.0
no auto-summary
```

## 六、配置广域网接入

### 1. 配置 ISDN

综合业务数字网(Integrated Service Digital Network, ISDN)是电话网络数字化的结果,由数字电话和数据传输服务两部分组成。ISDN 提供两种类型的访问接口,即基本速率接口(Basic Rate Interface, BRI)和主要速率接口(Primary Rate Interface, PRI)。



连接好线路后,就可以进行配置工作。

```
R1#config t
R1(config)#isdn switch-type ?
(查看交换机类型,在中国使用 basic-net3 类型的最多)
配置 R1:
R1(config)#isdn switch-type basic-net3 (设置交换机类型为 basic-net3)
R1(config)#interface bri0 (进入 BRI 接口配置模式)
R1(config-if)#ip address 192.168.1.1 255.255.255.0 (设置接口 IP 地址)
R1(config-if)#encapsulation ppp (设置封装协议为 ppp)
R1(config-if)#dialer string 800000002 (设置拨号串, R2 的 ISDN 号码)
R1(config-if)#dialer-group 1
//(设置拨号组号为 1, 把 BRI0 接口与拨号列表 1 相关联)
R1(config-if)#no shutdown (激活接口)
R1(config-if)#exit
R1(config)#dialer-list 1 protocol ip permit (设置拨号列表 1)
R1(config)#end
其中 dialer-list 1 protocol ip permit 允许 IP 协议包成为引起拨号的“感兴趣包”,即当有 IP 包需要在拨号线路上传送时可以引起拨号。
```

配置 R2:

```
R2(config)#isdn switch-type basic-net3 (设置交换机类型为 basic-net3)
R2(config)#interface bri0 (进入 BRI 接口配置模式)
R2(config-if)#ip address 192.168.1.2 255.255.255.0 (设置接口 IP 地址)
R2(config-if)#encapsulation ppp (设置封装协议为 ppp)
R2(config-if)#dialer string 800000001 (设置拨号串, R1 的 ISDN 号码)
R2(config-if)#dialer-group 1
(设置拨号组号为 1, 把 BRI0 接口与拨号列表 1 相关联)
R2(config-if)#no shutdown (激活端口)
R2(config-if)#exit
R2(config)#dialer-list 1 protocol ip permit (设置拨号列表 1)
R2(config)#end
R2#
```

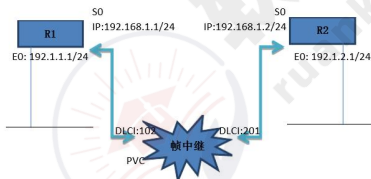
配置完成后,可以使用 debug 和 ping 命令来调试配置结果。

```
R1(config)#logging console (在终端上显示监测信息)
R1(config)#exit
R1#debug dialer (监测 dialer 信息)
Dial on demand events debugging is on
R1#ping 192.168.1.2 (内容省略...)
R1#undebug all (关闭所有调试信息)
还可以用 show isdn status 命令查看 ISDN 状态,
用 show dialer 命令显示当前的拨号及其配置等信息。
```

### 2. 配置帧中继

帧中继是一种高性能的 WAN 协议,运行在 OSI 参考模型的物理层和数据链路层。它是一种数据包交换技术,是 X.25 的简化版本。帧中继技术提供面向连接的数据链路层通信,帧中继广域网的设备分为 DTE 和 DCE,路由器作为 DTE 设备。

帧中继配置实例如图所示



(1) 配置基本的帧中继连接。

```
路由器 R1:
R1#config t
R1(config)#interface E0
R1(config-if)#ip address 192.1.1.1 255.255.255.0
R1(config-if)#no keepalive
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface s0
R1(config-if)#ip address 192.168.1.1 255.255.255.0
```

```
R1(config-if)#no shutdown
R1(config-if)#no frame-relay inverse-arp (关闭帧中继逆向 ARP)
R1(config-if)#frame map ip 192.168.1.2 cisco
```

路由器 R2:

```
R2#config t
R2(config)#interface E0
R2(config-if)#ip address 192.1.2.1 255.255.255.0
R2(config-if)#no keepalive
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#interface s0
R2(config-if)#ip address 192.168.1.2 255.255.255.0
R2(config-if)#encap frame-relay (该接口使用帧中继封装格式)
R2(config-if)#no shutdown
R2(config-if)#no frame-relay inverse-arp (关闭帧中继逆向 ARP)
R2(config-if)#frame map ip 192.168.1.1 cisco
R2(config-if)#end
R2#
```

配置完成后可以用下面的命令查看帧中继相关信息。

```
show frame pvc
show frame map
show frame traffic
show frame lmi
```

### 10、配置 IPsec

IKE 和 isakmp 是 synonym  
isakmp enable 启用或关闭 IKE  
isakmp policy 创建 IKE 策略  
isakmp key 配置预共享密钥  
show isakmp [policy] 验证 IKE 的配置  
access-list acl-name {permit|deny} protocol  
--src\_addr src\_mask [operator port[port]]  
--dest\_addr dest\_mask [operator port[port]]  
access-list 命令配置加密访问列表  
show 和 debug 用来测试和验证

### 11、ACL 配置 (分标准和扩展两类)

标准只对数据包的源地址进行过滤(1-99)  
Router(config)#access-list ACL # permit|deny conditions  
如: access-list 10 permit host 172.16.1.0 0.0.0.255  
access-list 10 deny host 172.16.1.1  
ip access-group 10 in/out(in 表示进站, out 表示出站)  
扩展的可以根据源地址和目的地址及端口号进行过滤(100-199)  
Access-list 100 permit udp any host 176.16.1.1 eq dns log  
表示允许来自任何源地址的 DNS 请求通过, 被查询的 DNS 服务器为 172.16.1.1

文件目录:

Linux 2012 年 9 月 19 日

/bin	存入普通用户可以使用的命令文件。目录/usr/bin 也可用来贮存用户命令
/sbin	存放非普通用户使用的命令(有时隔不久普通用户也可能用到)。目录/usr/sbin 中也包括了许多系统命令
/etc	系统的配置文件
/root	系统管理员(root 或超级用户)的主目录
/usr	包括与系统用户直接相关的文件和目录,一些主要的应用程序保存在该目录下
/home	用户主目录的位置,保存了用户文件(用户自己的配置文件,文档,数据等)
/dev	设备文件。在 Linux 中设备以文件形式表现,从而可以按照操作文件的方式简便地对设备进行操作
/mnt	文件系统挂载点、用于安装移动介质,其它文件系统的分区、网络共享文件系统或任何可安装文件系统
/lib	包含许多由/bin 和/sbin 中的程序使用的共享库文件。目录/usr/lib 中含有更多用于用户程序的库文件
/boot	包括内核和其它系统启动时使用的文件
/var	包含一些经常改变的文件。例如假脱机( spool ) 目录、文件日志目录、锁文件、临时文件等等
/initrd	在计算机启动时挂载 initrd.img 映像文件的目录以及载入阻挡层需设备模块的目录
/opt	存放可选择安装的文件和程序。主要由第三方开发者用于安装和卸装他们的软件包
/tmp	用户和程序的临时目录,该目录中的文件被系统自动清空
/lost+found	在系统修复过程中恢复的文件,统称为关机后,这里就存放了一些文件
/proc	操作系统的内存映像文件系统,是一个虚拟的文件系统。当您查看它们时,看到的是内存里的信息,这些文件夹有助于了解系统内部信息

目录文件类命令:

```
cd 切换目录    dir 显示目录内容    ls 显示目录内容
cat 显示内容, 适合小文件
less 分屏显示, 可前后翻
more 分屏显示内容, 不可向前翻页
head 显示文件头部内容    tail 显示文件尾部内容
touch 创建文件或更新文件访问时间
mkdir 创建目录    rmdir 删除目录    rm 删除文件或目录(-r)
cp 复制文件或目录    mv 移动或改名    chown 修改文件所有者
chgrp 修改文件所属组    chmod 修改文件目录权限
find 查找文件或目录
```

常用工具:

```
tar 打包工具    gzip/gunzip 压缩工具
bzip2/bunzip2 压缩工具    vi 文本编辑工具
```

**用户类命令：**

useradd 添加用户 userdel 删除用户  
 usermod 修改用户属性 passwd 设置密码  
 groupadd 添加组 groupmod 修改组属性  
 groupdel 删除组  
 gpasswd 将用户添加到组或从组中删除  
 id 显示当前用户  
 ID 属性  
 who 显示当前登录的用户 w 同上，略有不同  
 chfn 修改用户信息 su 切换用户  
 chsh 修改登录

**Shell 帮助类命令：**

help 显示内部命令帮助 man 查看手册  
 info 查看 texinfo 格式手册

**文件系统类命令：**

fdisk 分区命令 mkfs 格式化命令  
 e2label 设置卷标 mount 挂载文件系统  
 umount 解除挂载文件系统 fsck 文件系统检查  
 mkswap 创建

**swap 文件系统**

quotacheck 检查配额 quotaon 启用配额  
 quotaoff 关闭配额 edquota 设置用户磁盘配额

**软件包管理：**

rpm redhat 包管理工具 apt Debian 包管理工具  
 yum Yellow dog 包管理工具

**系统管理命令：**

date 显示 / 设置系统时间  
 shutdown 关闭系统 reboot 重启系统  
 halt 关闭系统 runlevel 显示运行级  
 init 切换运行级 grub-install 安装  
 GRUB cal 显示日历

**内核管理类命令：**

lsmod 显示已加载内核模块 insmod 添加内核  
 modprobe 添加内核模块 modinfo 显示内核模块信息  
 rmmod 移除内核模块

**进程管理类命令：**

ps 显示系统进程 top 进程管理工具  
 pstree 显示进程树 pidof 显示指定程序的进程号  
 nice 设置进程优先级

**网络基础类命令**

ifconfig 查看 / 设置网卡参数  
 ifup 启用网络设备  
 ifdown 关闭网络设备  
 lsof 显示指定端口由谁监听  
 sysctl 控制 TCP/IP 内核参数  
 adsl-setup 设置 ADSL 连接参数  
 adsl-status 显示 ADSL 连接状态  
 adsl-connect 启动 ADSL 连接  
 netstat 显示系统网络状态信息  
 route 查看路由表  
 ip 强大的网络管理工具  
 ping 测试连通性  
 traceroute 路径跟踪

ps 命令语法格式如下： ps [option] ps ax ps -ef

常用选项说明如下：

-e：显示所有进程。-f：全格式。-u：打印用户格式，显示用户名和起始时间。

ps 重要的输出字段

USER 进程 PID 进程号 STAT 进程状态，常见的值有

R:可执行的 S:睡眠状态 Z:僵尸 I:空闲

PPID: 父进程进程号 KILL: 结束进程

Linux 系统运行级别由列在/etc/rc.d/rc<x>.d 目录中的服务来定义，其中<x>是运行级别的数字：

- 0: 终止所有进程，关机。
- 1: 单用户模式，用于维护系统，只有少数进程运行。
- 2: 多用户模式，和运行级别 3 一样（除没有启动 NFS 服务）。
- 3: 完整的多用户模式，进入 Linux 系统的文本字符界面。
- 4: 没有使用（可由用户定义）。
- 5: 完整的多用户模式，进入 Linux 系统的基于 X 的图形界面。
- 6: 重新启动

A: 修改系统级别：#vi /etc/inittab

id:5:initdefault: //把 5 修改为想要的运行级别

#telinit n //n 为 0~6，只有 root 用户才能使用此命令

**1、ifconfig**

可以使用 ifconfig 命令来配置并查看网络接口的配置情况。

例如：

- (1) 配置 eth0 的 IP 地址，同时激活该设备。

```
#ifconfig eth0 192.168.1.1 netmask 255.255.0 up
```

- (2) 配置 eth0 别名设备 eth0:1 的 IP 地址，并添加路由。

```
#ifconfig eth0 192.168.1.3
```

```
#route add -host 192.168.1.3 dev eth0:1
```

- (3) 激活设备。 #ifconfig eth0 up

- (4) 禁用设备。 #ifconfig eth0 down

- (5) 查看指定的网络接口的配置。 #ifconfig eth0

- (6) 查看所有的网络接口配置。 #ifconfig

**2、route**

可以使用 route 命令来配置并查看内核路由表的配置情况。 例如：

- (1) 添加到主机的路由。

```
#route add -host 192.168.1.2 dev eth0:0
```

```
#route add -host 10.20.30.148 gw 10.20.30.40
```

- (2) 添加到网络的路由。

```
#route add -net 10.20.30.40 netmask 255.255.255.248 eth0
```

```
#route add -net 10.20.30.48 netmask 255.255.255.248 gw 10.20.30.41
```

```
#route add -net 192.168.1.0/24 eth1
```

- (3) 添加默认网关。

```
#route add default gw 192.168.1.1
```

- (4) 查看内核路由表的配置。 #route

- (5) 删除路由。

```
#route del -host 192.168.1.2 dev eth0:0
```

```
#route del -host 10.20.30.148 gw 10.20.30.40
```

```
#route del -net 10.20.30.40 netmask 255.255.255.248 eth0
```

```
#route del -net 10.20.30.48 netmask 255.255.255.248 gw 10.20.30.41
```

```
#route del -net 192.168.1.0/24 eth1
```

```
#route del default gw 192.168.1.1
```

对于 1 和 2 两点可使用下面的语句实现：

```
Ifconfig eth0 172.16.19.71 netmask 255.255.255.0
```

```
Route 0.0.0.0 gw 172.16.19.254
```

Service network restart

**3、traceroute**

可以使用 traceroute 命令显示数据包到达目的主机所经过的路由

**4、ping**

可以使用 ping 命令来测试网络的连通性

**5、hostname**

可以使用 hostname 命令来更改主机名

**6、arp** 可以使用 arp 命令来配置并查看 arp 缓存。例如：

- (1) 查看 arp 缓存。 #arp

- (2) 添加一个 IP 地址和 MAC 地址的对应记录。

```
#arp -s 192.168.33.15 00:60:08:27:CE:B2
```

- (3) 删除一个 IP 地址和 MAC 地址的对应缓存记录。

```
#arp -d 192.168.33.15
```

**介质选择：**

》550 米用单模 500 米内用多模 100 米用双绞线 25 米用同轴电缆

POE（无源）用网线连接（6 类双绞线），这个电源在网线中，四根信号线，2 根电源线。

**DMZ 表示有防火墙的工作区**

连接外网的一般是路由器，然后是防火墙，然后是核心交换机，再就是汇聚、接入交换机。

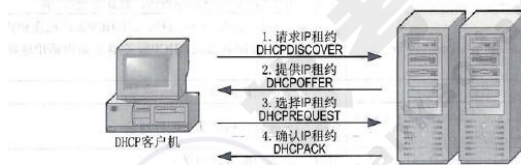
MPLS 中，P 表示核心路由器，CP 边界路由器、CE 表示客户路由器。

在 LINUX 中，命令格式，(service) 服务+名称+start/stop

无线网接入技术有：GSM 接入、CDMA 接入、GPRS 接入、WCDMA 接入、3G 通信

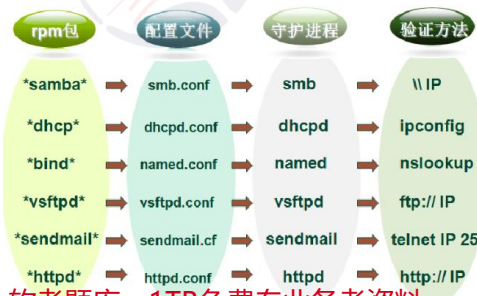
**DHCP**

- 请求 IP 租约——客户通过广播的形式发送 DHCP DISCOVER（DHCP 发现）报文；
- 提供 IP 租约——DHCP 服务器返回一个 DHCP OFFER 报文；
- 选择 IP 租约——客户设置服务器 ID 和 IP 地址，并发送给服务器一个 DHCP REQUEST 报文；
- 确认 IP 租约——服务器发送 DHCP ACK（DHCP 确认）确认报文，以确定此租约成立，在此报文中还包含其他 DHCP 选项信息。



客户机在发送 DHCP DISCOVER 报文时，客户机没有 IP，因此，以广播的形式发送，该报文源地址为 0.0.0.0，目标地址为 255.255.255.255。

当租约期限过了一半时，客户机向服务器发送更新 IP 租约





## 一、SMB 服务

1. SMB 服务功能：不同系统主机之间实现文件、打印机等资源共
2. SMB 服务主配置文件路径：/etc/samba/smb.conf/
3. SMB 服务启动（重启、停止）方法：# service smb start (restart、stop)
4. SMB 主配置文件片段：
 

Security = user (share)	安全模式
[ BDDY ]	共享名
comment = BDDY share	注释
path = /root/bddy	共享路径
public = no	匿名访问权限
writable = yes	允许写入权限
valid users = bob,tom,@bddy	访问限制
5. 在服务器安全模式设为 user 时，符合哪些条件的用户才能顺利访问 SMB 服务器？
 

答：存在用户，用户生效，为用户设置 smb 密码

```
# useradd XXX
# passwd XXX
# smbpasswd -a XXX
```
6. 客户端如何实现对 SMB 服务器的访问？
 

答：\\ samba 服务器 IP 地址

## 二、DHCP 服务

1. DHCP 服务功能：动态主机配置协议 自动分发 TCP/IP 参数
2. DHCP 服务主配置文件路径：/etc/dhcpd.conf。该文件组建安装成功后会生成一个范本，要复制过来：#cp /usr/share/doc/dhcp\*/dhcpd.conf.sample /etc/dhcpd.conf
3. DHCP 服务启动（重启、停止）方法：#service dhcpd start (restart、stop)
4. DHCP 主配置文件片段：
 

subnet 192.168.100.0 netmask 255.255.255.0	子网
option routers 192.168.100.1;	网关
option subnet-mask 255.255.255.0;	子网掩码
option domain-name-servers 192.168.100.2;	DNS 地址
range ... 192.168.100.100 192.168.100.250;	地址池范围
default-lease-time 21600;	默认租约时间
max-lease-time 43200;	最大租约时间
5. 客户端验证 DHCP 服务的功能：先修改客户端地址为自动获取 IP
 

```
ipconfig /all 自动获得 IP 地址
ipconfig /release 释放 IP 地址
ipconfig /renew 重新得到新的 IP 地址
```
6. 如果客户端有特殊要求，需要 DHCP 服务器实现 MAC-IP 地址的绑定，该如何实施？
 

```
host ns {
    hardware ethernet 00:50:56:C0:00:01; 客户端的物理地址
    fixed-address 192.168.100.100; 要给客户端的地址
}
```

## 三、DNS 服务

1. DNS 服务功能：名称解析
2. DNS 服务主配置文件和正反向区域文件路径：
 

/etc/named.conf	主配置文件
/var/named/wl.com.bd	正向区域文件
/var/named/192.168.100.bd	反向区域文件
3. DNS 服务启动（重启、停止）方法：
 

```
#service named start(restart、stop)
```
4. 正向区域文件片段：名称=>地址
 

NS	192.168.100.1.	
www	IN	A 192.168.100.2
ftp	IN	A 192.168.100.3
5. 反向区域文件片段：地址=>名称
 

NS	192.168.100.1.
2	PTR www.wl.com.
3	PTR ftp.wl.com.
6. Linux 客户端验证 DNS 服务：host  
Windows 客户端验证 DNS 服务：nslookup

## 四、FTP 服务

1. FTP 服务功能：实现文件上传、下载
2. FTP 服务主配置文件和用户权限限制文件路径？
 

/etc/vsftpd/vsftpd.conf	主配置文件
/etc/vsftpd/ftpusers	限制文件一：用户不在此文件里，可成功
/etc/vsftpd/user_list	限制文件二：若 vsftpd.conf 文件里 userlist=yes, 用户不在此文件里，可成功；若 vsftpd.conf 文件里 userlist=no, 用户在此文件里，可成功
3. FTP 服务启动（重启、停止）方法：
 

```
# service vsftpd start (restart、stop)
```
4. FTP 服务中的两个匿名用户是：ftp、anonymous
5. FTP 服务匿名访问默认的共享位置：匿名用户的根目录为 / var / ftp
6. 实现匿名用户的上传和下载，需要关注和修改配置文件中哪些语句？默认上传目录的权限又该如何修改？
 

```
anonymous_enable = YES 允许用户匿名登录
anon_upload_enable = YES 允许匿名用户上传文件
# chmod o+w /var/ftp/pub 修改权限
```
7. 实现特定用户访问 FTP 服务器的主配置文件片段：
 

```
anonymous_enable = NO 关闭匿名用户访问权限
local_root = / home 描述文件系统中共享路径
chroot_local_user = YES 将用户锁定在上述目录中，不能访问别处
```
8. 客户端对 FTP 服务器的访问：ftp://用户名：密码@服务器 IP

## 五、MAIL 服务

1. 安装 sendmail 邮件发送组件：#rpm -ivh sendmail-cf-\*  
安装 dovecot 邮件接收组件，顺序不可变：
 

```
#rpm -ivh perl-*
#rpm -ivh mysql-5.0.45-*
#rpm -ivh postgresql-libs-*
#rpm -ivh dovecot-1.07-*
```
2. 配置 DNS：正向区域文件添加 MX 记录和 A 记录  
反向区域文件添加 MX 记录和 PTR 记录
3. 配置邮件服务
  - (1) / etc / dovecot.conf 打开 dovecot.conf 配置文件，命令模式下 /protocols 查找 protocols，将“#”去掉 启动 dovecot 服务
  - (2) sendmail 先备份文件，打开 sendmail.mc 配置文件，作如下修改：命令模式下/DAEMON\_OPTIONS 查找，将回环地址改为服务器地址  
命令模式下/TRUST\_AUTH\_MECH 查找，将这一行和下一行的注释去掉，“dn1”命令模式下/LOCAL\_DOMAIN 查找，改为自己的域名  
用 m4 工具将编辑好的 sendmail.mc 文件内容重定向到 sendmail.cf 文件中  
mail # m4 sendmail.mc > sendmail.cf
3. 验证 DNS 服务命令片段：
 

```
# nslookup 验证命令
>set type = MX 查询本地域中邮件服务器名称
>set type = A 查询名称对应的 IP 地址
```
4. 在同一域里，如何实现邮件群发？
 

```
# vi / etc / aliases 别名：用户 1，用户 2，用户 3
```
5. 在 Linux 客户端验证 Mail 服务的方法
 

```
# telnet 邮件服务器 25
hello ****
mail from: 发送邮箱帐户
rcpt to: 接收邮箱帐户
data: 编辑邮件
# Su - 用户名 $ mail
```
6. 在 Windows 客户端验证 Mail 服务的方法  
outlook

## 六、WEB 服务

1. Apache 主配置文件的路径：/etc/httpd/conf/httpd.conf
2. Apache 默认的发布路径：/var/www/html 用户发布路径：/home/用户名/public\_html
3. 配置文件片段：
 

StartServers	8	默认开启进程数量
MinSpareServers	5	默认最小开启进程数量
MaxSpareServers	20	默认最大开启进程数量
DirectoryIndex	1.html index.html	可以被识别的首页文件
# UserDir	disable	开启普通用户发布网页权限
4. Web 服务中配置虚拟主机的作用？  
实现同一台 Web 服务器中多个站点的发布
5. 配置文件片段：
 

```
NameVirtualHost 192.168.100.1:80 启用申明
<VirtualHost 192.168.100.1:80> 头部
DocumentRoot /var/www/html 发布路径
ServerName www.wl.com 对应名称
</ VirtualHost >
尾部
```
6. 客户端验证 Web 服务的方法：http:// IP