

【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

网

络

工

程

师

目录

第一章：计算机网络概论.....	1
第二章：数据通信基础.....	4
第三章：广域通信网.....	15
第四章：局域网与城域网.....	22
第五章：无线通信网.....	30
第六章：网络互连与互联网（1）.....	36
第六章：网络互连与互联网（2）.....	43
第六章：网络互连与互联网（3）.....	49
第六章：网络互连与互联网（4）.....	58
第七章：下一代互联网.....	67
第八章：网络安全与应用（1）.....	71
第八章：网络安全与应用（2）.....	79
第九章：网络操作系统与应用服务器（1）.....	85
第九章：网络操作系统与应用服务器（2）.....	93
第九章：网络操作系统与应用服务器（3）.....	103
第九章：网络操作系统与应用服务器（4）.....	118
第十章：组网技术（1）.....	131
第十章：组网技术（2）.....	144
第十章：组网技术（3）.....	150
第十章：组网技术（4）.....	155
第十章：组网技术（5）.....	163
第十章：组网技术（6）.....	173
第十一章：网络管理.....	181
第十二章：网络规划与设计.....	199

第一章：计算机网络概论

考点 01: 计算机网络是通过通信线路和通信设备连接的许多的分散独立工作的计算机系统，遵从一定的协议用软件实现资源共享的系统。

考点 02: 组成为硬件、软件、协议三部分。

考点 03: 协议分为国际标准 OSI/RM 和公认标准 TCP/IP

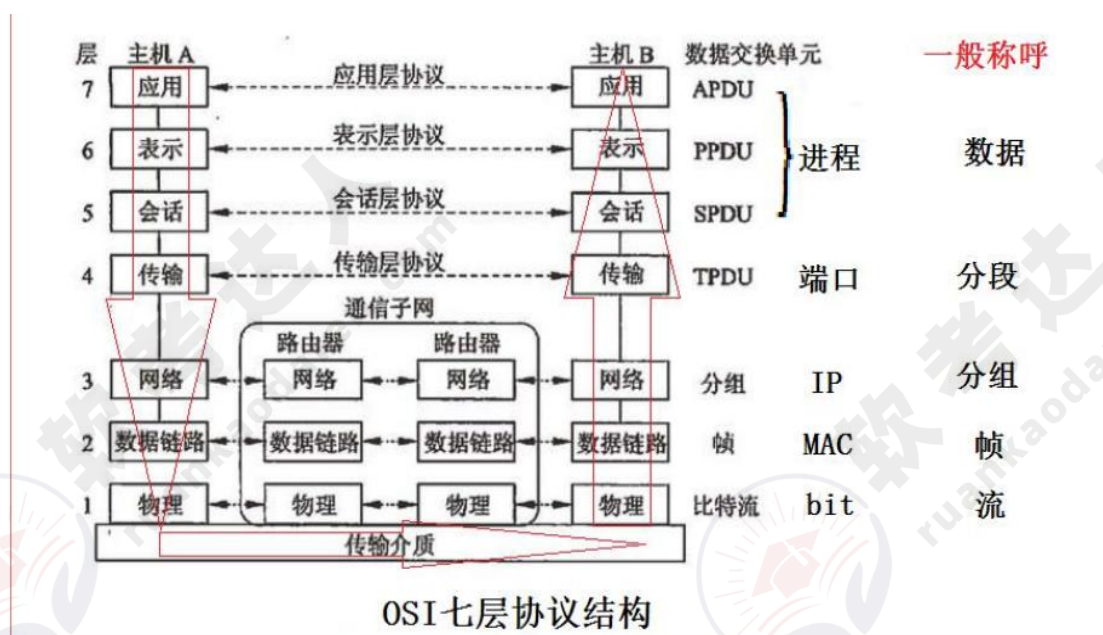
考点 04:

(1)按分布范围：分为局域网、城域网、广域网。

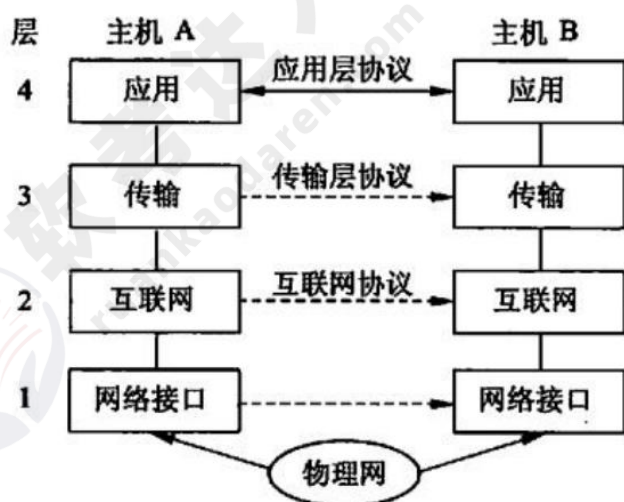
(2)按拓扑结构：分为星型、环型、树型等。

(3) 其他分类：公用网与专用网；通信网 ISP 与信息网 ICP；校园网与企业网；骨干网与接入网；有线网与无线网等。

考点 05: OSI/RM (开放系统互联参考模型) 七层是应用层、表示层、会话层、传输层、网络层、数据链路层、物理层。



考点 06： TCP/IP（因特网传输协议）四层是应用层、传输层、互联网层、网络接口层。



TCP/IP四层协议结构

考点 07： 七层 OSI 和四层 TCP/IP 协议对比

OSI 模型	TCP/IP 模型	主要协议
7 应用层	4 应用层	HTTP、FTP、DNS、SNMP TELNET、SMTP、POP3
6 表示层		
5 会话层		
4 传输层	3 传输层	TCP、UDP
3 网络层	2 互联网层	IP、ICMP
2 数据链路层	1 网络接口层	IEEE802系列、 HDLC、PPP
1 物理层		

OSI 模型与 TCP/IP 模型对比

考点 08： 七层协议各层实现功能如下表。

OSI 模型	TCP/IP 模型	主要协议
7 应用层	4 应用层	HTTP、FTP、DNS、SNMP TELNET、SMTP、POP3
6 表示层		
5 会话层		
4 传输层	3 传输层	TCP、UDP
3 网络层	2 互联网层	IP、ICMP
2 数据链路层	1 网络接口层	IEEE802系列、 HDLC、PPP
1 物理层		

OSI 模型与 TCP/IP 模型对比

考点 09：网络数据传输整个过程——数据封装

考点 09：网络数据传输整个过程——数据传输

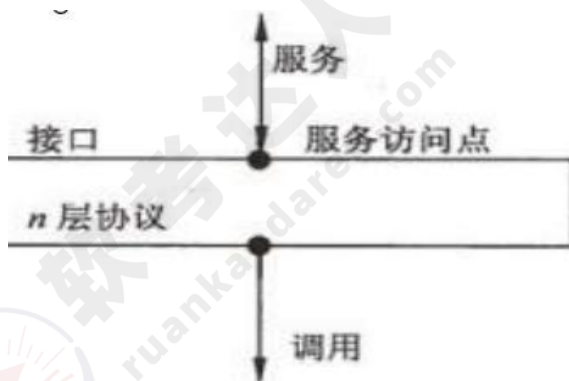
考点 09：网络数据传输整个过程——数据解封

考点 10：协议、接口、服务概念及三者关系

协议：三要素 语法（数据格式）、语义（完成动作）、时序（顺序排序）。

服务：两大类面向连接（电话）、无连接（寄信）。

接口：上下层服务访问点 AP

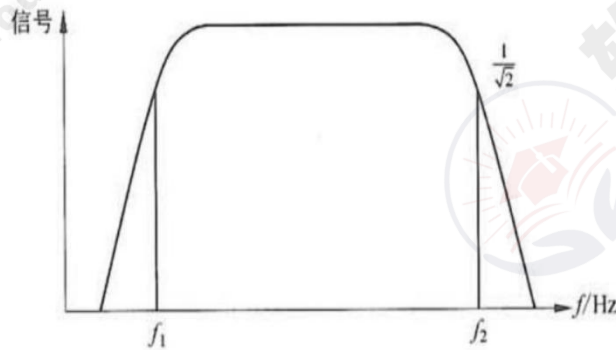


服务、接口和调用的关系图

第二章：数据通信基础

考点 01：基本概念：信源、信道、信宿；数字信号、模拟信号；模拟通信、数字通信（信道中传送）。

考点 02：模拟信道带宽计算： $W=f_2-f_1$ ，其中 f_1 是低频， f_2 是高频。



考点 03：数字信道带宽计算：奈奎斯特定理（无噪声） W 为带宽

奈奎斯特定理： $B=2W$ （ B 码元速率、波特率）

信息量 n （位）与码元种类 N ： $n=\log_2 N$

数据速率 $R=Bn = B\log_2 N = 2W\log_2 N$

考点 04：数字信道带宽计算：香农定理（有噪声）

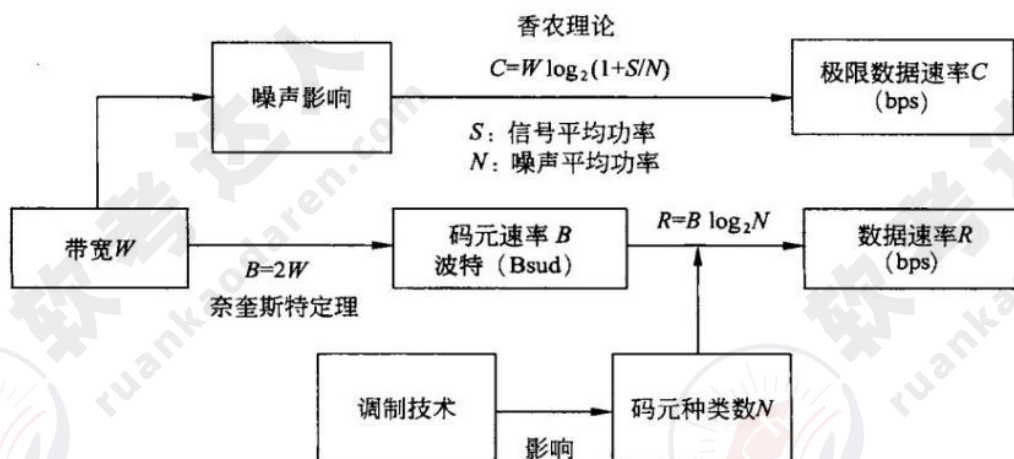
香农定理：
$$C = W \log_2 \left(1 + \frac{S}{N} \right)$$

其中， C 为数据速率， W 为信道带宽， S 为信号的平均功率， N 为噪声平均功率， S/N 为信噪比。

信噪比和分贝数： $\text{dB}=10\lg(S/N)$

考点 05：计算汇总：模拟带宽、数字带宽（1、无噪声：奈奎斯特定

理，2、有噪声：香农定理）



信道的数据速率计算公式

考点 06：常用考试数据：

单位换算：通信换算进率 1000，如 1G=1000M

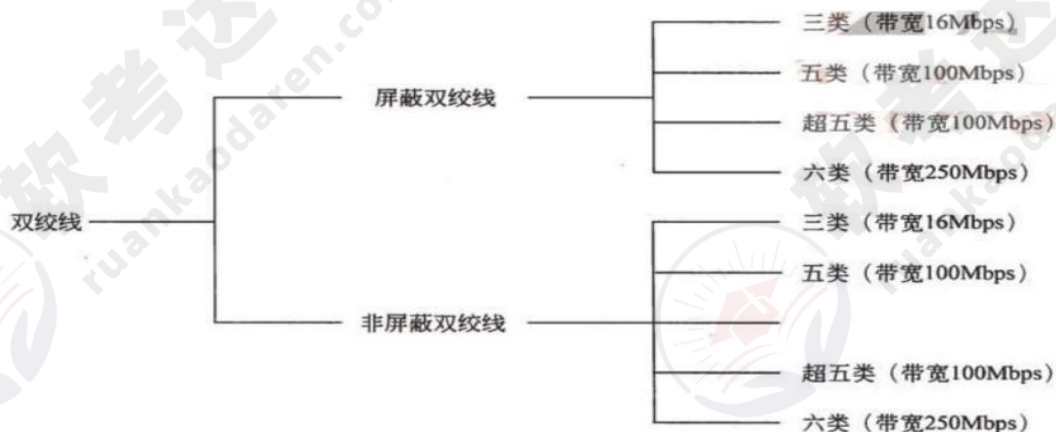
存储换算进率 1024，如 1G=1024M

信道延迟：电缆信道延迟 200m/us

(200km/ms, 200000km/s)

卫星信道延迟：270ms

考点 07：双绞线：分为非屏蔽双绞线 UTP，屏蔽双绞线 STP。100 米可以达到 100Mb/s。

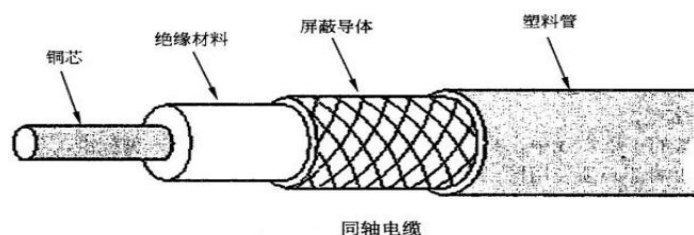


各种规格的双绞线

交叉线和直通线适用范围

线缆连接设备情况	所采用的线缆种类
计算机-计算机	交叉线
计算机-交换机	直通线
计算机-路由器	交叉线
交换机-交换机	交叉线
交换机-路由器	直通线
路由器-路由器	交叉线

考点 08：同轴电缆：分为粗同轴电缆、细同轴电缆。传送距离长，信号稳定，常用于电视、监视系统，音响设备传送音、视频信号。



考点 09：光纤(光缆)：分为单模光纤 SMF（1310、1550nm）、多模光纤 MMF（850、1300nm）。

考点 10：单模与多模光纤区别对比：单（身）美女的眼光：高细远

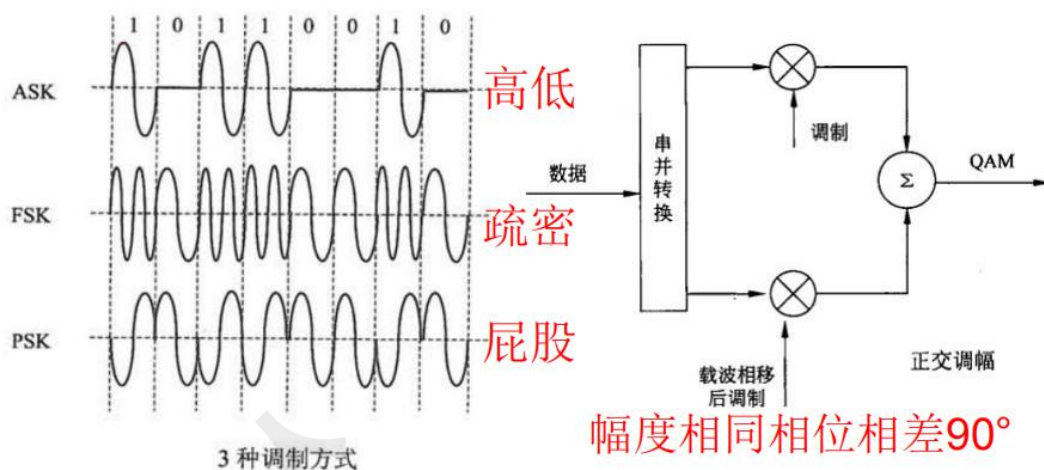
单模光纤与多模光纤的比较

项 目	单 模 光 纤	多 模 光 纤
距离	长（远）	短
速率	高（高）	低
光源	激光	发光二极管
直径	小（细）	大
端接	较难	较易
造价	高（贵）	低

考点 11：无线信道：分为无线电波和红外光波。

无线电波	长波		红外光波	近红外线
	中波			
	短波			中红外线
	超短波			
	微波	地面微波		远红外线
		卫星微波		

考点 12：模拟信道调制：分为调幅 ASK、调频 FSK、调相 PSK、正交调幅 QAM。

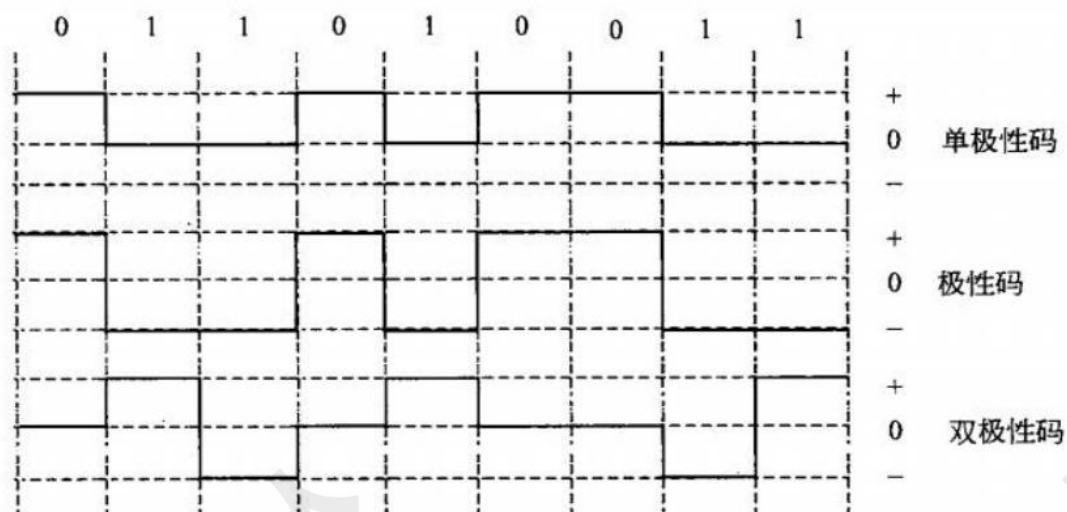


考点 13：数字信道编码：分为采样（2 倍）、量化（等级）、编码（二进制）三个步骤。

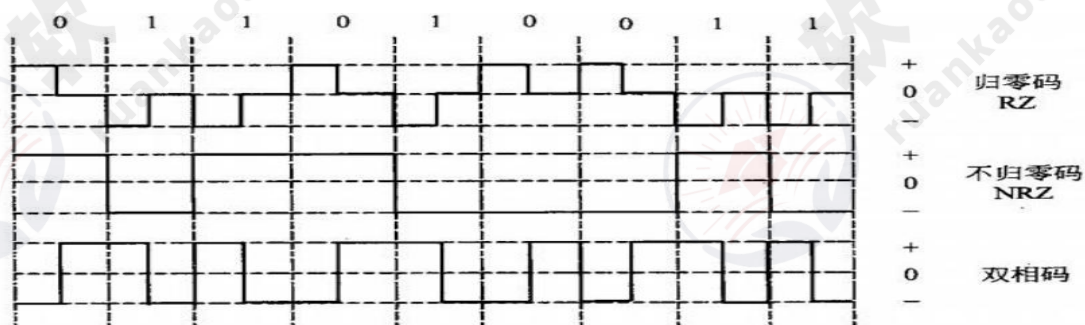
考点 14：调制技术与码元数： $n=\log_2 N$

调制技术	名称	码元种类N	比特位n
ASK	幅度键控	2	1
FSK	频移键控	2	1
PSK	相移键控（2相）	2	1
DPSK	4相键控	4	2
QPSK	正交相移键控	4	2

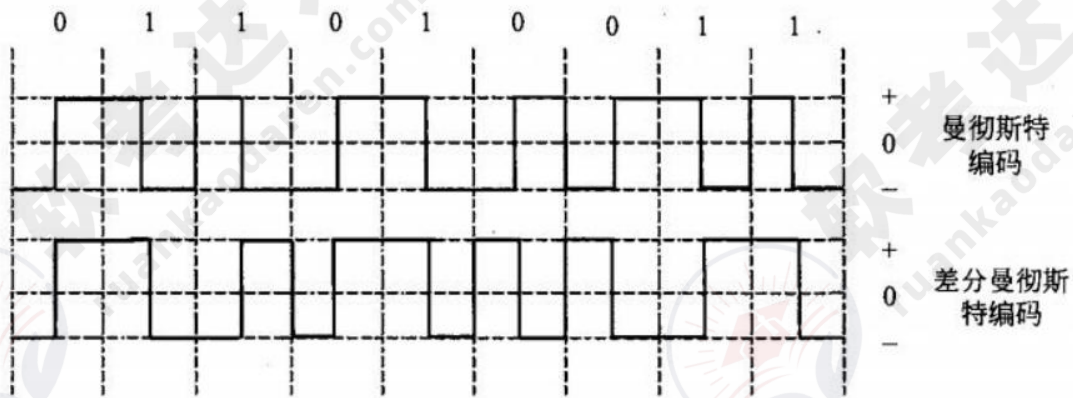
考点 15：极性编码：分为单极性、极性、双极性。



考点 16：归零性编码：归零码、不归零码（遇 1 翻转）。双相码（电平翻转）。



考点 17：曼码和差分曼码：曼码降 0 升 1 (降升 0) 效率 50%；差分曼码折 0 平 1，效率 50%



考点 18：各种编码效率：

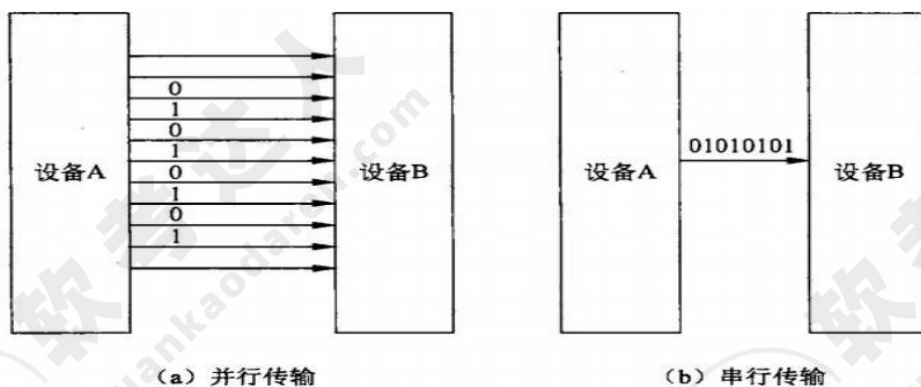
4B/5B 效率 80%，用于百兆以太网；

8B/10B 效率 80%，用于千兆以太网；

64B/66B 效率 97%，用于万兆以太网；

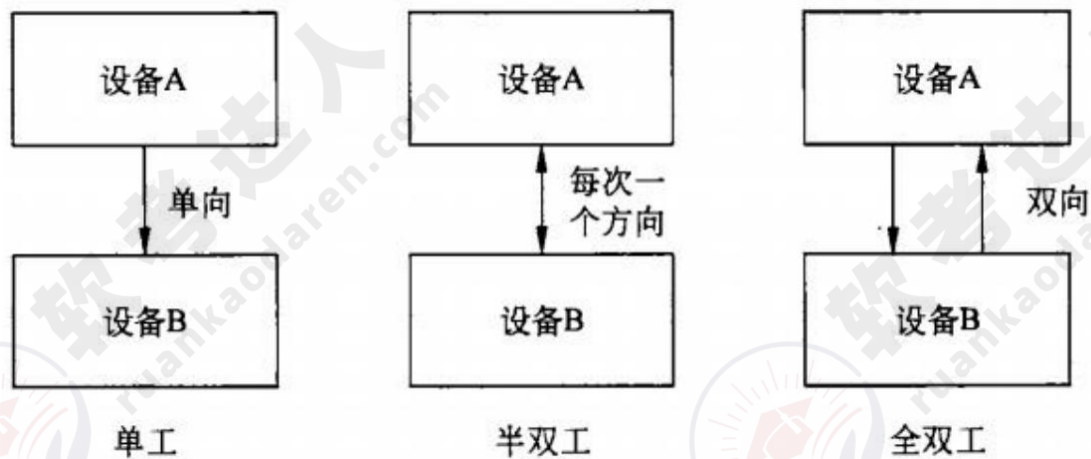
曼码和差分曼码效率 50%，用于以太网。

考点 19：串行通信与并行通信；基带传输(原始)与宽带(高于音频)传输；噪声、时延与衰减。

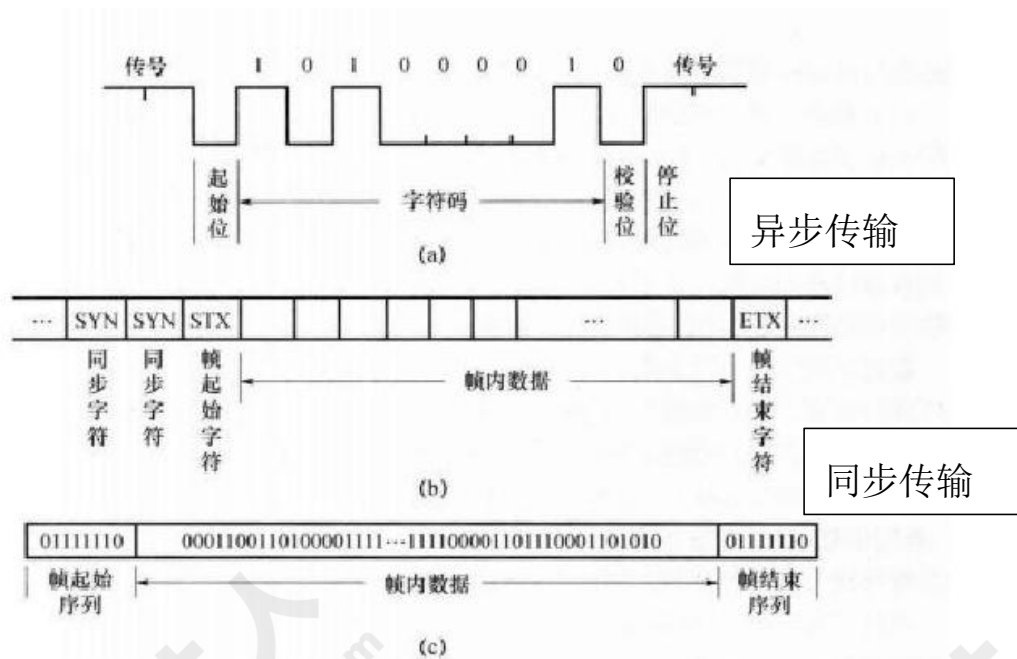


考点 20：带宽、时延、时延带宽积（容积）。相当于第一个比特到达接收方之前，发送方最多发送的比特。即链路上的最大比特数。

考点 21：通信方向：单工(电视)、全双工(手机)、半双工(对讲机)。

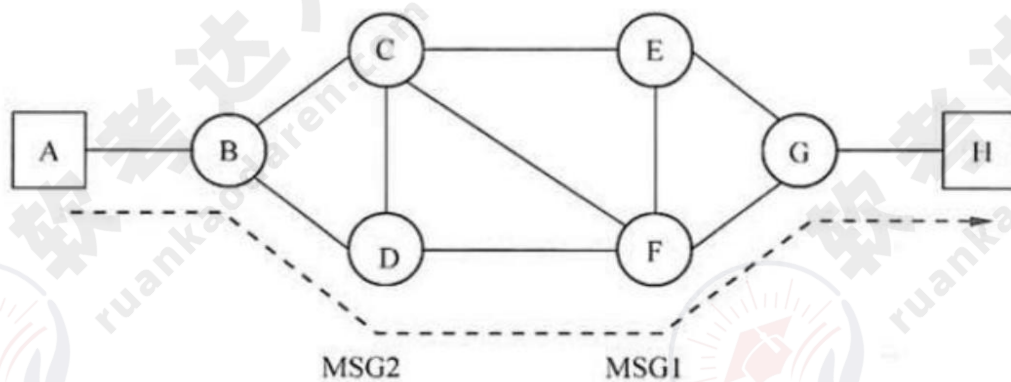


考点 22：传输方式：异步传输、同步传输特点。



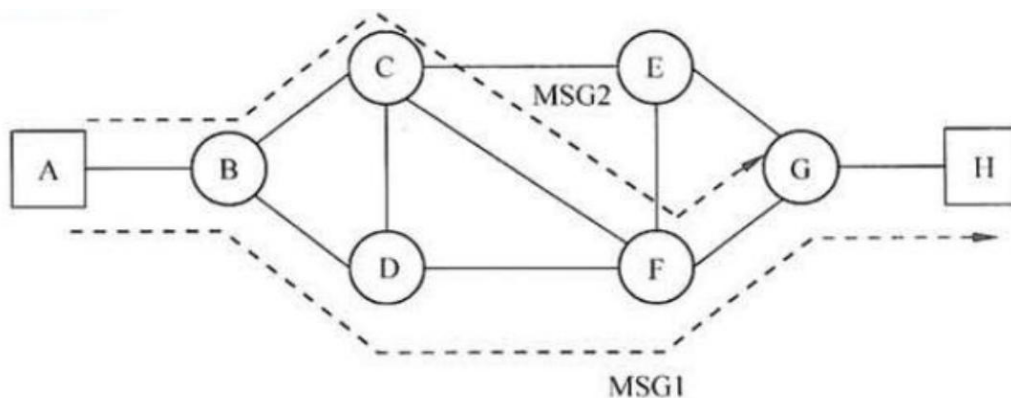
考点 23：电路交换：优点：独占性、实时性，适合传输大量的数据；

缺点：需建立一条物理连接，利用率低。比如早期的电话系统。



考点 24：报文交换：优点：不需要专用通道，线路利用率高，存储

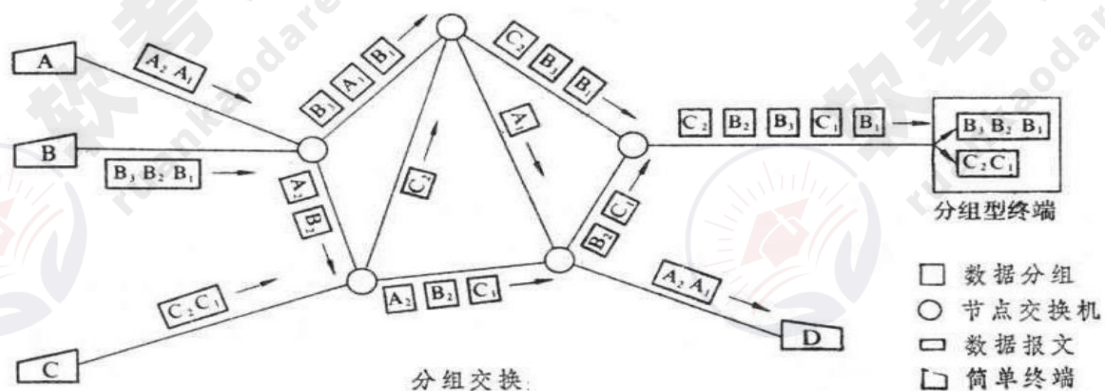
转发节点可校验纠错。缺点：有通信时延。比如物流包裹。



考点 25：分组交换：优点：利用率更高、可选路径、数据率转换、

支持优先级。缺点：时延、开销大。比如邮局寄信。分为数据报和虚

电路。

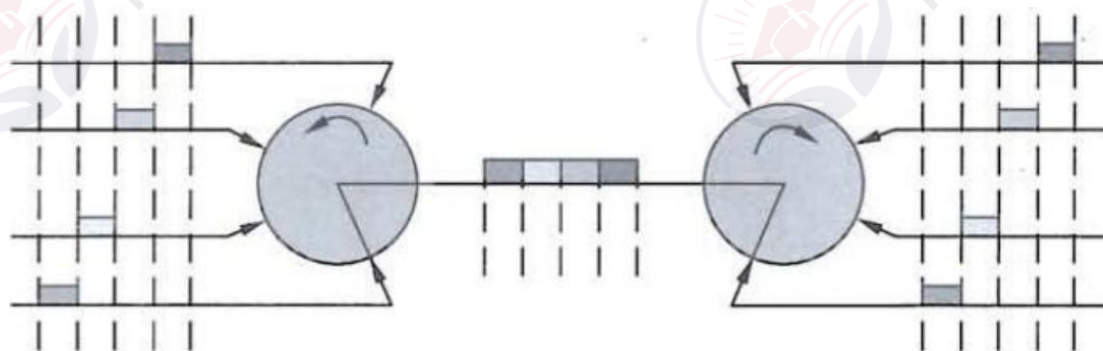


考点 26： 分组数据报：单向传送、无连接的。如普通信。

考点 27： 分组虚电路：交互式、逻辑链接。如挂号信。

考点 28： 频分复用 FDM：不同的频率，子信道隔离频带防串扰，如 CATV，WIFI。

考点 29： 时分复用 TDM：不同的时间，轮流占用，如手枪、手机。分为同步时分 T1、E1；统计时分，如 ATM。



时分多路复用

考点 30： 波分复用 WDM：不同的波长，如光纤。

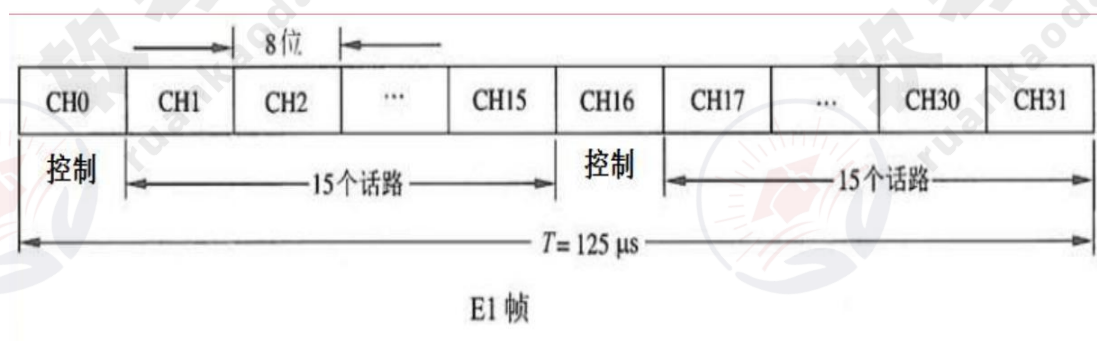
考点 31： T1 标准：1.544Mbps、125us=8000 次。

$1.544\text{Mbps} = [24 \times (7+1) + 1] \times 8000$ 。T2、T3、T4（美国和日本）

考点 32： E1 标准：2.048Mbps、125us=8000 次。

$2.048\text{Mbps} = [32 \times (7+1)] \times 8000$ 。CH0 和 CH16 控制信令，30 个话音数据。

E2、E3、E4 口诀：E444。（中国和欧洲）

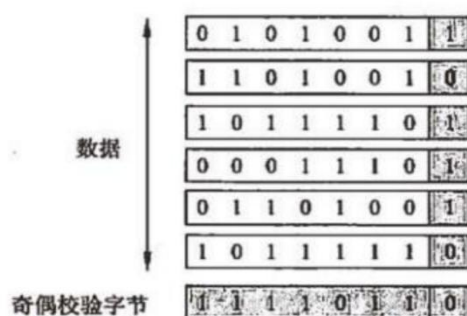


考点 33：SONET 标准(美国)和 SDH 标准(国际)：用于光纤网络。

155.520

Optical Level	Electrical Level	Line Rate /Mbps	Payload Rate /Mbps	Overhead Rate /Mbps	SDH Equivalent	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	1 244.160	1 202.688	41.472	STM-8	
OC-36	STS-36	1 866.240	1 804.032	62.208	STM-13	
OC-48	STS-48	2 488.320	2 405.376	82.944	STM-16	2.5Gbps
OC-96	STS-96	4 976.640	4 810.752	165.888	STM-32	
OC-192	STS-192	9 953.280	9 621.504	331.776	STM-64	10Gbps

考点 34：检错码：奇偶校验看 1 的个数是奇数/偶数。只能检错不能纠错。移动通信广泛采用。



考点 35：海明码：在数据位 m 后面增加冗余校验位 k ，组成信息 $m+k$ ，则满足 $m+k < 2^{k-1}$ 可纠正一位错误。不但检错还能纠错。

码距 d ：也叫海明距离，两个码字之间不同的最小的位数(比特数)。

可以查出多少位错误： $\leq d-1$

可以纠正多少位错误： $< d/2$

考点 36：CRC 码：冗余循环校验码，是一种循环码，通过循环移位，实现检错，硬件容易实现，广泛用于局域网。只能检错不能纠错。

计算 CRC 校验码：多项式除法，不进位加法。如生成多项式为

$G(x)=x^4 + x + 1$ ，信息码字为 10111，求 CRC 校验码。

- 1、写除数 1 0 0 1 1
- 2、写被除数
- 3、模2计算

$$\begin{array}{r}
 101110000 \quad \text{—— 最后4个0是补位} \\
 \underline{10011} \\
 10000 \\
 \underline{10011} \\
 1100 \quad \text{—— 余数}
 \end{array}$$

第三章：广域通信网

考点 01：什么广域网是？广域网是指长距离跨地区的各种局域网、计算机、终端互联在一起，组成一个资源共享的通信网络。

传统的广域网有：①公共交换电话网 PSTN、

②公共数据网 X.25

③帧中继网 FR

④综合业务数据网 ISDN

⑤异步传输模式 ATM

⑥虚拟专用网 VPN

现代的广域网有：①数字数据网 DDN

②光同步数字传输网 SDH

③多业务传送平台 MSTP

④光纤接入网 FTTX

⑤无源光网络 PON

⑥无线网 WiMAX、LTE（4G）

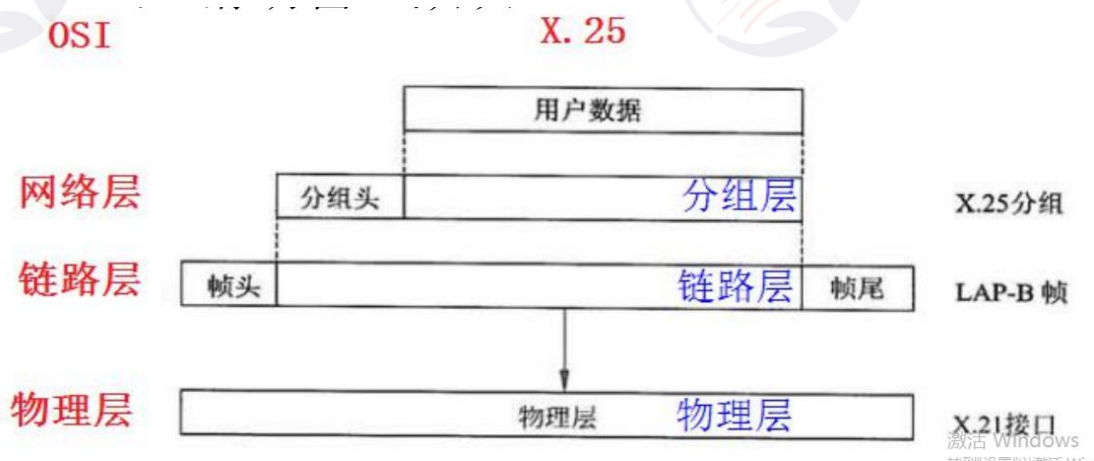
考点 02：公共交换电话网 PSTN：利用电话线上网，早期是电话+“猫”拨号上网。

机械特性	描述了 DTE 和 DCE 之间物理上的分界线，规定连接器的几何形状、尺寸大小、引线数、引线排列方式以及锁定装置等。在微型机的 RS-232-C 串行接口上大多使用 9 针连接器
电气特性	RS-232-C 采用了 V.28 标准电路，信号源产生 3~15V 的信号，±3V 之间是信号电平过渡区，另外两种常用的电气特性标准是 V.10 和 V.11
功能特性	对接口连线的功能给出明确的定义。RS-232-C 采用的标准是 V.24。V.24 为 DTE/DCE 接口定义了 44 条连线，为 DTE/ACE 定义了 12 条连线。ACE 为自动呼叫设备。按照 V.24 的命名方法，DTE/DCE 连线用“1”开头的三位数字命名；DTE/ACE 连线用“2”开头的三位数字命名
过程特性	规定了使用接口线实现数据传输的操作过程

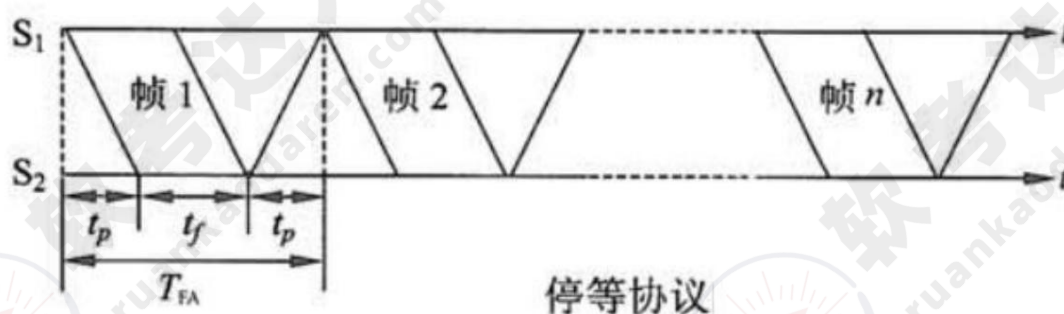
考点 03：调制解调器 Modem：俗称“猫”，作用是把电话线里面的模拟信号和数字信号互相转换，V.90 标准可以达到 56Kb/s。

考点 04：数据终端设备 DTE，如用户的计算机、电话等。数据电路设备 DCE，如调制解调器。DTE 和 DCE 两端要同步。

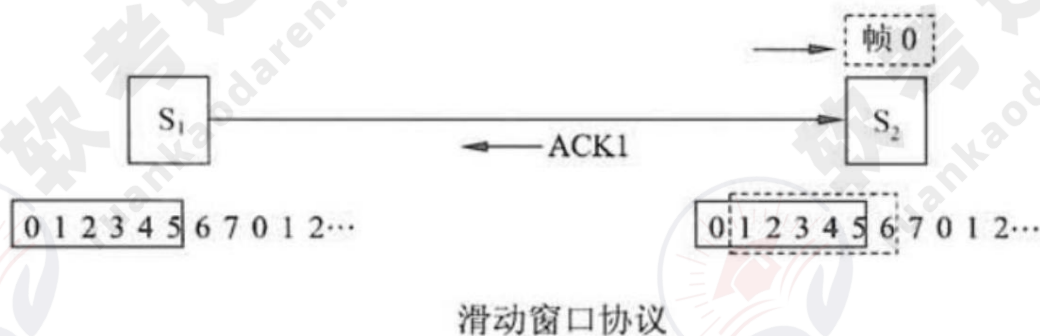
考点 05：X.25 使用分组交换，分为三层：物理层、链路层、分组层。对应于 OSI 的低三层。采用虚拟电路、面向连接的。采用后退 N 帧 ARQ、滑动窗口默认 2。



考点 06：流量控制技术：协调收发端流量。假设没有传输错误的流控技术：停等协议。发送一帧，等到应答，再发送；如果不应答，一直等。类似银行柜台存钱，一个个存钱。



考点 07：流量控制技术：协调收发端流量。假设没有传输错误的流控技术：滑动窗口协议。连续发送多个帧而无需应答。类似银行 ATM 机，一沓一沓存钱。



考点 08：差错控制技术：检查和纠正传输错误。

- ①肯定应答：收到肯定应答信号 ACK 继续发送。
- ②否定应答重发：收到否定应答信号 NAK 重发出错帧。
- ③超时重发：超过规定时间重发该帧。这种技术称为自动请求重发 ARQ。

ARQ 分为三种：停等 ARQ、选择重发 ARQ、后退 N 帧 ARQ。

考点 09：停等 ARQ：是停等流控和 ARQ 结合。类似银行柜台存钱，手续齐全办理，叫号等时间长下一位，忘带身份证不办理。



考点 10：选择重发 ARQ：是滑动窗口和 ARQ 结合。类似银行 ATM 一沓一沓存钱，这张是假币，选择这一张重发。



考点 11：后退 N 帧 ARQ：也是滑动窗口和 ARQ 结合。类似银行验钞机一沓一沓数钱，这张是假币，选择这一张包括后面的都要重发。



考点 12：各种流控和差错利用率计算如下表。

1, a 的计算有： $a = (d/v) / (L/R) = (Rd/v) / L$

$$a = (RT)/L$$

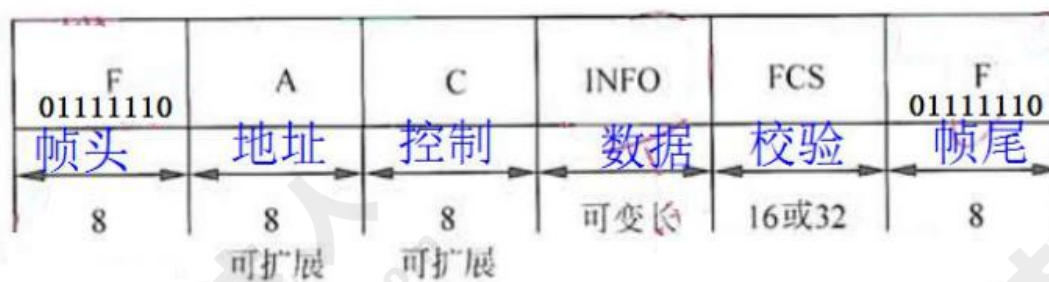
其中，R=数据速率，d=线路长度，v=传播速度，L=帧长，T=传播延迟。

2, 在后退 N 帧 ARQ 计算中，N=重发的帧数，当窗口值 $> 2a+1$ 时，

N 近似 $= 2a+1$ ；当窗口值 $\leq 2a+1$ 时，N=W。

协议名称	特 点	链路利用率
停等协议（单工通信）	发送站每传送一帧，就停止发送，等收到应答信号后再发送下一帧。在局域网中效率较高，对广域网而言效率太低	$E=1/(2a+1)$ a : 帧计数长度
滑动窗口协议（双工通信）	允许连续发送多个帧而无须等待应答，所允许的帧个数是固定值，也称为窗口。当成功收到一个确认包，窗口就向前滑动1位	$E=W/(2a+1)$ W : 窗口值
停等 ARQ 协议（有噪声环境的单工通信）	它是停等协议和自动请求重发技术的结合，发送站每传送一帧，就停止发送，等收到肯定应答信号（ACK）后再发送下一帧，如果收到否定应答（NAK）后重发该帧，在一定时间间隔内未收到 ACK，也重发	$E=(1-P)/(2a+1)$ P : 帧出错概率
选择重发 ARQ 协议（有噪声环境的双工）	它是滑动窗口协议与自动请求重发技术的结合，当收到否定应答（NAK）时，只重发出错的帧。为了避免异常，其最大值就小于帧编号总数的一半，即 $W_{\max}=W_{\min} \leq 2^{K-1}$	若窗口值 $> 2a+1$ ，则 $E=1-P$ ； 若窗口值 $\leq 2a+1$ ，则 $E=W(1-P)/(2a+1)$ W : 窗口值
后退 N 帧 ARQ 协议（有噪声环境的双工）	也是滑动窗口协议与自动请求重发技术的结合，只是当收到否定应答（NAK）时，将从出错处重发已发出过的 N 个帧。为了避免异常，必须限制发送窗口的大小 $W \leq 2^K-1$ （ K 为帧编号的位数）	若窗口值 $> 2a+1$ ，则 $E=(1-P)/(1-P+NP)$ 若窗口值 $\leq 2a+1$ ，则 $E=W(1-P)/(2a+1)(1-P+NP)$

考点 13: 高级数据链路控制协议 HDLC: 面向比特的。通常使用 CRC-16、CRC-32 校验。帧边界 01111110 “ 两头踢皮球 ”。用户数据字段 INFO 大小不固定。



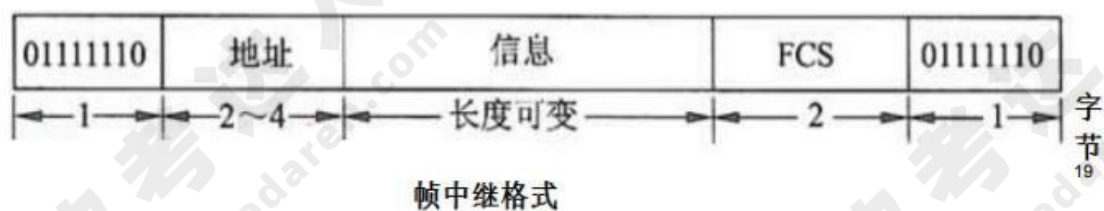
HDLC 帧结构

17

考点 14: 帧中继 FR 是 X.25 演变改进的。

- ①工作在 OSI 的低两层，即物理层和链路层。
- ②在第二层建立虚电路（与 X.25 一样，也支持永久虚电路 PVC 和交换虚电路 SVC），承载数据业务，因而第三层被简化拉。也是分组交换。

③FR 只做检错，不在重传，没有流控，只有拥塞控制，检错交高层，速率可以达到 64kb~2Mb。



考点 15：帧中继主要优点有：

- ①基于分组（帧）交换的透明传输，可提供面向连接的服务。
- ②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。
- ③数据速率可达 2~45Mbps。
- ④既可以接需要提供带宽，也可以应付突发的数据传输。
- ⑤没有流控和重传机制，开销很少。

考点 16：综合业务数据网 ISDN：基于电路交换，把数据、声音、视频信号三合一传输。分为窄带 ISDN（N-ISDN）和宽带 ISDN（B-ISDN）。

N-ISDN 两种速率：基本速率（2B+D）和基群速率（30B+D）。

B 信道数据信道；D 信道控制信道。

$$2B+D = 2 \times 64 + 16 = 144 \text{Kb/s};$$

$$30B+D = 30 \times 64 + 64 = 1.984 \text{Mb/s}.$$

考点 17：异步传输模式 ATM：最早是 B-ISDN 标准的一部分，分为四层模型，如下表。

ATM B-ISDN 各层的功能			
层 次	子 层	功 能	与 OSI 的对应
高层		对用户数据的控制	高层
ATM 适配层	汇聚子层	为高层数据提供统一接口	第四层
	拆装子层	分割和合并用户数据	
ATM 层		虚通路和虚信道的管理 信元头的组装和拆分 信元的多路复用 流量控制	第三层
物理层	传输汇聚子层	信元校验和速率控制 数据帧的组装和拆分	第二层
	物理介质子层	位定时 物理网络接入	第一层

24

考点 18：ATM 采用 53 字节信元分组交换，使用统计时分 TDM。采用双绞线或光线，典型数据速率 155M，面向连接，使用虚电路的虚通路 VPI 和虚信道 VCI。

ATM 业务类型

业务类型	特 点	适用应用
CBR（固定比特率业务）	没有错误检查、流控和其他处理	交互式语音和视频流
RT-VBR（实时性变化比特率业务）	能够对信元的延迟和延迟变化进行控制	交互式压缩视频信号
NRT-VBR（非实时性变化比特率业务）	能够满足按时提交的需求	多媒体电子邮件
ABR（有效比特率业务）		突发式通信
UBR（不定比特率业务）	发生拥塞，信元可丢弃	IP 分组传送

第四章：局域网与城域网

考点 01：什么是局域网？单一机构所拥有的专用计算机网络，中等规模地理范围，实现多种设备互联、信息交换和资源共享。



局域网体系结构与 OSI/RM 的对应关系

4

考点 02：LAN / MAN 的 IEEE 802 标准，重点掌握：802.3、802.11、802.16。

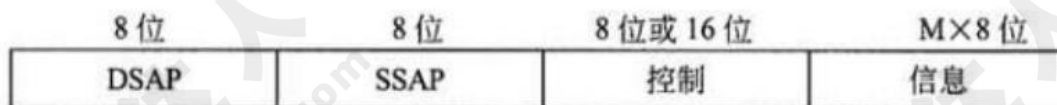


5

考点 03：

- 1，逻辑链路控制 LLC：目的是屏蔽不同的介质访问控制方法，以向，高层(网络层)提供统一的服务和接口。LLC 地址是 SAP。
- 2，这个标准与 HDLC 是兼容的，无帧校验字段，放到了 MAC 层。

同时提供目标地址和源地址字段。



考点 04：介质访问控制 MAC：其中，长度字段表示数据实际长度，最大 1500。同时还可以表示上层协议类型，1501 以上的值。

MAC 地址：采用 16 进制数表示，共 6B（48 位），有 IEEE 和厂家烧制到网卡上。



考点 05：CSMA/CD 协议：载波监听多路访问/冲突检测。是分布式介质访问控制方法。

非坚持型：有礼貌，等一会下楼。

1 坚持性：霸道点，一直要下楼。

P 坚持性：和事佬，概率等下楼。

监听算法	信道空闲时	信道忙时	特点
非坚持型监听算法	立即发送	等待 N，再监听	减少冲突，信道利用率降低
1-坚持型监听算法	立即发送	继续监听	提高信道利用率，增大了冲突
P-坚持型监听算法	以概率 P 发送	继续监听	有效平衡，但复杂

考点 06：最小帧长计算：为了检测到冲突。 $L=2R \times d/v$ 其中，R 为网络数据速率，d 为最大段长，v 为信号传播速度。

二进制后退指数算法：

- ①考虑网络负载变化；
- ②后退次数和负载大小有关。
- ③重发次数最大为 16，然后上报高层协议。

考点 07：以太网：早期的 802.3 局域网，10Mbps。来源于光在空气中传播的介质“以太网（ether）”，由此得名“以太网（ethernet）”，寓意无处不在的网络。

交换式以太网核心部件是交换机，有一个高速底板，插上一些插槽，插槽上有一些连接器，用于连接 10M 网卡的主机。如：E0/0，F0/1，（插槽/接口）；G0/0/0（插槽/模块/接口）

E：以太网，F：快速以太网，G 吉比特以太网

考点 08：快速以太网：802.3u 标准，速率可到 100M，采用 100Base-T/F 规范。

标准	传输介质	线对数	传输距离
100Base-T2	3类UTP	2对	100m
100Base-T4	3类UTP	4对	100m
100Base-TX	5类UTP	2对	100m
	STP	2对	100m
100Base-FX	多模光纤	1对	2km(全双工)
	单模光纤	1对	40km(全双工)

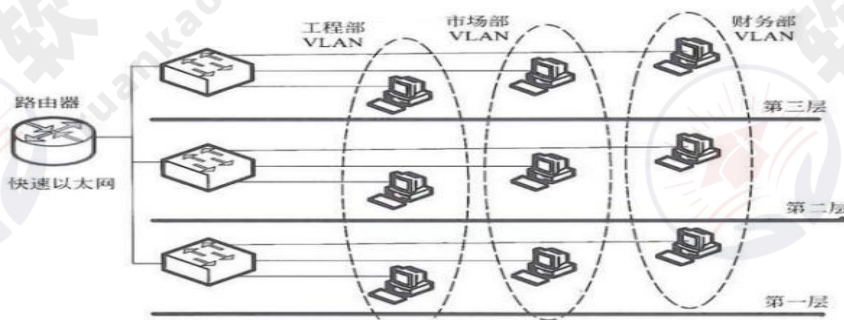
考点 09：千兆以太网：802.3z 标准，速率可到 1000M（1Gbps），兼容 10M/100M 以太网。

标准	名称	传输介质	传输距离
IEEE 802.3z	1000Base-LX	62.5μm 多模光纤	550m
		50μm 多模光纤	550m
		10μm 单模光纤	5km
	1000Base-SX	62.5μm 多模光纤	275m
		50μm 多模光纤	550m
	1000Base-CX	2对STP	25m
IEEE 802.3ab	1000Base-T	4对5类UTP	100m

考点 10：万兆以太网：802.3ae 标准，速率可达万兆（10Gbps），只支持光纤，只支持全双工，不再采用 CSMA/CD，可用于城域网。

名 称	传输介质	传输距离	特 点
10GBase-S (Short)	50μm 的多模光纤	300m	850nm 串行
	62.5μm 的多模光纤	65m	
10GBase-L (Long)	单模光纤	10km	1 310nm 串行
10GBase-E (Extended)	单模光纤	40km	1 550nm 串行
10GBase-LX4	单模光纤	10km	1 310nm
	50μm 的多模光纤	300m	4×2.5Gbps 波分多路复用 (WDM)
	62.5μm 的多模光纤	300m	

考点 11：虚拟局域网 VLAN 概念：根据管理功能、组织机构或应用类型，对物理网络进行分段而形成的逻辑网络，与用户的物理位置无关。



考点 12:

VLAN 划分方式:

- ①静态分配 VLAN: 基于端口。
- ②动态分配 VLAN: 基于 MAC 地址(2 层)、网络层 IP(3 层)、规则策略(高层)等。

VLAN 划分的好处:

- ①控制网络流量, 抑制广播风暴。
- ②提高网络安全性, 不同 VLAN 之间可做控制。
- ③网络管理灵活, 用户可以随地接入网络。

不同 VLAN 之间通信: 需要路由器或三层交换机。

考点 13: VLAN 标准 802.1q(dot1q): 在原来的以太帧中增加了 4B 的控制信息, 其中包含 12 位 VLAN 标识符 VID。可用 4094 个 VLAN。

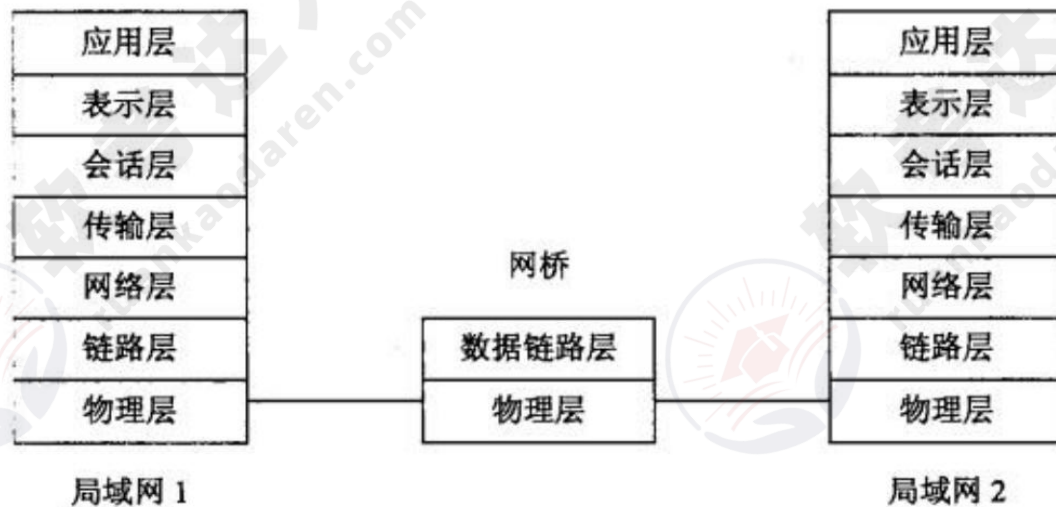


考点 14: VLAN 两种端口: 接入端口 Access

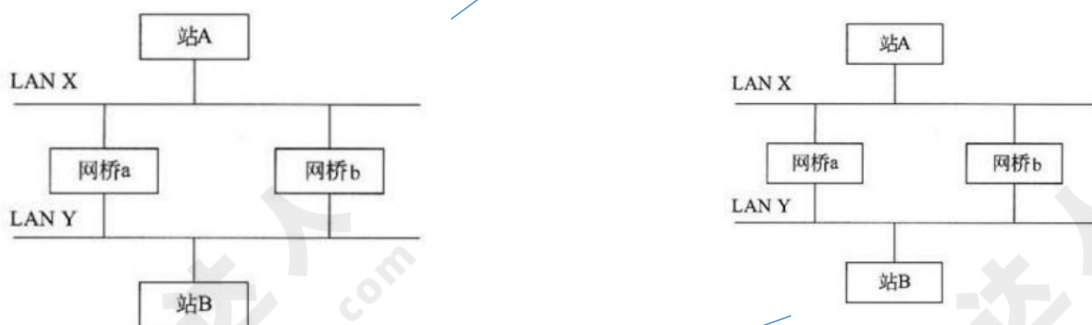
(通过单个 VLAN) 和中继端口 Trunk (通过多个 VLAN)。



考点 15:局域网互联设备:2 层网桥(生成树、源路由)、3 层交换机、路由器。网桥要求 3 层以上协议相同, 1、2 层协议不同可互联



考点 16:生成树网桥:又叫透明网桥, IEEE 802.1d, 生成树算法。基本思想是在网桥之间传递 BPDU, 比较参数, 根据 STP 打开好端口, 阻塞差端口, 沿着好的端口建立路径。边走边拐弯。用于以太网。



考点 17:生成树网桥步骤

- ①确定根桥
- ②确定根端口
- ③确定指定桥
- ④确定指定端口
- ⑤阻塞剩余端口
- ⑥形成无环网络

考点 18:生成树网桥计算数据

- ①确定根桥 ID:优先级+MAC 地址，都选最小优先级 0~65535，默认 32768(± 4096)。
- ②确定根端口:优先级+编号，都选最小的优先级 0~255，默认 128
- ③三小原则:优先级、MAC 地址、通路费用。

考点 19:生成树端口的四种状态:

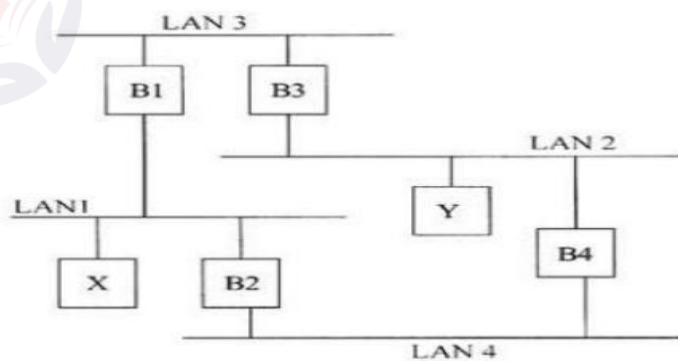
- ① Blocking(阻塞):接收 BPDU，不学习 MAC 地址，不转发数据，20S
- ②Listening(侦听):接收 BPDU，不学习 MAC 地址，不转发数据帧，但交换机向其他交换机通告该端口，参与选举根端口或指定端口。
- ③ Learning(学习):接收 BPDU，学习 MAC 地址，不转发数据帧。
- ④ Forwarding(转发):正常转发数据帧。阻塞→20 秒一侦听→15 秒→学习 15 秒→转发

考点 20:生成树种类和标准

- | | | |
|--------|-------|-------------|
| ①多生成树 | MSTP | IEEE802.1S |
| ②快速生成树 | RSTP | IEEE802.1w |
| ③生成树 | STP | IEEE 802.1d |
| ④端口认证 | 证基于用户 | IEEE802.1x |

口诀:多块生(人)口，是 S 我 W 弟 d 兄 x

考点 21:源路由网桥:IEEE802.5, 基本思想是发送探测帧到目的节点, 返回路径以后沿着路径再传送。发送帧在这条路径上就传送, 不在这条路径上就发送广播, 查询路径, 选择最优路径再传送。选好路再走。令牌环网。



考点 22:什么是城域网?城域网比局域网传输距离远, 能够覆盖整个城市。能够提供分组传输的数据、语音和视频等多媒体业务。更大的传输容量, 更高的传输效率

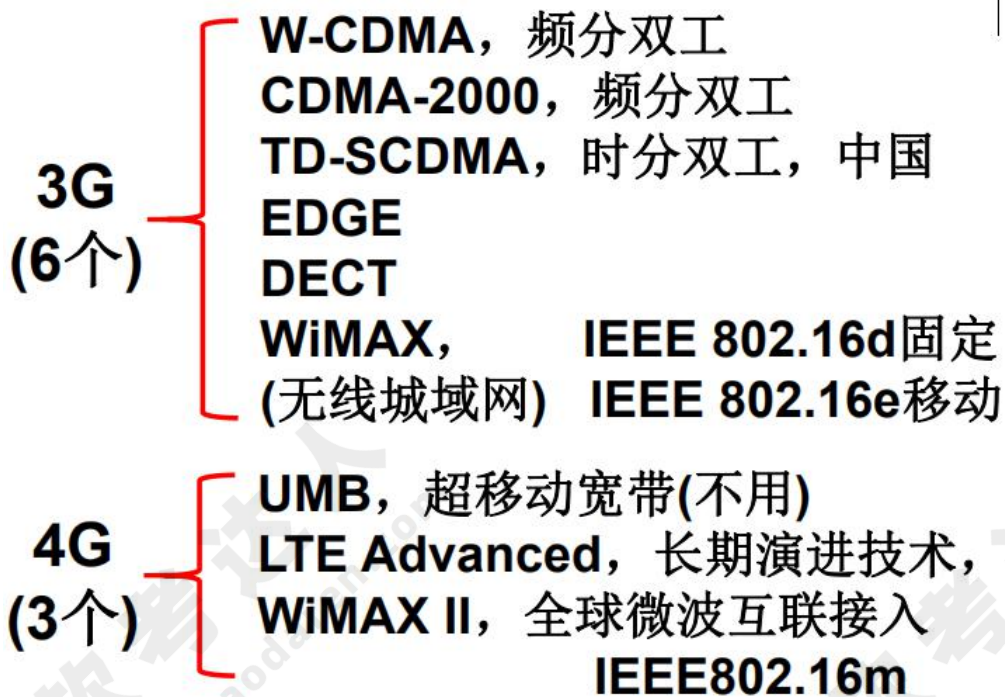
城域以太网:①以太网专用线、②以太网虚拟专线、③以太网局域网服务(E-LAN)最看好。

无线城域网标准: WIMAX(802.16d 固定、802.16e 移动)、, WIMAXI(802.16m4G)。

考点 23:Q-in-Q:运营商网桥协议(PBP)IE802.1ad。MAC-IN-MAC:运营商主干网桥(PBB)IEEE 802.1ah

第五章：无线通信网

- **考点01：**各种移动通信标准：
- 1 G：第一代模拟蜂窝：频分双工FDD。
- 2 G：第二代数字蜂窝①GSM(全球移动通信)采用TDMA、②CDMA(码分多址通信)。
- 2.5G：第2.5代通用分组无线业务GPRS。
- 2.75G：第2.75代增强型GPRS叫EDGE。
- 3 G：第三代，速率可达2Mbps。
- 4G：第四代，速率可达100Mbps。
- 4G+、4.5G、5G



- **考点02：** 4G：至少100Mbps，下1Gbps，上500Mbps，使用正交频分多址接入OFDM和MIMO技术。包含 TDD和FDD两种制式。



各种无线网的作用范围

6

- **考点03：** 无线局域网WLAN：两大阵营：
①IEEE 802.11面向数据无连接。②欧洲邮电委HIPERLAN，面向语音有连接。奥迪A5。

名称	发布时间	工作频段	调制技术	数据速率
802.11	1997 年	2.4GHz ISM 频段	DB/SK DQPSK	1Mbps 2Mbps
802.11b	1998 年	2.4GHz ISM 频段	CCK	5.5Mbps, 11Mbps
802.11a	1999 年	5GHz U-NII 频段	OFDM	54Mbps
802.11g	2003 年	2.4GHz ISM 频段	OFDM	54Mbps
802.11n	2009 年	2.4/5 GHz 频段	OFDM MIMO	300Mbps 600Mbps
802.11ac	2012 年	5GHz U-NII 频段	OFDM MIMO	500Mbps 1Gbps

8

- **考点04：** 无线局域网WLAN：两种结构：①基础设施网络、②特殊网络Ad Hoc。



(a) 基础设施网络



(b) Ad hoc 网络

9

● **考点05：**无线局域网WLAN：两种AP

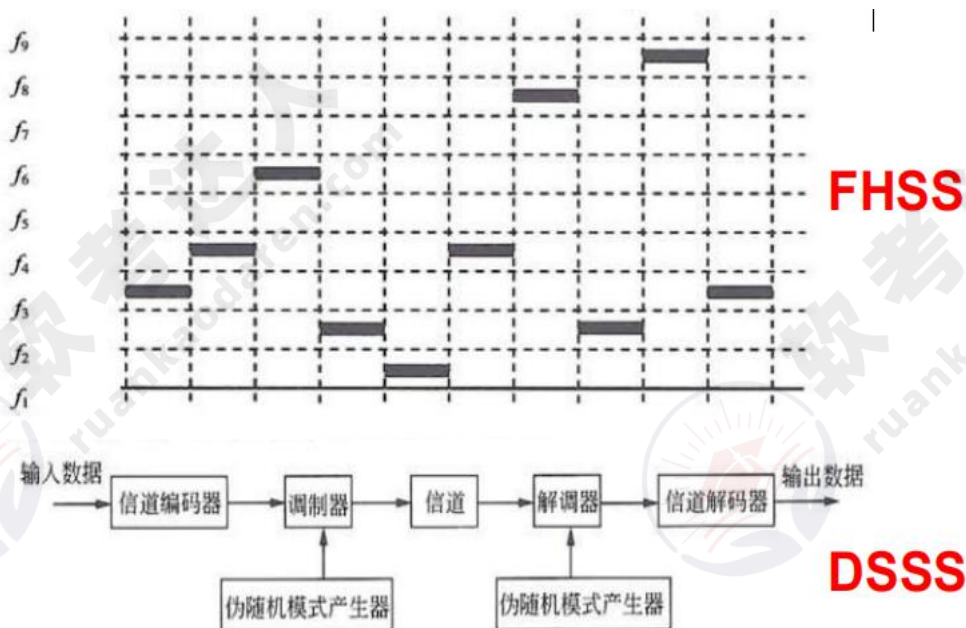
- **胖AP(FAT)**一般指无线路由：胖AP多用于家庭和小型网络，功能比较全，一般一台设备就能实现接入、认证、路由、VPN、地址翻译。。。甚至防火墙功能
- **瘦AP(FIT)**一般指无线网关或网桥：瘦AP多用于要求较高的场合，要实现认证一般需要认证服务器或者支持认证功能的交换机配合。

10

● **考点06：**无线局域网WLAN：三种技术：①红外线，②扩展频谱，③窄带微波。

- 红外线分为：定向光束红外线、全向广播红外线，漫反射红外线。
- 扩展频谱分为：频率跳动FHSS、直接序列DSSS。
- 窄带微波分为：申请许可证RF，免许可证RF。

11



- **考点07：CSMA/CA：**载波监听多路访问冲突避免，解决隐蔽终端问题。
 - 1、传数据先检测，如果探测到网络中没有数据，则等待一个IFS时间，再随机选择一个时间片继续探测，如果无线网路中还没有活动的话，就将数据发送出去。
 - 2、送出数据前，先送一段小小的请求报文给目标端，收到目标端回应后，在传送大量的数据，确保不会碰撞，开销最小。
- **考点08：**三种帧间隔IFS：
 - ①DIFS（分布式协调IFS）最长，优先级最低。
 - ②PIFS（点协调IFS）中等长度，优先级居中。
 - ③SIFS（短IFS）最短，优先级最高立即响应。
- **考点09：**无线加密协议WEP：认证和加密，明文的。无线保护接入WPA/WPA2：802.1x认证、RC4加密和TKIP数据完整性。

- **考点10：** Ad Hoc网络：节点之间对等。每个节点既是主机，又是路由器。形成自组织网MANET。



MANET 网络

15

- **考点11：** MANET中的路由协议：

扁平的路由协议

分层的路由协议
(分部门，选领导)

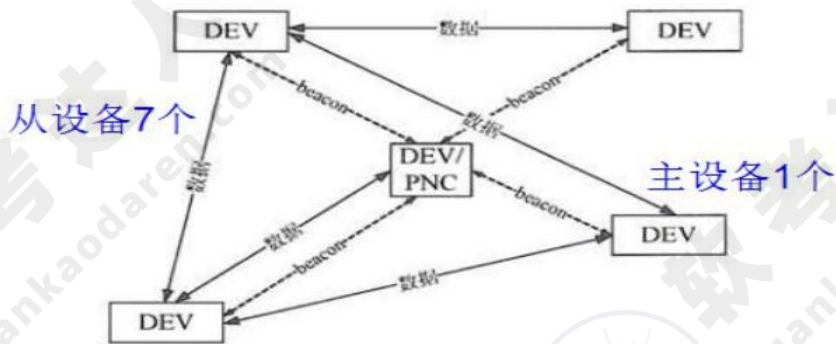
地理信息的路由协议
(GPS定位)

先验式：周期交换，开销大。周期检查身体花销大。

反应式：按需分配，开销少。有病再查身体花销少。

- **考点12：** DSDV路由协议：目标排序的距离矢量协议，扁平式，先验式，利用序列号解决环路。
- **考点13：** AODV路由协议：按需分配的距离矢量协议，扁平式，反应式，开销少，适合快速变化的网络。
- **考点14：** 无线网的安全：隐藏SSID、MAC过滤、WEP/WPA/WPA2、802.11i四个方面。

- **考点15：**无线个人网WPAN：小范围，10米左右，手持设备。IEEE 802.15.1/2/3/4标准。



微微网 piconet 网络模型

19

- **考点16：**蓝牙(Bluetooth) 技术IEEE 802.15.1：
1主设备、7从设备。四个重要协议：RF无线电频率协议、链路控制协议LCP、链路管理协议LMP和链路控制自适应协议L2CAP。
- **考点17：**ZigBee(蜜蜂网)技术IEEE 802.15.4：
全功能设备FFD，简单功能设备RFD，RFD之间不能通信。一般用于物联网。
- **考点18：**无线城域网IEEE 802.16：WiMAX：
802.16d（无线固定），802.16e（无线移动）。WiMAX II：802.16m（4G）。
- **关键技术：**正交频分多路复用OFDM、多输入多输出MIMO、频分/时分双工FDD/TDD。

第六章：网络互连与互联网（1）

考点 01:常用网络互联设备：

- 1 层物理层:中继器、集线器
- 2 层链路层:网桥、交换机
- 3 层网络层:路由器、三层交换机
- 4 层以上高层:网关

OSI 层	互联设备	功能
物理层	中继器集线器	在电缆段间复制比特流
数据链路层	网桥第二层交换机	在 LAN 间存储转发帧
网络层	路由器第三层交换机	在不同网间存储转发包
传输层以上	网关	提供不同体系间互联接口

常见网络互联设备介绍

考点 02:网络互联设备:①中继器 Repeater 集线器 Hub (又叫多端口中继器)，传输比特 01，放大信号，延长传输距离。

考点 03:网络互联设备:②网桥 Bridge、交换机 Switch，又叫多端口网桥，传输帧，有源地址、目的地址，有自己的物理地址 MAC 地址。

网桥种类：透明网桥、源选径网桥

透明网桥的工作原理：基于转发表的学习（源地址）、过滤（本网段帧）、转发（异网段帧）、广播（未知帧）。

考点 04:网络互联设备:③路由器 Router，选择网络路径，传输分组，

有自己的逻辑地址 IP 地址。

特点：一个网络上的分组有条件地被转发到另一个网络； 扩展后的网络被路由器分隔成多个子网。

功能：在不同的网络之间存储转发分组（数据报文）。

考点 5：网关

功能：一、（3 种方式支持不同种协议系统之间的通信）完成网络层以上的某种协议之间的转换，将不同网络的协议进行转换。

二、同时可以进行（1）远端业务协议封装（2）本地业务协议封装（3）协议转换

三、实现不同体系结构网络之间的互联。

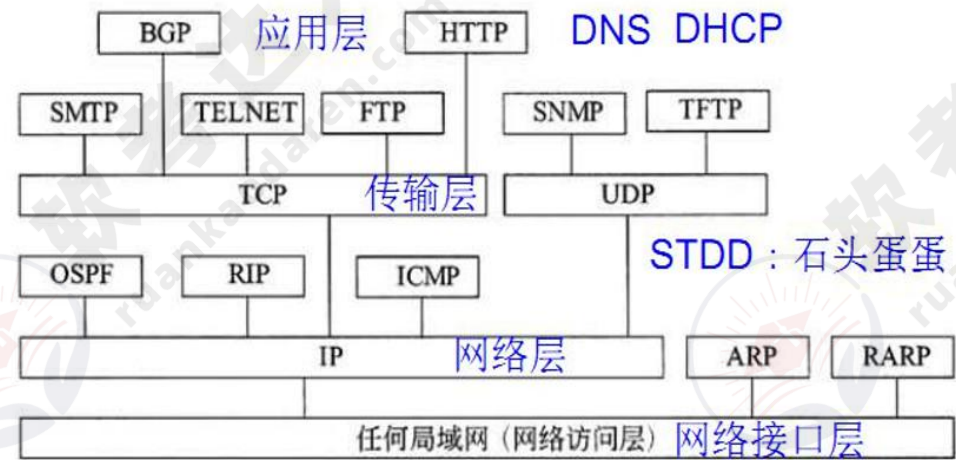
四、网络互联的层次越高，代价就越大，效率越低。

特点：网络互联的层次越高，代价就越大，网络效率越低。

考点 06：TCP/IP 协议簇分为四层

TCP/IP 协议簇与 OSI/RM				
OSI		TCP/IP		
7	应用层	4	进程/应用层	
6	表示层			
5	会话层			
4	传输层	3	主机-主机层	
3	网络层	2	网络互连层	
2	数据链路层	1	网络访问层	
1	物理层			
Ethernet 帧头		IP 头部	TCP 头部	上层数据
				FCS

考点 07：TCP/IP 协议簇主要协议 STDD



TCP/IP 的主要协议https://blog.csdn.net/qq_35428201

考点 08：TCP/IP 协议簇：常用的协议端口号

常见的端口及其服务

端口	服务	端口	服务
20	文件传输协议（数据）	80	超文本传输协议（WWW）
21	文件传输协议（控制）	110	POP3 服务器（邮箱发送）
23	Telnet 终端仿真协议	139	Win98 共享资源端口
25	SMTP 简单邮件发送协议	143	IMAP 电子邮件
42	WINS 主机名服务	161	SNMP - snmp
53	域名服务器（DNS）	162	SNMP-trap -snmp

考点 9：IP 协议：因特网协议，网络层最重要的协议。无连接的、不可靠的，数据包交换。

版本号	IHL	服务类型	总长度
固定部分 20 字节	生存期 TTL	标识符 TCP 协议 UDP	禁止多段 段偏置值 首部最大 60 字节
可变部分 40 字节	源地址	目标地址	任选数据+补丁
最大传输单元 MTU=1500 - 20(IP 报头)=1480 字节数	用户数据	MTU	总长度最大 65535 字节
Ethernet 帧头	IP 头部	TCP 头部	上层数据
			FCS

TCP/IP 报文封装

考点 10：IP 协议数据单元，几个重要字段

- IHL：IP 头长度，20 字节
- 服务类型：区分优先级
- 总长度：包含 IP 头在内
- 头检验和：只校验 IP 头，不包括数据
- 源地址：IP 地址；目的地址：IP 地址
- 生存期：路由器个数+1，超过定值丢弃
- 用户数据：MAC 帧长 1518，MTU1500，
 $1518-14-4-20=1480-20=1460$ 。

考点 11：网络层 IP 地址：4 个字节 32 位，采用 “•” 分隔，十进制表示，如 192.168.1.22，叫点分十进制。

IP 地址结构	
31 比特	0
网络号 (net-id)	主机号 (host-id)

0 网络地址	主机地址	A
10 网络地址	主机地址	B
110 网络地址	主机地址	C
1110 组播地址		D
11110 保留		E

A	1.0.0.0~127.255.255.255	128	255.0.0.0	/8
B	128.0.0.0~191.255.255.255	64	255.255.0.0	/16
C	192.0.0.0~223.255.255.255	32	255.255.255.0	/24
D	224.0.0.0~239.255.255.255	16	不区分网络位、主机位	
E	240.0.0.0~255.255.255.255	16		

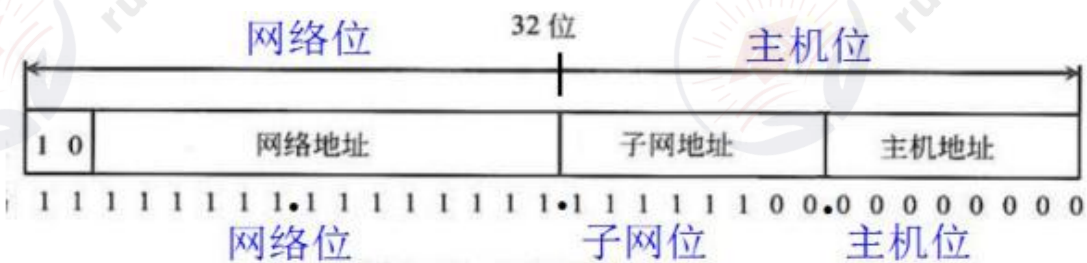
考点 12：IP 私有地址：不能用于公网，只能在内部局域网使用，它们在 Internet 上也不会被路由，但可以通过 NAT 等技术与公网通信。
下表为标准 A、B、C 类私有 IP 地址块。

私网 IP 地址空间

类 型	网络地址	网 络 数	主机数量
A 类	10.0.0.0~10.255.255.255	1	$2^{24}-2$
B 类	172.16.0.0~172.31.255.255	16	$2^{16}-2$
C 类	192.168.0.0~192.168.255.255	256	2^8-2

考点 13：几种 IP 特殊地址：具有特殊意义。

- ① 0.0.0.0：不确切地址，一般设备刚启动尚无 IP 临时使用，表示本机。也叫默认路由地址。
- ② 255.255.255.255：限制(受限)广播地址，同一广播域内的主机，表示本网所有主机。“大广播”。
- ③ 127.0.0.1：回环(送)地址，别名 Localhost，向自己发送测试数据。用于测试。
- ④ 169.254.x.x：自动专用地址，找不到 DHCP 服务器，主机给自己分配的一个 IP。
- ⑤ 网络地址：主机号各位全为 0，表示本网络整个网络，不分配。
- ⑥ 广播地址：主机号各位全为 1，发送给特定网络的所有主机，不分配。也叫直接广播地址，也叫子网广播地址，“小广播”。
- ⑦ 组播地址：224.0.0.1，从 224.0.0.0 到 239.255.255.255，表示一个组内的主机。



考点 14：ICMP 协议：因特网控制报文协议，网络层的协议，协议号为 1。传送有关通信控制和差错报文。就像侦查员、探子。封装在 IP 包中，因而也不可靠。ICMP 的校验和是整个 ICMP，也是必需有的。

考点 15：ICMP 协议报文类型及功能

类型	代 码	校验和	8个 字节
参 数			
信息（可变长）			

ICMP 报文格式

IP 首部	ICMP 报文
IP 数据报	

ICMP 报文类型	类型的值	ICMP 报文的类型	功 能
拐两个弯不可达	3	终点不可达	当路由器不能把数据报转交给目的站时，就向源站发送终点不可达报文
堵塞事故源抑制	4	源站抑制	当路由器由于拥塞而丢弃数据报时，就向源站发送源站抑制报文，使源站放慢数据报的发送速度
拐一个弯重定向 差错报告报文	5	改变路由	当路由器发现主机可以把数据报发送给另外一个路由器，使数据报沿着更短更好的路由被转发
像....时间超时了	11	时间超时	当路由器收到一个 IP 数据报时，发现它的生存时间为 0，或主机在预订的时间内无法完成数据报的重装，则向源站发送时间超时报文
	12	参数问题	当路由器或目的站发现收到的数据报首部字段中有不正确的字段时，就向源站发送参数问题报文
喇叭口有回声吗 询问报文 一生一世时间戳	8 或 10	回送请求或回答	当需要测试某一目的站点是否可达时，就发送一个 ICMP 回送请求报文，然后目的站点会向发送站回送一个 ICMP 回答报文
	13 或 14	时间戳请求或回答	当需每个路由器或主机给出当前的日期和时间时，就发送时间戳请求报文，然后被请求方会回送一个时间戳回答报文，告知自己当前的日期和时间。这样可以用来测试通信延迟

考点 16：子网掩码：屏蔽 IP 地址的网络部分的“全 1”比特模式。将某个 IP 地址划分成网络地址和主机地址两部分。子网

掩码不能单独存在，它必须结合 IP 地址一起使用。类似于“一把刀”，切开西瓜。如：255.0.0.0 表示二进制

11111111.00000000.00000000.00000000

A 类：默认的子网掩码是 255.0.0.0 /8；

B 类：默认的子网掩码是 255.255.0.0 /16；

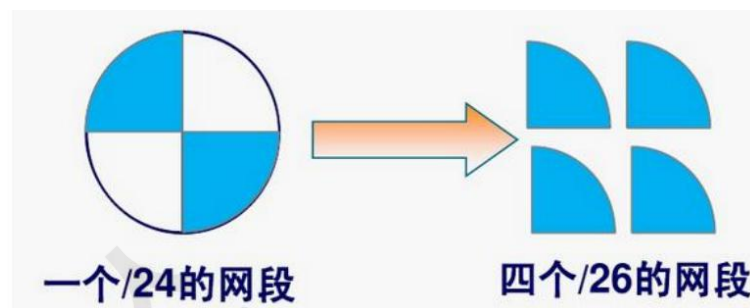
C 类：默认的子网掩码是 255.255.255.0 /24。

考点 17：子网划分原理：为啥划分，借主机位。

①网段：是指标准子网掩码产生的一段网络 IP 范围。

②子网：借用“主机位”将网段划分更小的网络，称为子网。一般指往右“借位”VLSM。

③超网：借用“网络位”将网段合成更大的网络，称为超网。一般指往左“借位”CIDR。



第六章：网络互连与互联网（2）

- **考点01：**地址解析协议ARP：IP查询MAC地址，询问/回答机制。ARP缓存表、ARP欺骗、ARP病毒、代理ARP、反向RARP。

硬件类型 以太网1		IP协议	协议类型 0800
硬件地址长度	协议地址长度	1、2	操作 3、4
6B	4B		
发送节点硬件地址		MAC	
发送节点协议地址		IP	
目标节点硬件地址		MAC	
目标节点协议地址		IP	

ARP/RARP 分组格式

4

- **考点02：**地址解析协议ARP：缓存表：开始-运行-cmd，输入arp -a（-s、-d等）回车。

```
C:\Windows\system32\cmd.exe

C:\Users\DELL>arp -a

接口: 10.1.6.192 --- 0x4

Internet 地址      物理地址      类型
10.1.4.1          00-18-82-2d-83-d2 动态
10.1.7.255        ff-ff-ff-ff-ff-ff 静态
224.0.0.2         01-00-5e-00-00-02 静态
224.0.0.22        01-00-5e-00-00-16 静态
224.0.0.252       01-00-5e-00-00-fc 静态
224.0.1.60        01-00-5e-00-01-3c 静态
239.11.20.1       01-00-5e-0b-14-01 静态
239.255.255.250   01-00-5e-7f-ff-fa 静态
```

5

- **考点03：**地址解析协议ARP：代理ARP，有路由器充当第三方代理，进行ARP请求/回答。

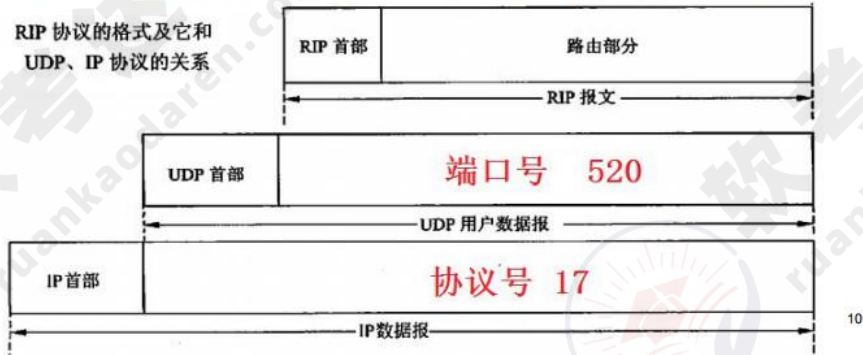


- **考点04：**反向地址解析协议RARP：有MAC查找IP，常用语无盘工作站，设备没有硬盘，无法记录IP，刚启动时发送一个广播，用MAC去获取IP。需要一台RARP服务器，记录MAC与IP的对应关系。
- **考点05：**ARP欺骗和ARP病毒：假如向某一主机发送伪装ARP应答报文，使其发送的信息无法到达预期的主机或到达错误的主机，这就构成了一个ARP欺骗。例如：网管软件获取全网MAC地址。病毒伪装网关MAC收集信息。

- **考点06：**网络层路由协议：选择转发数据路径。



- **考点07：** 路信息由协议RIP：距离矢量算法，计算跳数，最大15跳，16跳不可达。30s更新、180s不存在、240s删除“口诀168”。支持等费用负载均衡和链路冗余。使用UDP的520端口。



- **考点08：** 两种版本：RIPV1和RIPV2区别，适合小型网络。

RIPV1	RIPV2
有类不携带子网掩码	无类携带子网掩码
采用广播更新	采用组播224.0.0.9
周期性更新30s	采用触发更新
不支持VLSM、CIDR	支持VLSM、CIDR
不提供认证	提供明文和MD5认证

1

- **考点09：** 路信息由协议RIP：防止环路的办法。

- ①最大跳数： 当一个路由条目发送出去会自加1跳，跳数最大为16跳，意味着不可达。
- ②水平分割： 一条路由信息不会发送给信息的来源。
- ③反向毒化的水平分割： 把从邻居学习到的路由信息设为16跳，在发送给那个邻居。更安全。
- ④抑制定时器 和 触发更新也可以防止环路。

- **考点10：**开放最短路径优先协议OSPF：链路状态算法，包括：连通、距离、时延、带宽等状态，Dijkstra的SPF算法。触发更新、分层路由。支持大型网络。



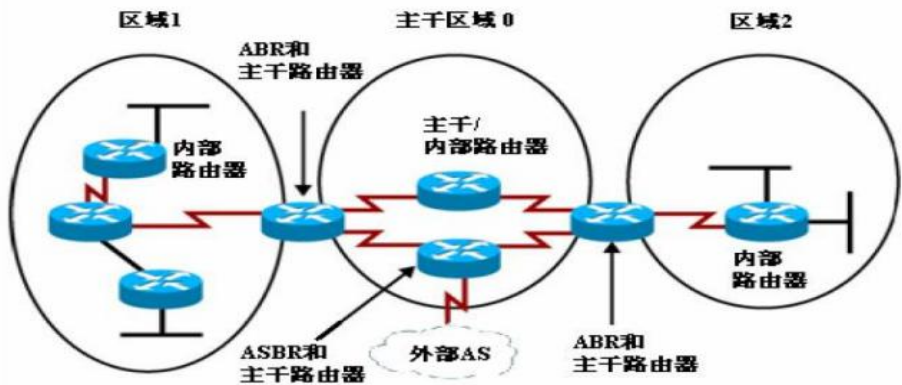
- **考点11：**OSPF区域类型：主干区域(32位)，Area 0.0.0.0或者Area 0来表示。

主干区域	连接其他区域，都要经过主干区域，也接受任何路由信息。
标准区域	接受任何路由信息。
完全存根区域	只接受本区域内的路由信息，其他一概不接收。cisco的。
不完全存根区域	除接受本区域内的路由信息，还接受类型7的。

- **考点12：** 开放最短路径优先协议OSPF：根据物理连接和拓扑结构，分为以下网络类型：

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

- **考点13：** OSPF路由器分类：根据不同区域之间的功能分为：BR、IR、ABR、ASBR。



- **考点14：** OSPF的五种报文类型：Hello报文默认10s(30s)更新一次，40s失效，目标地址是224.0.0.5所有路由器。用于发现建立邻居、还用于选出区域内的指定路由器DR和备份指定路由器BDR（DR/BDR组播地址是224.0.0.6）。

类型	报 文 类 型	功 能 描 述
1	Hello 建立外交关系	用于发现相邻的路由器
2	数据库描述 DBD 外交(数据)内容	表示发送者的链路状态数据库内容
3	链路状态请求 LSR 向对方请求消息	向对方请求链路状态信息
4	链路状态更新 LSU 向对方发送更新	向邻居路由器发送链路状态通告
5	链路状态应答 LSAck 对外交更新回答	对链路状态更新报文的应答

- **考点15：**边界网关协议BGP：是外部网关协议，不同自治系统AS之间。寻找较好的路由策略。通过TCP的179端口建立连接。支持子网VLSM和CIDR，是一种路径矢量协议。目前最新BGP4，而BGP4+支持IPV6。



BGP 协议的格式及它与 TCP 和 IP 协议的关系

20

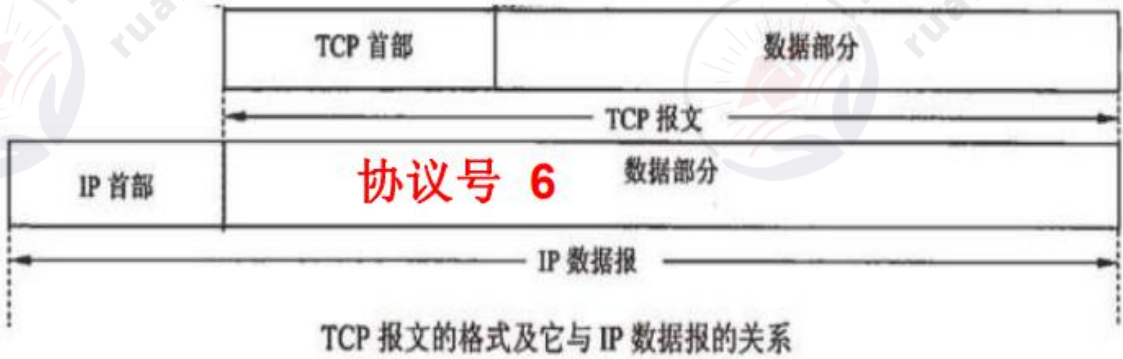
- **考点16：**BGP的四种报文：Open建立邻居，Keepalive周期性探测邻居存活。每一个自治系统要选择至少一个路由器作为该自治系统的“BGP发言人”。增量更新，支持认证。可靠传输，防止环路。自治通信，策略选路。支持无类、支持聚合。

报 文 类 型	功 能 描 述
打开（Open）	建立邻居关系 建立外交
更新（Update）	发送新的路由信息 更新外交信息
保持活动状态（Keepalive）	对 Open 的应答/周期性地确认邻居关系 保持外交活动
通告（Notification）	报告检测到的错误 发布外交通告

21

第六章：网络互连与互联网（3）

- **考点01：** TCP协议：传输控制协议，面向字节流按顺序、连接、可靠、全双工，可变滑动窗口、缓冲累积传送。协议号6。



TCP 报文的格式及它与 IP 数据报的关系

- **考点02：** TCP协议：传输控制协议，下面是 TCP段(段头)，TCP头(传输头)，TCP包头(报头)格式：

源端口		2^16		目标端口		2^16	
固定		发送序号		首部大		20字节	
20字节		接收序号		60字节			
偏置值	保留	URG	ACK	PSH	RST	SYN	FIN
校验和		所有		可变		窗口	
紧急指针		总长度最大		65535字节			
可选项+补丁		任选项+补丁					
MTU=1500-20(IP报头)		用户数据		- 20(TCP报头)=1460字节			

TCP 传输头格式

- **考点03：** TCP协议：几个重要字段
- 源端口、目的端口：16位， 2^{16} （0-65535）
- URG：紧急指针有效
- ACK：应答序号有效
- PSH：推进功能有效
- RST：复位为初始状态
- SYN：建立同步连接
- FIN：结束释放连接
- 校验和：包括TCP段头、数据、伪段头

6

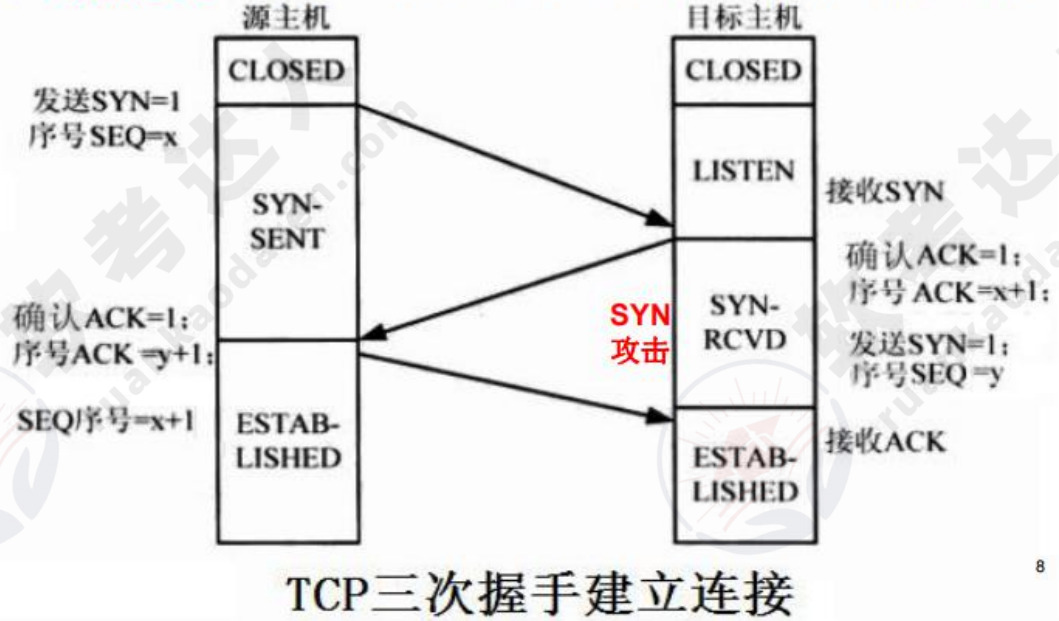
- **考点04：** TCP端口：连接不同的程序，常用协议端口号。更多协议端口，见网络协议神图。

常见的端口及其服务

端口	服务	端口	服务
20	文件传输协议（数据）	80	超文本传输协议（WWW）
21	文件传输协议（控制）	110	POP3 服务器（邮箱发送）
23	Telnet 终端仿真协议	139	Win98 共享资源端口
25	SMTP 简单邮件发送协议	143	IMAP 电子邮件
42	WINS 主机名服务	161	SNMP - snmp
53	域名服务器（DNS）	162	SNMP-trap -snmp

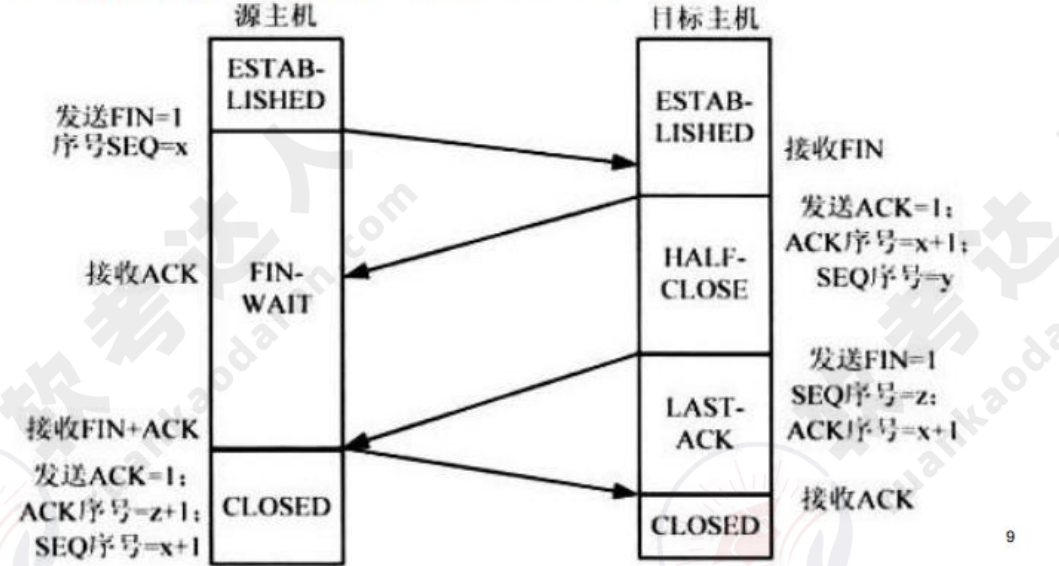
7

● **考点05：** TCP三次握手：防止产生错误的连接。



8

● **考点06：** TCP四次挥手：释放连接。



9

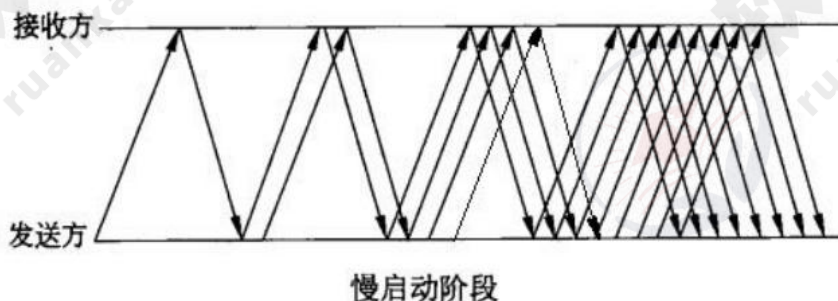
- **考点07：** TCP拥塞控制：报文到达速率大于路由器的转发速率，产生拥塞。解决方法有：
 - ①重传计时器
 - ②慢启动（慢开始）
 - ③拥塞避免
 - ④快速重传
 - ⑤可变滑动窗口
 - ⑥选择重发ARQ
- 总结：差错控制、流量控制、拥塞控制

10

- **考点08：** TCP拥塞控制：超时重传计时器，重传是保证TCP可靠的重要措施。TCP每发送一个报文段，就对这个报文段设置一次计时器。只要计时器设置的时间到了，但还没有收到确认，就重传这一报文段。
- 重传时间要设置的合理，一般和往返时间、平均时延、时间偏差等有关。大多数采取观察最近一段时间的报文时延来估算往返时间。

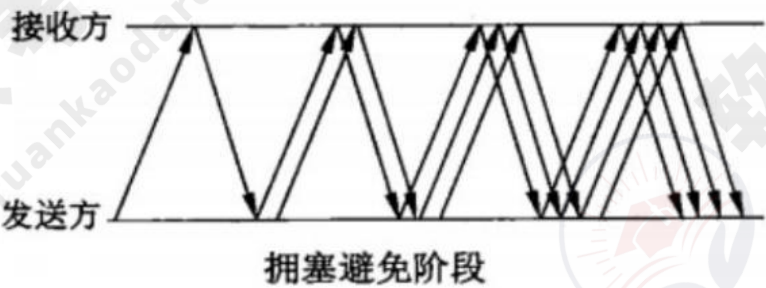
11

- **考点09：** TCP拥塞控制：慢启动，发送方在接收到确认之前逐步扩大窗口的大小。1、2、4、8等按指数规律翻倍，最后达到门限阈值。出现超时，讲拥塞窗口回到1，再次开始慢启动。



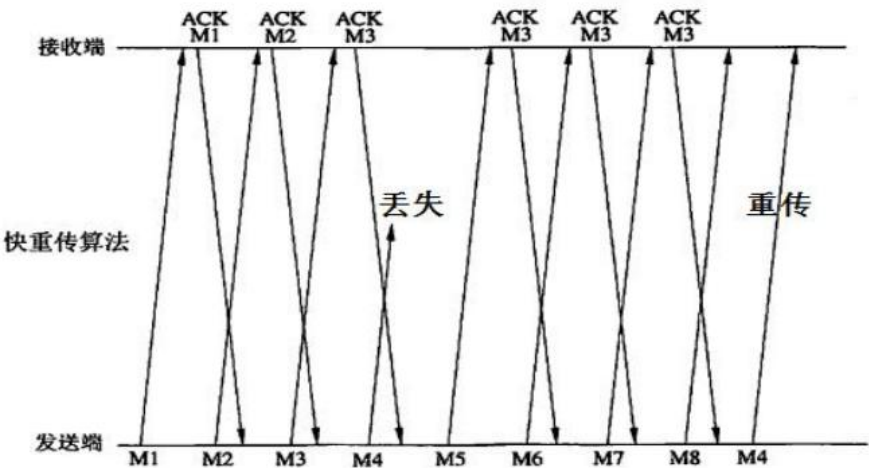
2

- **考点10：** TCP拥塞控制：拥塞避免，窗口达到门限阈值以后，进入拥塞避免阶段，TCP采用线性增加方式放大窗口，按照+1递增。发生拥塞，门限阈值减半。再发生再减半。按指数规律乘倍减半。



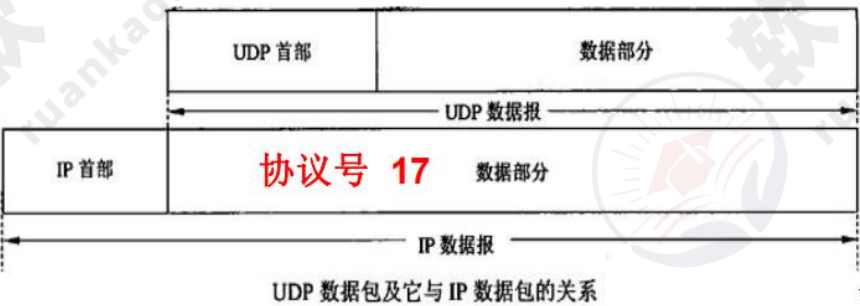
13

- **考点11：** TCP拥塞控制：快速重传，发送端一连收到3个重复的ACK，就重传，不等计时器。



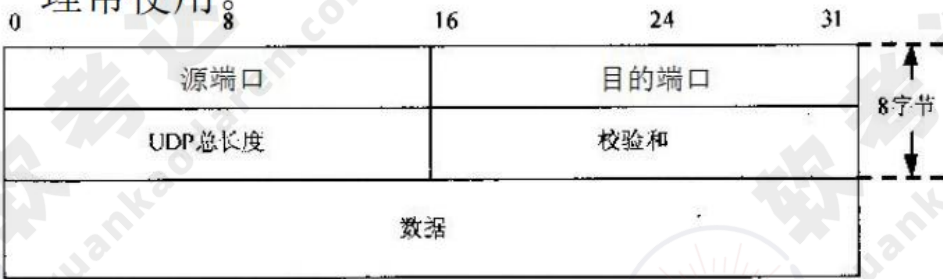
14

- **考点12：** UDP协议：用户数据报协议，无连接的、不可靠的、不保证顺序的、无差错流控机制。校验和包括：UDP头部、数据、伪头部。协议号17。



16

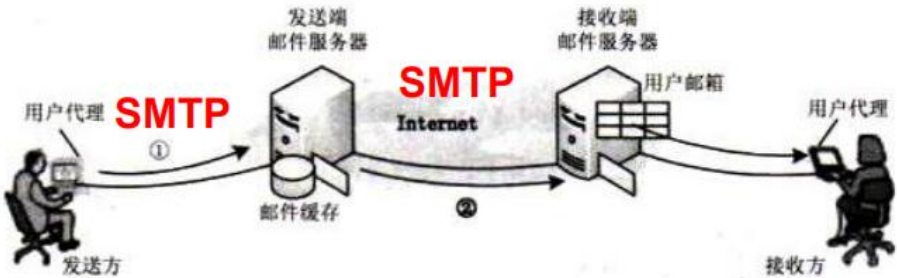
- **考点13：**UDP协议：UDP报文格式如下：少量传输数据，高层程序负责解决数据排序、差错控制等。开销少（头部8个字节），网络管理常使用。



- TCP支持数据传输，UDP支持音视频传输。

17

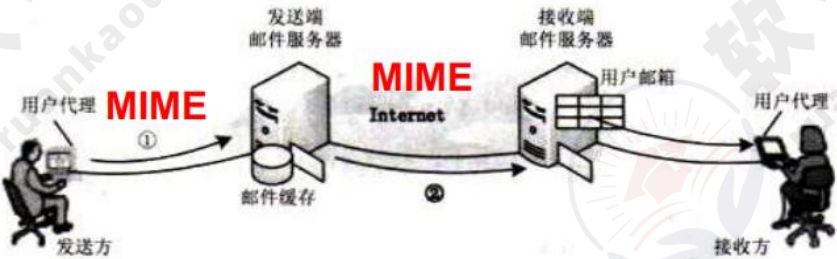
- **考点14：**电子邮件协议：SMTP简单邮件传输协议，负责将邮件上传到服务器，采用TCP的25端口，C/S工作。仅传送ASCII码文本。



电子邮件系统的工作原理示意图

19

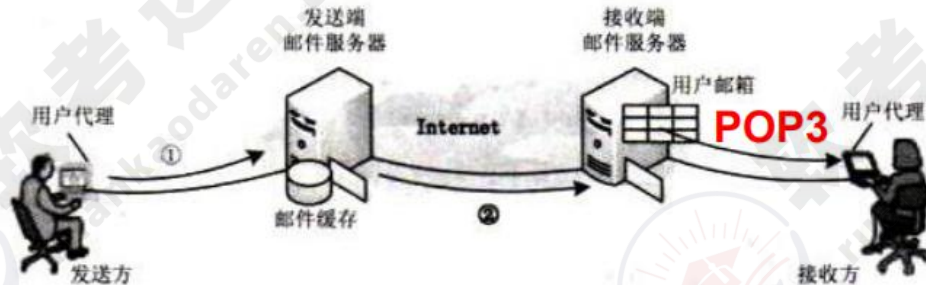
- **考点15：**电子邮件协议：S/MIME多用途互联网邮件扩展协议，负责将多媒体邮件安全上传到服务器，包含文本、图像、音频、视频以及其他应用程序专用的数据。



电子邮件系统的工作原理示意图

20

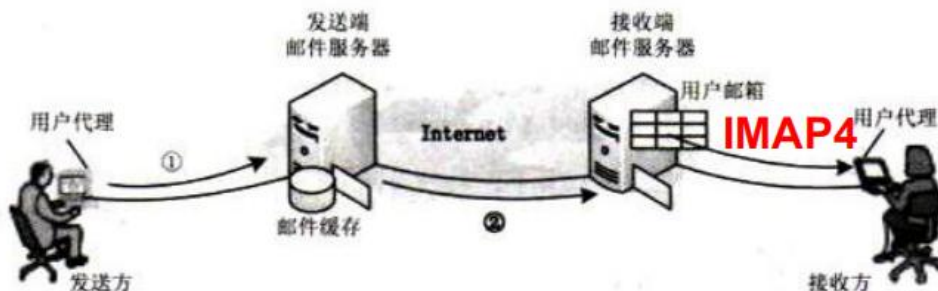
- **考点16：**电子邮件协议：POP3邮局协议，负责将邮件下载到客户机，采用TCP的110端口，C/S工作。用户从服务器读取邮件后，服务器就删除该邮件。



电子邮件系统的工作原理示意图

21

- **考点17：**电子邮件协议：IMAP4互联网消息访问协议，提供摘要浏览，选择下载。采用TCP的142端口，C/S工作。用户从服务器读取邮件后，服务器仍会保存该邮件。

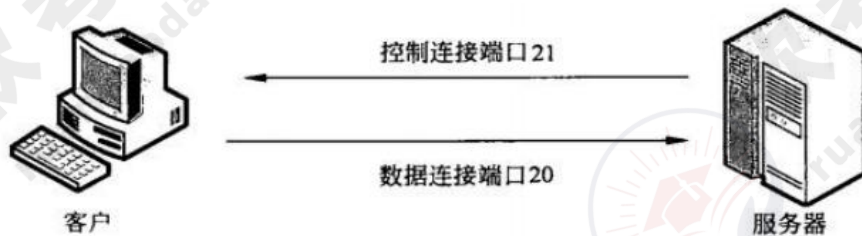


电子邮件系统的工作原理示意图

22

- **考点18：**电子邮件协议：PGP电子邮件加密协议，包括加密、鉴别、签名和压缩等技术。使用IDEA(128位)加密数据，RSA加密密钥，MD5认证。
- PEM增强保密邮件协议，使用多种加密方法提供机密性、认证和信息完整性的因特网电子邮件协议，采用每个报文一次一密的方法加密。其他和PGP功能差不多。

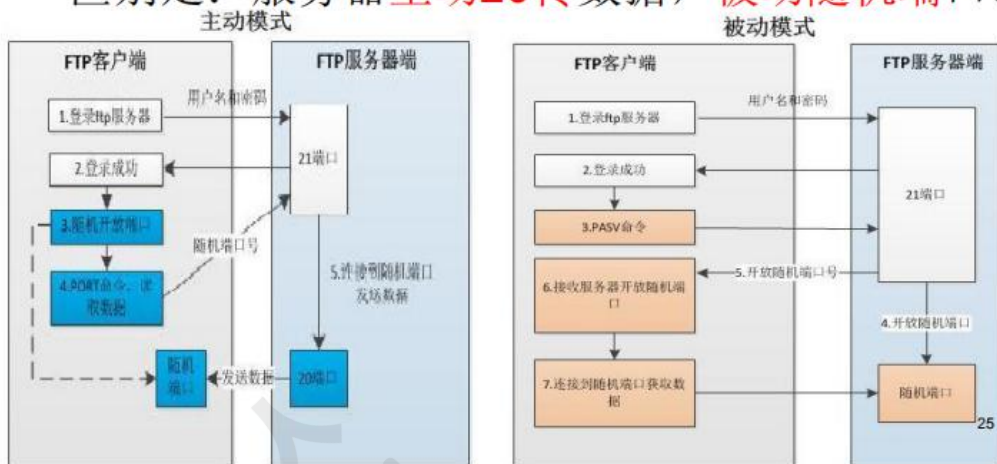
- **考点19：** 文件传输协议：FTP，负责文件通过服务器上传传送。采用TCP的两条连接：数据连接20端口，控制连接21端口，C/S工作。合法访问和匿名访问(anonymous)。一般访问方式ftp://192.168.92.58或ftp://www.dtwlxy.com



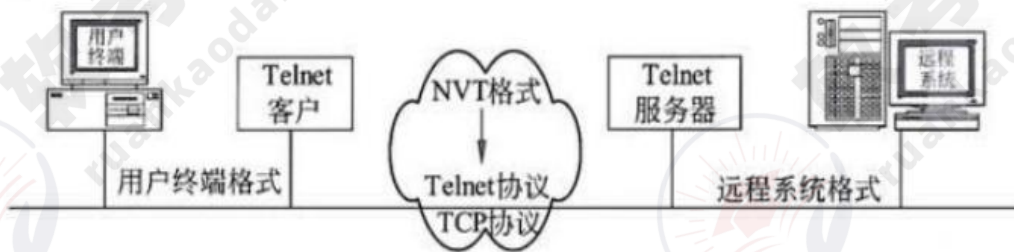
FTP 控制连接和数据连接

24

- **考点20：** 文件传输协议：FTP，有主动模式(PORT/Standard)和被动模式(PASV/Passive)。区别是：服务器**主动20**传数据，**被动随机端口**。



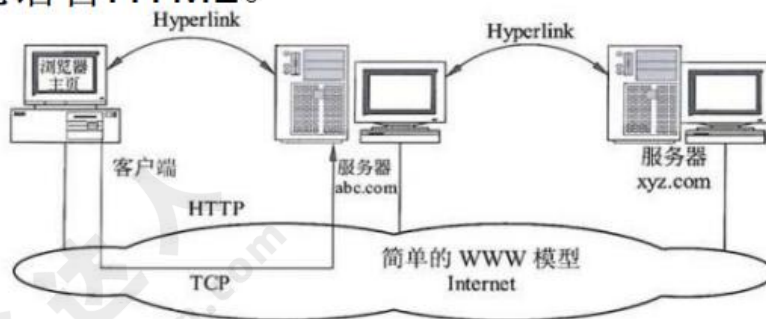
- **考点21：**远程登录协议：Telnet，TCP/IP终端仿真协议，登录到远程主机上操作，网络虚拟终端NVT支持异构主机，采用TCP的23端口，C/S工作。使用命令telnet 192.168.1.254。



Telnet 客户端/服务器概念模型

26

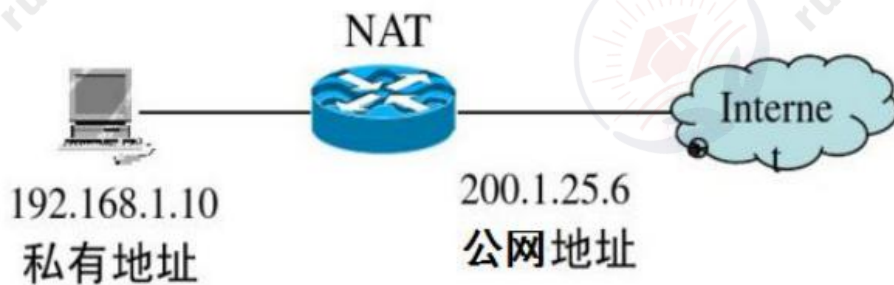
- **考点22：**超文本传输协议：HTTP，万维网WWW(Web)服务器提供全球的、分布的、动态的、多平台的、交互的、多媒体信息。TCP的80端口，B/S工作。统一资源定位器URL，如，<http://bbs.dtwlxy.com/index.asp>。超文本标记语言HTML。



27

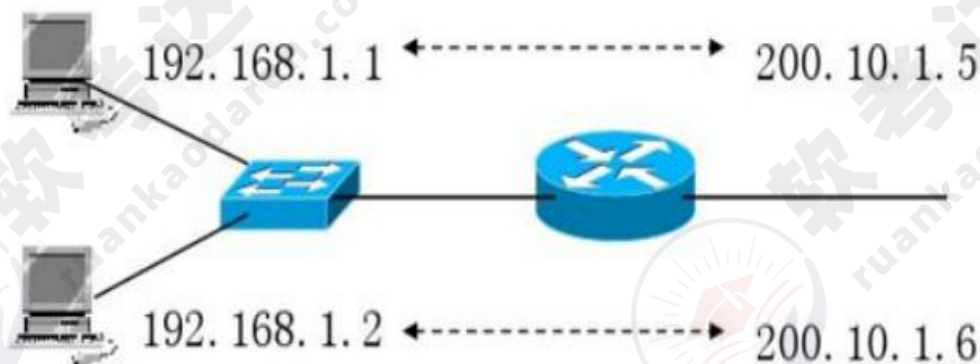
第六章：网络互连与互联网（4）

- **考点01：**路由器技术NAT：网络地址翻译，¹解决IP短缺，路由器内部和外部地址进行转换。
- 静态地址转换：静态NAT（一对一）
- 动态地址转换：动态NAT（多对少）
- 网络地址端口转换：NAPT（多对一）

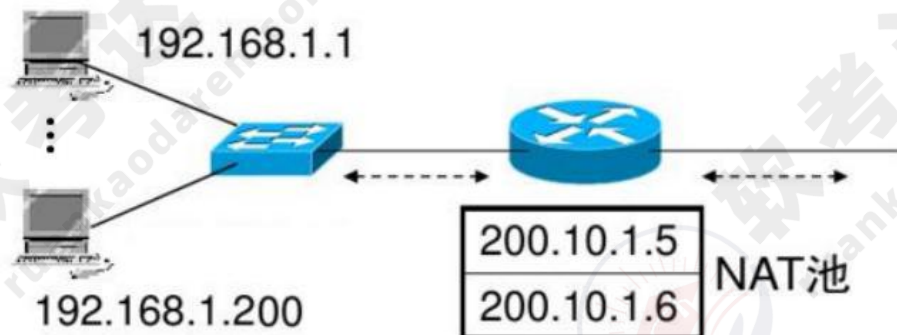


4

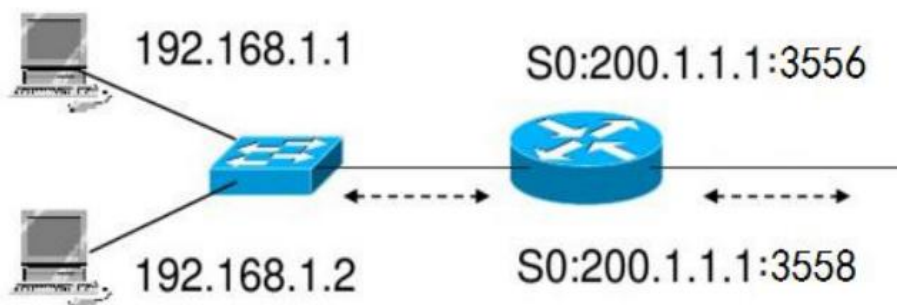
- **考点02：**路由器技术NAT：静态NAT，内外一对一转换，用于web服务器，ftp服务器等固定IP的主机服务器。



- **考点03：**路由器技术NAT：动态NAT，内外多对少转换，用于内部局域网较多用户访问外部网络。外部需要地址池（pool）。



- **考点04：**路由器技术NAT：网络地址端口转换：NAPT(PAT)（多对一）内外多对一转换，使用外部一个IP，多个端口号对应内部IP。也称为IP伪装，可以隐藏内部主机。



7

- **考点05：**路由器技术VLSM：可变长子网掩码。在有类的IP地址的基础上，从它们的主机号部分借出相应的位数来做网络号，也就是增加网络号的位数，子网划分。
- 各类网络可以用来再划分子网的位数为：A类有24位可以借，B类有16位可以借，C类有8位可以借。前面学习的“三步划分子网”。
- VLSM是把标准网络分割成更小的子网的技术，而CIDR是把几个标准网络合并成一个大网络的技术。

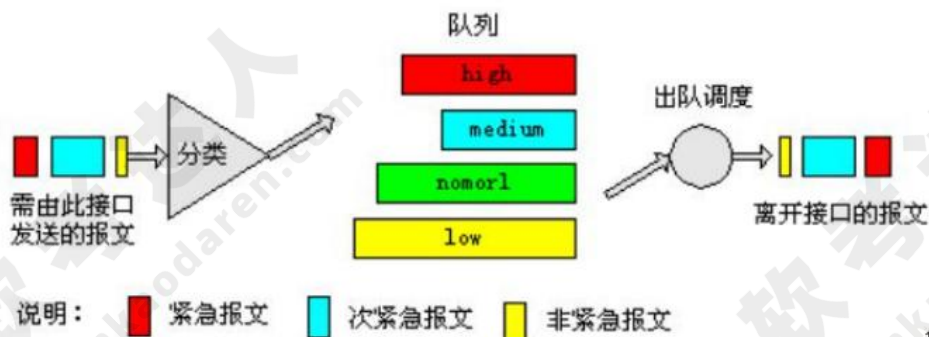
9

- **考点06：**路由器技术CIDR：无类域间路由，解决路由缩放问题，采用/比特位，无类不区分A、B、C类，称为CIDR地址块，路由汇聚。
- 例如下面有4个路由条目如下，要进行汇聚
172.18.129.0/24、172.18.130.0/24、
172.18.132.0/24、172.18.133.0/24，
则能覆盖这4个路由的条目是：172.18.128.0/24。

解题思路：也可应用“三步划分子网”，根据网络地址是块大小的倍数。第三段， $133-129+1=5$ ，块大小8，8的倍数接近129的是128。

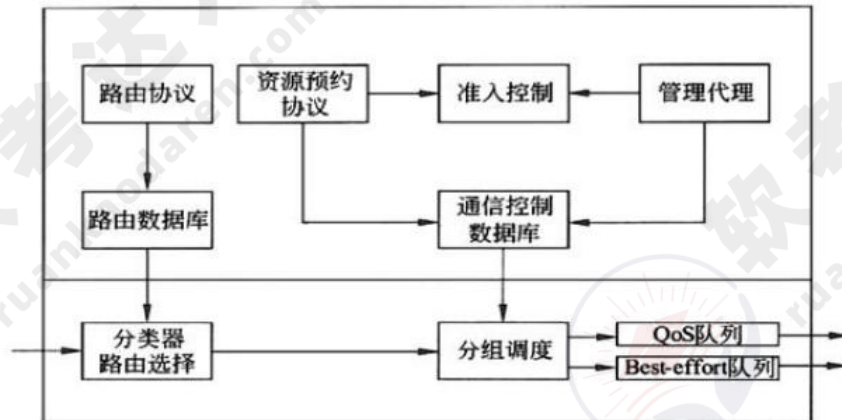
10

- **考点07：**路由器技术QoS：网络服务质量。将网络数据流分成不同的等级，提供不同的服务。有集成服务(IntServ)和区分服务(DiffServ)两种标准。



12

- **考点08：** 路由器技术QoS： 集成服务(IntServ)
分成三种： 保证质量的服务、控制负载的服务、
尽力而为的服务（目前因特网提供的服务）。

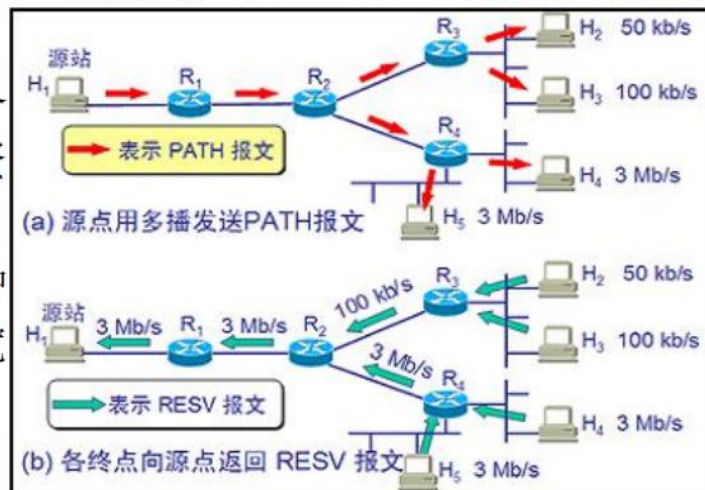


13

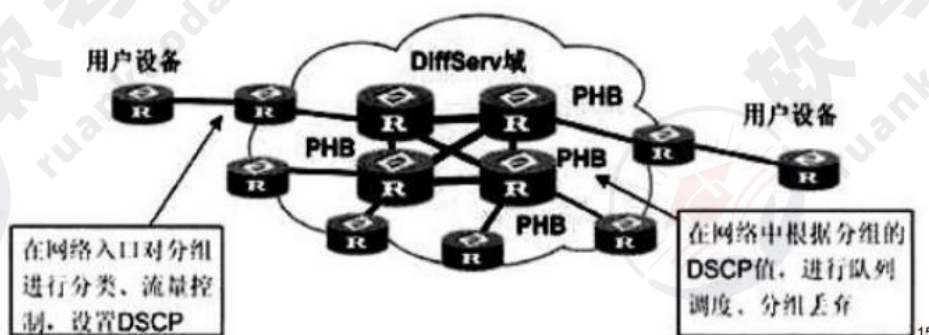
- **考点09：** 集成服务（IntServ）：资源预约协议

RSVP。

每个业务流申请资源预留，包括缓冲区及带宽的大小，每一跳。



- **考点10：** 路由器技术QoS： 区分服务(DiffServ)
不再使用资源预约，而是区分不同的业务流。
分为三种： 尽力服务BE、优质服务AF、加速服务EF。



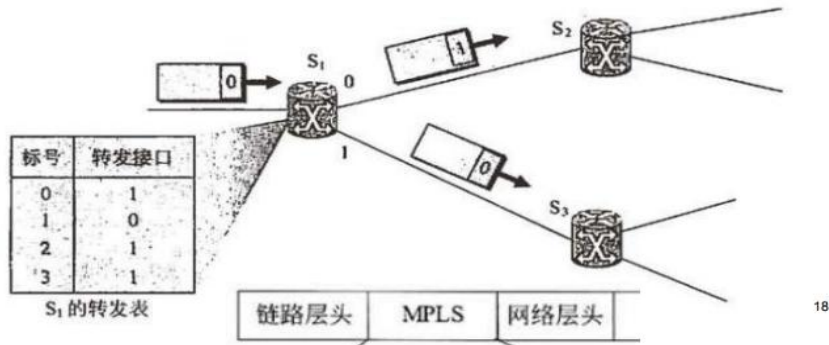
15

- **考点11：**区分服务(DiffServ)：区分服务代码点DSCP，利用IP包头的服务类型字段ToS。
- 逐跳行为PHB：逐级跳的转发方式，每个PHB对应一种转发方式。

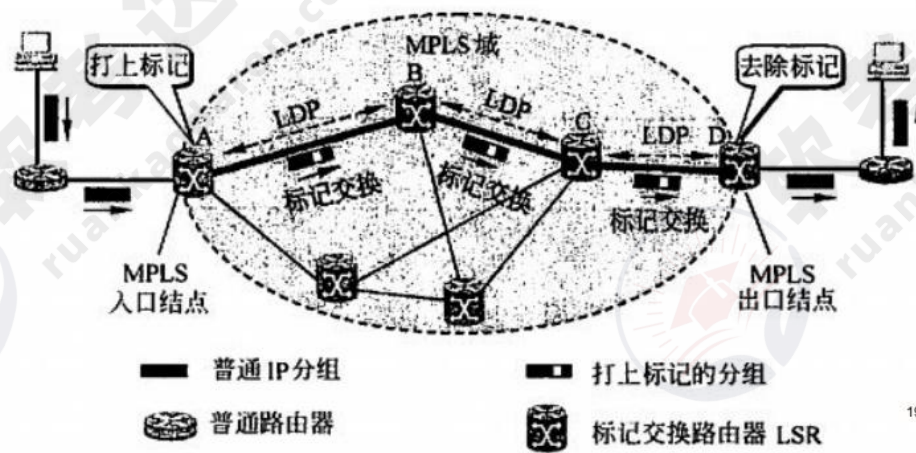
DSCP 与 PHB 的映射关系

DSCP	PHB	说 明
000000	BE	尽力而为的服务，不保证 QoS 需求
001×××	AF1	4 种保证转发服务的 QoS 介于 EF 和 BE 之间。 可以为每一种 AF 服务指定 3 种不同的丢弃优先级， 总共可以组成 12 种不同的 AF 聚集
010×××	AF2	
011×××	AF3	
100×××	AF4	
101110	EF	绝对保证 QoS 的服务

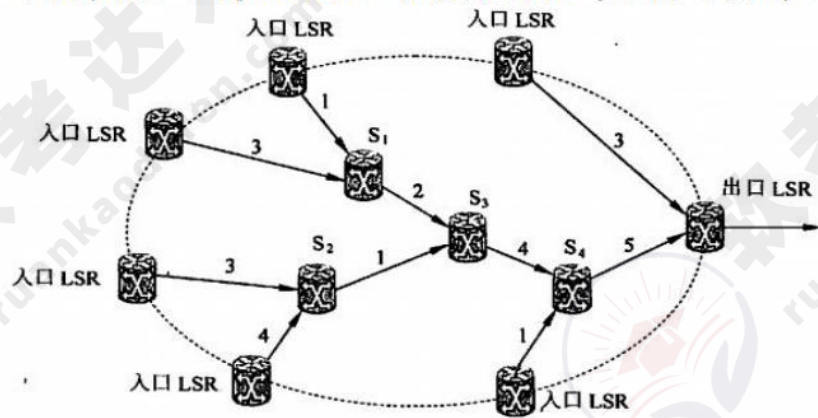
- **考点12：**路由器技术MPLS：多协议标签交换，属于2.5层，一般认为是第三层交换，硬件交换、速度快，叫一次路由，多次交换。用标签交换代替复杂的路由运算。



- **考点13：**路由器技术：MPLS基本原理。标记边缘路由器LER，标记交换路由器LSR。

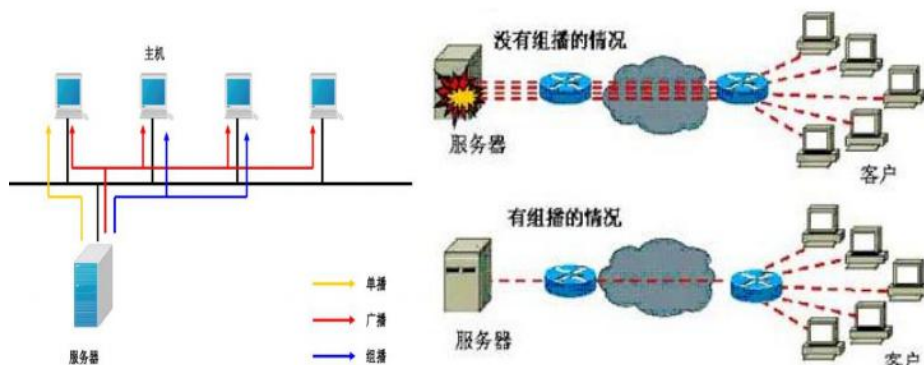


- **考点14：** 路由器技术：MPLS转发等价类 (FEC)，把等价的通信流汇聚转发。标记具有局部性。提供QoS、粒度控制、负载均衡等。



20

- **考点15：** 路由器技术：IP组播，有一个源向一组主机发送信息，D类地址。（一个IP地址代表一个主机，称为单播地址。）



- **考点16：** 路由器技术：IP组播用途，用于视频点播、网络电视、视频会议等点到多点的业务。IP组播地址分为三类：
- 保留组播：224.0.0.0~224.0.0.255用于路由协议，如224.0.0.1代表所有主机，224.0.0.2代表所有路由器。
- 用户组播：224.0.1.0~238.255.255.255，全球范围分配，类似公网IP。
- 本地组播：239.0.0.0~239.255.255.255本地子网分配，类似私网IP。

23

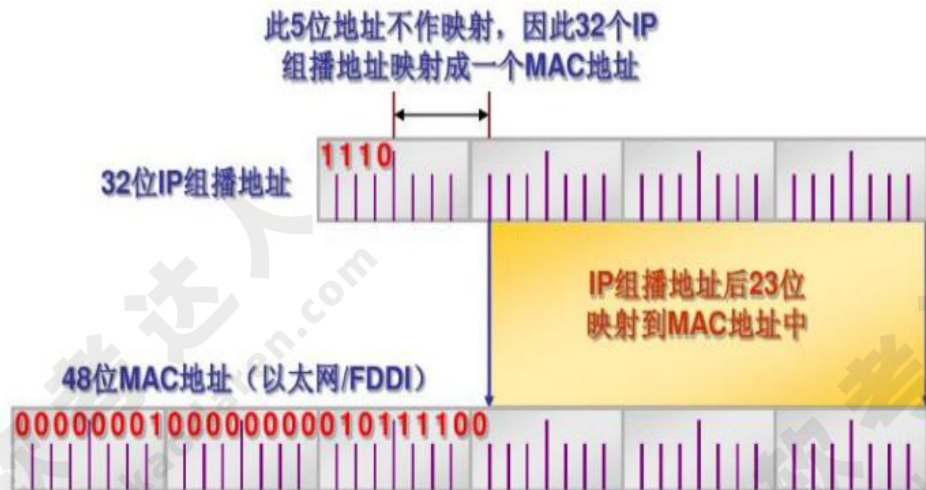
● **考点17：** 路由器技术： 常考IP组播地址：

- 224.0.0.1 所有主机的地址
- 224.0.0.2 所有组播路由器的地址
- 224.0.0.5 所有ospf路由器
- 224.0.0.6 ospf DR/BDR
- 224.0.0.9 rip-2路由器
- 224.0.0.10 Eigrp路由器
- 224.0.0.12 dhcp 服务器/中继代理
- 224.0.0.13 所有pim路由器

组播MAC地址：
01-00-5e-xx-xx-xx

24

● **考点18：** 路由器技术： IP组播地址与MAC地址： 组播MAC地址： 01-00-5e-xx-xx-xx。



25

- **考点19：**IP组播协议：IGMP因特网组管理协议，管理主机加入或离开组播组。IGMP封装在IP中，协议号2。IGMPv3报文：分为三种
- ①成员资格询问报文：组播路由器发出，询问是否有主机加入组播。
- ②成员资格报告报文：主机加入组播组。
- ③组记录报文：记录组播的状态和信息。



- **考点20：**IP组播路由协议：用来建立组播树，是实现组播传输的关键技术。源分发树和共享分发树。



- **考点21：**IP组播路由协议：名词解释

- PIM：协议无关组播

- PIM-DM：密集模式PIM

- DVMRP：距离矢量组播路由协议

- MOSPF：组播开放式最短路径优先

- CBT：基于核心的树

- PIM-SM：稀疏模式PIM

- **考点22：**IP组播路由协议：PIM-DM：密集模式PIM。用于组播成员集中，且较多，如局域网。

- 采取“泛洪扩散-修剪丢弃”维护组播分发树。使用“推”的机制，**先给你，可以不要。**

- 关键技术是利用反向通路，使用自己找回来的路径。

- 使用源分发树：以组播源为根节点构造到所有组播组成员的生成树，通常也称为最短路径树（SPT）。

29

- **考点23：**IP组播路由协议：PIM-SM：稀疏模式PIM，用于组播成员较少，且稀疏分布，如广域网。

- 采用选择性的建立和维护分布树。只有发送请求的才会收到数据。使用“拉”的机制，**你要了，才会给你。**

- 使用共享分发树：确定一个汇聚点。先发给汇聚点，再有汇聚点发给其他路由器。

第七章：下一代互联网

- **考点01：**IPV6概念：下一代互联网NGI，目前主要是IPV6。IPV6分组格式如下：



- **考点02：**IPV6各个字段的解释含义：
- 版本0110，代表IPV6
- 通信类型：8位，IP分组优先级，同服务类型
- 流标记：20位，标记特殊处理的分组
- 负载长度：16位，除了固定，扩展和负载
- 下一头部：8位，指明下一头部的类型
- 跳数限制：检测路由循环
- 源地址：128位，发送端的地址
- 目标地址：128位，接收端的地址

● **考点03：**IPV6分组封装：IPV6跳槽记

- (1) IPv6 头部。
- (2) 逐跳选项头。
- (3) 目标选项头（第一个目标节点要处理的信息）。
- (4) 路由选择头。
- (5) 分段头。
- (6) 认证头。
- (7) 封装安全负荷头。
- (8) 目标选项头（最后的目标节点要处理的信息）。
- (9) 上层协议头部。

IPV6跳槽记

情景记忆法

- **考点04：**IPV6地址：128位，冒分十六进制。
8000:0000:0000:0000:0123:4567:89AB:CDEF（8段，每4位二进制，写成十六进制）

- IPV6地址简化书写：①前面的0可以省，后面的不可以省。②多个0可以用冒号，但只能一次。③多个0可以压缩为一个0。④IPV4 兼容写法::192.168.1.10。

- IPV6格式前缀：12AB00000000CD3/60简写
12AB::CD30:0:0:0:0/60、12AB:0:0:CD30::/60

- **考点05：**IPV6地址分类：单播地址、任意播地址、组(多)播地址。分配到接口，一个接口可以被赋予任何类型的多个地址或地址范围。
- 任意播：①不能作源，只能作目标。②不能给主机，只能给路由器。
 - 组(多)播：一组接口。没有广播，格式前缀1111 1111。
 - 单播：①可聚合全球单播。②链路本地地址。③站点本地地址。④特殊单播地址。

● **考点06：**IPV6单播地址分类。

- ①可聚合全球单播（相当于公网IP）：格式前缀001。
- ②链路本地地址（相当于自动专用IP）：前缀1111 1110 10。
- ③站点本地地址（相当于私有IP）：格式前缀1111 1110 11。
- ④特殊单播地址：不确定地址0:0:0:0:0:0:0:0，不分配，初始用，能作源，不能目。回环地址0:0:0:0:0:0:0:1，发给自己，可作源和目。

● **考点07：**IPV6和IPV4的地址比较，如下表。

0123456789A(10)B(11)C(12)D(13)E(14)F(15)

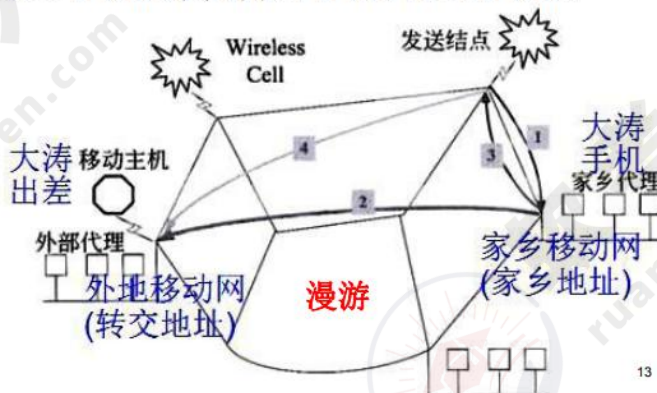
IPv4 地址	IPv6 地址
点分十进制表示	带冒号的十六进制表示，0 压缩
分为 A、B、C、D、E 5 类	不分类
组播地址 224.0.0.0/4	组播地址 FF00::/8
广播地址（主机部分为全 1）	任意播（限于子网内部）
默认地址 0.0.0.0	不确定地址:: 0:0:0:0:0:0:0:0
回环地址 127.0.0.1	回环地址::1 0:0:0:0:0:0:0:1
公共地址	可聚合全球单播地址 FP=001 前缀001
私网地址 10.0.0.0/8; 172.16.0.0/12; 192.168.0.0/16	站点本地地址 FEC0::/48 1111 1110 11
自动专用 IP 地址 169.254.0.0/16	链路本地地址 FE80::/48 1111 1110 10

- **考点08：**移动IP的概念：移动主机在移动的同时，能够在任何地方使用他的家乡地址进行联网。



- **考点09：**移动IP的原理：移动主机分配一个家乡地址作为永久标识。如果到外地赋予一个转交地址，家乡地址会获得外地的转交地址。

- 1、在老家大涛拿手机号
- 2、大涛出差我帮你问问
- 3、给你大涛出差的手机
- 4、直接联系外地的大涛



- **考点10：**IPV6过渡技术：①隧道技术。②协议翻译技术。③双协议栈技术。
- **隧道技术：**用于解决IPV6节点之间通过IPV4网络进行通信的问题。（通过隧道）
- **协议翻译技术：**使得纯IPV6节点之间和纯IPV4节点之间可以通信。（英汉翻译）
- **双协议栈技术：**使得IPV4和IPV6共存于同一设备和同一网络中。（英汉两种）

15

- **考点11：**IPV6路由协议：定义了五种协议
- **RIPng：**RIPv2的扩展，UDP 521端口。
- **OSPFv3：**OSPFv2的扩展，做了较大改进。
- **BGP4+：**BGP4的扩展，用来支持IPV6。
- **ICMPv6：**ICMP的扩展，集成了ARP功能。
- **IS-IS：**中间系统到中间系统，IS-IS属于内部网关路由协议。IS-IS是一种链路状态协议，与TCP/IP网络中的OSPF协议非常相似，使用最短路径优先算法进行路由计算。

第八章：网络安全与应用（1）

- **考点01：**网络安全威胁和漏洞类型：

- | | |
|---------------|-------|
| ● 窃听 | 病毒 |
| ● 假冒 | 木马 |
| ● 重放 | 诽谤 |
| ● 流量分析 | 非授权访问 |
| ● 破坏完整 | 拒绝服务 |

- 漏洞：物理、软件、不兼容、其他等。

- **考点02：**网络安全信息数据五大特征：

- 完整性：信息数据完整不破坏。
- 保密性：信息数据需授权不泄露。
- 可用性：信息数据攻击后迅速恢复可用。
- 不可否认性：信息数据参与者补课否认不可抵赖，身份真实有效。
- 可控性：信息数据可以管控传播范围。

● **考点03：**网络安全基本技术：

- 数据加密：数据按照规则打乱，重新组合。
- 数字签名：证明发送者签发，也可完整性。
- 身份认证：用户合法性，身份真实没假冒。
- 防火墙：控制内外数据进出，阻挡病毒木马。
- 入侵检测：采用异常检测特征保护网络。
- 网络隔离：内外网隔离分开使用，如网闸。

● **考点04：**现代信息加密技术：对称和非对称。

{	对 称	{ DES、3DES、IDEA、 AES、RC4等
	非对称	{ RSA（基于大素数分解 3人） ECC（椭圆曲线密码编码学） Elgamal（基于离散对数 1人）

DES数据加密标准、3DES三重DES加密、
IDEA国际数据加密算法、AES高级加密标准、
RC4流加密算法第四版 2人等

● **考点05：**现代信息加密技术对称密钥总结表：

类型	名称说明	密钥长度	分组长度	安全性
DES	数据加密标准，速度较快，适用于加密大量数据的场合；	56	64	依赖密钥受穷举法攻击
3DES	在DES基础上，用2个不同的密钥进行3次加密，强度更高	112	64	军事级，可抗差值等相关分析
AES	高级加密标准，下一代加密算法标准，速度快，安全级别高	128、192 256	64	安全级别高，高级加密标准
IDEA	国际数据加密算法，使用 128 位密钥提供非常强的安全性	128	64	能抵抗差分密码分析的攻击
MD5	信息-摘要算法 Message-Digest 5	128	512	主要是为数字签名而设计的
SHA	安全散列算法 Secure Hash Algorithm	160	512	可实现数字签名，和MD5相似

- **考点06：**公钥加密RSA：加密体系：公钥加密，私钥解密。（签名体系：私钥加密，公钥解密）

①选两个大素数 p 和 q

②令 $n=p*q$ ， $z=(p-1)(q-1)$

③符合公式 $e*d=1 \pmod{z}$ ， e 公钥， d 私钥。

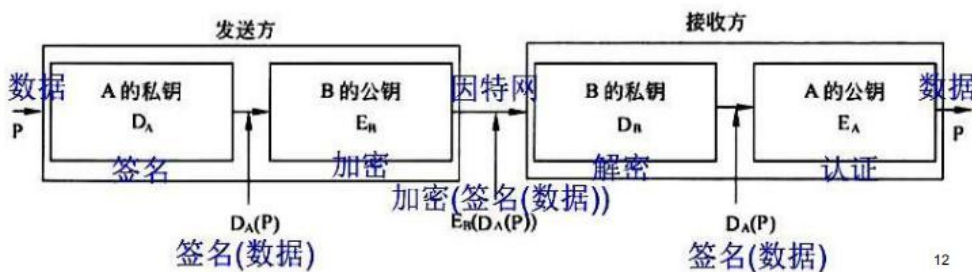
mod 为模运算，也就是取余数计算，例如：

$e*d=1 \pmod{z}$ 可变形为 $(e*d) / z$ 余数为1

10

- **考点07：**数字签名技术：数字签名用于确认发送者身份和消息完整性。满足三个条件：①接收者能够核实发送者。②发送者事后不能抵赖。③接收者不能伪造签名。

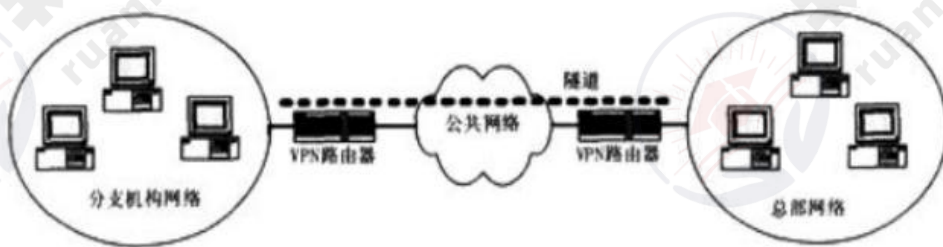
- 下图为基于公钥的签名和加密体系示意图：



12

- **考点08：**密钥管理体系：KMI、PKI、SPK
- **KMI：**密钥管理基础结构，第三方KDC，秘密物理通道，适用于封闭的内网使用。
- **PKI：**公钥基础结构，不依赖秘密物理通道。适用于开放的外网。
- **SPK：**适用于规模化专用网。

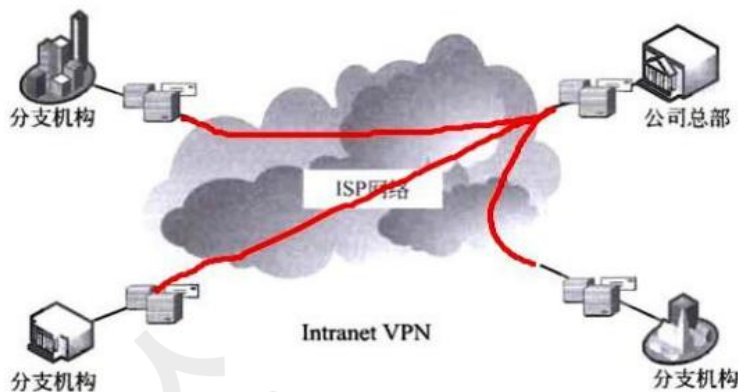
- **考点09：**VPN技术：虚拟专用网，①建立在公网上。②虚拟性，没有专用物理连接。③专用性，非VPN用户无法访问。
- **VPN四个关键技术：**①隧道技术。②加解密技术。③密钥管理技术。④身份认证技术。



16

- **考点10：**VPN三种应用解决方案：

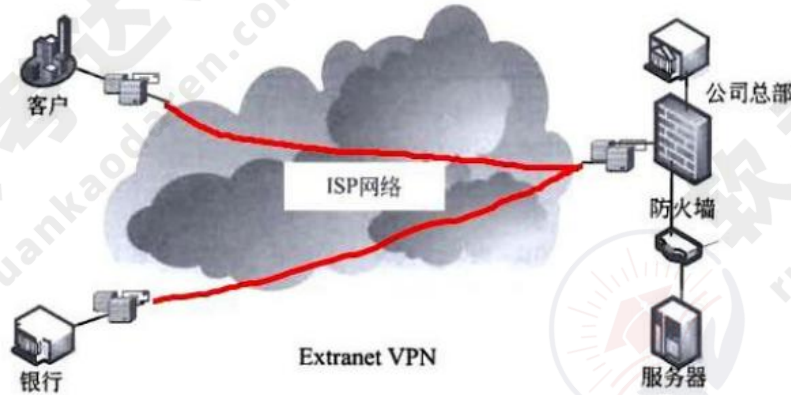
①内联网VPN（Intranet VPN）：企业内部用于连通总部和分布各个LAN。



17

● **考点11：** VPN三种应用解决方案：

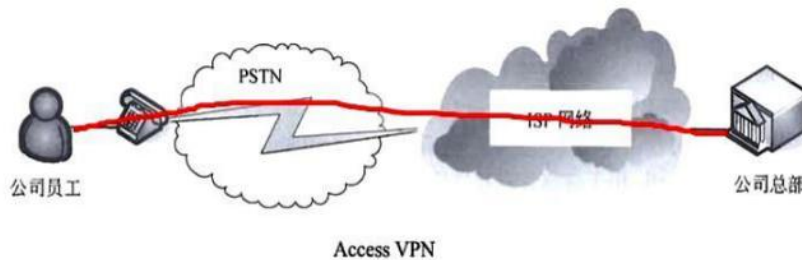
②外联网VPN（Extranet VPN）：企业外部用于实现企业与客户、银行、供应商互通。



18

● **考点12：** VPN三种应用解决方案：

③远程接入VPN（Access VPN）：解决远程用户出差访问企业内部网络。



19

● **考点13：** VPN在七层协议中使用的技术汇总：

VPN { 二层：PPP、PPTP、L2TP
三层：IPSec、GRE
四层：SSL/TLS

PPP点对点协议、 PPTP点对点隧道协议
L2TP第二层隧道协议、 IPSec IP安全性、
GRE通用路由封装协议、 SSL/TLS安全套接层。

● **考点14：** PPP、PPTP、L2TP技术对比汇总：

PPP	{	LCP：链路控制协议（2层）
		NCP：网络控制协议（3层）
PPP	{	PAP：口令认证协议（明文）
		CHAP：挑战握手协议（密文）
PPTP	{	PAC：PPTP接入集中器
		PNS：PPTP网络服务器
L2TP	{	LAC：L2TP访问集中器
		LNS：L2TP网络服务器

21

● **考点15：** PPTP与L2TP的区别比较：

- ①PPTP要求IP网络，L2TP适用各种网络。
- ②PPTP只能建立1条隧道，L2TP建立多条。
- ③PPTP包头占用6字节，L2TP占用4字节
- ④PPTP不支持隧道验证，L2TP支持。

总结：L2TP一个字“好”，四个字“好好好好”。

- **考点16：IPSec：IP安全性**，在IP层通过加密与数据源验证，来保证数据包传输安全。
- ①认证头AH，用于数据完整和数据源认证、防重放。
- ②封装安全负荷ESP，提供数据保密、数据完整、辅助防重放。
- ③密钥交换协议IKE，生成分发密钥。
- IPSec两种模式：传输模式和隧道模式。

23

- **考点17：IPSec：传输模式和隧道模式。**

原来的IP头	TCP	数据
--------	-----	----

原来的IP头	AH	TCP	数据
--------	----	-----	----

传输模式的认证头

新的IP头	AH	原来的IP头	TCP	数据

隧道模式的认证头

24

- **考点18：**SSL安全套接层：和TLS（传输层安全标准）是双胞胎。在传输层上4.5层套接安全协议。SSL/TLS被称为HTTPS，工作在传输层，对传输层、应用层都可以控制。

潜伏 余则成 的故事



25

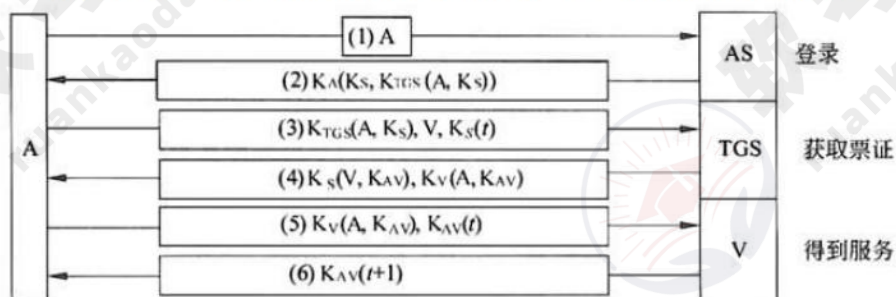
- **考点19：**SSL和IPSec的区别比较：
- ①IPSec在网络层建立隧道，适用于固定的VPN。SSL是通过应用层的web连接建立的，适合移动用户远程访问公司的VPN。
- ②IPSec工作在网络层，灵活性小。SSL工作在传输层，灵活性大。

26

第八章：网络安全与应用（2）

- **考点01：**应用层安全协议SHTTP和HTTPS：
- SHTTP：Sec HTTP，安全超文本传输协议，是HTTP扩展，使用TCP的80端口。
- HTTPS：HTTP+SSL，使用TCP的443端口。大部分web应用采用这个。
- SET：安全的电子交易，主要应用电子商务。

- **考点02：**应用层安全协议Kerberos(刻薄肉丝)：是一项认证服务，3A(AAA)认证有验证、授权和记账。防重放、保护数据完整性。AS认证服务器，TGS票据授予服务器，V应用服务器。



V4时间戳，V5序列号。口诀：无T加T，有T加1⁵。

- **考点03：**病毒：一段可执行的程序代码，通过其他可执行程序启动和感染传播，可自我复制，难以清除，破坏性强。（强盗）
- 木马：一种潜伏在计算机里并且秘密开放一个甚至多个数据传输通道的远程控制程序。C/S结构，客户端也称为控制端。偷偷盗取账号、密码等信息。（间谍）
- 恶意代码：又称恶意软件。也称为广告软件、间谍软件，没有作用却会带来危险。（恶搞）

7

- **考点04：**常见病毒木马的特征分类：
- ①文件宏病毒：感染office文件，前缀Macro或者word/excel等。
- ②蠕虫病毒：前缀Worm通过系统漏洞传播。
- ③木马病毒：前缀Trojan，黑客病毒前缀Hack，往往成对出现。
- ④系统病毒：前缀Win32、PE、Win95等。
- ⑤脚本病毒：前缀Script，脚本语言编写的，通过网页传播。

8

- **考点05：**黑客与骇客：黑客技术高超，帮助测试建设网络。骇客专门搞破坏或恶作剧。
- 黑客攻击：①拒绝服务攻击。②缓冲区溢出攻击。③漏洞攻击。④欺骗攻击。
- 攻击预防：安装杀毒软件和防火墙，合理设置安全策略。

考点 6:

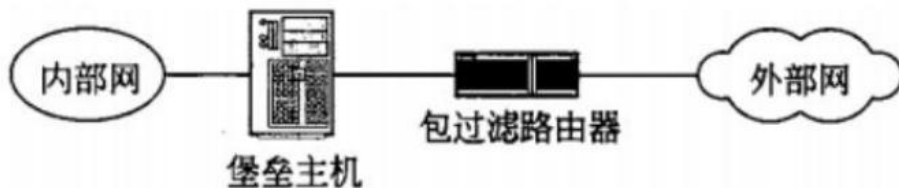
防火墙的主要功能：①访问控制功能。②内容控制功能。③全面的日志功能。④集中管理功能。⑤自身的安全功能。

- 防火墙的附加功能：①流量控制。②网络地址转换NAT。③虚拟专用网VPN。
- 防火墙的局限性：①关闭限制了一些服务带来不便。②对内部的攻击无能为力。③带来传输延迟单点失效等。④还有其他局限。

12

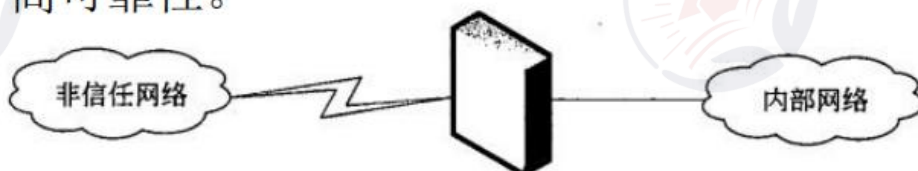
考点 7:

防火墙的体系结构：①双宿主主机模式：防火墙具有两个网卡接口，通过包过滤代理访问网络。这是比较简单的一种结构。一般可以根据IP地址和端口号进行过滤。



双宿主主机模式

- **考点 8:** 防火墙的定义：来源于建筑物“防火墙”一词，位于两个或多个网络之间，执行访问控制策略，过滤进出数据包的一种软件或硬件设备。
- 防火墙的要求：①所有进出网络的通信流量都必须经过防火墙。②只有内部访问策略授权的通信才能允许通过。③防火墙本身具有很强的可靠性。



11

考点 9： 防火墙PIX的配置简介：Cisco的硬件防火墙，典型的设备是PIX525。

- 三种接口：①内部接口（inside）：连接内网和内网服务器。②外部接口（outside）：连接外部公共网络。③中间接口（DMZ）：连接对外开放服务器。
- 常用命令有：nameif、interface、ip address、nat、global、route、static、conduit、fixup、telnet等。

15

考点 10： 防火墙nameif、interface、ip add

PIX525#conf t	//进入配置模式
PIX525(config)#nameif ethernet0 outside security 0	//设置安全级 0
PIX525(config)#nameif ethernet1 inside security100	//设置安全级 100
PIX525(config)#nameif ethernet2 dmz security 50	//设置安全级 50
PIX525(config)#interface ethernet0 auto	//设置自动方式
PIX525(config)#interface ethernet1 100full	//设置全双工方式
PIX525(config)#interface ethernet2 100full	//设置全双工方式
PIX525(config)#ip address outside 133.0.0.1 255.255.255.252	//设置接口 IP
PIX525(config)#ip address inside 10.66.1.200 255.255.0.0	//设置接口 IP
PIX525(config)#ip address dmz 10.65.1.200 255.255.0.0	//设置接口 IP

考点 11： 防火墙global、nat、route、acl

PIX525(config)#global (outside) 1 133.1.0.1-133.1.0.14	//定义的地址池
PIX525(config)#nat (inside) 1 0 0	//0 0 表示所有
PIX525(config)#route outside 0 0 133.0.0.2	//设置默认路由
PIX525(config)#static (dmz, outside) 133.1.0.1 10.65.1.101	//静态 NAT
PIX525(config)#static (dmz, outside) 133.1.0.2 10.65.1.102	//静态 NAT
PIX525(config)#static (inside, dmz) 10.65.1.200 10.66.1.200	//静态 NAT
PIX525(config)#access-list 101 permit ip any host 133.1.0.1 eq www	//设置 ACL

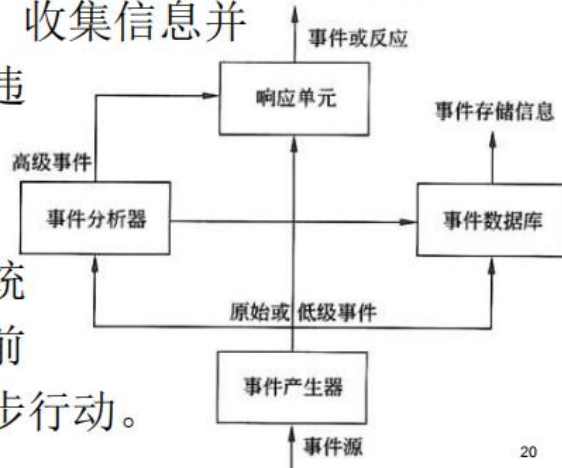
17

考点 12： 防火墙访问规则：

- 1、inside可以访问任何outside和dmz区域
- 2、dmz可以访问outside区域
- 3、outside访问dmz需配合static(静态地址转换)
- 4、inside访问dmz需要配合acl(访问控制列表)

- 其他软件防火墙：天网防火墙、ISA Server（微软公司）。

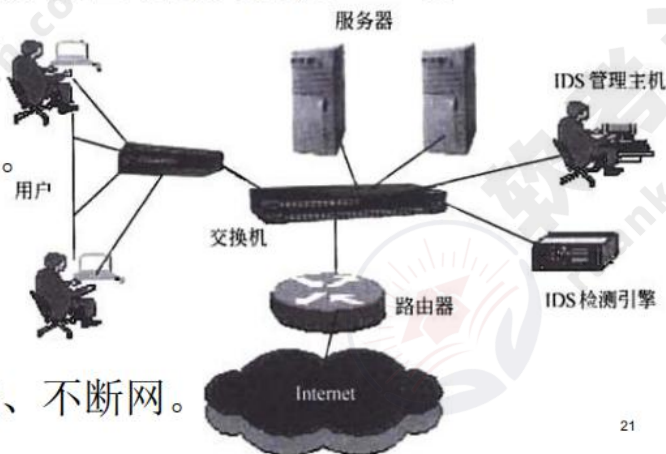
考点 13： 入侵检测系统IDS：位于防火墙之后的第二道安全屏障，是防火墙的有力补充。通过对网络关键点 收集信息并 对其分析，检测到违反安全策略的行为和入侵的迹象，做出自动反应，在系统损坏或数据丢失之前阻止入侵者的进一步行动。



20

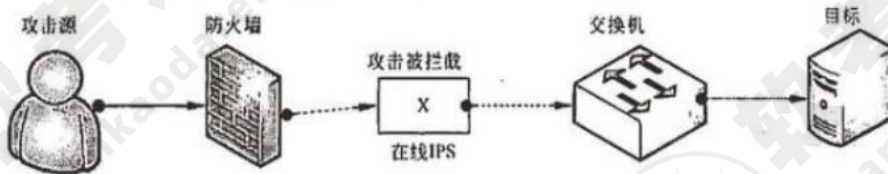
考点 14： 入侵检测系统IDS：安装部署位置通常是：①服务器区域的交换机上。②Internet接入路由器之后的第一台交换机上。③其他重点保护网段的交换机上。

- 通常是并联、不断网。



21

考点 15： 入侵防御系统IPS：位于防火墙之后的第二道安全屏障，是防火墙的有力补充。通过对网络关键点 收集信息并对其分析，检测到攻击企图，就会自动将攻击包丢掉或采取措施阻挡攻击源，切断网络。



- 通常是串联、会断网。

22

考点 16： IPS/IDS和防火墙区别：防火墙一般只检测网络层和传输层的数据包，不能检测应用层的内容。IPS/IDS可以检测字节内容。

- IPS和IDS的区别：IPS是串接在网络中，会切断网络。IDS是旁路式并联在网络上，不切断网络。
- IDS/IPS：连接在需要把交换机端口配置成镜像端口上，可以检测到全网流量。

23

第九章：网络操作系统与应用服务器（1）

- **考点01：**网络操作系统：用统一的方法管理各主机之间的通信和资源的共享。
- 主要功能：网络通信、共享资源、网络管理、网络服务、互操作、网络接口。
- 四大特征：并发、资源共享、虚拟、异步性。
- 安全性：用户账号、时间限制、地点限制、磁盘空间限制、传输介质、加密审计等。
- **考点02：**网络服务器Windows Server 2008：微软基于Windows XP/NT5.1开发的服务器操作系统，于2008年发布，原定2018结束支持，后延期至2026年。企业版、标准版、Web版数据中心版等8个版本。
- 专为下一代网络、应用程序和Web服务设计，R2升级版提升了虚拟机、系统管理、信息安全，仅支持64位，服务于大、中、小企业。
- 新增功能：①网站IIS7.0。②虚拟机化Hyper-V。③可靠可扩展。④管理中心增强。
- **考点03：**网络服务器Red Hat Enterprise Linux 7.0：红帽子，是开放源代码的产品，是Linux操作系统的一种。因为它具备最好的图形界面，无论是安装、配置还是使用都十分方便，而且运行稳定，适合做服务器。
- 在第9个版本之后，Red Hat公司不再发行Red Hat Linux，而开始发行Fedora。同时将其商业化的努力全部转向了Red Hat Enterprise Linux系列，目前最新版是RHEL 7.0。

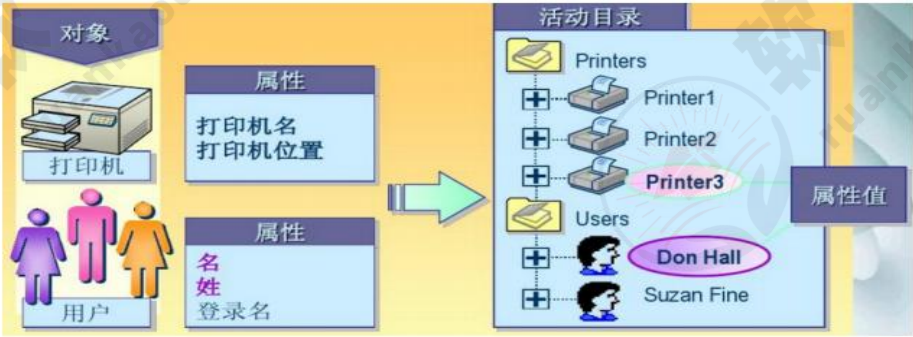
● **考点04：** Windows Server 2008本地用户与组：

- 用户：就是包含用户名、密码、权限以及说明。
- 用户组：具有相同性质的用户归结在一起，统一授权，组成用户组。
- 用户组分类：全局组、本地组、特殊组。
- 创建用户和组：计算机--右键--管理--配置--本地用户和组。

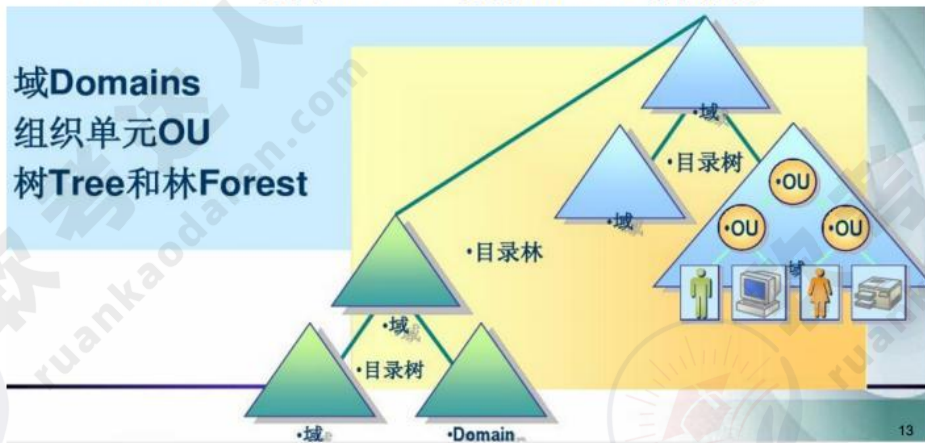
● **考点05：** 常见用户和组的权限，列表如下：

组名	描述信息
Administrators	具有 完全控制权限 ，并且可以向其他用户分配用户权利和访问控制权限
Backup Operators	加入该组的成员可以 备份和还原 服务器上的所有文件
Guests	拥有一个在登录时创建的 临时 配置文件，在注销时该配置文件将被删除
Network Configuration Operators	可以 更改 TCP/IP 设置 并更新和发布 TCP/IP 地址
Power Users	该组具有 创建用户账户和组账户 的权利，可以在 Power Users 组、Users 组和 Guests 组 中添加或删除用户，但是不能管理 Administrators 组成员 可以创建和管理 共享资源
Print Operators	可以管理 打印机
Users	可以执行一些 常见任务 ，例如运行应用程序、使用本地和网络打印机以及锁定服务器 用户不能共享目录或创建本地打印机

- **考点06：** Windows Server 2008活动目录：是指网络资源信息的目录，是一个数据库，如用户、计算机、进程、服务、应用程序等。有了活动目录，才能登陆域，才能访问网络资源。



- **考点07：**活动目录结构：组织单元OU、域domain、域树tree、域林forest等构成。



- **考点08：**活动目录中的工作组：①全局组：来自本域用于全林。②通用组：来自全林用于全林。③域本地组：来自全林用于本域。
- 活动目录的安装和配置：①需要NTFS分区。②需要安装DNS服务器。开始→运行→执行dcpromo.exe，启动域控服务器安装向导。



- **考点09：**Windows 2008 R2 远程桌面服务：为了满足同时允许多个用户同时远程一台服务器，就需要开启多个Windows远程桌面连接才能满足自己的要求。
RD：远程桌面
- 有6个组件：①远程桌面会话主机，RD的服务端。②远程桌面Web访问，提供通过Web浏览器或者APP访问。③远程桌面授权，给RD客户端颁发许可证。④远程桌面网关，可以给RD客户机通过外网连接网。⑤远程桌面连接代理，支持连接APP程序或虚拟机。⑥远程桌面虚拟化主机，集成了Hyper-V。

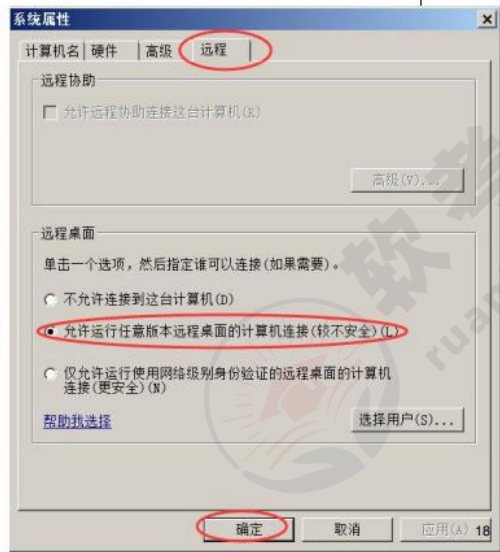
RD 服务器
安装：开始
管理工具--
服务器管理
器--角色--
添加角色--
服务器角色
--远程桌面
服务。



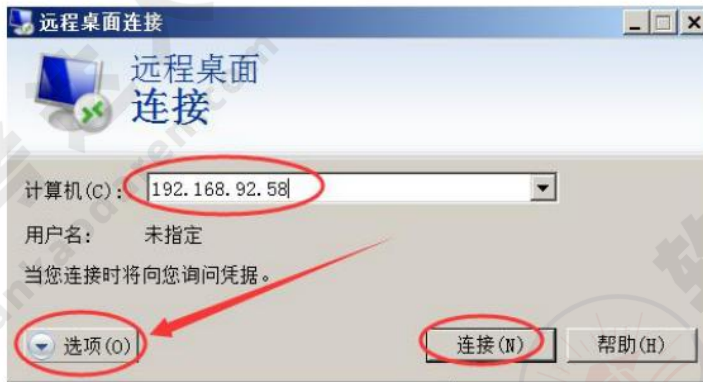
● RD服务器
配置方法：
开始--管理
工具--远程
桌面服务--
远程桌面会
话主机配置
--右击RDP-
Tcp--属性。



● **考点10：**远程桌面
连接：提供一种连接
远程工作站桌面的一
种远程管理工具。①
计算机--右击--属性--
远程设置--远程--勾选
允许...远程桌面连接
②防火墙放行。③设
置系统密码。



- 开始--所有程序--附件-远程桌面连接，或者开始--运行--输入mstsc.exe后回车--输入IP地址。



19



- **考点11：**微软管理控制台MMC：它本身不执行管理功能，但可以集成许多管理工具以方便管理。开始--运行--MMC，打开控制台--文件--添加删除...



21

- **考点12：Linux用户和组：**Linux是一个多用户、多任务的分时操作系统。每个文件和程序必须属于某一个用户，每个用户对应个账号。其中最重要的一个超级用户root。
- 超级用户root承担了系统管理的一切任务，可以控制所有的程序，访问所有文件，使用系统中的所有功能和资源。
- 其他用户和组都是有root来创建的。

23

- **考点12：Linux用户和组3个重要配置文件：**
- /etc/passwd：用户文件，存储用户和密码的信息，对所有用户可读。
- /etc/shadow：用户文件，也是存储用户和密码等信息，只有超级用户root可以读。目前一般采用这个，保密性好。
- /etc/group：用户组文件。使用组同时赋予多个用户相同的文件访问权限。一个用户可以同时属于多个组。

24

- **考点13:** Linux用户和组4个重要管理命令：
- **useradd:** 新增用户，暂时锁定，是因为没有初始密码。
- **passwd:** 配置密码，包括设置、修改、锁定密码等。
- **userdel:** 删除用户，必要时删除用户的主目录。
- **su:** 切换用户，比如由普通用户切换到root用户。
(增、删、改、换)

25

- **考点14:** Linux文件目录管理：文件格式有EXT2、EXT3、EXT5等。采用树型根目录结构，用/表示。其他所有目录都是从根目录出发生成的。将所有的硬件、软件都作为文件来管理。
- **/bin**存放系统命令。**/dev**所支持全部的设备文件。**/etc**系统管理配置文件。**/lib**函数库数据库命令。**/mnt**空目录，安装拆卸文件硬件等。**/tmp**存放临时文件。**/usr**程序存放主目录。**/home**默认用户主目录。**/proc**内存虚拟目录。

26

- **考点15:** Linux文件权限：五种类型、四种权限、三个分组。口诀543。例如：
- **-rw-r--r-- 1 root root 0 10-27 13:05 test**
普通文件，用户权限可读可写，用户组权限可读，其他用户可读。

普通文件 -
目录文件 d
链接文件 l
设备文件 b
管道文件 p
5个文件类型



27

● **考点16：**Linux文件和目录操作命令：

- cat滚动显示
- more分屏显示
- less按页显示
- cp文件复制
- mv文件移动
- rm文件删除
- mkdir创建目录
- rmdir删除目录
- cd改变目录
- pwd当前目录
- ls列出目录
- chmod改变权限
- ln文件链接
- touch改变文件时间
- find查找文件
- grep表达式查找

28

● **考点17：**Linux网络配置文件：

- /etc/sysconfig/network，服务器上网络配置。
- /etc/hostname，主机名和完整域名
- /etc/hosts，IP和主机名映射，别名
- /etc/host.conf，和主机名解析顺序
- /etc/resolv.conf，DNS客户机配置
- /etc/services，服务名和端口号之间的映射。
- /etc/rc.d/init.d/network，网络配置脚本，开机通过脚本文件来读取相应的初始配置。

29

● **考点18：**Linux网络配置命令：

- ifconfig，网络接口(网卡)命令
ifconfig up、ifconfig down、ifconfig eth0
- route，配置路由命令
route add、route del、route gw
- ping，网络测试命令
ping -a、ping -t、ping -n、ping -l
- netstat，网络查询命令
netstat -r、netstat -a、netstat -n

第九章：网络操作系统与应用服务器（2）

（WEB 服务器安装配置）

- **考点01：**Windows Server 2008 R2 IIS服务简介：Internet Information Services，互联网信息服务。微软Windows平台下的一种Web（网页）服务组件，其中包括Web服务器、FTP服务器、管理工具等。（去掉了SMTP和POP3）
- **IIS7.5安装过程：**开始--管理工具--服务器管理器--角色--添加角色--勾选Web服务器IIS--下一步--勾选“Web服务器IIS”、“管理工具”、“FTP服务器”--下一步开始安装。如下图。



● 考点02: WEB服务器网站配置:

- ①基本配置：网站名称、物理路径(主目录)。
- ②文档配置：默认文档，也可添加、删除等。
- ③身份验证配置：属于安全配置。

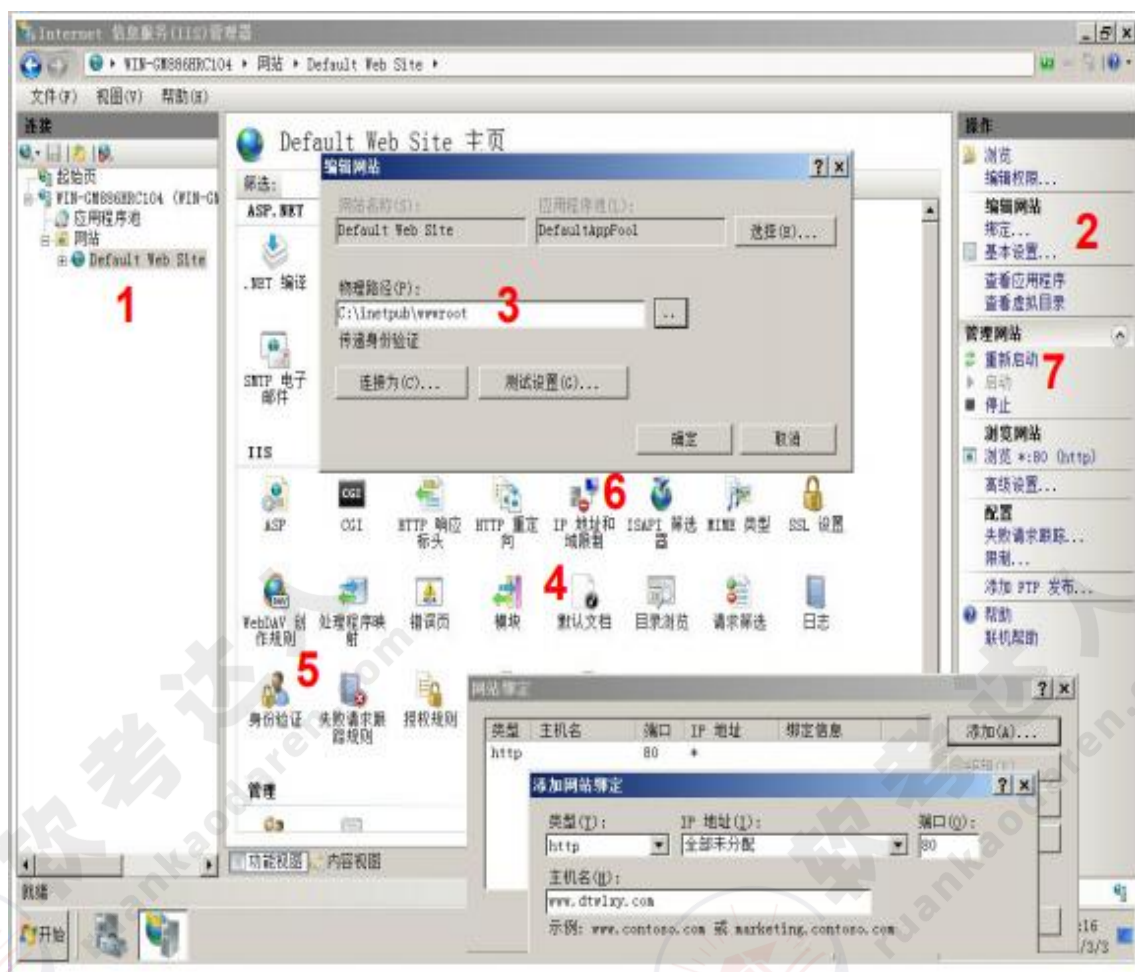
一般设为匿名身份验证。

- ④IP限制配置：属于安全配置。

允许或拒绝，一个IP或IP范围。

- 访问：http://IP或域名、http://IP或域名:端口

14





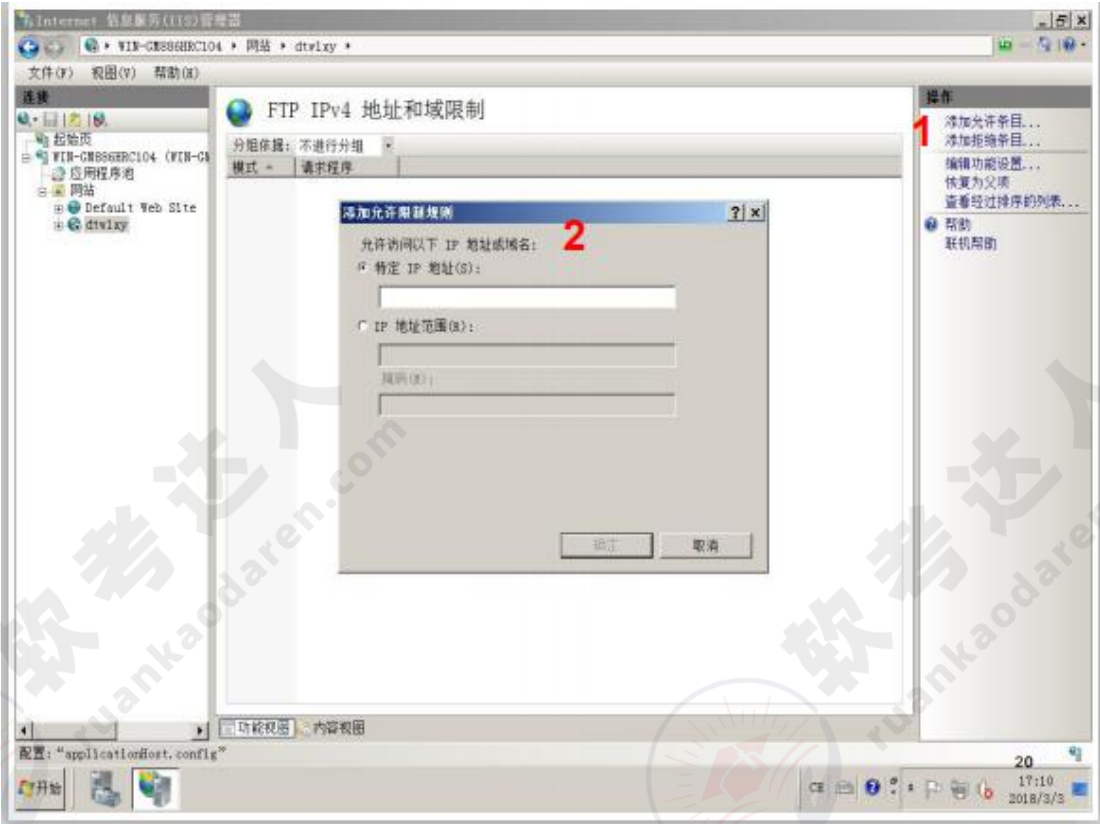
(FTP 服务器安装配置)

● 考点03：FTP服务器选项设置：

- ①添加FTP站点：开始--管理工具--IIS服务器--网站右键--添加FTP站点，下一步。
- ②设置站点名称和物理路径(主目录)
- ③绑定IP和SSL设置。
- ④配置身份验证和授权。
- ⑤配置IP地址限制。

- FTP访问：ftp://IP或域名、ftp://IP或域名:端口
- FTP软件：Server-U、FlashFXP、CuteFTP

18



● 考点04：隔离的FTP服务器安装设置：

- ①首先需要在FTP服务器中创建多个用户账户名，如datao01、datao02等，密码统一为dtwlxyvip。
- ②服务器文件格式要为NTFS，且要建一个主目录，比如文件夹C:/dtwlxy。
- ③在主目录下建一个LocalUser的子文件夹，比如：C:/dtwlxy/LocalUser。
- ④在LocalUser文件夹下在创建与账户名字一致的对应的文件夹，如果匿名，则创建Public，如C:/dtwlxy/LocalUser/datao01(或Public)。

21



- **考点05：**Apache服务器：音译为“阿帕奇”，跨平台，也是Linux下最流行的WEB服务器。
- 在RHEL系统中，Apache服务器可采用RPM和源码编译两种方式进行安装，守护进程是httpd。
- Apache服务器的主配置文件是httpd.conf，用于对Apache服务器进行功能和性能的配置管理。
- 下面是Apache服务器常用文件目录：

24

目录或文件	描述
/etc/httpd/	Apache服务器的根目录
/etc/httpd/conf/httpd.conf	Apache服务器的主配置文件
/var/www/html/	Apache服务器的文档根目录
/etc/init.d/httpd	Apache服务器启动脚本文件
/var/log/httpd/access_log	Apache服务器访问日志文件
/var/log/httpd/error_log	Apache服务器错误日志文件
*.htaccess	Apache服务器权限控制文件
/etc/init.d/httpd start	启动Apache(restart、stop)

25

● **考点06：**httpd.conf 主配置文件部分内容：

设置项	说明
ServerRoot	设置Apache服务器的根（Root）目录
ServerAdmin	设置Apache服务器管理员的E-mail地址
ServerName	设置Apache服务器的主机名
DocumentRoot	设置Apache服务器网页（文档）根目录
Listen	设置Apache服务器监听的网络端口号
DirectoryIndex	默认的索引页文件

● 注释行以“#”开始

● **考点07：**虚拟主机：在一台物理机器上提供多个WEB网站。有基于IP和基于域名的两种。

● 多种方法：多IP、多端口、多主机头。（虚拟目录【Alisa】）

● Apache服务器访问控制：*.htaccess文件

✓Allow(Deny) from all

允许(拒绝)所有主机的访问

✓Allow(Deny) from 202.96.0.97 202.96.0.98

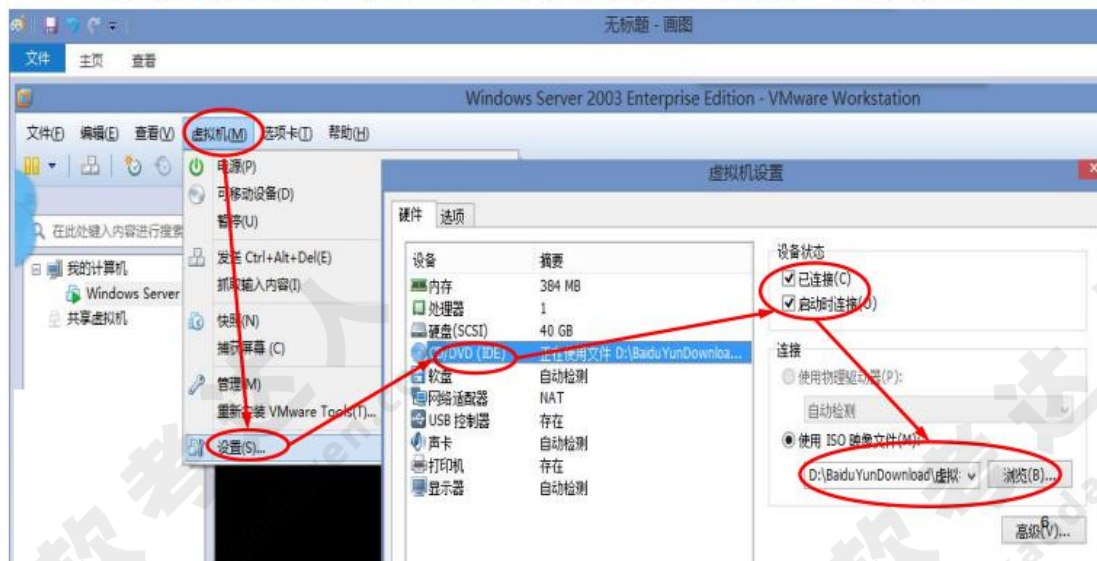
允许(拒绝)来自指定IP地址主机的访问

27

(VM10 虚拟机安装配置)

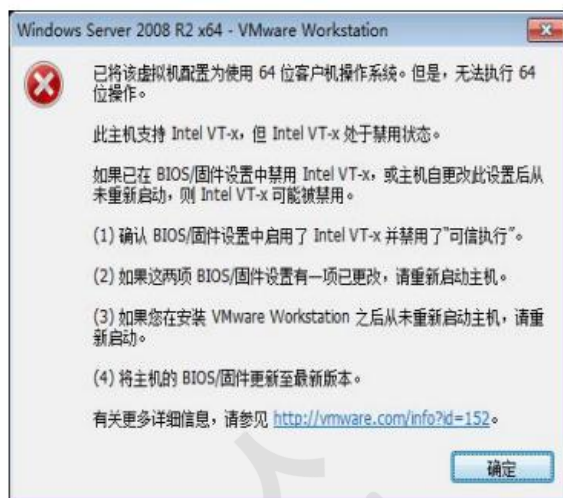
考点 8:

- 虚拟机VM简介：Virtual Machine ware，中文名“威睿”，虚拟机软件，可以使你在一台机器上同时运行二个或更多DOS、Windows、LINUX系统，每个操作系统你都可以进行虚拟的分区、配置而不影响真实硬盘的数据，比较适合学习和测试。
- 在使用上，这台虚拟机和真正的物理主机没有太大的区别，都需要分区、格式化、安装操作系统、安装应用程序和软件，总之，一切操作都跟一台真正的计算机一样。
- 虚拟机VM设置：加载光盘和光驱，安装组件。



- 虚拟机VM几个注意事项：**CPU要支持虚拟化**。
- 安装VMWare Tools工具：可以实现虚拟机和真机之间的复制粘贴。
- 虚拟机--管理-克隆：可以快速复制一个系统。
- 2008登陆密码：dtwlxy_VIP 要符合复杂度。
- VMware 10 永久许可密钥
5A6ZT-20JD2-LZWZ9-H38N0-92L62
- VMware 14 永久许可密钥
FF31K-AHZD1-H8ETZ-8WWEZ-WUUVA
- Windows Server 2008 R2只支持64位的主机。
需要主机BIOS中CPU支持64位并开启虚拟化。

7



- 电脑主机BIOS中的CPU开启虚拟化支持的方法。

1、进BIOS。开机按F2或F12或DEL等键（Fn）。

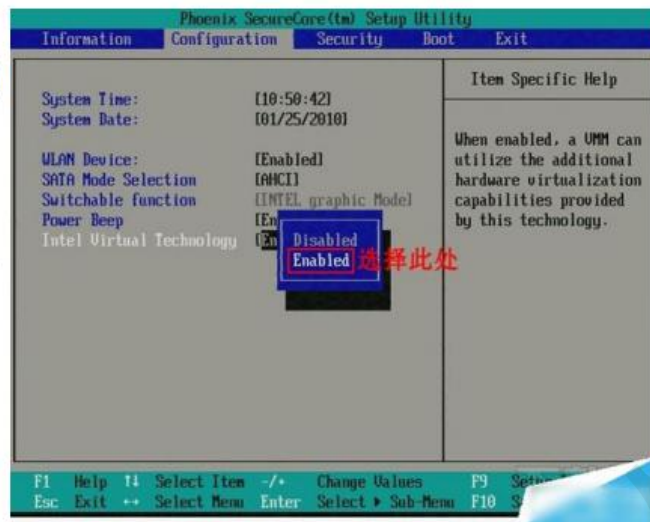
2、Configuration选项，Intel **Virtual** Technology并回车，将光标移至Enabled，然后再回车，最后按F10保存并退出。

- 如果找不到Configuration选项，尝试一下方法：

1、某些HP(惠普)电脑进入BIOS后，需要选择SystemConfiguration菜单，然后选择Device Configuration，找到**Virtualization** Technology，设置为Enabled。

2、某些Thinkpad(联想)电脑进入BIOS后，需要选择Security菜单，然后选择**Virtualization**，设置为Enabled。

3、某些DELL(戴尔)电脑进入BIOS后，需要选择Processor Settings菜单，然后选择**Virtualization** Technology，设置为Enabled。



第九章：网络操作系统与应用服务器（3）

- **考点01：** DNS协议：域名解析协议，用于把主机域名解析为对应的IP地址。是一个分布式数据库，C/S工作方式。主要基于UDP协议，少数使用TCP，端口号都是53。常用域名如下

域名名称	作用	域名名称	作用
.com	商业机构	.biz	商业
.edu	教育机构	.info	网络信息服务组织
.gov	政府部门	.pro	会计、律师和医生
.int	国际组织	.name	个人
.mil	美国军事部门	.coop	商业合作团体
.net	网络组织，现在任何人都可以注册	.aero	航空工业
.org	非盈利组织	国家代码	国家（如 cn 代表中国） ³

- **考点02：** DNS协议：DNS服务器，专门用来域名解析，采用C/S结构，域名和IP一一对应。分层式命名空间，例如：www.edu.dtwlxy.com.

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 ⁴

● 考点03：DNS协议：DNS服务器，分类二¹

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 5

- 考点04：DNS协议：解析顺序工作原理。¹
- ①查本地缓存，有两种来源：本地hosts文件和以前本机进行的DNS查询记录。
- ②查本地首选DNS服务器和备用DNS服务器。
- ③如果找不到就请求远方的DNS服务器(转发或根DNS)。
- ④根DNS指定一个顶级DNS，下一级DNS，本地DNS，返回客户端。
- ⑤转发至上一级DNS服务器，如果不能解析，找根DNS重复④。

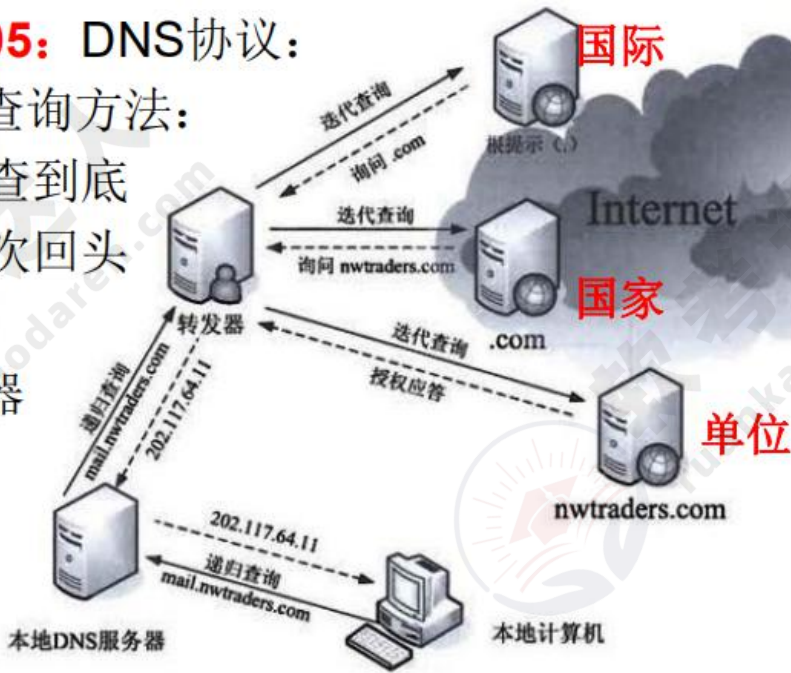
6

● **考点05：** DNS协议：

● 两种查询方法：

递归一查到底
迭代多次回头

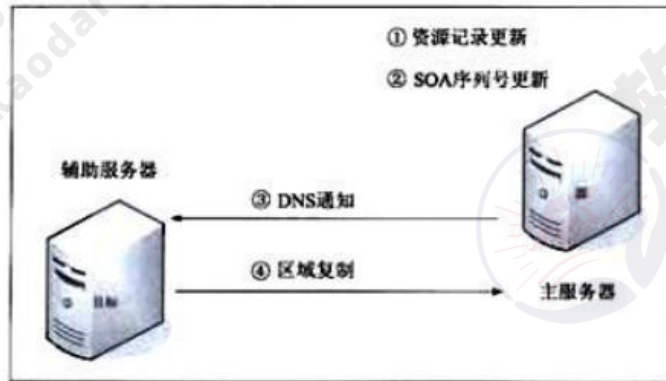
● 转发器



● **考点06：** DNS协议：区域文件由资源记录组成的文本文件，保存在主、辅服务器。类型有

记录类型	说 明	示 例
开始授权 (SOA)	指明区域主服务器 (primary nameserver) 指明区域管理员的邮件地址及区域复制信息:	区域 microsoft.com 的主服务器为 ns1.microsoft.com
地址 (A)	最常用的资源记录 把主机名解析为 IP 地址	computer1.microsoft.com 被解析为 10.1.1.4
指针 (PTR)	用于反向查询的资源记录 把 IP 地址解析为主机名	10.1.1.4 被解析为 computer1.microsoft.com
名字服务器 (NS)	为一个域指定了授权服务器 该域的所有子域也被委派给这个服务器	域 microsoft.com 的授权服务器为 ns2.microsoft.com
邮件服务器 (MX)	指明区域的 SMTP 服务器	区域 microsoft.com 的邮件服务器为 mail.microsoft.com
别名 (CNAME)	指定主机的别名 把主机名解析为另一个主机名	www.microsoft.com 的别名为 webserver12.microsoft.com

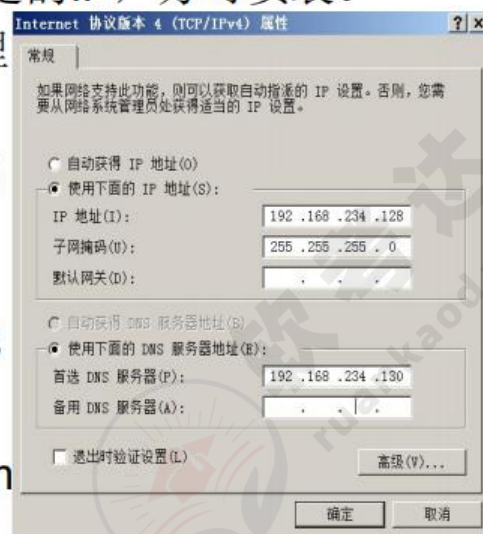
- **考点07：** DNS协议：其他考点：
- DNS查询方向：正向查询A，反向查询PTR。
- DNS区域复制：主辅：完全复制，渐增复制。
- DNS通知：推进(主→辅)、安全机制(通知)。



9

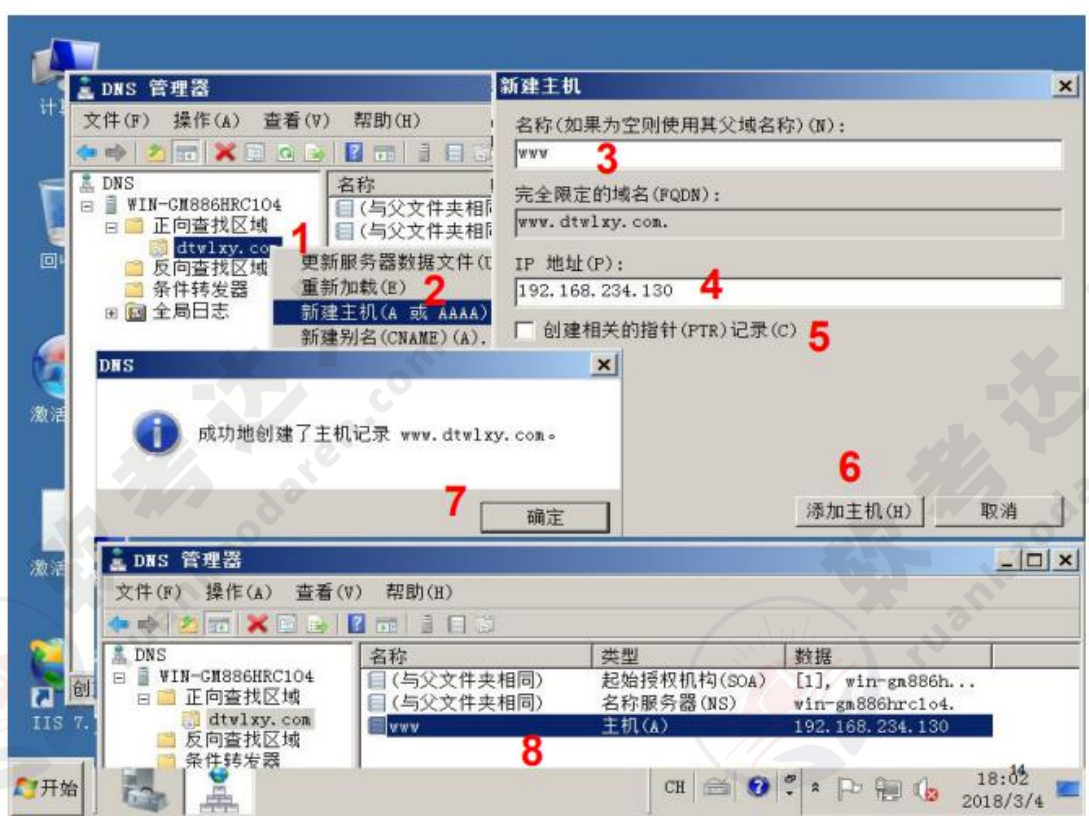
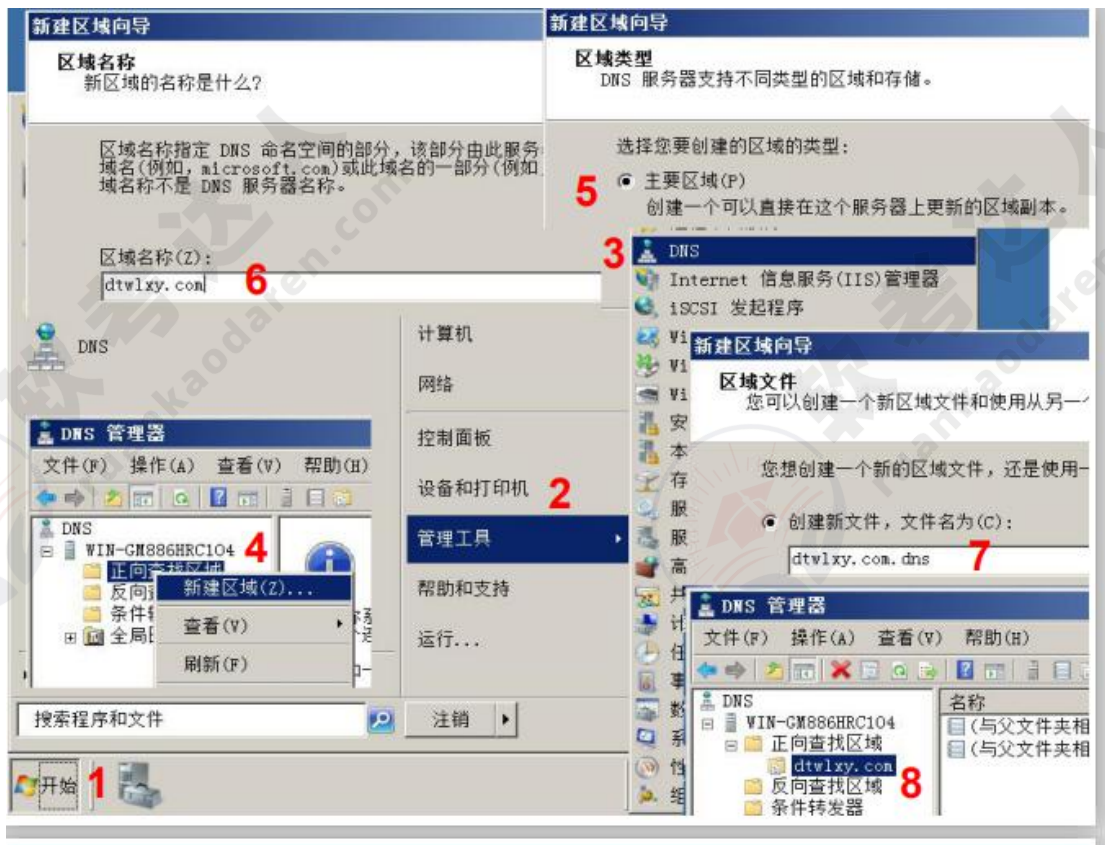
- **考点08：** DNS服务器安装：如下图：
- 首先给服务器设置一个固定的IP，方可安装。
- 服务器端安装：开始--管理工具--服务器管理--角色--添加角色--服务器角色--DNS服务器--下一步--安装完成。

- PC客户端设置：首选DNS服务器--输入DNS服务器IP。
- 访问<http://www.dtwlxy.com>





- **考点9：DNS服务器配置：**主要配置DNS解析区域，实现域名和IP的解析功能。
- 开始--管理工具--服务器管理器--角色--DNS服务器--依次展开--正向查找区域.....
- 开始--管理工具--DNS--正向查找区域--新建区域--主要区域--输入区域名称--区域文件--下一步--完成。
- 创建域名--区域名称--新建主机--名称输入www - -IP地址输入Web服务器的IP--添加主机--创建成功--完成。



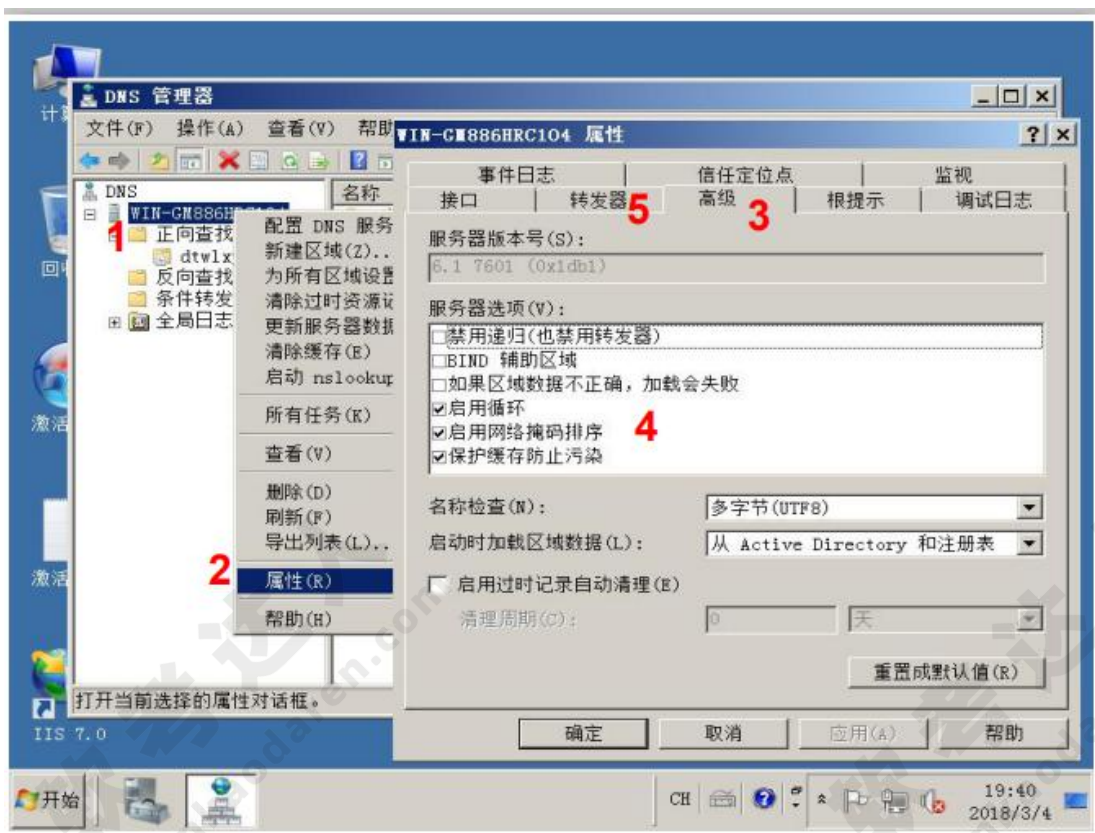
● 考点10：DNS服务器安全：

- ①转发器、高级选项卡等。
- ②禁用递归、启用循环、启用网络掩码排序、保护缓存防止污染。
- ③新建主机、新建别名等。

● Linux客户端验证DNS服务：host

Windows客户端验证DNS服务：nslookup

15



● **考点11：** Lniux DNS服务器BIND:

● 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
/etc/resolve.conf	客户端配置文件

● DNS服务启动（重启、停止）方法:

#service named start(restart、stop)

17

● **考点12：** Lniux DNS服务器BIND:

● 正向区域文件片段： 名称=>地址

	NS			192.168.100.1.
www	IN	1H	A	192.168.100.2
ftp	IN	1H	A	192.168.100.3

● 反向区域文件片段： 地址=>名称

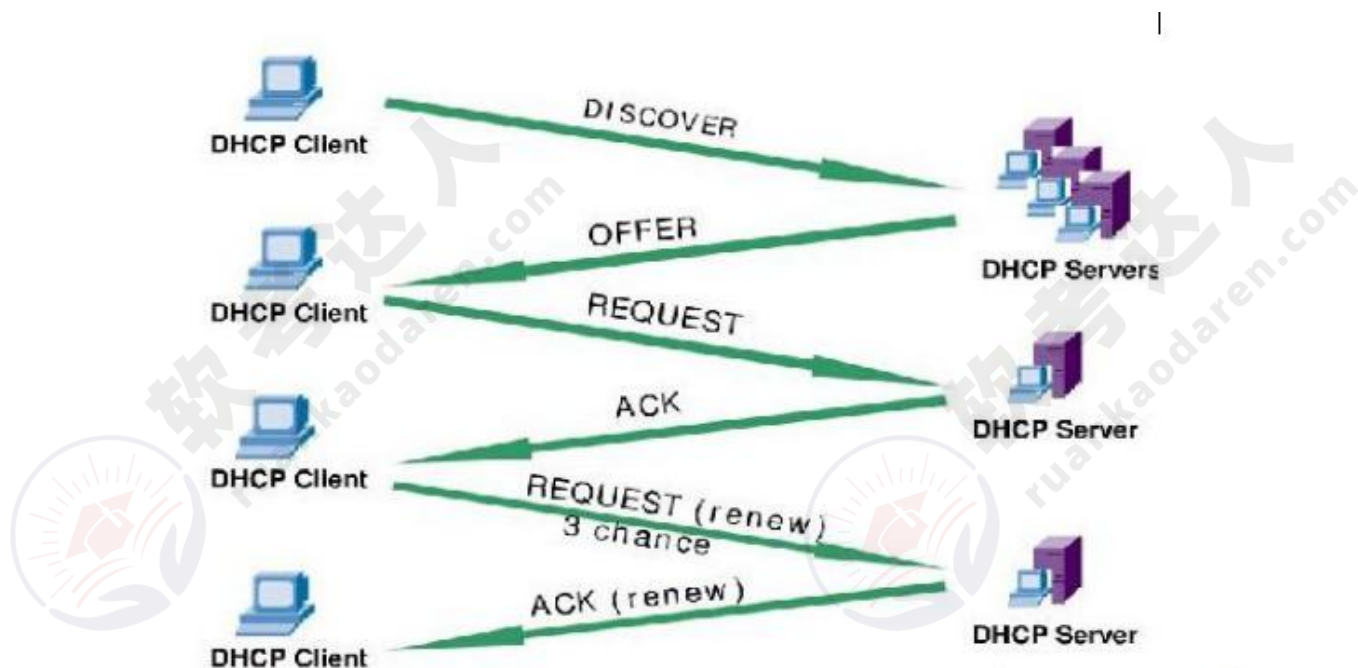
	NS	192.168.100.1.
2	PTR	www.wl.com.
3	PTR	ftp.wl.com.

- **考点13：** DHCP协议：动态主机配置协议，可以自动为局域网内的主机分配一个IP地址。
- DHCP的好处：①管理员可以迅速地验证IP地址和其他配置参数，而不用去检查每个主机。②DHCP不会从一个范围里同时租借相同的IP地址给两台主机。③可以为每个DHCP范围（或者说所有的范围）设置若干选项（例如默认网关、DNS和WINS服务器的地址）。④如果主机物理上被移动到了不同的子网上，该子网上的DHCP服务器将会自动用配置该主机。

20

- **考点14：** DHCP协议工作原理和过程：
- (1)当DHCP客户端首次启动时，客户端向DHCP服务器发送一个Dhcpdiscover数据包，该数据包表达了客户端的IP租用请求。0.0.0.0
255.255.255.255 0-4次
- (2)当DHCP服务器接收到Dhcpdiscover数据包后，该服务器从地址范围中向那台主机提供(dhcpoffer) 一个还没有被分配的有效的IP地址。当你的网络中包含不止一个DHCP服务器时，主机可能收到好几个dhcpoffer，在大多数情况下，主机或客户端接受收到的第一个dhcpoffer。

21

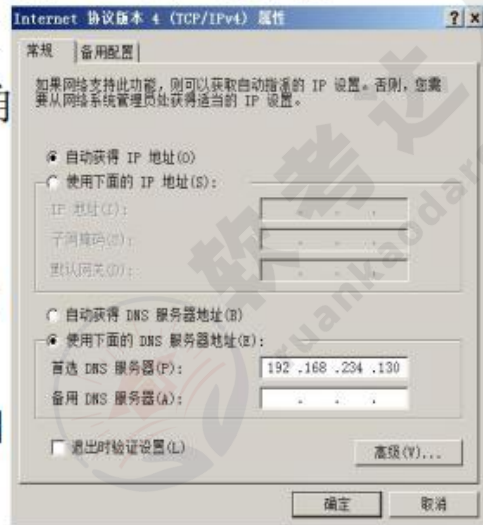


22

- (3)该DHCP服务器向客户端发送一个确认 (dhcpack). 该确认里面已经包括了最初发送的IP地址和该地址的一个稳定期间的租约（默认情况是8天）。服Dhcpnack，客DhcpDecline
- (4)当租约期过了一半时（50%即是4天），客户端将和设置它的TCP/IP配置的DHCP服务器更新租约。当租期过了87.5%时，如果客户端仍然无法与当初的DHCP服务器联系上，它将与其它DHCP服务器通信，如果还没有任何DHCP服务器，该客户端必须停止使用该IP。
电脑重启发送 DhcpRequest

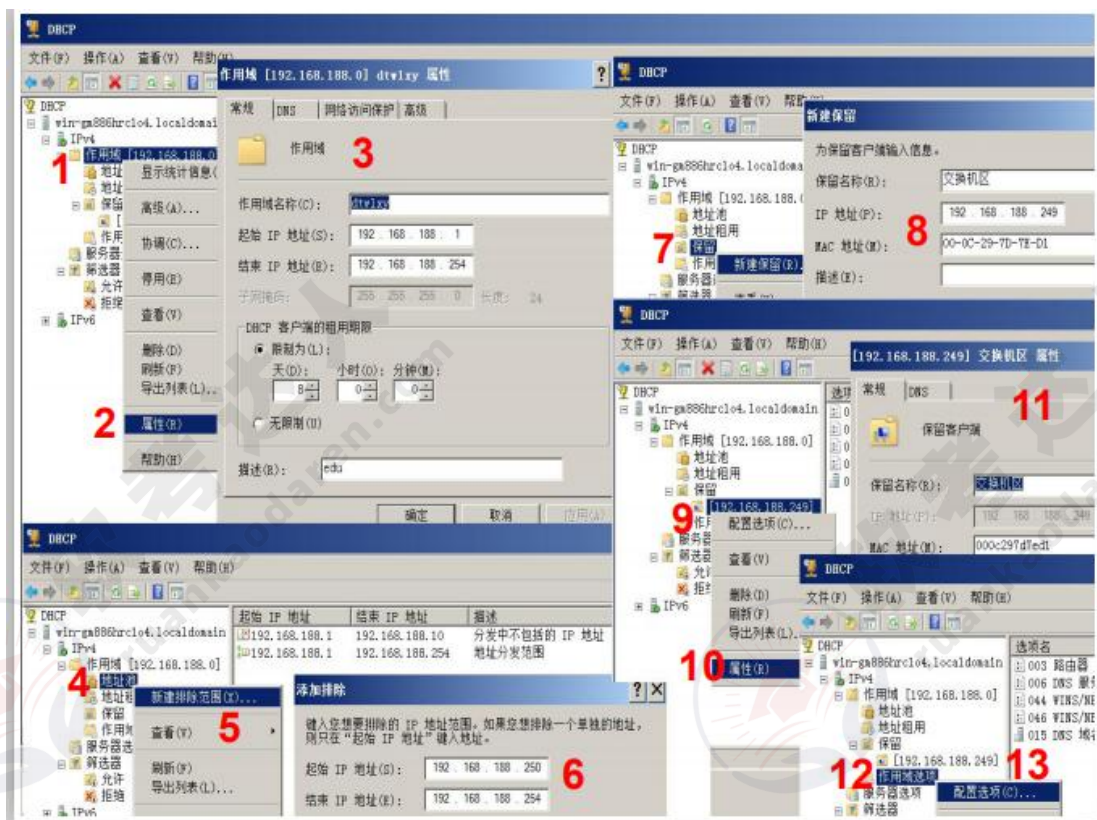
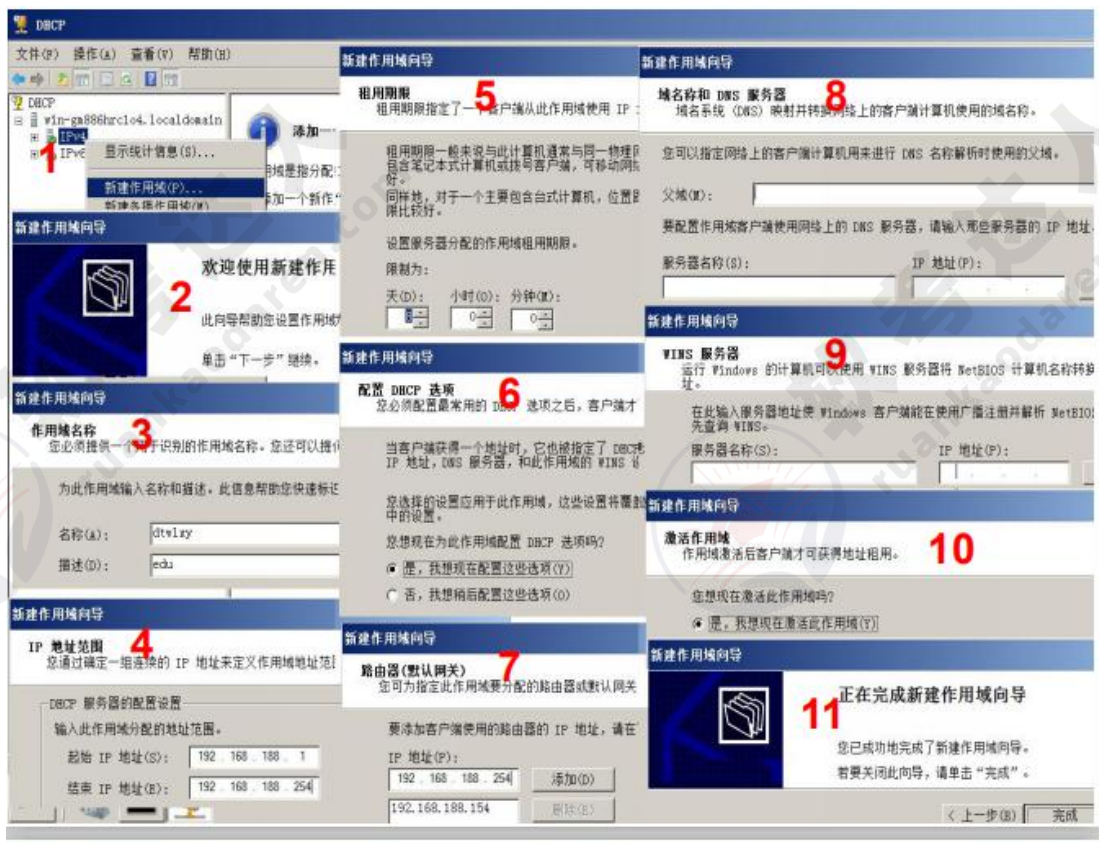
23

- **考点15：DHCP服务器安装设置：**如下图
- 首先给服务器设置一个固定的IP，方可安装。
- 服务器安装：开始--管理工具--角色--添加角色--服务器角色--DHCP服务器--完成。
- 客户端设置：网络连接--自动获得IP地址
- 打开：开始--管理工具--DHCP--DHCP控制台。





- **考点16：**创建DHCP作用域：开始--管理工具--DHCP--DHCP控制台--IPV4--新建作用域--名称和描述--IP地址范围--添加排除--租约--是--下一步--是--完成。
- 作用域：常规等选项卡。
- 作用域选项：配置选项（DNS、网关等）
- 地址池：新建排除范围（分发中不包括）
- 保留：新建保留（分发但会绑定）
- 服务器：备份、还原
- 筛选器：指定接受的DHCP



- **考点17：**Linux DHCP服务器配置：
- DHCP服务主配置文件路径：/etc/dhcpd.conf。
- DHCP服务启动（重启、停止）
service dhcpd start (restart 、 stop)
- DHCP主配置文件片段：
subnet 192.168.100.0 netmask 255.255.255.0 {
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;

range ... 192.168.100.100 192.168.100.250;
default-lease-time 21600; 默认租约时间
max-lease-time 43200; 最大租约时间

- 客户端验证DHCP服务的功能：
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

考点18：实现MAC-IP地址的绑定：

```
host ns { hardware ethernet 0:50:56:C0:00:01;  
fixed-address 192.168.100.100; }
```

	选 项	解 释
1	subnet-mask	为客户端设定子网掩码
2	domain-name	为客户端指明 DNS 名字
3	domain-name-servers	为客户端指明 DNS 服务器的 IP 地址
4	host-name	为客户端指定主机的名称
5	routers	为客户端设定默认网关
6	broadcast-address	为客户端设定广播地址
	ntp-server	为客户端设定网络时间服务器 IP 地址
	time-offset	为客户端设定和格林威治时间的偏移时间，单位是秒

32

考点19： none： 不支持DNS动态更新
interim： DNS互动更新模式
ad-hoc： 特殊DNS更新模式

	参 数	参 数 含 义
1	ddns-update-style	配置 DHCP-DNS 更新模式。更新模式包括 none、interim 和 ad-hoc
2	default-lease-time	指定默认的 IP 地址租赁时间，单位是秒
3	max-lease-time	指定最大租赁时间长度，单位是秒
4	hardware	指定网卡接口类型和 MAC 地址
5	server-name	DHCP 服务器名称
6	subnet	描述一个 IP 地址是否属于该子网
7	range	提供动态分配 IP 的范围
8	host	用于定义保留主机

33

第九章：网络操作系统与应用服务器（4）

- **考点01：** Samba服务器： Samba是Linux上实现和Windows系统局域网上共享文件和打印机的一种通信协议，由服务器及客户端程序构成。支持SMB/CIFS协议，实现共享资源。
- 最主要的一个配置文件smb.conf，可以使用vi编辑器修改。守护进程： smbd。启动samba服务service smb start（restart、stop）。启动脚本/etc/rc.d/init.d/smb start（restart）。

3

- **考点02：**配置文件smb.conf三个主要部分：全局设置global、共享目录设置homes、共享打印机设置printers。

- [global] 全局文件设置

```
workgroup = hackase           //设置工
netbios name = wsljhost      //设置网上邻居显示名
server string = bzserver     //服务器名备注信息
; hosts allow = 192.168.1. 192.168.2. 127.
//限制可访问此服务的IP范围,默认是全部允许的
```

```
interfaces = 192.168.12.2/24 192.168.13.2/24
```

//监听某个IP或网段，多网段要在这里列出;

```
log file = /var/log/samba/m.log
```

//为登录服务器用户建立不同日志文件.

```
max log size = 0
```

//日志文件的大小，"0"代表无限制，单位KB。

```
security = share             //安全性级别共四种
```

(share无需用户名密码、user需用户名密码、server其他服务器验证、domain域服务器验证)

- **考点03：**配置文件smb.conf三个主要部分：全局设置global、共享目录设置homes、共享打印机设置printers。

- [homes] 共享目录设置

comment = zhushi	//对共享注释说明
browseable = no	//设定目录是否浏览
writable = yes	//用户是否写入权限
path = /home/share	//共享目录路径
guest ok = yes	//是否允许guest账户

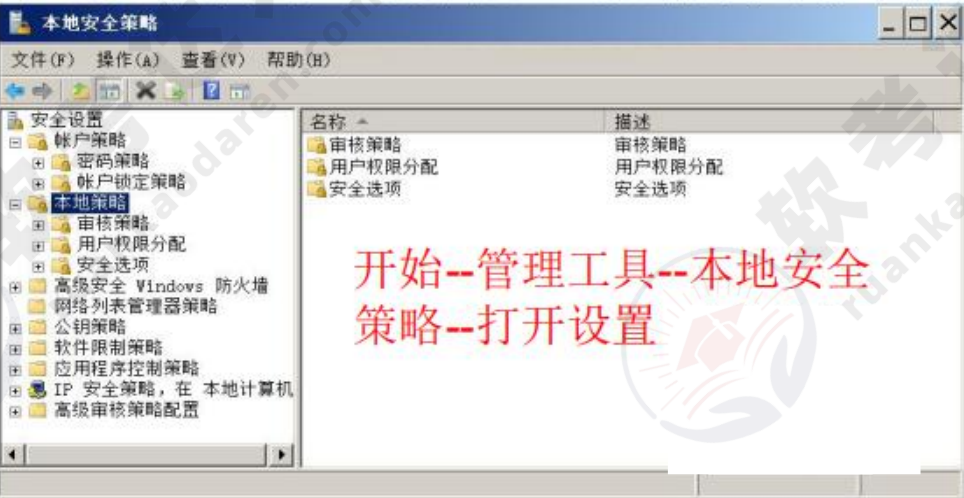
6

- **考点04：**配置文件smb.conf三个主要部分：全局设置global、共享目录设置homes、共享打印机设置printers。

- [printers] 共享打印机设置

path = /var/spool/samba	//打印目录位置
browseable = no	//设定目录是否浏览
writable = no	//必须设为no
guest ok = yes	//是否允许guest账户

- **考点05：**安全策略的概念：实现定义好的一系列应用计算机的行为准则。保护网络上的数据资源。本地策略用于单个计算机，组策略用于域范围内。



- **考点06：**账户策略配置：(1)密码策略。开始--管理工具--本地安全策略--账户策略--密码策略。
- 密码复杂度：至少6位，不含用户名或连续2个字符。符合下面4选3。大写、小写、数字、字符。



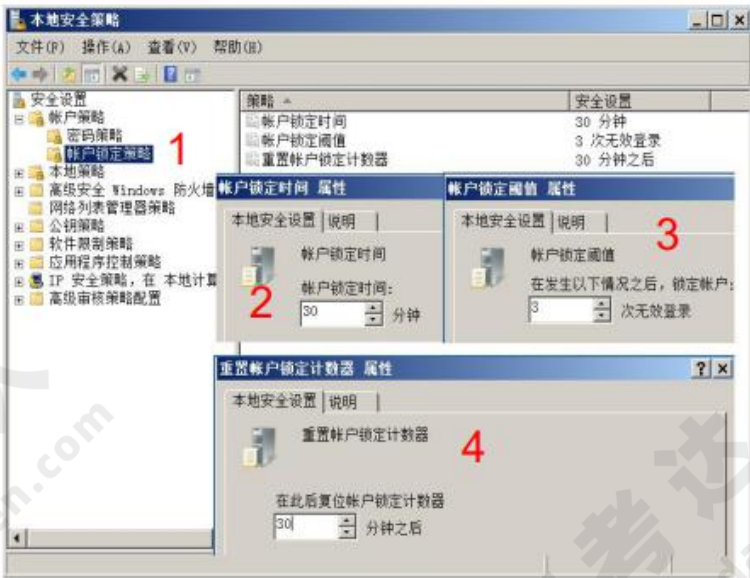
- 密码长度最小值：1-14位，0空密码。
- 密码最长使用期限：1-999天，0永不过期。
- 密码最短使用期限：1-998天，0立即更改。
- 强制密码历史：0-24。
- 加密存储密码。



(2)账户锁定策略。账户锁定时间：0永远锁定，直到管理员解锁。

账户锁定阈值：
在1-999之间，
0永不锁定。

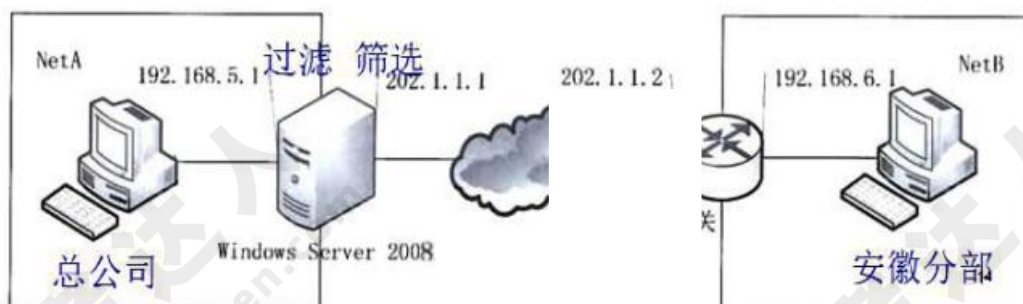
重置账户锁定
计数器：小于
等于账户锁定
时间。

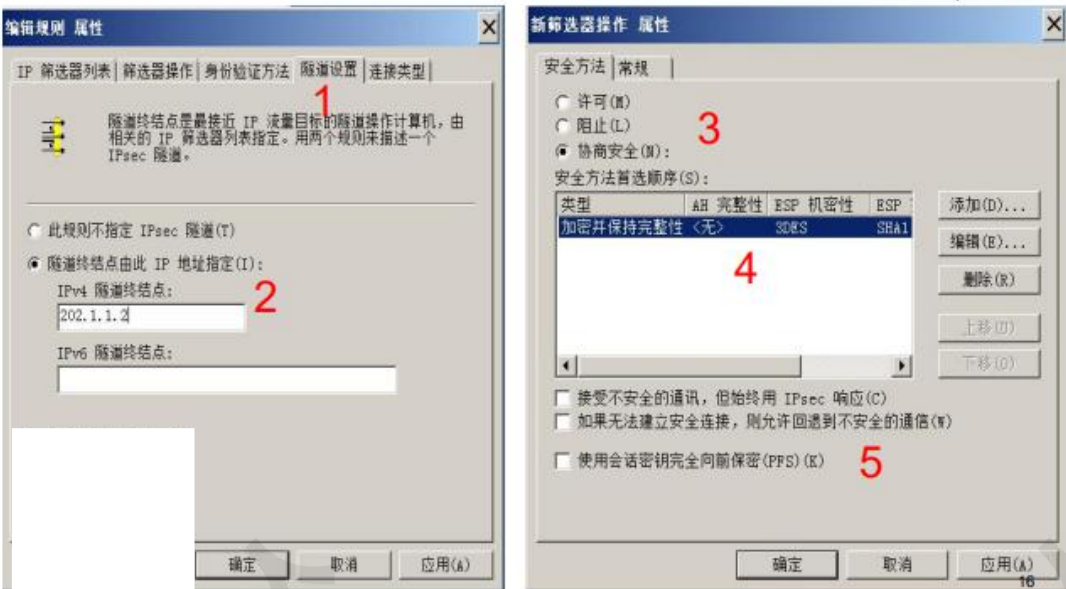
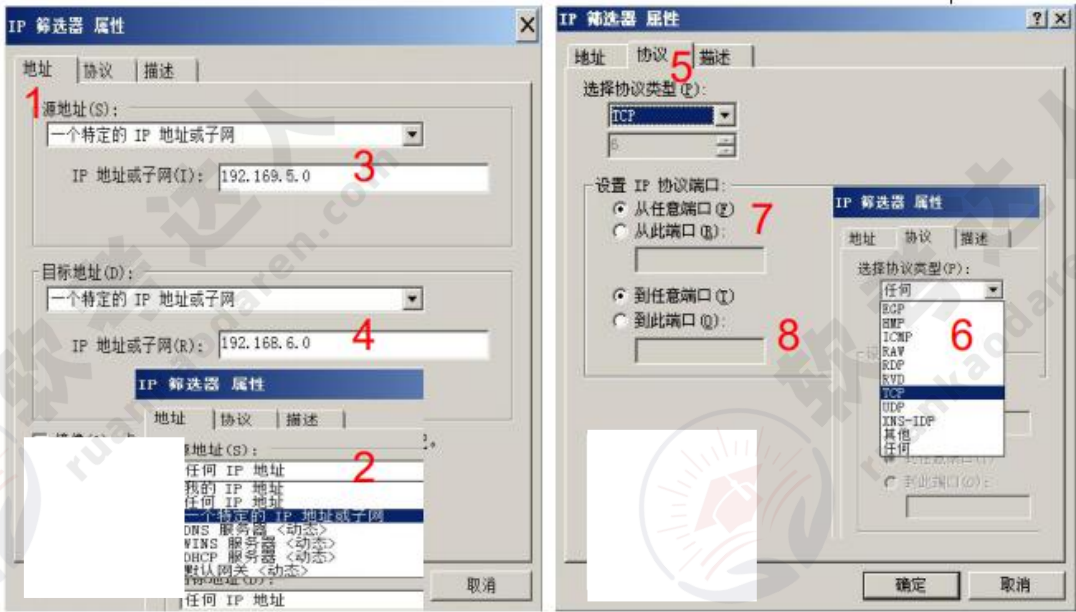


● **考点07：**组策略配置：开始-运行--gpedit.msc



- **考点08：**IPSec策略设置：用于两个网络NetA和NetB之间建立安全的通信传输。通过设置筛选器实现对进入外出的数据包进行IP、端口、协议方面的过滤控制。①创建IPSec策略。②创建筛选器列表。③配置隧道规则。④指派。



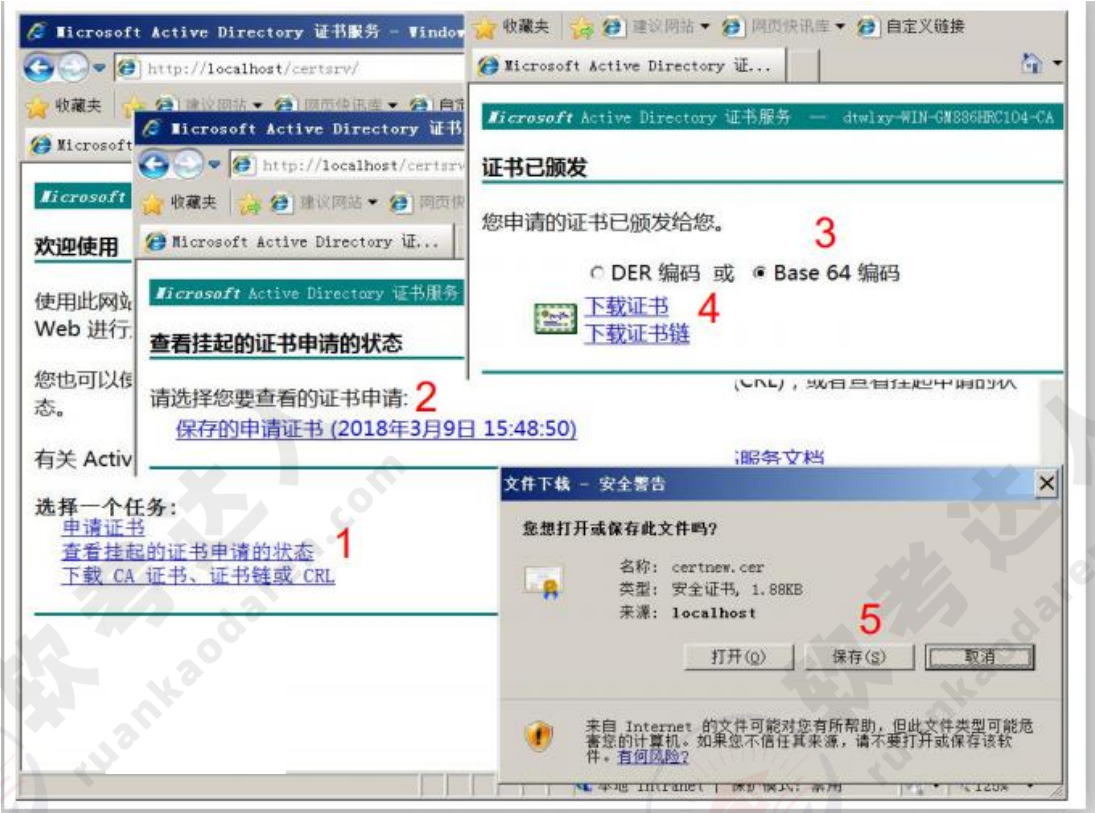
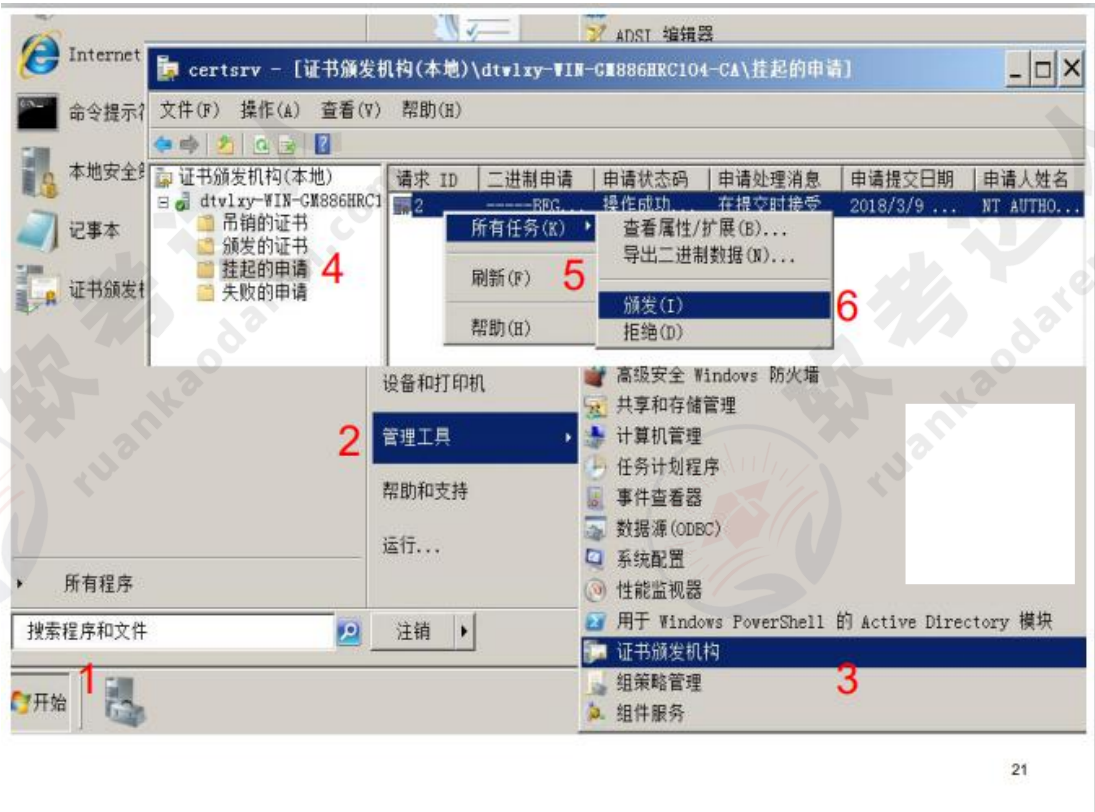


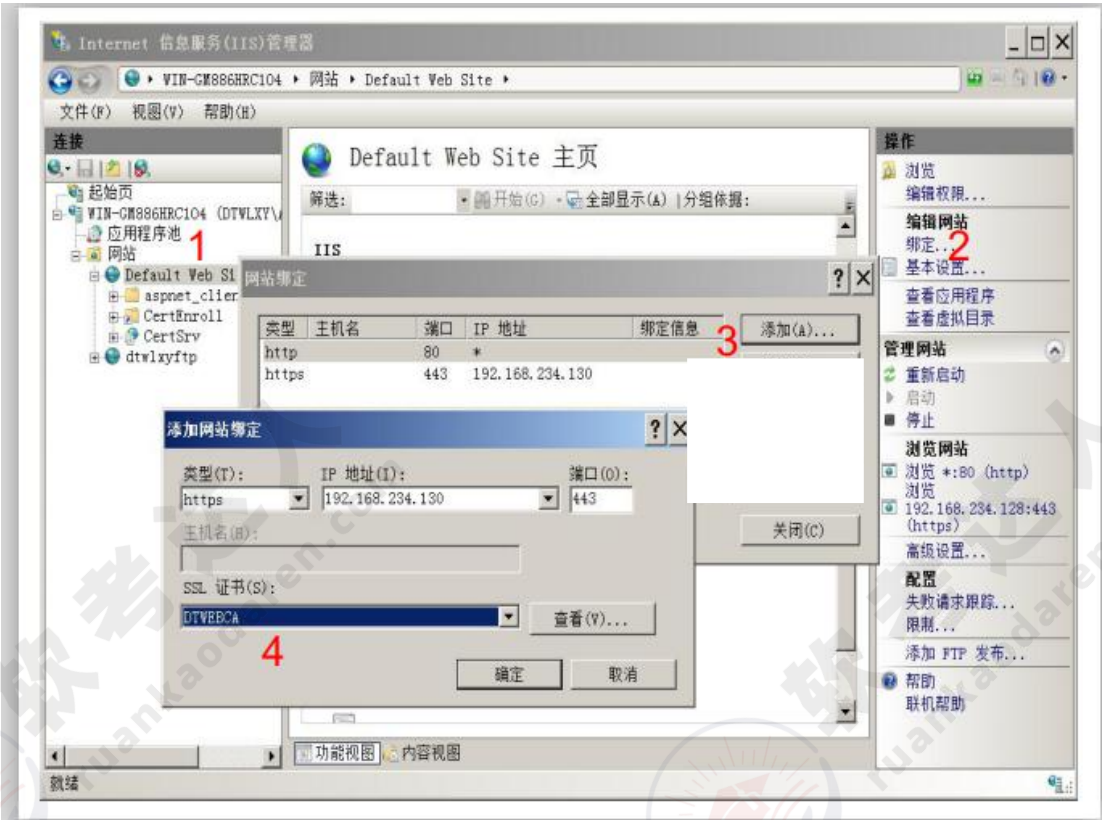
- **考点09：安全Web站点配置：HTTPS在HTTP的基础上加入了SSL协议，即数字证书验证。**
- 一、安装证书服务。开始--管理工具--服务器管理器--角色--添加角色--AD证书服务--证书颁发机构--独立--根--新建私钥--直到完成安装。
- 二、配置CA证书。①创建申请文件。②申请证书。③颁发证书。④下载证书。⑤保存证书。
- 三、配置HTTPS。①绑定CA证书。②启用SSL。③实现安全访问。

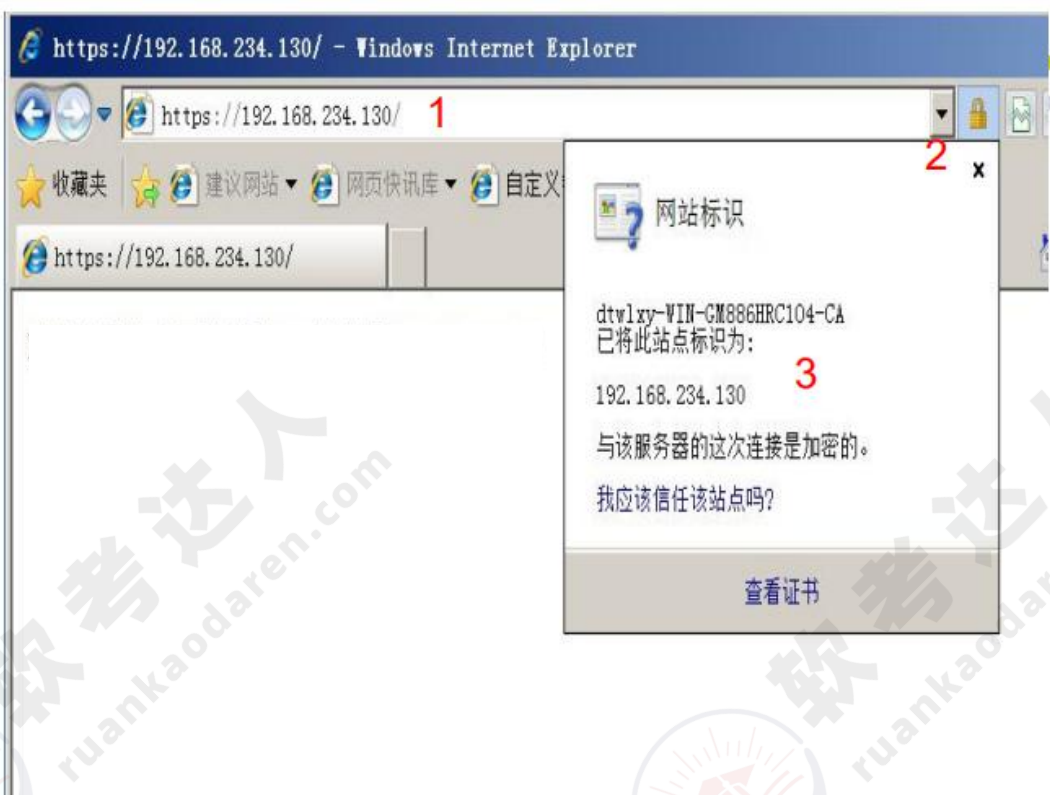
17











- **考点08：**华为模拟器：**eNSP**。是网络工程师经常使用的网络实验模拟软件，它可以很快捷的模拟网络中的各种设备(交换机、路由器、台式电脑、笔记本电脑、服务器、网络云)，搭建各种网络环境，模拟网络拓扑结构等。



第十章：组网技术（1）

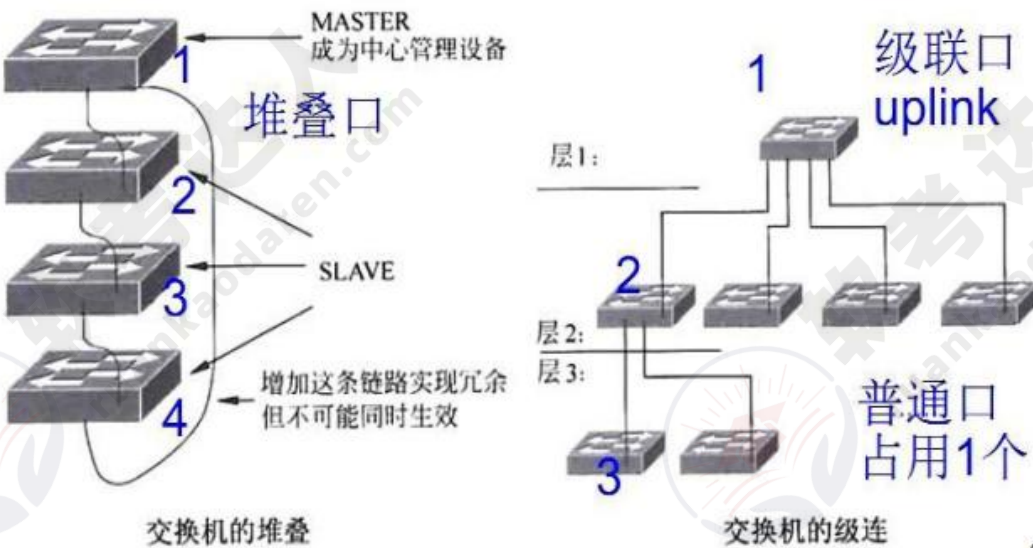
- **考点01：**交换机简介和分类：交换机（Switch）意为“开关”是一种用于电（光）信号转发的网络设备。它可以为接入交换机的任意两个网络节点提供独享的电信号通路。工作于第2层或3层。最常见的交换机是以太网交换机。下图是思科的Huawei S2700系列以太网交换机。



- **考点02：**交换机分类：有多种分类方法如下

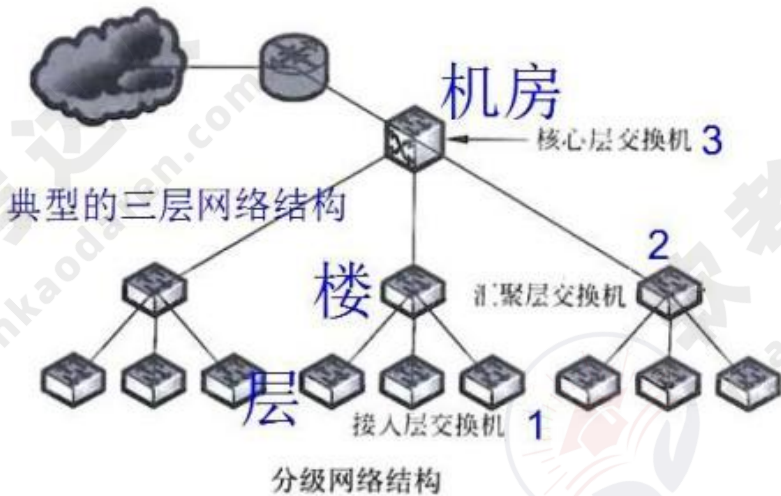
划分方式	交换分类	特点
交换方式	存储转发	存储、校验、延时大
	直通式	直接、不校验、速度快
	碎片过滤	64字节，小的丢弃
协议层次	二层交换	MAC地址交换
	三层交换	IP地址交换
	多层交换	端口号、协议交换
交换结构	固定式	固定数量端口，如24口
	模块式	预留插槽、插入模块扩展
配置方式	堆叠式	堆叠口、4到9层、统一
	非堆叠	级联、不超4层
管理类型	网管型	支持SNMP和MIB网管协议
	非网管	傻瓜交换机、无需配置
	智能型	支持WEB配置和SNMP、MIB
适用范围	接入层	用户接入，多端口
	汇聚层	策略控制ACL、VLAN、Qos
	核心层	高速转发、冗余、均衡

● **考点03：**交换机堆叠和级联：形如并联，串联



6

● **考点04：**交换机典型三级：①接入层交换机，如S2700。②汇聚层交换机，S3700。③核心层交换机，如S5700。



7

- **考点05：**交换机性能参数和计算公式：
 - 包转发率：端口吞吐率，64字节数据包转发能力，单位pps（包/秒）。计算公式如下：
包转发率=千兆端口数×1.488Mpps+百兆端口数×0.1488Mpps+其余端口×相应包转发pps
 - 背板带宽：端口处理器和数据总线之间单位时间内传输的最大数据量。单位Gbps（吉比特/秒）。计算公式如下：
总带宽=端口数×端口速率×2（全双工）

8

- **考点06：**路由器简介和分类：路由器（Router）用来连接不同的局域网，路由器可以学习和传播各种路由信息，并根据这些路由信息将网络中的分组转发到正确的网络中。路由器工作在第3层网络层，具有局域网和广域网两种接口。通过路由表为进入路由器的数据分组选择最佳的路径，并将分组传输到适当的端口。



9

考点07：路由器根据功能、性能、应用分为：

①骨干路由器：主干网络互连，模块化、热备份、双电源等冗余技术。如国家级、省级骨干网互连。如NE40E以上系列。

②企业级路由器：用于一个企业出入口，提供多种功能，完成企业组网。可实现数据、语音、视频等应用。如AR3600系列。

③接入级路由器：边缘路由器，小型企业，或者部门组网。如AR2200系列。

● **考点08：**路由器上的一些常见端口：

①Serial端口：高速同步串口，与广域网连接，可连接DDN、帧中继、X.25、PSTN等网络。

②Console端口：初次配置控制台端口，利用终端仿真程序，如超级终端、SecureCRT对路由器进行本地配置。

③RJ-45端口：以太网口，通过双绞线连接局域网，有的标识ETH，有的标识为10/100 b TX。

④AUX端口：远程配置路由器，连接Modem。

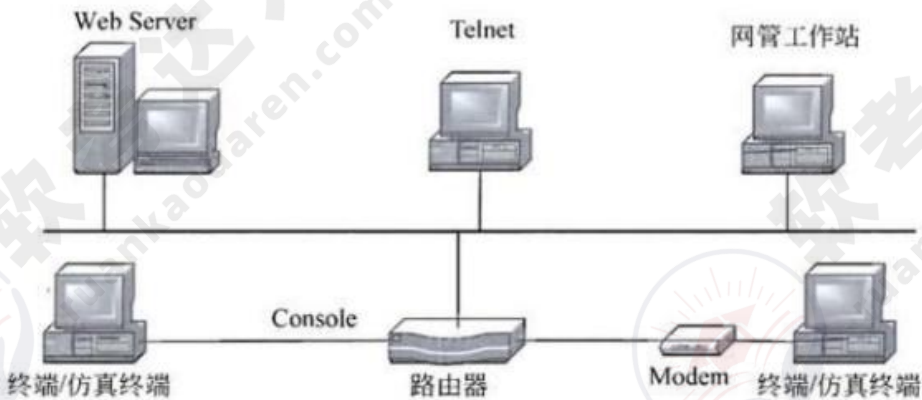
- **考点09：**交换路由的操作系统VRP：是华为公司为其网络设备开发的操作维护系统。用户通过运行命令行CLI，对网络设备进行功能设置。

- VRP有3种命令模式：



- 用华为eNSP模拟器。

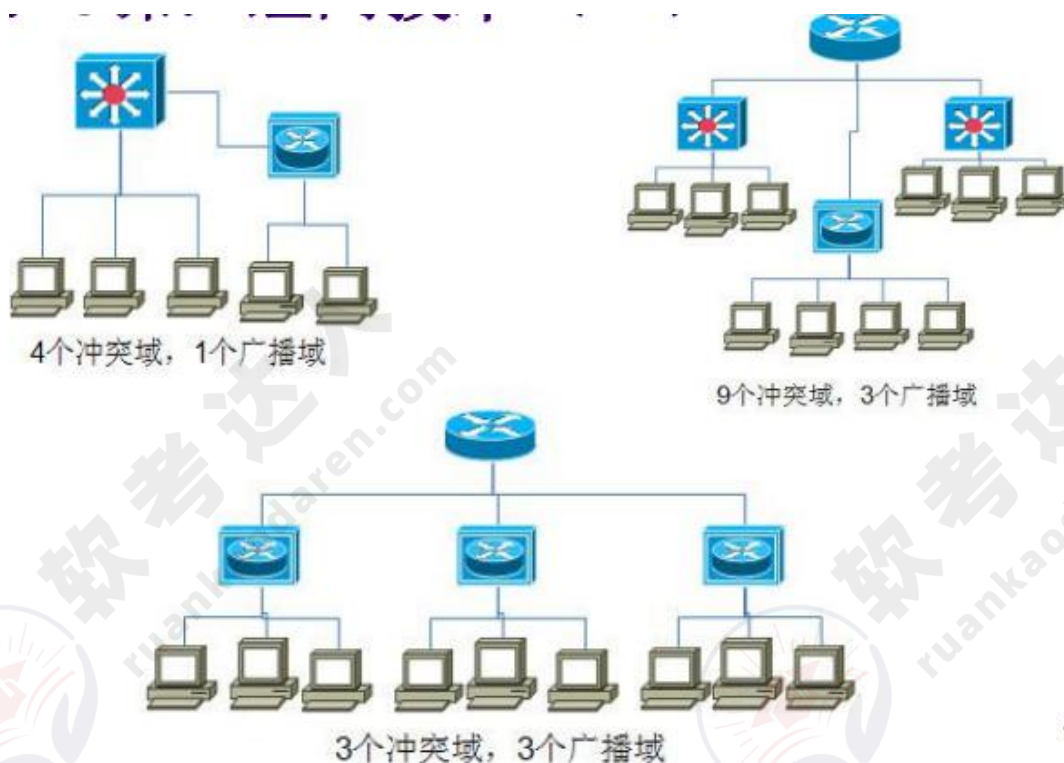
- **考点10：**访问交换机和路由器的几种方法：
 - ①Console口，初次配置。
 - ②AUX口远程拨号。
 - ③Telnet带外远程。
 - ④Web浏览器输入IP。
 - ⑤网管软件。



13

- **考点11：**交换和路由中的广播域和冲突域：
- 冲突域：在同一个冲突域中的每一个节点都能收到所有被发送的帧。简单的说就是同一时间内只能有一台设备发送信息的范围。**交换机能分隔冲突域。一个端口一个冲突域。**
- 广播域：网络中能接收任一设备发出的广播帧的所有设备的集合。简单的说如果站点发出一个广播信号，所有能接收收到这个信号的设备范围称为一个广播域。**路由器能分隔广播域。一个端口一个广播域。**

14



15

● **考点12：**交换机基本配置实验：S5700为例。



● 开始--程序--附件--通信--超级终端--回车
交换机 Console 端口的默认参数如下。

- 端口速率：9 600bps。
- 数据位：8。
- 奇偶校验：无。
- 停止位：1。
- 流控：无。

关闭域名解析：
undo info-center enable

17

● **考点13：**配置交换机名称、管理VLAN、IP地址

```
<HUAWEI> //用户视图提示符
<HUAWEI>system-view //进入系统视图
[HUAWEI]sysname Switch1 //修改设备名称为 SW1
[Switch1] vlan 5 //创建交换机管理 VLAN 5
[Switch1-VLAN5] management-vlan
[Switch1-VLAN5] quit
[Switch1] interface vlanif 5 //创建交换机管理 VLANIF
[Switch1-vlanif5] ip address 10.10.1.1 24 //配置 VLANIF 接口 IP 地址
[Switch1-vlanif5] quit
```

18

● 考点14：配置交换机的远程登陆管理Telnet:

```
[Switch1] telnet server enable           //Telnet 默认是关闭的，需要打开
[Switch1] user-interface vty 0 4        //开启 VTY 线路模式
[Switch1-ui-vty0-4] protocol inbound telnet //配置 telnet 协议
[Switch1-ui-vty0-4] authentication-mode aaa //配置认证方式
[Switch1-ui-vty0-4] quit
[Switch1] aaa                            simple 明文密码
[Switch1-aaa] local-user admin password cipher Hello@123
//配置用户名和密码，用户名不区分大小写，密码区分大小写
[Switch1-aaa] local-user admin privilege level 15 //将管理员的账号权限设置为 15
[Switch1-aaa]quit
[Switch1]quit
< Switch1>save                          //在用户视图下保存配置
```

19

- 登陆Telnet到交换机，出现如下视图提示，¹需要注意的是，输入密码的时候是不显示的。

```
C:\Documents and Settings\Administrator> telnet 10.10.1.1
```

//输入交换机管理 IP

```
Login authentication
```

```
Username:admin
```

//输入用户名和密码

```
Password:
```

```
Info: The max number of VTY users is 5, and the number
of current VTY users on line is 1.
```

```
The current login time is 2016-07-03 13:33:18+00:00.
```

```
< Switch1>
```

//用户视图命令行提示符

20

● **考点15：**配置交换机端口隔离、速率、双工等。

#配置接口 GE1/0/1 和 GE1/0/2 的端口隔离功能，实现两个接口之间的

< Switch1> system-view 二层数据隔离，三层数据互通

[Switch1] port-isolate mode l2

[Switch1] interface gigabitethernet 1/0/1

[Switch1-GigabitEthernet1/0/1] port-isolate enable group 1

[Switch1-GigabitEthernet1/0/1] quit

[Switch1] interface gigabitethernet 1/0/2

[Switch1-GigabitEthernet1/0/2] port-isolate enable group 1

[Switch1-GigabitEthernet1/0/2] quit

21

#配置以太网接口 GE0/0/1 在自协商模式下协商速率为 100Mb/s

< Switch1> system-view

[Switch1] interface gigabitethernet 0/0/1

[Switch1-GigabitEthernet0/0/1] negotiation auto

[Switch1-GigabitEthernet0/0/1] auto speed 100

#配置以太网电接口 GE0/0/1 在自协商模式下双工模式为全双工模式

< Switch1> system-view

[Switch1] interface gigabitethernet 0/0/1

[Switch1-GigabitEthernet0/0/1] negotiation auto

2

● **考点16：**查看交换机MAC、VLAN下MAC绑定

#执行命令 display mac-address，查看所有的 MAC 地址表项

< Switch1> display mac-address

MAC Address	VLAN/VSI	Learned-From	Type
00e0-0900-7890	10/-	-	blackhole
00e0-0230-1234	20/-	GE1/0/1	static
0001-0002-0003	30/-	Eth-Trunk1	dynamic

Total items displayed = 3

#在 MAC 地址表中增加静态 MAC 地址表项，目的 MAC 地址为 0001-0002-0003，VLAN 5 的报文从接口 gigabitethernet0/0/5 转发出去

[Switch1] mac-address static 0001-0002-0003 gigabitethernet 0/0/5 vlan 5

23

#执行命令 display interface vlanif 5，显示 VLANIF 接口的 MAC 地址

< Switch1> display interface vlanif 5

Vlanif5 current state : DOWN

Line protocol current state : DOWN

Description:

Route Port,The Maximum Transmit Unit is 1500

Internet Address is 192.168.1.1/24

IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 00e0-0987-7891

Current system time: 2016-07-03 13:33:09+08:00

Input bandwidth utilization : --

Output bandwidth utilization : --

关闭域名解析：

undo info-center enable

24

● **考点17：** 路由器基本配置实验： AR3260为例。

#设置系统的日期、时间和时区

<Huawei> clock timezone BJ add 08:00:00

<Huawei> clock datetime 20:10:00 2015-03-26

#设置设备名称和管理 IP 地址

<Huawei> system-view

[Huawei] sysname Server

[Server] interface gigabitethernet 0/0/0

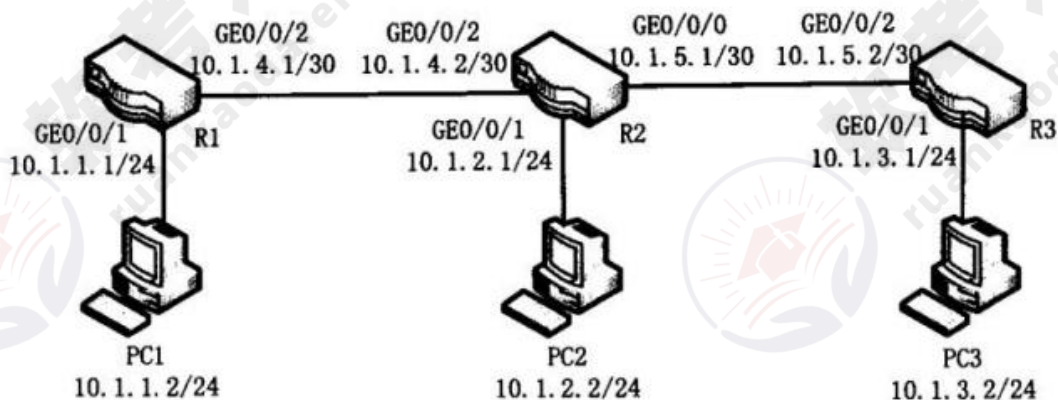
[Server-GigabitEthernet0/0/0] ip address 10.137.217.177 24

[Server-GigabitEthernet0/0/0] quit



26

- **考点18：** 路由器静态路由实验：实现R1、R2、R3三者之间互相ping通。第一步：首先配置各接口IP地址。第二步：配置静态路由命令。第三步：再ping验证或display ip routing。



- 在三台路由器上都执行如下接口、静态命令：

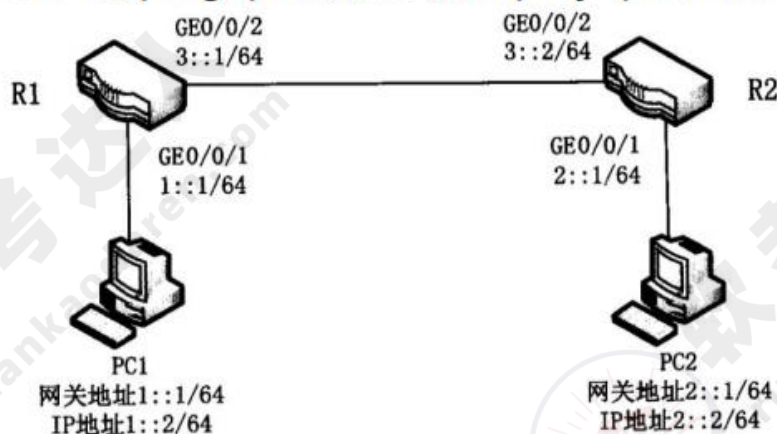
```
interface GigabitEthernet0/0/1 // 配置接口IP地址
ip address 10.1.1.1 255.255.255.0
interface GigabitEthernet0/0/2
ip address 10.1.4.1 255.255.255.252
ip route-static 10.1.2.0 255.255.255.0 10.1.4.2 //配置的静态路由
ip route-static 10.1.3.0 255.255.255.0 10.1.4.2
return
```

此处以R1为例

- 在路由器上执行命令display ip routing-table查看路由表。在PC上ping其它，可以通信。

28

- 考点19：**路由器静态路由IPV6实验：实现R1、R2；PC1、PC2之间互相ping通。第一步：首先配置各接口IP地址。第二步：配置静态路由命令。第三步：再ping ipv6验证或display ipv6 routing。



29

- 在2台路由器上都执行如下接口、静态命令：

ipv6 //启用路由器 IPv6 报文转发能力

interface GigabitEthernet0/0/1

ipv6 enable

//在接口上启用 IPv6 功能

ipv6 address 1::1 64

interface GigabitEthernet0/0/2

此处以R1为例

ipv6 enable

ipv6 address 3::1 64

ipv6 route-static 2:: 64 3::2

//配置 R1 到 2::64 网段的静态路由

return

- 在路由器上执行命令display ipv6 routing-table查看路由表。在PC上使用ping，可以通信。

30

第十章：组网技术（2）

- **考点01：** 交换机GVRP：VLAN注册协议，在VLAN增加、删除、调整时，自动发广播，保持全网所有的交换机VLAN信息是一致的。
- GVRP把交换机分为3种注册模式：
 - ①Normal模式：VLAN增删改，广播保持一致。
 - ②Fixed模式：只传播手动配置的VLAN信息。
 - ③Forbidden模式：只传播VLAN1不传其他VLAN。
- 交换机默认：透明模式，VLAN1，所有端口。

4

- **考点02：** 基于接口划分VLAN：静态VLAN！

```

<HUAWEI> system-view                //进入交换机系统视图
[HUAWEI] sysname SwitchA             //交换机命名
[SwitchA] vlan batch 2                //批量方式建立 VLAN 2
[SwitchA] interface gigabitethernet 0/0/1 //进入交换机接口视图
[SwitchA-GigabitEthernet0/0/1] port link-type access //配置接口类型
[SwitchA-GigabitEthernet0/0/1] port default vlan 2 //将接口加入 VLAN 2
[SwitchA-GigabitEthernet0/0/1] quit
[SwitchA] interface gigabitethernet 0/0/2
[SwitchA-GigabitEthernet0/0/2] port link-type trunk
[SwitchA-GigabitEthernet0/0/2] port trunk allow-pass vlan 2
[SwitchA-GigabitEthernet0/0/2] quit
    
```

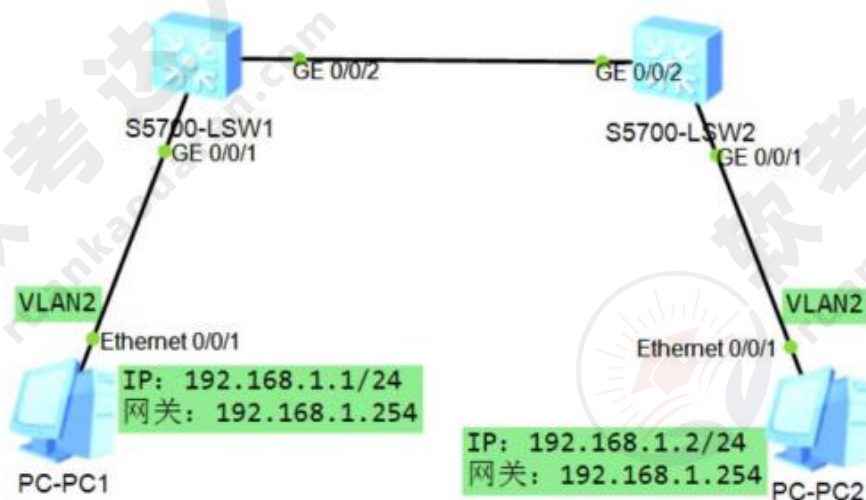
5

● 考点03：基于MAC划分VLAN：动态VLAN。

```

<HUAWEI> system-view
[HUAWEI] sysname SwitchA
[SwitchA] vlan batch 2
[SwitchA] interface gigabitethernet 0/0/1                //在接口视图配置上联接口
[SwitchA-GigabitEthernet0/0/1] port link-type hybrid    //配置上联接口类型
[SwitchA-GigabitEthernet0/0/1] port hybrid tagged vlan 2 //通过 VLAN2
[SwitchA-GigabitEthernet0/0/1] quit
[SwitchA] interface gigabitethernet 0/0/2                //进入交换机接口视图
[SwitchA-GigabitEthernet0/0/2] port link-type hybrid    //配置接口类型
[SwitchA-GigabitEthernet0/0/2] port hybrid untagged vlan 2 //将接口加入 VLAN2
[SwitchA-GigabitEthernet0/0/2] quit
[SwitchA] vlan 2
[SwitchA-vlan2] mac-vlan mac-address 22-22-22          //PC 的 MAC 地址与 VLAN2 关联
[SwitchA-vlan2] quit
[SwitchA] interface gigabitethernet 0/0/2
[SwitchA-GigabitEthernet0/0/2] mac-vlan enable          //基于 MAC 地址启用接口
[SwitchA-GigabitEthernet0/0/2] quit
    
```

● 考点04：基于GVRP的VLAN配置实验：可在LSW1创建VLAN2，LSW2可以学到，ping通。



- **第一步：**交换机LSW1基本配置：LSW2参考配置。

```
<Huawei>
<Huawei>system-view
[Huawei]un in en
[Huawei]sysname SwitchA
[SwitchA]gvrp
[SwitchA]vlan 2
[SwitchA]int vlan 2
[SwitchA-Vlanif2]ip add 192.168.1.254 24
```

- **第二步：**交换机LSW1端口配置：LSW2参考下。

```
[SwitchA]
[SwitchA]int g0/0/1
[SwitchA-G0/0/1]port link-type access
[SwitchA-G0/0/1]port default vlan 2

[SwitchA]int g0/0/2
[SwitchA-G0/0/2]port link-type trunk
[SwitchA-G0/0/2]port trunk allow-pass vlan all
```

- **第三步：**交换机LSW1配置GVRP：LSW2参考下。

```
<SwitchA>sys
[SwitchA]int g0/0/2
[SwitchA-GigabitEthernet0/0/2]gvrp
```


● **第四步：**配置PC1的IP，ping验证：PC2参考。

```
[SwitchA]dis gvrp statistics
```

```
GVRP statistics on port GigabitEthernet0/0/2
```

```
GVRP status : Enabled
```

```
GVRP registrations failed : 0
```

```
GVRP last PDU origin : 4c1f-cccc-0583
```

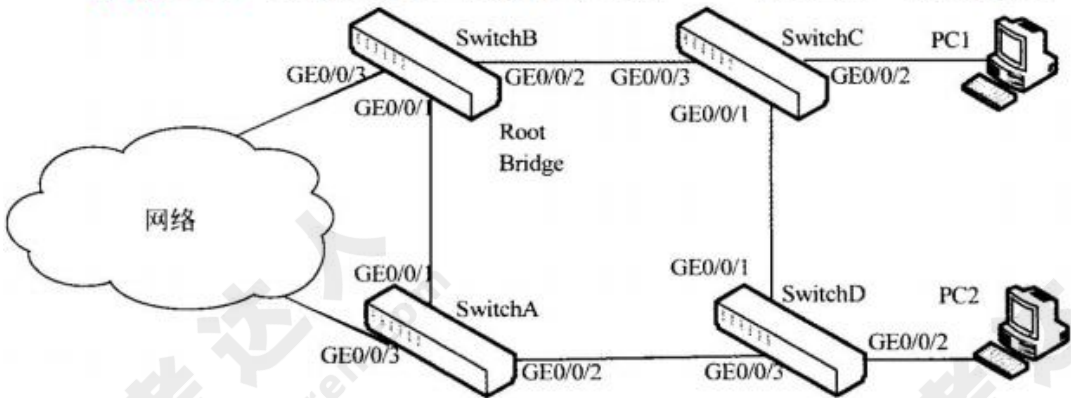
```
GVRP registration type : Normal
```

```
[SwitchB]dis vlan
```

VID	Status	Property	MAC-LRN	Statistics	Description
1	enable	default	enable	disable	VLAN 0001
2	enable	default	enable	disable	VLAN 0002

10

● **考点05：**交换机生成树协议STP配置：优先级



(1) 配置 STP 基本功能。

配置环网中的设备生成树协议工作在 STP 模式。

12

#配置 SwitchA 的 STP 工作模式，SwitchB、SwitchC、SwitchD 的配置相同

```
<HUAWEI> system-view
```

```
[HUAWEI] sysname SwitchA
```

```
[SwitchA] stp mode stp
```

配置根桥和备份根桥设备

#配置 SwitchA 为根桥

```
[SwitchA] stp root primary
```

#配置 SwitchB 为备份根桥

```
[SwitchB] stp root secondary
```

13

● 考点06：交换机生成树协议STP配置：路径值

#配置 SwitchA 的端口路径开销计算方法为华为计算方法，SwitchB、

[SwitchA] stp pathcost-standard legacy SwitchD 配置方法相同

#配置 SwitchC 端口 GigabitEthernet0/0/1 端口路径开销值为 20000

```
[SwitchC] stp pathcost-standard legacy
```

```
[SwitchC] interface gigabitethernet 0/0/1
```

```
[SwitchC-GigabitEthernet0/0/1] stp cost 20000
```

```
[SwitchC-GigabitEthernet0/0/1] quit
```

#配置 SwitchD 端口 GigabitEthernet0/0/2 为边缘端口并启用端口的

[SwitchB] interface gigabitethernet 0/0/2 BDPDU 报文过滤功能

```
[SwitchB-GigabitEthernet0/0/2] stp edged-port enable
```

```
[SwitchB-GigabitEthernet0/0/2] stp bpdu-filter enable
```

```
[SwitchB-GigabitEthernet0/0/2] quit
```

#配置 SwitchC 端口 GigabitEthernet0/0/2 为边缘端口并启用端口的

[SwitchC] interface gigabitethernet 0/0/2 BDPDU 报文过滤功能

```
[SwitchC-GigabitEthernet0/0/2] stp edged-port enable
```

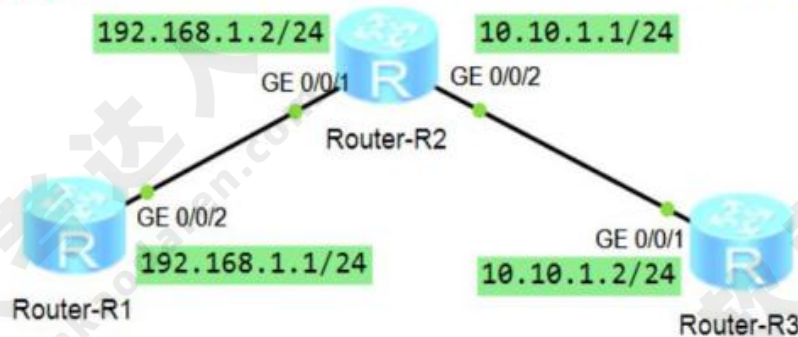
```
[SwitchC-GigabitEthernet0/0/2] stp bpdu-filter enable
```

```
[SwitchC-GigabitEthernet0/0/2] quit
```

设备全局启用 STP，所有设备配置相同。

#设备 SwitchA 全局启用 STP

- **考点07：**动态路由RIP：距离矢量，拓扑下图



- **第一步：**配置各接口IP：R1、R2、R3参考如下

```

<Huawei>sys
[Huawei]un in en
[Huawei]int g0/0/2
[Huawei-GigabitEthernet0/0/2]ip add 192.168.1.1 24
  
```

- **第二步：**配置RIP协议：R1、R2、R3参考如下

```

<Huawei>sys
[Huawei]un in en
[Huawei]rip
[Huawei-rip-1]network 192.168.1.0
[Huawei-rip-1]network 10.0.0.0
  
```

- **第三步：**验证配置结果：dis ip routing、ping。

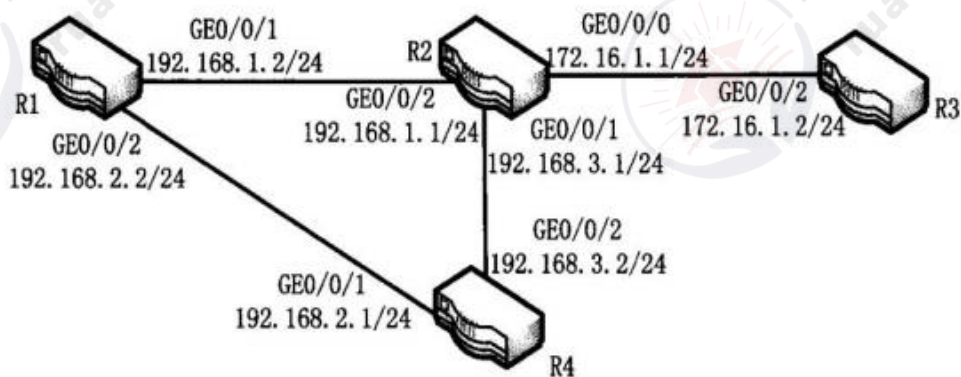
```

<Huawei>dis ip routing
Destination/Mask  Proto  Pre   NextHop
10.0.0.0/8       RIP    100   192.168.1.2
  
```

目标网段 RIP获取 管理距离 下一跳

第十章：组网技术（3）

- **考点01：** BFD：双向转发检测，可以提供毫秒级的检测，可以实现链路的快速检测，BFD通过与上层路由协议联动。当主链路发生故障时，业务流量会快速切换到另一条路径进行传输。



- **第一步：** 配置各接口IP：R1、R2、R3参考如下。

```
[R1] interface gigabitethernet 0/0/1
```

```
[R1-GigabitEthernet0/0/1] ip address 192.168.1.2 24
```

```
[R1-GigabitEthernet0/0/1] quit
```

```
[R1] ] interface gigabitethernet 0/0/2
```

```
[R1-GigabitEthernet0/0/2] ip address 192.168.2.2 24
```

```
[R1-GigabitEthernet0/0/2] quit
```

- **第二步：** 配置RIP协议：R1、R2、R3参考如下。

```
[R1] rip 1
```

```
[R1-rip-1] version 2
```

```
[R1-rip-1] network 192.168.1.0
```

```
[R1-rip-1] network 192.168.2.0
```

- **第三步：**配置R1上BFD联动，R2参考配置如下。

[R1] bfd

[R1-bfd] quit

单位：ms

[R1] rip 1

[R1-rip-1] bfd all-interfaces enable

//启用 bfd 功能

[R1-rip-1] bfd all-interfaces min-rx-interval 100 min-tx-interval
100 detect-multiplier 10 配置最小发送、时间间隔

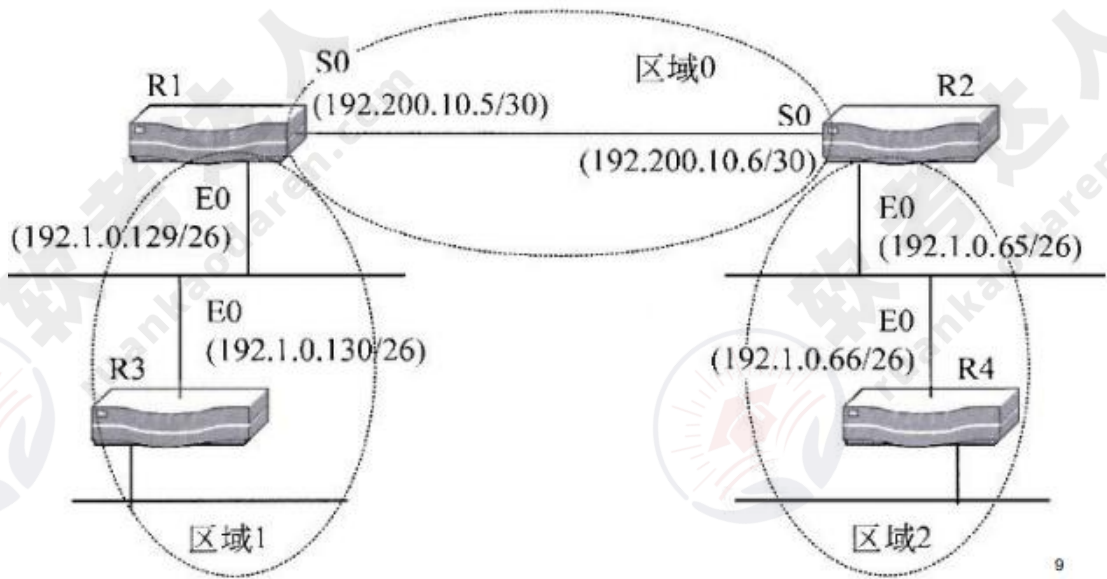
- **第四步：**验证配置结果：dis ip routing、dis rip 1 neighbor、dis rip 1 bfd session all、shutdown。

6

- **考点01：**OSPF：开放最短路径用协议，链路状态。路由器之间通过网络接口状态LSA来建立链路状态数据库（邻居表），使用迪杰斯特拉Dijkstra算法，来计算最短路径（拓扑表），每个路由器使用这些最短路径构造（路由表）。
- 简化原理：发Hello报文建立邻接关系（邻居表）——形成链路状态数据库（拓扑表）——SPF算法形成路由表（路由表）。
- OSPF采用触发更新，和30分钟周期更新。支持不连续子网和CIDR。管理距离：10、150。

8

● **考点02：** OSPF实验拓扑如图： 配置参数如图。



● **第一步：** 配置R1接口IP： R2、 R3、 R4参考配置。

```
<Huawei>sys
[Huawei]un in en
[Huawei]int e0/0/0
[Huawei-E0/0/0]ip add 192.1.0.129 26
[Huawei-E0/0/0]int s0/0/0
[Huawei-S0/0/0]ip add 192.200.10.5 30
<Huawei>dis cu
```

● **第二步：** 配置R1的OSPF： R2、 R3、 R4参考配。

```
[Huawei]ospf
[Huawei-ospf-1]area 0
[Huawei-ospf-1-area-0]net 192.200.10.4 0.0.0.3
[Huawei-ospf-1-area-0]area 1
[Huawei-ospf-1-area-1]netw 192.1.0.128 0.0.0.63
[Huawei-ospf-1-area-1]return
<Huawei>dis cu
```


● **第三步：**验证ping、dis ip routing、dis cu。

<Huawei>dis ip routing

以R3为例

Destination/Mask	Proto	Pre	Cost	Flags	NextHop
127.0.0.0/8	Direct	0	0	D	127.0.0.1
127.0.0.1/32	Direct	0	0	D	127.0.0.1
192.1.0.64/26	OSPF	10	1564	D	192.1.0.129
192.1.0.128/26	Direct	0	0	D	192.1.0.130
192.1.0.130/32	Direct	0	0	D	127.0.0.1
192.200.10.4/30	OSPF	10	1563	D	192.1.0.129

<Huawei>dis cu

以R1为例

```
ospf 1
area 0.0.0.0
network 192.200.10.4 0.0.0.3
area 0.0.0.1
network 192.1.0.128 0.0.0.63
```

**dis ospf peer
dis ospf routing**

11

- **考点03：**IS-IS：中间系统-中间系统，路由器称为中间系统IS。和OSPF协议很类似。
- **Net-Entity：**网络实体。运行IS-IS的路由器必须配置一个网络实体地址。格式为：**SEL**服务访问点

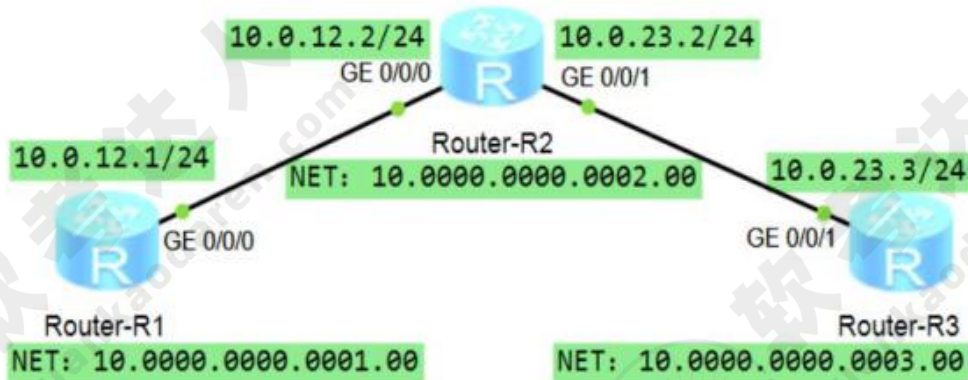
区域ID	系统ID	SEL
1字节	16字节	1字节

例如：4A.2000.00E0.008C.00十六进制表示

- **IS-IS**在路由域内采用两级的分层结构。骨干区域与非骨干区域。并定义了路由器的三种角色：区域内**Level-1**、区域间**Level-2**、同属于**Level-1-2**。默认路由器接口为**Level-1-2**。

13

- **考点04：** IS-IS实验拓扑如图：配置参数如图。



- **第一步：** 配置R1接口IP： R2、 R3参考配置(略)。
- **第二步：** 配置R1的IS-IS： R2、 R3参考如下配置。

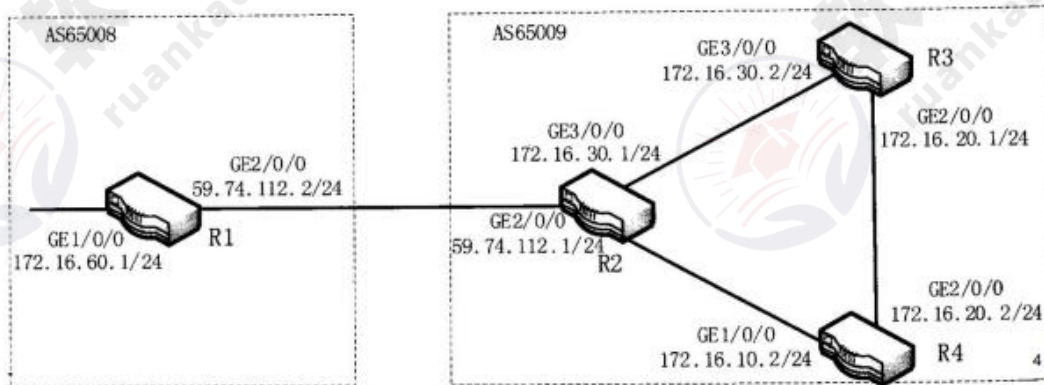
```

<Huawei>sys
[Huawei]un in en
[Huawei]isis
[Huawei-isis-1]
[Huawei-isis-1]network-entity 10.0000.0000.0001.00
[Huawei-isis-1]quit
[Huawei]
[Huawei]int g0/0/0
[Huawei-G0/0/0]
[Huawei-G0/0/0]isis enable
[Huawei-G0/0/0]int g0/0/1
[Huawei-G0/0/1]isis enable
  
```

- **第三步：** 验证ping、dis ip routing、dis isis peer、dis cu、dis isis route。

第十章：组网技术（4）

- **考点01：** BGP：边界网关协议，在自制系统AS之间选择最佳路由，距离矢量。支持多出口大型网络。路由采用增量更新。除了下一跳还有经过的AS列表通过信息。允许CIDR和VLSM，支持鉴别、验证等。分为EBGP(外部)和IBGP(内部)。



- **第一步：** 配置R1到R4接口IP的基本配置(略)。
- **第二步：** 配置IBGP：R2、R3、R4如下配置。

```
[R2] bgp 65009                                     //启动BGP及AS号
[R2-bgp] router-id 2.2.2.2                         //配置BGP的RouterID
[R2-bgp] peer 9.1.1.2 as-number 65009             //配置BGP对等体
[R2-bgp] peer 9.1.3.2 as-number 65009
```

```
[R3] bgp 65009
[R3-bgp] router-id 3.3.3.3
[R3-bgp] peer 9.1.3.1 as-number 65009
[R3-bgp] peer 9.1.2.2 as-number 65009
[R3-bgp] quit
```



```
[R4] bgp 65009
[R4-bgp] router-id 4.4.4.4
[R4-bgp] peer 9.1.1.1 as-number 65009
[R4-bgp] peer 9.1.2.1 as-number 65009
[R4-bgp] quit
```

- **第三步：**配置EBGP：R1、R2如下配置。

```
[R1] bgp 65008
[R1-bgp] router-id 1.1.1.1
[R1-bgp] peer 59.74.112.1 as-number 65009

[R2-bgp] peer 59.74.112.2 as-number 65008
```

6

- **第四步：**配置R1发布路由，如下配置。

```
[R1-bgp] ipv4-family unicast //进入IPV4地址族视图
[R1-bgp-af-ipv4] network 172.16.60.0 255.255.255.0
[R1-bgp-af-ipv4] quit
```

- **第五步：**配置R2引入路由，如下配置。

```
[R2-bgp] ipv4-family unicast
[R2-bgp-af-ipv4] import-route direct //引入路由表
```

- **第六步：**验证BGP用到的命令。

dis bgp peer、dis bgp routing、dis cu、ping。

7

- **考点02：ACL：**访问控制列表，可以根据源地址、目标地址、源端口、目标端口、协议信息对数据包进出过滤控制。
- **两个方向：**入口inbound是指数据流进入路由器(进门)、出口outbound是指数据流从路由器流出(出门)。**两种动作：**允许permit、拒绝deny。

分类	规则定义描述	编号范围
基本 ACL	仅使用报文的源 IP 地址、分片信息和生效时间段信息来定义规则	2000~2999
高级 ACL	既可使用 IPv4 报文的源 IP 地址,也可使用目的 IP 地址、IP 协议类型、ICMP 类型、TCP 源/目的端口、UDP 源/目的端口号、生效时间段等来定义规则	3000~3999
二层 ACL	使用报文的以太网帧头信息来定义规则,如根据源 MAC (Media Access Control) 地址、目的 MAC 地址、二层协议类型等	4000~4999
用户 ACL	既可使用 IPv4 报文的源 IP 地址,也可使用目的 IP 地址、IP 协议类型、ICMP 类型、TCP 源端口/目的端口、UDP 源端口/目的端口号等来定义规则	6000~6031

- **考点03：基本ACL：**编号2000~2999

```

<Huawei> system-view
{
  [Huawei] acl 2001      命令 动作 源地址 IP 反掩码
  [Huawei-acl-basic-2001] rule permit source 172.16.10.3 0
}

1 <Huawei> system-view
2 [Huawei] acl 2001
3 {
  [Huawei-acl-basic-2001] rule permit source 172.16.10.3 0
  [Huawei-acl-basic-2001] rule deny source 172.16.10.0 0.0.0.255
  [Huawei-acl-basic-2001] description Permit only 172.16.10.3 through
}

```

- 1、进入系统 2、配置编号 3、ACL列表
- 基本ACL，基于源地址，放置到目的端路由器。

● **考点04：**基本ACL命令规则：编号2000~2999

acl [number] *acl-number* [match-order { auto | config }]
命令 可选 编号 匹配 排序 排序 顺序

acl name *acl-name* { basic | *acl-number* } [match-order { auto | config }]

rule [rule-id] { deny | permit } [source
命令 步长数字 拒绝 允许 源地址

{ source-address source-wildcard | any }
源IP 反掩码 任何

[[fragment | none-first-fragment] | logging
分片 不分片 日志

| time-range time-name]
时间 名称

11

<Huawei> system-view

[Huawei] time-range working-time 8:00 to 18:00 working-day

[Huawei] acl name work-acl basic

[Huawei-acl-basic-work-acl] rule deny source 172.16.10.0
0.0.0.255 time-range working-time

<Huawei> system-view

[Huawei] acl 2001

[Huawei-acl-basic-2001] rule deny source 172.16.10.0
0.0.0.255 none-first-fragment

● **善用Tab键补全命令和问号?键帮助命令。**

12

● **考点05：** ACL几个重点知识：

- **ACL执行原则：** ①自上而下排序原则。②先匹配原则（特例在前，其他在后）。③默认丢弃原则（deny any）。
- **反掩码：** 0.0.0.0，单个主机，同host，如：
192.168.1.1 0.0.0.0 = host 192.168.1.1
- **反掩码：** 255.255.255.255，任意主机，同any，通常与0.0.0.0一起使用，例如：
0.0.0.0 255.255.255.255 = any

13

● **考点06：** 高级ACL： 编号3000~3999

- ```

{
 <Huawei> system-view
 [Huawei] acl 3001
 [Huawei-acl-adv-3001] rule permit icmp source 172.16.10.3 0
 命令 动作 协议 源端 IP
 destination 172.16.20.0 0.0.0.255
 目的 IP 反掩码
1 { <Huawei> system-view
2 { [Huawei] acl name deny-telnet
3 { [Huawei-acl-adv-deny-telnet] rule deny tcp destination-port eq telnet
 命令 动作 协议 目的端口 等于 23
 source 172.16.10.3 0 destination 172.16.20.0 0.0.0.255
 源端 IP 反掩码 目的 IP 反掩码

```

- 高级ACL，基于目的，放置到源端的路由器。

14

### ● 考点08：高级ACL命令规则：编号3000~3999

```
rule [rule-id] { deny | permit } { protocol-number | udp }
命令 步长数字 拒绝 允许 协议号 协议
[destination { destination-address destination-wildcard | any } |
目的 IP 反掩码 任何
destination-port { eq | gt | lt port | range port-start port-end } | source
目的端口 等于 端口号 范围 开始端口 结束端口 源
{ source-address source-wildcard | any } | source-port { eq | gt | lt port
IP 反掩码 任何 源端口 等于 端口号
| range port-start port-end } | logging | time-range time-name]
范围 开始端口 结束端口 日志 时间 名称
```

15

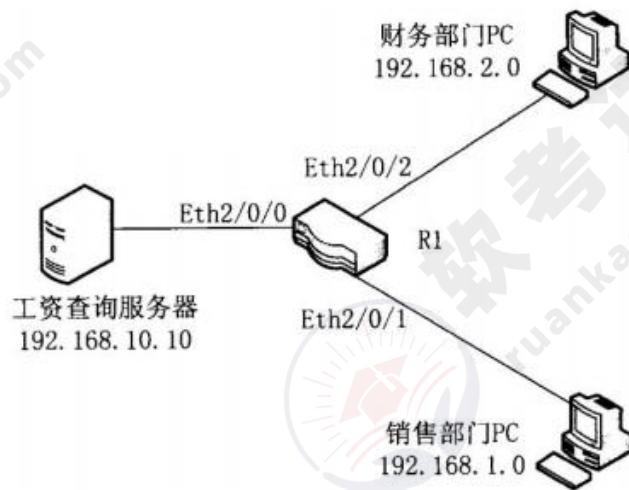
### ● 考点09：几个重要参数

| 操 作 符   | 解 释        | 操 作 符 | 解 释           |
|---------|------------|-------|---------------|
| lt      | 小于         | neq   | 不等于           |
| gt      | 大于         | range | 指定范围          |
| eq      | 等于         |       |               |
| 传 输 协 议 | 上 层 协 议    | 端 口 号 | 命 令 参 数 关 键 字 |
| TCP     | 文件传输协议——数据 | 20    | ftp-data      |
| TCP     | 文件传输协议——控制 | 21    | ftp           |
| TCP     | 远程连接       | 23    | telnet        |
| TCP     | 简单邮件传输协议   | 25    | smtp          |
| UDP     | 域名服务       | 53    | dns           |
| UDP     | 简单文件传输协议   | 69    | tftp          |
| TCP     | 超文本传输协议    | 80    | www           |
| UDP     | 简单网络管理协议   | 161   | snmp          |
| UDP     | 简单网络管理协议   | 162   | snmp-trap     |
| UDP     | 路由信息协议     | 520   | rip           |

16

- **考点10：**高级ACL实验一：限制用户在特定时间访问特定服务器。

- 要求禁止销售部门在上班时间（8:00-18:00）访问工资查询服务器，财务部门不受限制，可以随时访问，如图。



17

- **第一步：**配置IP、配置VLAN、VLANIF等。

```
<Huawei> system-view 以E2/0/1口为例
[Huawei] sysname R1
[R1] vlan batch 10 20 100
[R1] interface ethernet 2/0/1
[R1-Ethernet2/0/1] port link-type trunk
[R1-Ethernet2/0/1] port trunk allow-pass vlan 10
[R1-Ethernet2/0/1] quit
[R1] interface vlanif 10
[R1-Vlanif10] ip address 192.168.1.1 255.255.255.0
[R1-Vlanif10] quit
```

18



- **第二步：**配置基于时间的ACL访问规则等。

#配置 8:00 至 18:00 的周期时间段

```
[R1] time-range satime 8:00 to 18:00 working-day
```

#配置销售部门到工资查询服务器的访问规则

```
[R1] acl 3001
```

```
[R1-acl-3001] rule deny ip source 192.168.1.0 0.0.0.255
destination 192.168.10.10 0.0.0.0 time-range satime
```

- Mon(周一)、Tue(周二)、Wed(周三)、Thu(周四)、Fri(周五)、Sat(周六)、Sun(周日)、working-day(周一到周五)、off-day(周六周日)daily(周一到周日)、数字0-6(每周几)。

- **第三步：**配置基于ACL的流分类策略。

#配置流分类 c\_xs，对匹配 ACL 3001 的报文进行分类

```
[R1] traffic classifier c_xs
```

```
[R1-classifier-c_xs] if-match acl 3001
```

```
[R1-classifier-c_xs] quit
```

#配置流行为 b\_xs，动作为拒绝报文通过

```
[R1] traffic behavior b_xs
```

```
[R1-behavior-b_xs] deny
```

```
[R1-behavior-b_xs] quit
```

- **第四步：**应用基于ACL的流策略。

#配置流策略 p\_xs，将流分类 c\_xs 与流行为 b\_xs 关联

```
[R1] traffic policy p_xs
```

```
[R1-trafficpolicy-p_xs] classifier c_xs behavior b_xs
```

```
[R1-trafficpolicy-p_xs] quit
```

#由于销售部门访问服务器的流量从接口 Eth2/0/1 进入 Router，所以可以在 Eth2/0/1 接口的入方向应用流策略 p\_xs

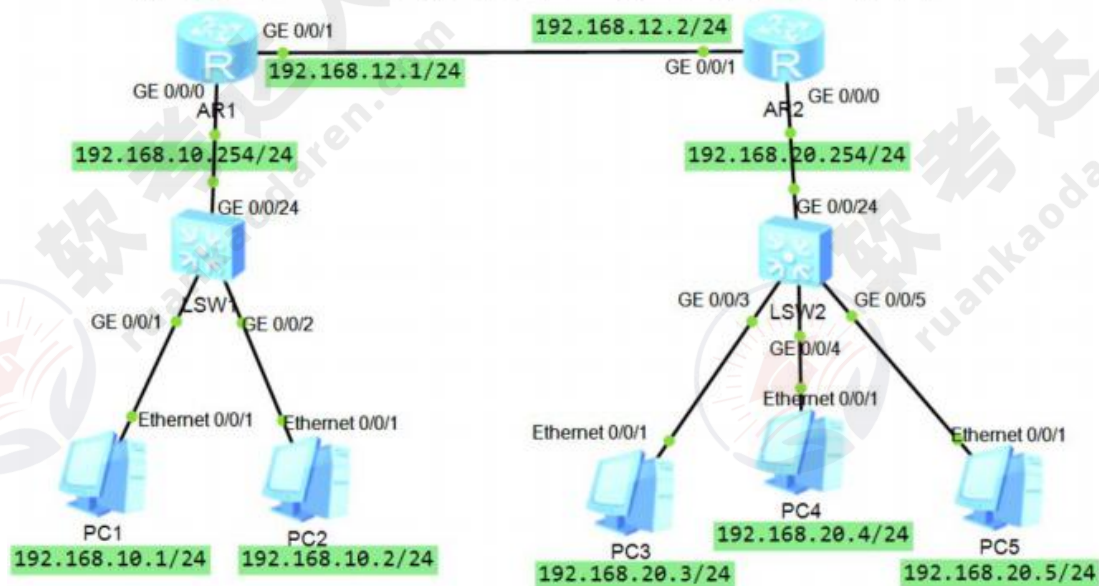
```
[R1] interface ethernet2/0/1
```

```
[R1-Ethernet2/0/1] traffic-policy p_xs inbound
```

```
[R1-Ethernet2/0/1] quit
```

## 第十章：组网技术（5）

- 路由技术ACL实验技术，拓扑配置如下图。



- **第一步：**配置各设备IP：R1、R2及各PC。
- **第二步：**配置静态路由或RIP全网联通。
- **第三步：**配置ACL、ACL规则，并应用。

```
[R2]acl 3000
```

```
[R2-acl-advance-3000]rule 5 deny ip
```

```
source 192.168.20.1 0
```

```
destination 192.168.10.1 0
```

```
[R2]int g0/0/0
```

```
[R2-G0/0/0]traffic-filter inbound acl 3000
```

- **第四步：**验证ACL。display acl 3000、dis cu、dis acl all、ping命令。

- **附加题：**配置ACL，使PC5可以访问PC1-PC4，其他都不可以访问。

```
rule permit ip source 192.168.20.5 0
```

```
rule 100 deny ip
```

```
interface g0/0/0
```

```
traffic-filter inbound acl XXX
```



## （华为专题）

- **考点01：**配置交换机的名称和密文密码： |
- <Huawei> //用户视图
- <Huawei>system-view //进入系统视图配置
- [Huawei] //系统视图
- [Huawei]quit 或return //退出系统视图模式
- [Huawei]sysname DTWLXY //设置主机名
- [Huawei]user-interface console 0 //进入控制台
- [Huawei-ui-console0]authentication-mode password
- [Huawei-ui-console0]set authentication password
- cipher huawei //配置密文密码

- **考点02：**配置交换机的远程管理IP地址：
- [Huawei]interface Vlanif 1 //进入VLAN1
- [Huawei-Vlanif1]ip add 192.168.1.254 24 //配置IP
- [Huawei-Vlanif1]undo shutdown //开启接口
- [Huawei]dns domain dtwlxy.com //设置域名
- [Huawei]dns server 192.168.254.254 //设置域名IP
- dis vlan 显示vlan
- save保存配置
- dis curr 显示当前配置
- reboot重启设备
- <Huawei>undo terminal monitor //取消提示信息

10

● **考点03：**配置交换机端口速率、双工、ARP：

- [Huawei]int g0/0/1 //进入接口
- [Huawei-g0/0/1]description dtwlyx //端口描述
- [Huawei-g0/0/1]undo negotiation auto //取消协商
- [Huawei-GigabitEthernet0/0/1]duplex full //全双工
- [Huawei-GigabitEthernet0/0/1]auto duplex full //自动
- [Huawei-GigabitEthernet0/0/1]speed 10 //速率10M
- [Huawei-GigabitEthernet0/0/1]auto speed 100 //自动
- [Huawei]arp static 192.168.1.8 5489-98cf-2603//绑定
- [Huawei]dis arp [Huawei]dis arp all //查看ARP<sub>1</sub>

● **考点04：**配置路由器接口IP和静态路由：

- [Huawei]int g0/0/1 //进入接口
- [Huawei-g0/0/1]ip add 192.168.1.6 24 //配IP地址
- [Huawei-GigabitEthernet0/0/1]undo shutdown //开启
- <Huawei>dis cur 或 [Huawei]dis cur //查看ARP
- //配置静态路由
- [Huawei]ip route-static 192.168.20.0 24 10.0.12.2
- [Huawei]ip route-static 192.168.10.0 24 serial 0/0/1
- [Huawei]ip route-static 0.0.0.0 0 192.168.1.5 //默认
- [Huawei]display ip routing-table //查看路由表<sub>2</sub>



● **考点05：**配置交换机VLAN相关命令：

- [Huawei]vlan 10 或 [Huawei]vlan 20 //创建VLAN
- [Huawei-vlan10]description dtwlxy //VLAN描述
- [Huawei]vlan batch 30 40 //创建多个VLAN
- [Huawei]int g0/0/1 //进入接口
- [Huawei-g0/0/1]port link-type access //访问口
- [Huawei-g0/0/1]port default vlan 10 //加入VLAN
- [Huawei-g0/0/2]port link-type trunk //干道口
- [Huawei-g0/0/2]port trunk allow-pass vlan 10 20 允许
- [Huawei-g0/0/2]port trunk allow-pass vlan all //所有<sup>13</sup>

- [Huawei]int e0/0/2 //进入接口
- [Huawei-E0/0/2]port link-type hybrid //混合口模式
- [Huawei-E0/0/2]undo port default vlan //删除默认vlan
- [Huawei-E0/0/2]port hybrid untagged vlan 20 //去标签
- [Huawei-E0/0/2]port hybrid pvid vlan 2 //设置默认vlan
- [Huawei-E0/0/2]port trunk allow-pass vlan 10 to 100  
//允许（前面加undo不允许）
- [Huawei]dis port vlan //查看vlan
- [Huawei]display vlan //查看vlan



- **考点06：**配置交换机VLAN一致性GVRP：通用VLAN注册协议，国际标准。双向注册。
- Normal模式：（类似cisco交换机服务器模式）  
[Huawei]gvrp //开启gvrp 也是默认模式
- Fixed模式：（类似cisco交换机客户机模式）  
[Huawei-g0/0/2]gvrp registration fixed
- Forbidden模式：（类似cisco交换机透明模式）  
[Huawei-g0/0/3]gvrp registration forbidden
- dis vlan summary //查看vlan汇总  
dis gvrp status //查看gvrp状态

- **考点07：**配置路由器RIP协议：RIPv1 RIPv2
- [Huawei]rip //启用RIP默认v1  
[Huawei-rip-1]network 192.168.1.0 //发布直连网段  
[Huawei-rip-1]version 2 //配置v2版本
- [Huawei]dis rip //查看rip  
[Huawei]dis rip database //查看rip数据库  
[Huawei]dis ip routing-table //查看路由表
- 优先级：直连 0、静态 60、rip 100、ospf 10/150

16

● **考点8：**配置路由器OSPF协议：

- [Huawei]ospf 1 //启用OSPF 默认是进程1
- [Huawei-ospf-1]area 0 //进入区域0
- [Huawei-ospf-1-area-0.0.0.0]network 192.168.3.0  
0.0.0.255 //发布直连网段
- [Huawei-ospf-1]silent-interface g0/0/2 //被动接口
- [Huawei]dis ospf interface //查看ospf通告
- [Huawei]dis ospf peer //查看ospf邻居
- [Huawei]dis ip routing-table //查看路由表
- [Huawei]dis ospf routing //查看ospf路由表<sup>17</sup>

● **考点9：**配置基于全局的DHCP协议：

- [Huawei]dhcp enable //开启dhcp
- [Huawei]ip pool dtwlxy //地址池名
- [Huawei-ip-pool-dtwlxy]network 192.168.1.0 //地址池
- [Huawei-ip-pool-dtwlxy]lease day 2 //租约默认1
- [Huawei-ip-pool-dtwlxy]gateway-list 192.168.1.254
- [Huawei-ip-pool-dtwlxy]excluded-ip-address //网关  
192.168.1.250 192.168.1.253 //排除IP范围
- [Huawei-ip-pool-dtwlxy]dns-list 8.8.8.8 //DNS服务器
- [Huawei-G0/0/0]dhcp select global //基于全局<sup>8</sup>



● **考点10：**配置基于接口的DHCP协议：

- [Huawei]dhcp enable //开启dhcp
- [Huawei]int g0/0/1 //进入接口
- [Huawei-G0/0/1]dhcp select interface //基于接口
- [Huawei-G0/0/1]dhcp server lease day 2 //租约默认1
- [Huawei-G0/0/1]dhcp server excluded-ip-address  
192.168.1.1 192.168.1.10 //排除IP范围
- [Huawei-G0/0/1]dhcp server dns-list 8.8.8.8 //DNS
- [Huawei]dis ip pool //查看dhcp  
客户机：自动获取， 查看ipconfig、ifconfig。

● **考点11：**配置路由器基本ACL：2000-2999

- [Huawei]acl 2000 //配置基本acl
- [Huawei-acl-basic-2000]rule 5 permit source 1.1.1.1  
0 //允许源IP(注意反掩码0，默认步长5)
- [Huawei-acl-basic-2000]rule 10 deny any //拒绝任意
- [Huawei]user-interface vty 0 4 //进入接口
- [Huawei-ui-vty0-4]acl 2000 inbound //应用acl
- [Huawei]dis acl all //查看所有acl
- [Huawei]dis acl 2000 //查看acl 2000



- **考点12：**配置路由器高级ACL：3000-3999

- [Huawei]acl 3000 //配置高级acl
- [Huawei-acl-adv-3000]rule permit ip source 1.1.1.1 0  
  destination 4.4.4.4 0 //允许访问
- [Huawei]user-interface vty 0 4 //进入虚拟接口
- [Huawei-ui-vty0-4]acl 3000 outbound //应用acl
- [Huawei]int g0/0/1 //进入接口
- [Huawei-G0/0/1]traffic-filter inbound acl 3000 //应用
- [Huawei]dis acl all //查看所有acl

21

- **考点13：**配置路由器动态NAT：(多对少)

- [Huawei]nat address-group 1 202.169.10.50  
  202.169.10.60 //外部IP
- [Huawei]acl 2001 //配置ACL
- [Huawei-acl-basic-2001]rule 5 permit source  
  172.17.1.0 0.0.0.255 //内部IP
- [Huawei]int g0/0/1 //进入接口
- [Huawei-GigabitEthernet0/0/0]nat outbound 2001  
  address-group 1 no-pat //应用NAT
- [Huawei]dis nat outbound //查看NAT

22

- **考点14：**配置路由器静态NAT：(一对一)

- [Huawei]int g0/0/1 //进入接口
- [Huawei-GigabitEthernet0/0/1]nat static global  
202.169.10.5 inside 172.16.1.1 //一对一转换

- 配置路由器动态NAPT：(多对一)

- [Huawei]int g0/0/0 //进入接口
- [Huawei-G0/0/0]nat outbound 2001 //多对一转换
- [Huawei]dis nat static //查看静态NAT

23

- **考点15：**配置三层交换机VLAN间路由：

- 首先基本配置，IP、VLAN等。
- [Huawei]int vlanif 10 //进入接口
- [Huawei-Vlanif10]ip add 192.168.1.254 24 //配IP
- [Huawei]int vlanif 20 //进入接口
- [Huawei-Vlanif20]ip add 192.168.2.254 24 //配IP
- [Huawei]dis ip interface brief //接口简略信息
- [Huawei]dis port vlan //接口vlan信息
- [Huawei]dis vlan //查看vlan信息

- **考点16：**配置单臂路由VLAN间通信：

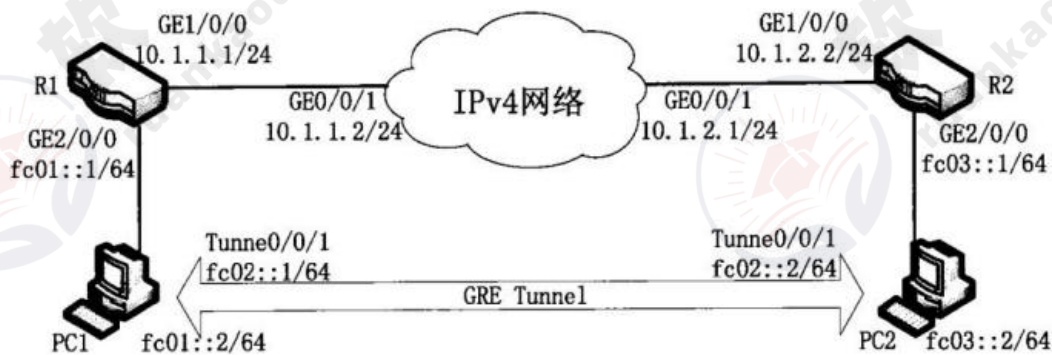
- 首先基本配置，IP、VLAN等。
- [Huawei-G0/0/1.1]ip add 192.168.1.254 24 //配置IP
- [Huawei-G0/0/1.1]dot1q termination vid 10 //封装
- [Huawei-G0/0/1.1]arp broadcast enable //开启arp
- [Huawei]dis ip interface brief //查看接口
- [Huawei]dis ip routing-table //查看路由表
- [Huawei]display current-configuration //查看配置

25



## 第十章：组网技术（6）

- **考点01：**路由技术IPV6隧道实验，拓扑配置如下。  
GRE(通用路由协议封装)规定了用一种网络协议去封装另一种网络协议的方法。下面是IPV6-over-IPV4GRE隧道配置实验。



4

- **第一步：**配置各设备IP：R1、R2及各PC。

```
<Huawei> system-view
```

```
[Huawei] sysname R1
```

```
[R1] interface gigabitethernet 1/0/0
```

```
[R1-GigabitEthernet1/0/0] ip address 10.1.1.1 255.255.255.0
```

```
[R1-GigabitEthernet1/0/0] quit
```

```
[R1] ipv6
```

**//全局启用IPV6**

```
[R1] interface gigabitethernet 2/0/0
```

```
[R1-GigabitEthernet2/0/0] ipv6 enable
```

**//接口启用IPV6**

```
[R1-GigabitEthernet2/0/0] ipv6 address fc01::1 64
```

```
[R1-GigabitEthernet2/0/0] quit
```



```
<Huawei> system-view
[Huawei] sysname R2
[R2] interface gigabitethernet 1/0/0
[R2-GigabitEthernet1/0/0] ip address 10.1.2.2 255.255.255.0
[R2-GigabitEthernet1/0/0] quit
[R2] ipv6
[R2] interface gigabitethernet 2/0/0
[R2-GigabitEthernet2/0/0] ipv6 enable
[R2-GigabitEthernet2/0/0] ipv6 address fc03::1 64
[R2-GigabitEthernet2/0/0] quit
```

- **第二步：**配置R1、R2的IPV4静态路由。

```
[R1] ip route-static 10.1.2.2 255.255.255.0 10.1.1.2
```

```
[R2] ip route-static 10.1.1.1 255.255.255.0 10.1.2.1
```

- **第三步：**配置R1、R2的Tunnel接口。

```
[R1] interface tunnel 0/0/1 //进入隧道口
```

```
[R1-Tunnel0/0/1] tunnel-protocol gre //隧道协议GRE
```

```
[R1-Tunnel0/0/1] ipv6 enable
```

```
[R1-Tunnel0/0/1] ipv6 address fc02::1 64
```

- [R1-Tunnel0/0/1] source 10.1.1.1 //源IP地址  
[R1-Tunnel0/0/1] destination 10.1.2.2 //目的IP地址  
[R1-Tunnel0/0/1] quit

```
[R2] interface tunnel 0/0/1
[R2-Tunnel0/0/1] tunnel-protocol gre
[R2-Tunnel0/0/1] ipv6 enable
[R2-Tunnel0/0/1] ipv6 address fc02::2 64
[R2-Tunnel0/0/1] source 10.1.2.2
[R2-Tunnel0/0/1] destination 10.1.1.1
[R2-Tunnel0/0/1] quit
```

- **第四步：**配置R1、R2的Tunnel静态路由。

```
[R1] ipv6 route-static fc03::1 64 tunnel 0/0/1
```

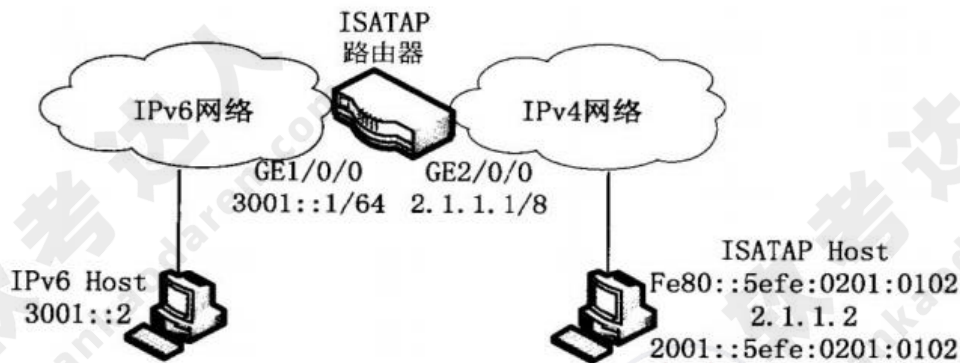
```
[R2] ipv6 route-static fc01::1 64 tunnel 0/0/1
```

- **第五步：**验证检查配置结果

```
[R2]ping 10.1.1.1
```

```
[R2]ping ipv6 fc01::1
```

- **考点02：**路由技术IPV6的ISATAP隧道实验如下。



- **第三步：**配置IPV6网络主机。  
C:\> netsh interface ipv6 set route 2001::/64 3001::1
- **第一步：**配置路由器接口IP、双栈。

10

```
<Huawei> system-view
[Huawei]sysname Router
[Router] ipv6
[Router] interface gigabitethernet 1/0/0
[Router-GigabitEthernet1/0/0] ipv6 enable
[Router-GigabitEthernet1/0/0] ipv6 address 3001::1/64
[Router-GigabitEthernet1/0/0] quit
[Router] interface gigabitethernet 2/0/0
[Router-GigabitEthernet2/0/0] ip address 2.1.1.1 255.0.0.0
```

11



```
[Router] interface tunnel 0/0/2
[Router-Tunnel0/0/2] tunnel-protocol ipv6-ipv4 isatap
[Router-Tunnel0/0/2] ipv6 enable //隧道协议ISATAP
[Router-Tunnel0/0/2] ipv6 address 2001::/64 eui-64
[Router-Tunnel0/0/2] source gigabitethernet 2/0/0
[Router-Tunnel0/0/2] undo ipv6 nd ra halt //发送RA消息
```

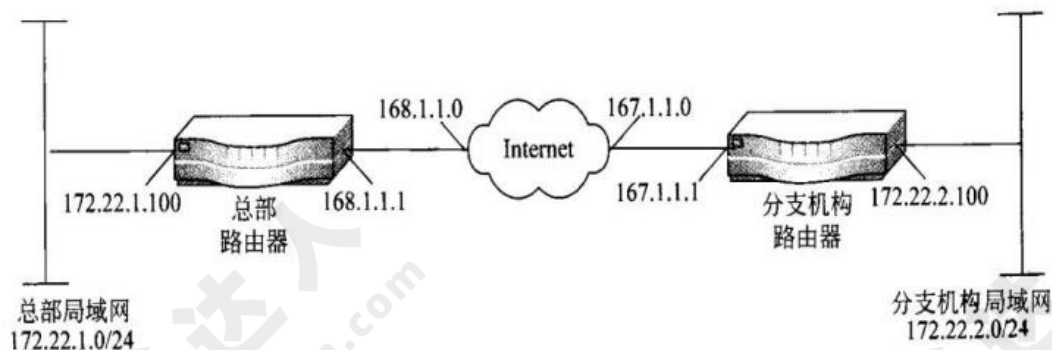
● **第二步：**配置ISATAP主机。

```
C:\> netsh interface ipv6 isatap set router 2.1.1.1
```

```
C:\> netsh interface ipv6 isatap set router 2.1.1.1 enabled
```

12

- **考点02：**路由技术IPSec实验，拓扑配置如下。  
某公司总部和分支机构构成，通过IPSec VPN实现网络安全，具体机构和配置如下。



- **第一步：**配置R1、R2的接口IP和静态路由。

14

<Huawei> system-view  
[Huawei] sysname R1  
[R1] interface gigabitethernet 1/0/0  
[R1-GigabitEthernet1/0/0] ip address 168.1.1.1 255.255.255.0  
[R1-GigabitEthernet1/0/0] quit  
[R1] interface gigabitethernet 2/0/0  
[R1-GigabitEthernet2/0/0] ip address 172.22.1.100 255.255.255.0  
[R1-GigabitEthernet2/0/0] quit  
[R1] ip route-static 167.1.1.1 255.255.255.0 168.1.1.2  
[R1] ip route-static 172.22.2.0 255.255.255.0 168.1.1.2

15

<Huawei> system-view  
[Huawei] sysname R2  
[R2] interface gigabitethernet 1/0/0  
[R2-GigabitEthernet1/0/0] ip address 167.1.1.1 255.255.255.0  
[R2-GigabitEthernet1/0/0] quit  
[R2] interface gigabitethernet 2/0/0  
[R2-GigabitEthernet2/0/0] ip address 172.22.2.100 255.255.255.0  
[R2-GigabitEthernet2/0/0] quit  
[R2] ip route-static 168.1.1.0 255.255.255.0 167.1.1.2  
[R2] ip route-static 172.22.1.0 255.255.255.0 167.1.1.2

16

- **第二步：**配置R1、R2的ACL保护数据流。

```
[R1] acl number 3101
```

```
[R1-acl-adv-3101] rule permit ip source 172.22.1.0 0.0.0.255
destination 172.22.2.0 0.0.0.255
```

```
[R2] acl number 3101
```

```
[R2-acl-adv-3101] rule permit ip source 172.22.2.0 0.0.0.255
destination 172.22.1.0 0.0.0.255
```

- **第三步：**配置R1、R2的IPSec安全协议。

```
[R1] ipsec proposal tran1 //创建IPSec安全提议
```

```
[R1-ipsec-proposal-tran1] esp authentication-algorithm sha2-256
```

```
[R1-ipsec-proposal-tran1] esp encryption-algorithm aes-128
```

```
[R2] ipsec proposal tran1 //ESP采用SHA认证 SEA加密
```

```
[R2-ipsec-proposal-tran1] esp authentication-algorithm sha2-256
```

```
[R2-ipsec-proposal-tran1] esp encryption-algorithm aes-128
```

- **第四步：**配置R1、R2的IKE对等体。

```
[R1] ike peer spub
```

```
[R1-ike-peer-spub] undo version 2
```

```
[R1-ike-peer-spub] ike-proposal 5 //创建IKE安全提议
```

```
[R1-ike-peer-spub] pre-shared-key cipher huawei
```

```
[R1-ike-peer-spub] remote-address 167.1.1.1 //预共享密钥
//对等体(对端IP)
```

18



```
[R2] ike peer spua
[R2-ike-peer-spua] undo version 2
[R2-ike-peer-spua] ike-proposal 5
[R2-ike-peer-spua] pre-shared-key cipher huawei
[R2-ike-peer-spua] remote-address 192.168.1.1
```

- **第五步：**配置R1、R2的安全策略组。

```
[R1] ipsec policy map1 10 isakmp //创建安全策略
[R1-ipsec-policy-isakmp-map1-10] ike-peer spub
[R1-ipsec-policy-isakmp-map1-10] proposal tran1
[R1-ipsec-policy-isakmp-map1-10] security acl 3101
```

19

```
[R2] ipsec policy use1 10 isakmp
[R2-ipsec-policy-isakmp-use1-10] ike-peer spua
[R2-ipsec-policy-isakmp-use1-10] proposal tran1
[R2-ipsec-policy-isakmp-use1-10] security acl 3101
```

- **第六步：**安全策略组应用R1、R2的接口上。

```
[R1] interface gigabitethernet 1/0/0
[R1-GigabitEthernet1/0/0] ipsec policy map1

[R2] interface gigabitethernet 1/0/0
[R2-GigabitEthernet1/0/0] ipsec policy use1
```

20

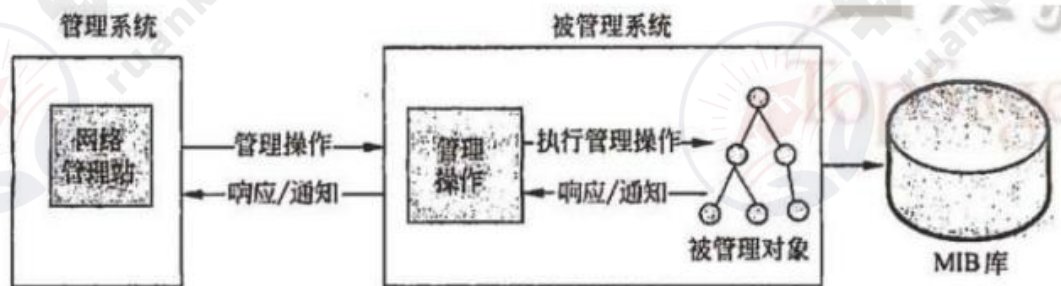
- **第七步：**测试配置验证结果。

```
display ipsec statistics
display ike sa
display ipsec proposal
```

配置成功后，总部和分支机构的PC执行ping命令操作正常，他们之间的数据传输将被加密。

## 第十一章：网络管理

- **考点01：**网络管理模型：包括网络监测和网络控制两部分。以下是一个网络管理模型。分为管理站，被管理代理、管理信息库MIB三部。MIB采用管理信息结构SMI（ASN.1国际标准的子集）。



3

- **考点02：**两种管理结构：

①集中式：集中控制整个网络。平衡优化网络。适用小网络。

②分布式：灵活性和伸缩性，适用中、大型网络。

- **考点03：**两种通信机制：

①轮询：是一种请求-响应式的交互方式。管理站向代理发出请求，代理做出响应，从信息管理库取出信息，返回给管理站。类似领导安排工作。

②事件报告：代理根据管理站的要求，向管理站主动发送状态报告。类似员工汇报工作。

4



● **考点04：** 网络管理中的五大管理功能：

- ①**计费管理：** 计算收取用户使用网络服务费用。
- ②**安全管理：** 提供信息的保密、认证和完整性。
- ③**性能管理：** 性能检测、性能分析、性能管理。
- ④**配置管理：** 监测和控制网络的状态以及配置。
- ⑤**故障管理：** 发现和纠正网络故障，维护网络的正常运行。包括报警、检测、定位、测试、恢复以及日志记录等。

**口诀：计安性配故。**

● **考点05：** 网络管理协议五种标准：

- ①**ISO制定：** CMIS/CMIP 公共管理信息服务规范。
- ②**基于TCP/IP：** 简单网络管理协议SNMP V1、SNMP V2、SNMP V3三种版本。
- ③**基于局域网：** 远程监控网络RMON，RMON-1、RMON-2两个版本。
- ④**IEEE制定：** 基于物理层和数据链路层CMOL。
- ⑤**ITU-T：** 电信网络管理标准TMN。

6



- **考点06：**SNMP：简单网络管理协议：应用层协议，采用UDP，不会增加网络负担，效率高。UDP161（代理）、UDP162（管理站）。

- **考点07：**SNMPv1：四种报文①GetRequest、②GetNextRequest、③SetRequest、④Trap、⑤GetResponse。

其中④用于事件报告，

⑤用于代理站。

采用团体明文认证。

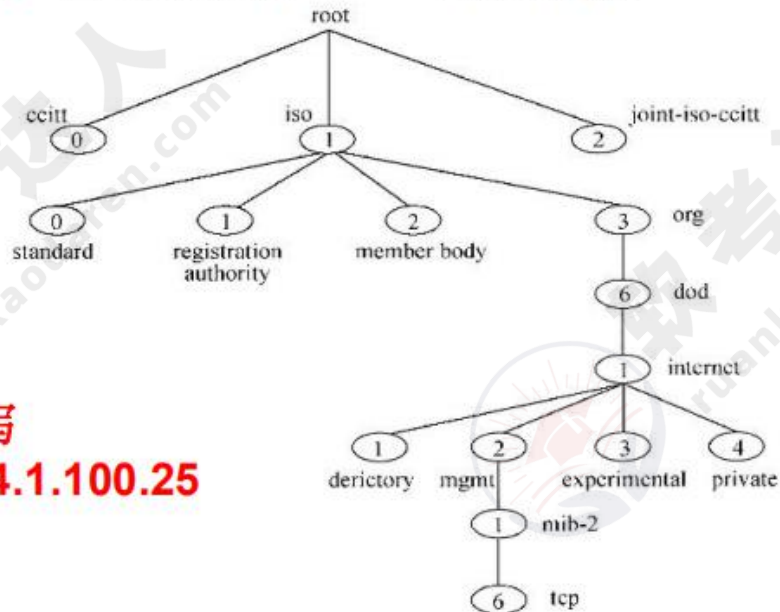


- **考点08：**SNMPv2：又叫SNMPv2c，支持集中，也支持分布式管理。

- 增强改进3方面：①管理里信息结构的扩充。②管理站之间的通信能力。③新的协议操作。Get BulkRequest块操作、InformRequest通信请求。

- **考点09：**SNMPv3：把管理和代理统一叫做实体（包括引擎和应用），并提供认证和加密。基于用户的安全模型，把安全威胁分为主要的和次要的。基于视图的访问控制模型，划分安全级别。

● **考点10：**管理信息库MIB-2树形结构：



反推正写

1.3.6.1.4.1.100.25

11

● **考点11：**管理信息库MIB-2的10个功能组：

- system：关于系统的总体信息。
- interfaces：系统到子网接口的信息。
- at(address translation)：描述 Internet 到子网的地址映射。
- ip：关于系统中 IP 的实现和运行信息。
- icmp：关于系统中 ICMP 的实现和运行信息。
- tcp：关于系统中 TCP 的实现和运行信息。
- udp：关于系统中 UDP 的实现和运行信息。
- egp：关于系统中 EGP 的实现和运行信息。
- dot3(transmission)：有关每个系统接口的传输模式和访问协议的信息。
- snmp：关于系统中 SNMP 的实现和运行信息。

12

## ● 考点12：远程网络监控RMON的管理信息库：

rmon (mib-2 16)

### ● 先事件组再 警报组

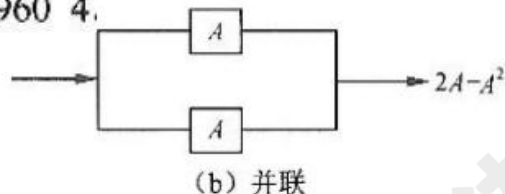
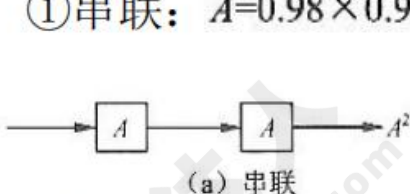
### ● 先主机组再 N台主机组

### ● 先过滤组再 捕获组

- statistics(1)以太网的统计信息
- 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

## ● 考点13：网络管理常考零部件可靠性计算：

① 串联： $A=0.98 \times 0.98=0.9604$



② 并联： $A=2 \times 0.98 - 0.98 \times 0.98 = 1.96 - 0.9604 = 0.9996$

$$R=1-(1-R1) \times (1-R2) \times (1-R3) \times \dots \times (1-Rn)$$

### ● 轮询设备和时间计算：

$$N \leq T/\Delta = 15 \times 60 / 0.202 = 4500$$

$N$ ——被轮询的代理数；

$T$ ——轮询间隔；

$\Delta$ ——单个轮询需要的时间。



- **考点14：**网络管理命令：ipconfig，同winipcfg，用来查看网络配置信息，如IP地址、子网掩码、网关IP、DNS、DHCP等。

| 选 项         | 描 述                                                                                            |
|-------------|------------------------------------------------------------------------------------------------|
| /all        | 显示所有适配器的完整 TCP/IP 配置信息。在没有该参数的情况下，只显示 IP 地址、子网掩码和各个适配器的默认网关值                                   |
| /renew      | 更新所有适配器或特定适配器的 DHCP 配置。仅在具有配置为自动获取 IP 地址的网卡的计算机上可用                                             |
| /release    | 发送 DHCPRELEASE 消息到 DHCP 服务器，以释放所有适配器或特定适配器的当前 DHCP 配置并丢弃 IP 地址配置。同样仅在具有配置为自动获取 IP 地址的网卡的计算机上可用 |
| /flushdns   | 清理并重设 DNS 客户解析器缓存的内容                                                                           |
| /displaydns | 显示 DNS 客户解析器缓存的内容，包括从本地主机文件预装载的记录以及由计算机解析的名称查询而最近获得的任何资源记录                                     |

```

Windows IP Configuration

Host Name : x4ep512rdszujzp
Primary Dns Suffix :
Node Type : Unknown
IP Routing Enabled. : Yes
WINS Proxy Enabled. : Yes

Ethernet adapter 本地连接:

Connection-specific DNS Suffix . :
Description : SiS 900-Based PCI Fast Ethernet Adapter
Physical Address. : 08-03-0D-07-03-7F
DHCP Enabled. : Yes
Autoconfiguration Enabled . . . : Yes
IP Address. : 100.100.17.24
Subnet Mask : 255.255.255.0
Default Gateway : 100.100.17.254
DHCP Server : 192.168.254.10
DNS Servers : 218.30.19.40
 61.134.1.4
Lease Obtained. : 2009年1月5日 8:10:14
Lease Expires : 2009年1月5日 12:10:14

```

- **考点15：**网络管理命令：ping。利用ICMP报文来测试网络的连通性、是否丢包、名称解析等。例如：ping 127.0.0.1 检查TCP/IP协议、ping 本机IP 检查网卡工作、ping 网关 等。

| 选 项      | 描 述                                                           |
|----------|---------------------------------------------------------------|
| -t       | 中断前持续发送回响请求信息到目的地，按 Ctrl+Break 组合键中断并显示统计信息，按 Ctrl+C 组合键中断并退出 |
| -a       | 对目的 IP 地址进行反向名称解析，若解析成功，将显示相应的主机名                             |
| -n Count | 指定发送回响请求消息的次数。默认值为 4                                          |
| -l Size  | 指定发送消息中“数据”字段的长度。默认值为 32B，最大值是 65 527B                        |
| -f       | 指定发送的回响请求消息带有“不要拆分”标志，用于检测并解决“路径最大传输单位(PMTU)”的故障              |

18

```
C:\Documents and Settings\Administrator>ping www.163.com.cn

Pinging www.163.com.cn [219.137.167.157] with 32 bytes of data:

Reply from 219.137.167.157: bytes=32 time=29ms TTL=54
Reply from 219.137.167.157: bytes=32 time=29ms TTL=54
Reply from 219.137.167.157: bytes=32 time=29ms TTL=54
Reply from 219.137.167.157: bytes=32 time=29ms TTL=54
```

```
C:\Documents and Settings\Administrator>PING 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.1:
 Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

- **考点16：**网络管理命令：arp。用于显示和修改ARP缓存中的表项。-s参数可以绑定IP和MAC以防止ARP病毒，如arp -s 192.168.1.1 AA-00-4F-2A-9C。但重启后会丢失，如果写入注册表是个永久的办法。

| 选 项 | 描 述               |
|-----|-------------------|
| -a  | 显示所有接口的当前ARP缓存表   |
| -d  | 删除ARP缓存表项         |
| -s  | 绑定ARP表项，如IP和MAC绑定 |

20

```
C:\Documents and Settings\Administrator>arp -a

Interface: 100.100.17.17 --- 0x10003
Internet Address Physical Address Type
100.100.17.254 00-0f-e2-29-31-c1 dynamic

C:\Documents and Settings\Administrator>arp -s 202.117.17.254 00-1c-4f-52-2a-8c

C:\Documents and Settings\Administrator>arp -a

Interface: 100.100.17.17 --- 0x10003
Internet Address Physical Address Type
100.100.17.72 00-1c-8c-ad-f9-ce dynamic
100.100.17.75 00-40-d0-53-bf-86 dynamic
100.100.17.254 00-0f-e2-29-31-c1 dynamic
202.117.17.254 00-1c-4f-52-2a-8c static

Microsoft Windows [版本 5.2.3790]
(C) 版权所有 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator>arp -s 192.168.1.1 00-0e-a0-5b-63-75

C:\Documents and Settings\Administrator>
```



- **考点17：**网络管理命令：**netstat**。用来显示网络活动状态，如TCP/UDP的IP、端口号，统计信息等。一些参数可结合使用。

| 选 项         | 描 述                                 |
|-------------|-------------------------------------|
| -a          | 显示所有活动的 TCP 连接以及计算机侦听的 TCP 和 UDP 端口 |
| -e          | 显示以太网统计信息，如发送和接收的字节数、数据包数。          |
| -n          | 显示活动的 TCP 连接，不过，只以数字形式表现地址和端口号      |
| -o          | 显示活动的 TCP 连接并包括每个连接的进程 ID(PID)。     |
| -p Protocol | 显示 Protocol 所指定的协议的连接。              |
| -s          | 按协议显示统计信息。默认显示 TCP、UDP、ICMP 和 IP    |
| -r          | 显示 IP 路由表的内容。该参数与 route print 命令等价  |

```
C:\Documents and Settings\Administrator>netstat -o 4
```

Active Connections

| Proto | Local Address        | Foreign Address     | State    | PID  |
|-------|----------------------|---------------------|----------|------|
| TCP   | x4ep512rdszwjzp:1172 | 121.11.159.208:http | SYN_SENT | 1572 |

Active Connections

| Proto | Local Address        | Foreign Address     | State    | PID  |
|-------|----------------------|---------------------|----------|------|
| TCP   | x4ep512rdszwjzp:1173 | 121.11.159.208:http | SYN_SENT | 1572 |

Active Connections

| Proto | Local Address        | Foreign Address     | State    | PID  |
|-------|----------------------|---------------------|----------|------|
| TCP   | x4ep512rdszwjzp:1173 | 121.11.159.208:http | SYN_SENT | 1572 |

Active Connections

| Proto | Local Address        | Foreign Address    | State       | PID  |
|-------|----------------------|--------------------|-------------|------|
| TCP   | x4ep512rdszwjzp:1176 | 124.115.3.126:http | ESTABLISHED | 3096 |
| TCP   | x4ep512rdszwjzp:1178 | 124.115.6.52:http  | ESTABLISHED | 3096 |
| TCP   | x4ep512rdszwjzp:1179 | 124.115.6.52:http  | ESTABLISHED | 3096 |
| TCP   | x4ep512rdszwjzp:1180 | 124.115.6.52:http  | ESTABLISHED | 3096 |
| TCP   | x4ep512rdszwjzp:1182 | 124.115.3.126:http | ESTABLISHED | 3096 |
| TCP   | x4ep512rdszwjzp:1183 | 124.115.6.52:http  | ESTABLISHED | 3096 |
| TCP   | x4ep512rdszwjzp:1184 | 124.115.6.52:http  | ESTABLISHED | 3096 |
| TCP   | x4ep512rdszwjzp:1185 | 222.73.73.173:http | ESTABLISHED | 3096 |
| TCP   | x4ep512rdszwjzp:1186 | 222.73.78.14:http  | SYN_SENT    | 3096 |

- **考点18：**网络管理命令：tracert。利用ICMP报文，来探测到达目标的路径。通常配合-d。

```
C:\Documents and Settings\Administrator>tracert www.163.com.cn

Tracing route to www.163.com.cn [219.137.167.157]
over a maximum of 30 hops:

 0 26 ms 15 ms 11 ms 100.100.17.254
 1 <1 ms <1 ms <1 ms 254.20.168.128.cos.it-comm.net [128.168.20.254]
 2 <1 ms <1 ms <1 ms 61.150.43.65
 3 <1 ms <1 ms <1 ms 222.91.155.5
 4 <1 ms <1 ms <1 ms 125.76.189.81
 5 1 ms <1 ms <1 ms 61.134.0.13
 6 28 ms 28 ms 28 ms 202.97.35.229
 7 28 ms 29 ms 29 ms 61.144.3.17
 8 29 ms 29 ms 32 ms 61.144.5.9
 9 32 ms 32 ms 32 ms 219.137.11.53
 10 29 ms 29 ms 28 ms 219.137.167.157

Trace complete.
```

- **考点19：**网络管理命令：pathping。把ping和tracert结合起来，探测路径、延时、丢包率等。
- 网络管理命令：nbtstat。用来显示NetBIOS的名称缓存。
- 网络管理命令：route。显示修改本地IP路由表。add添加、delete删除、change修改、print显示路由表（同netstat -r）。
- 网络管理命令：netsh。命令行脚本程序，可修改计算机的网络配置。
- 网络管理命令：net。管理网络服务。

25

```

Tracing route to corp1 [10.54.1.196]
over a maximum of 30 hops:
 0 172.16.87.35
 1 172.16.87.218
 2 192.168.52.1
 3 192.168.80.1
 4 10.54.247.14
 5 10.54.1.196
Computing statistics for 125 seconds...

```

| Hop | RTT  | Source to Here<br>Lost/Sent = Pct | This Node/Link<br>Lost/Sent = Pct | Address       |
|-----|------|-----------------------------------|-----------------------------------|---------------|
| 0   |      |                                   |                                   | 172.16.87.35  |
| 1   | 41ms | 0/ 100 = 0%                       | 0/ 100 = 0%                       | 172.16.87.218 |
| 2   | 22ms | 16/ 100 = 16%                     | 3/ 100 = 3%                       | 192.168.52.1  |
| 3   | 24ms | 13/ 100 = 13%                     | 0/ 100 = 0%                       | 192.168.80.1  |
| 4   | 21ms | 14/ 100 = 14%                     | 1/ 100 = 1%                       | 10.54.247.14  |
| 5   | 24ms | 13/ 100 = 13%                     | 0/ 100 = 0%                       | 10.54.1.196   |

```

Trace complete.

```

- **考点20：**网络管理命令：**nslookup**。用来测试DNS服务器域名解析的。交互式和非交互式。

(1) 应用默认的 DNS 服务器根据域名查找 IP 地址。

```
C:\>nslookup ns1.isi.edu
```

```
Server: ns1.domain.com
```

```
Address: 202.30.19.1
```

```
Non-authoritative answer:
```

#给出应答的服务器不是该域的权威服务器

```
Name: ns1.isi.edu
```

```
Address: 128.9.0.107
```

#查出的 IP 地址

27



- 网络管理命令：nslookup非交互式。

(2) 应用默认的 DNS 服务器根据 IP 地址查找域名。

```
C:\>nslookup 128.9.0.107
```

```
Server: ns1.domain.com
```

```
Address: 202.30.19.1
```

```
Name: ns1.isi.edu
```

#查出的 IP 地址

```
Address: 128.9.0.107
```

- 网络管理命令：nslookup交互式。

(2) set type=mx：这个命令查询本地域的邮件交换器信息。

```
C:\> nslookup
```

```
Default Server: ns1.domain.com
```

```
Address: 202.30.19.1
```

```
> set type=mx
```

```
> 163.com.cn
```

```
Server: ns1.domain.com
```

```
Address: 202.30.19.1
```

```
Non-authoritative answer:
```

```
163.com.cn MX preference = 10, mail exchanger =mx1.163.com.cn
```

```
163.com.cn MX preference = 20, mail exchanger =mx2.163.com.cn
```

```
mx1.163.com.cn internet address = 61.145.126.68
```

```
mx2.163.com.cn internet address = 61.145.126.30
```

29

- 网络管理命令：nslookup交互式。

(3) server NAME: 由当前默认服务器切换到指定的名字服务器 NAME。

```
C:\> nslookup
Default Server: ns1.domain.com
Address: 202.30.19.1
> server 202.30.19.2
Default Server: ns2.domain.com
Address: 202.30.19.2
```

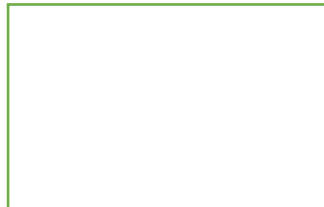
- (4) set type=any显示所有的资源记录。A、PTR、MX、CNAME、NS、SOA等。

30

- **考点20：**网络管理命令：nslookup。用来测试DNS服务器域名解析的。交互式和非交互式。

(1) 应用默认的DNS服务器根据域名查找IP地址。

```
C:\>nslookup ns1.isi.edu
Server: ns1.domain.com
Address: 202.30.19.1
```



Non-authoritative answer:

#给出应答的服务器不是该域的权威服务器

Name: ns1.isi.edu

Address: 128.9.0.107

#查出的IP地址

27

- 网络管理命令：nslookup非交互式。

(2) 应用默认的 DNS 服务器根据 IP 地址查找域名。

```
C:\>nslookup 128.9.0.107
Server: ns1.domain.com
Address: 202.30.19.1
```

Name: ns1.isi.edu

#查出的 IP 地址

Address: 128.9.0.107

- 网络管理命令：nslookup交互式。

(2) set type=mx：这个命令查询本地域的邮件交换器信息。

```
C:\> nslookup
Default Server: ns1.domain.com
Address: 202.30.19.1
> set type=mx
> 163.com.cn
Server: ns1.domain.com
Address: 202.30.19.1
Non-authoritative answer:
163.com.cn MX preference = 10, mail exchanger =mx1.163.com.cn
163.com.cn MX preference = 20, mail exchanger =mx2.163.com.cn
mx1.163.com.cn internet address = 61.145.126.68
mx2.163.com.cn internet address = 61.145.126.30
```

29



- 网络管理命令：nslookup交互式。

(3) server NAME: 由当前默认服务器切换到指定的名字服务器 NAME。

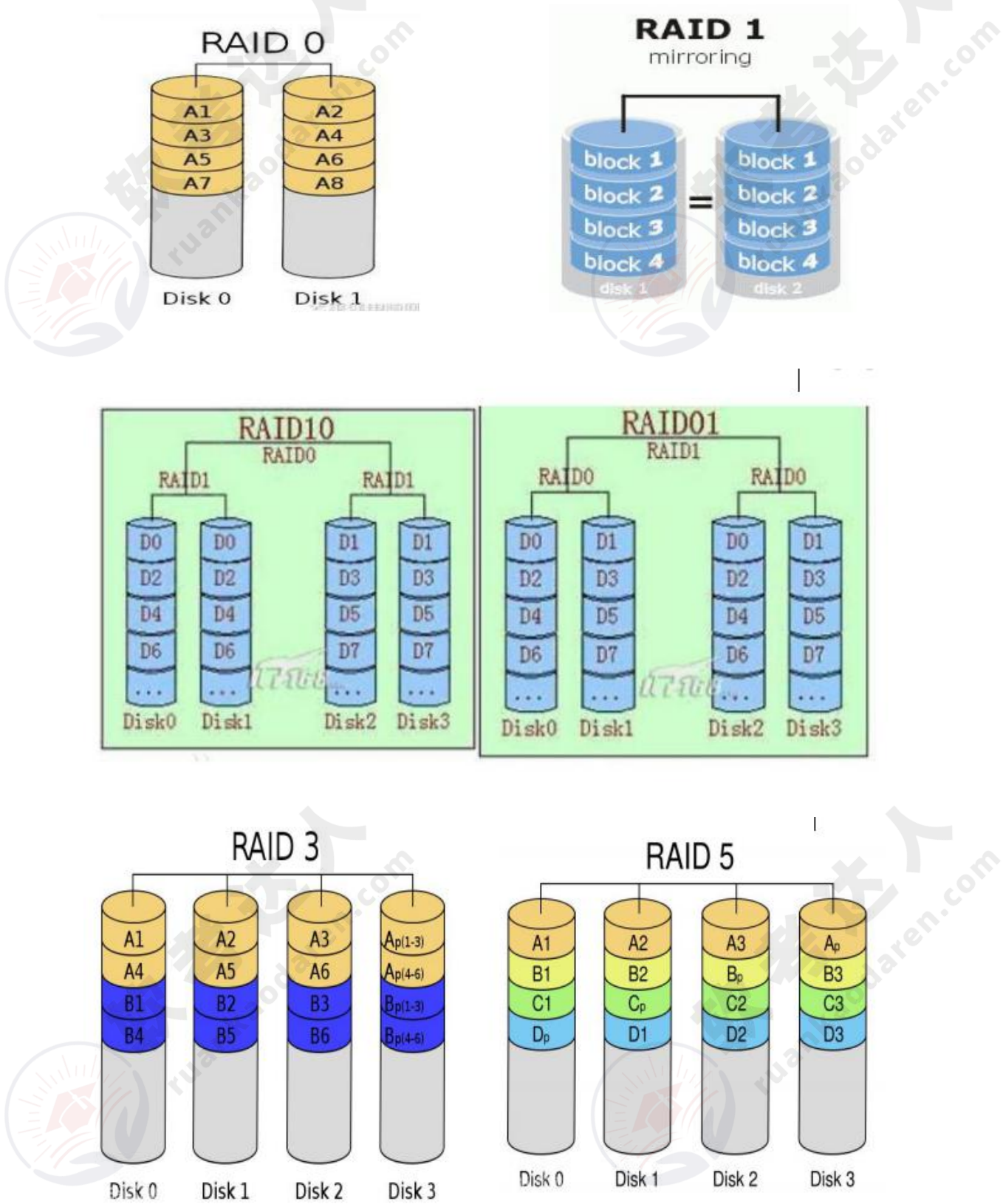
```
C:\> nslookup
Default Server: ns1.domain.com
Address: 202.30.19.1
> server 202.30.19.2
Default Server: ns2.domain.com
Address: 202.30.19.2
```

- (4) set type=any显示所有的资源记录。A、PTR、MX、CNAME、NS、SOA等。

30

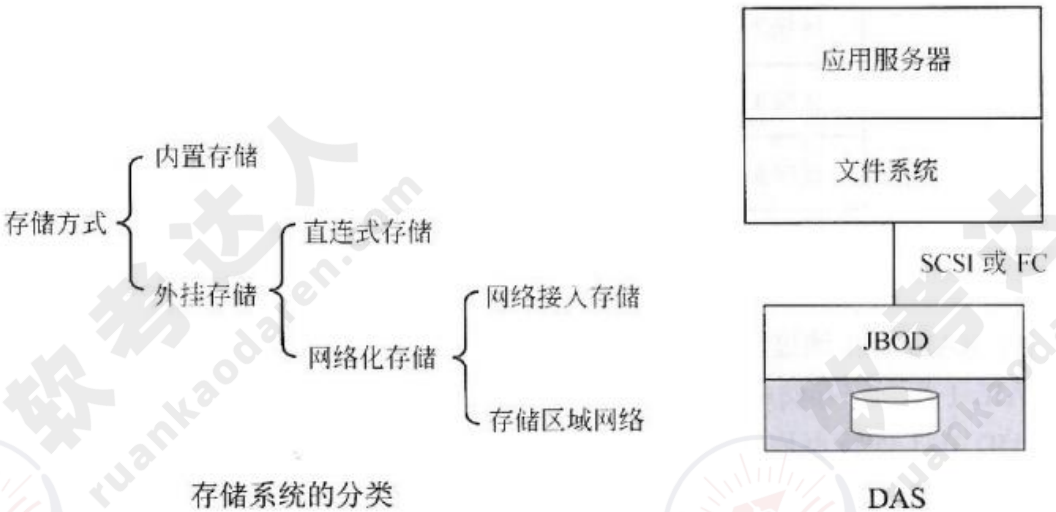
- **考点21：**网络管理工具：网络嗅探器sniffer、HP Open View、IBM Tivoli、Cisco Works。
- 混杂模式：需要通过sniffer软件设置网卡为混杂模式，接受全网流量，进行抓包分析，网络监测和控制。
- 镜像端口：通过在交换机或路由器上，将一个或多个源端口的数据流量转发到某一个指定端口来实现对网络的监听，称之为“镜像端口”。

- **考点22：**网络存储技术：RAID，廉价磁盘冗余阵列。RAID0 ~ RAID50多种。RAID卡。



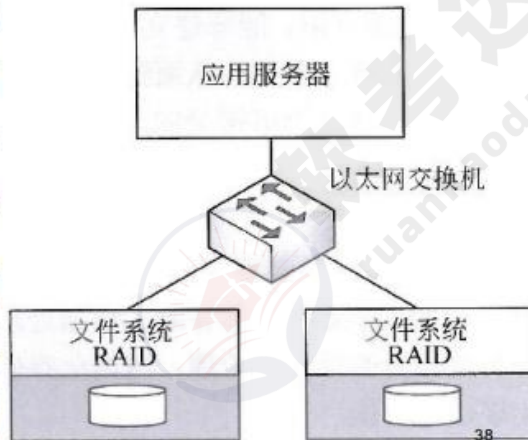
| RAID 级别 | RAID-0                   | RAID-1                     | RAID-3                      | RAID-5                       | RAID-10                |
|---------|--------------------------|----------------------------|-----------------------------|------------------------------|------------------------|
| 别名      | 条带                       | 镜像                         | 专用奇偶位条带                     | 分布奇偶位条带                      | 镜像阵列条带                 |
| 容错性     | 没有                       | 有                          | 有                           | 有                            | 有                      |
| 冗余类型    | 没有                       | 复制                         | 奇偶校验                        | 奇偶校验                         | 复制                     |
| 热备盘选项   | 没有                       | 有                          | 有                           | 有                            | 有                      |
| 需要的磁盘数  | 一个或多个                    | 只需 2 个或 $2 \times N$ 个     | 三个或更多                       | 三个或更多                        | 只需 4 个或 $4 \times N$ 个 |
| 可用容量    | 总的磁盘的容量                  | 只能用磁盘容量的 50%               | $(n-1)/n$ 的磁盘容量。其中 $n$ 为磁盘数 | $(n-1)/n$ 的总磁盘容量。其中 $n$ 为磁盘数 | 磁盘容量的 50%              |
| 典型应用    | 无故障的迅速读写，要求安全性不高，如图形工作站等 | 随机数据写入，要求安全性高，如服务器、数据库存储领域 | 连续数据传输，要求安全性高，如视频编辑，大型数据库等  | 随机数据传输，要求安全性高，如金融，数据库，存储等    | 要求数据量大，安全性高，如银行，金融等领域  |

● 考点23：网络存储技术：直连式存储DAS

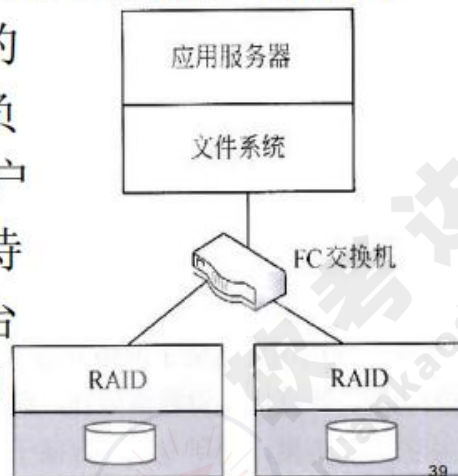




- **考点24：**网络存储技术：**NAS**网络接入存储。将存储设备连接到现有的网络上提供数据存储和文件访问服务的设备。**NAS**服务器是在专用主机上安装简化了的瘦操作系统（只具有访问权限控制、数据保护和恢复等功能）的文件服务器。**NAS**服务器内置了与网络连接所需要的协议，可以直接联网

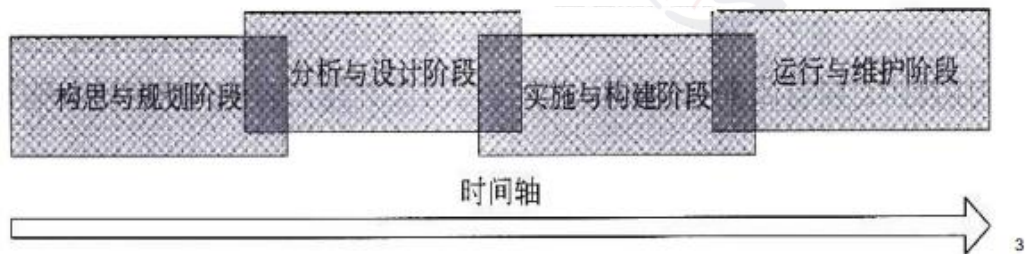


- **考点25：**网络存储技术：**SAN**存储区域网络。是一种连接存储设备和存储管理子系统的专用网络，专门提供数据存储和管理功能。**SAN**可以被看作是负责数据传输的后端网络，而前端网络则负责正常的TCP/IP传输。用户也可以把**SAN**看作是通过特定的互连方式连接的若干台存储服务器组成。分为2种结构：**IP SAN**与**FC SAN**。



## 第十二章：网络规划与设计

- **考点01：**网络系统生命周期：从构思到淘汰。
- 四阶段周期（重叠）：能够快速适用新的需求变化，成本低，灵活性好，适用网络规模较小，需求较为明确，网络结构简单的工程项目。  
（口诀：小明花钱少。）

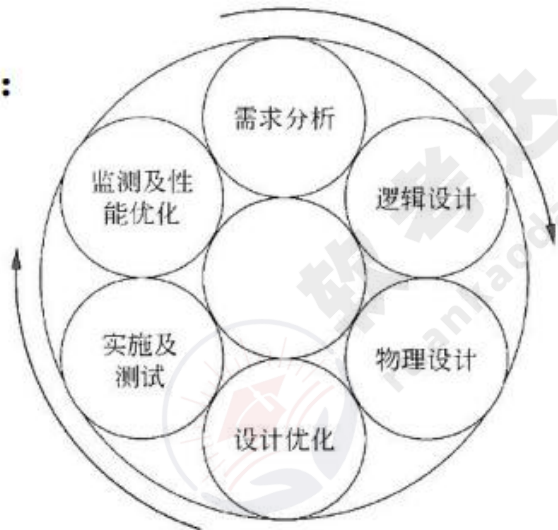


- **考点02：**网络系统生命周期：从构思到淘汰。
- 五阶段周期（瀑布）：比较死板，不灵活，较为严谨，适用于网络规模大，需求较为明确，需求变更较小的网络工程。常用此模型。  
（口诀：大明看瀑布。）



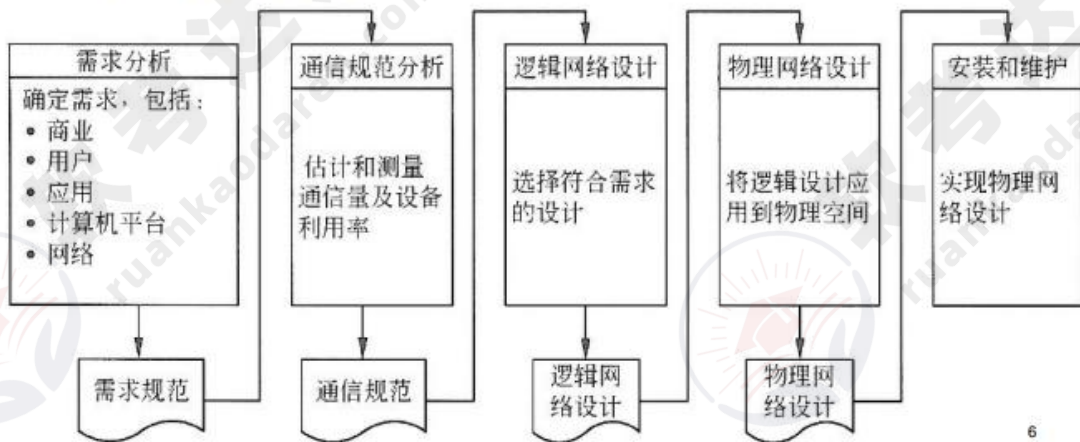
● **考点03：**网络系统生命周期：从构思到淘汰。

- 六阶段周期（测试）：  
偏重于测试和优化，  
适合大型网络，适  
合经常变更。



5

- **考点04：**网络开发过程：其中，通信规范分析又叫现有网络体系分析。以便在升级时尽量保护已有的投资。



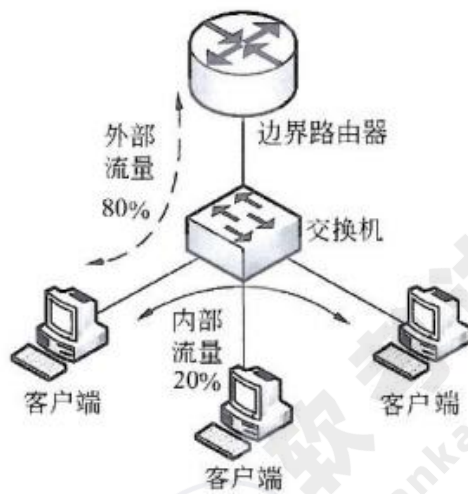
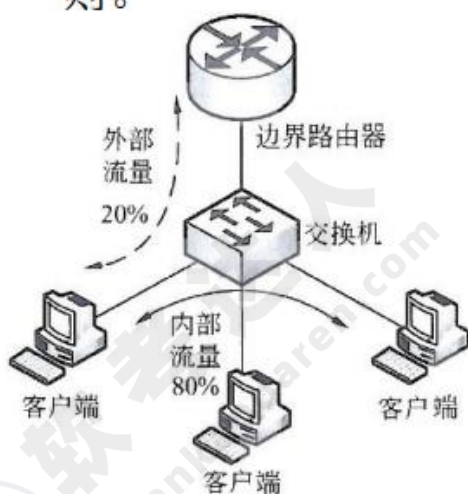
6



- **考点05：**通信流量模式分析：对等模式、C/S模式、B/S模式。
- 对等模式：双向对等，如QQ、BT、P2P等。
- C/S模式：S→C流量大，如VOD、Web服务器、ERP。C→S流量大，如SNMP。双向流量大，如FTP、邮件服务器、数据库服务器。
- B/S模式：S→B流量大，而web服务器与数据库则属于双向流量大。

8

- **考点06：**通信流量分析方法：80/20、20/80规则。



9

- **考点07：**通信流量计算公式：分为两种，如下
- 某个业务应用网络流量的计算公式为：应用的数据传输速率 = 平均事务量大小 × 每字节位数 × 每个会话事务数 × 平均用户数 / 平均会话长度。
- 考虑峰值用户数和应用增长率等因素后公式为：应用的数据传输速率 = 平均事务量大小 × 每字节位数 × 每个会话事务数 × 峰值用户数 × (1+增长率) / 平均会话长度。

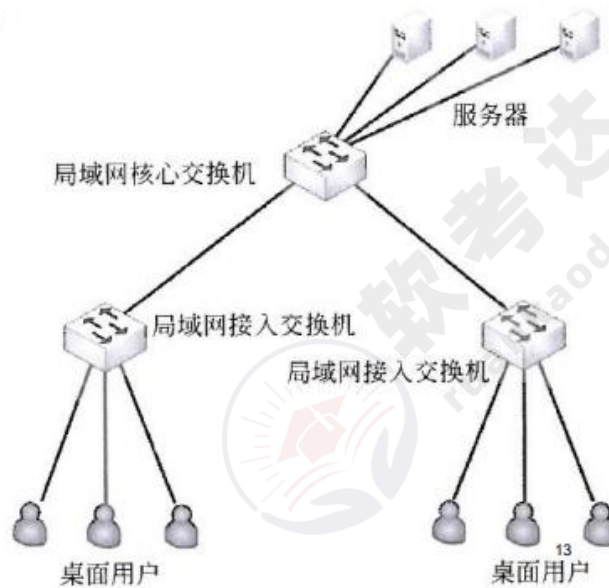
10

- **考点08：**逻辑网络设计工作内容：

- (1) 网络结构的设计。
- (2) 物理层技术的选择。
- (3) 局域网技术的选择与应用。
- (4) 广域网技术的选择与应用。
- (5) 地址设计和命名模型。
- (6) 路由选择协议。
- (7) 网络管理。
- (8) 网络安全。
- (9) 逻辑网络设计文档。

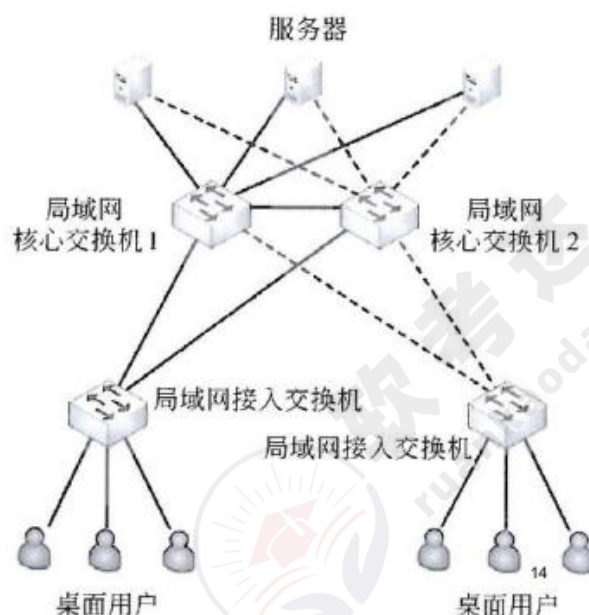
● **考点09：**局域网结构设计：单核心局域网结构

- 单核心简单、投资少、地理范围小，适合小型网络。
- 缺点是单点故障，导致全网失效。扩展能力有限。
- 桌面用户不应与核心连接。



● **考点10：**局域网结构设计：双核心局域网结构

- 可做负载均衡热备，如HSRP、VRRP、GLBP。可靠性高、可热切换、接入方便、服务器直连核心，高速访问。
- 投资高、维护技术高。



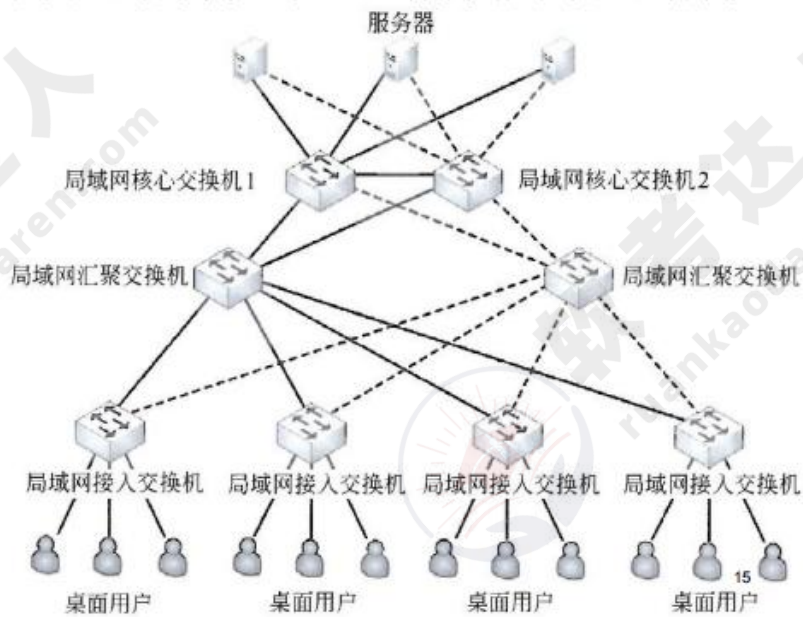


# ● 考点11：局域网结构设计：三层次局域网结构

● 核心层：  
高速转发

● 汇聚层：  
策略控制

● 接入层：  
用户接入

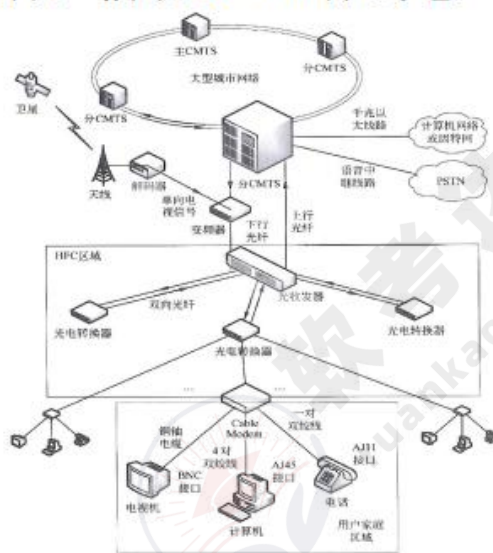


# ● 考点12：广域网结构设计：线缆调制解调器接入网，广电网络属于这种，借助CATV有线电视实现。

● 局端设备为CMTS，  
客户Cable Modem

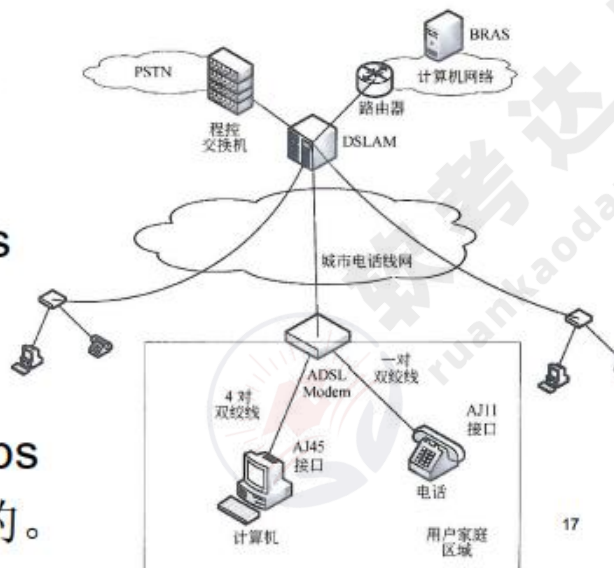
● 下行50Mbps，上行  
3Mbps。

● 采用HFC技术，光纤  
/铜缆混合传输。



- **考点13：**广域网结构设计：数字用户环路远程接入网xDSL，电信网络属于这种，借助电话线实现。

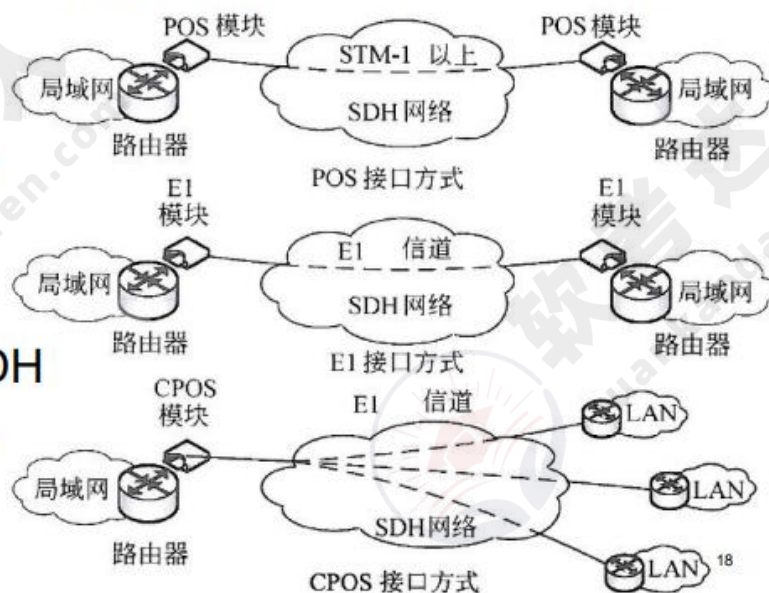
- 局端DSLAM，客户端ADSL Modem。
  - ADSL：下行8Mbps
  - SDSL：下1.544M
  - HDSL：下2.048M
  - VDSL：下行50Mbps
- 口诀：AVRC不对称的。



- **考点14：**广域网结构设计：同步数字体系接入网SDH。

- STM-1：  
155.520M

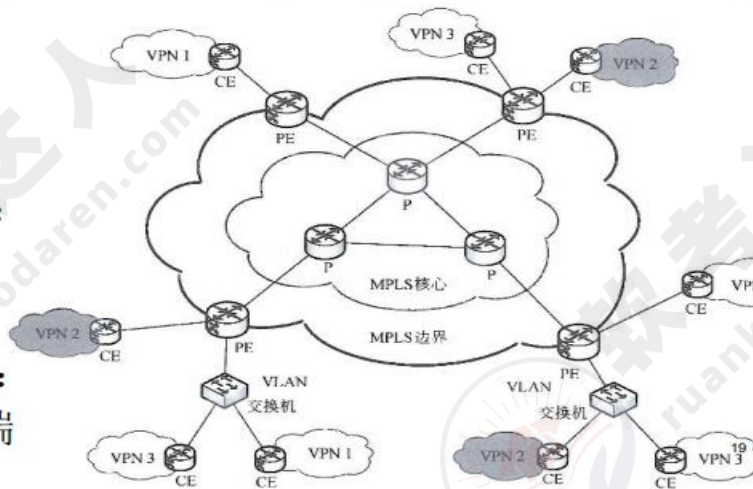
- IP over SDH
- PDH兼容：  
63个2M。





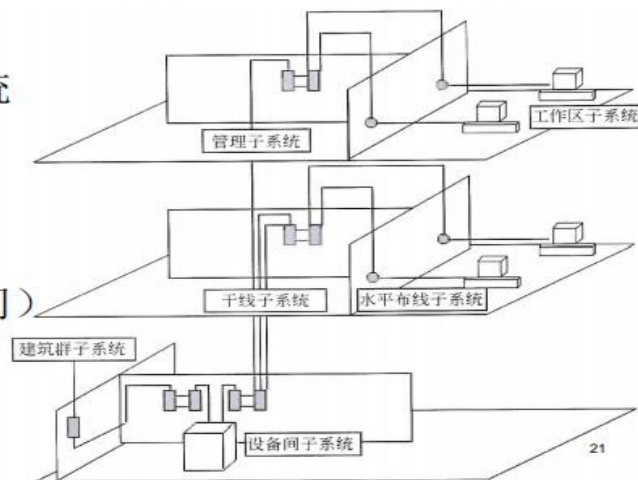
● **考点15：** MPLS VPN接入网：利用MPLS实现。

- **P设备：**  
核心高速转发
- **PE设备：**  
边缘路由标签
- **CE设备：**  
连客户端



● **考点16：** 建筑物综合布线系统PDS：

- ①工作区子系统
- ②水平布线子系统  
(90m+10m)
- ③干线子系统
- ④设备间子系统  
(机房，楼层中间)
- ⑤管理子系统  
(楼层配线间)
- ⑥建筑群子系统



● **考点17：** 综合布线性能参数：双绞线、光纤。

- **衰减值：** 由于绝缘损耗、连接电阻等因素，造成信号沿链路传输损失。
- **近端串扰：** 当信号在一个线对上传输时，会同时将一小部分信号感应到其他线对上，这种感应信号成为串扰。
- **光纤：** 包括连通性、输入/输出功率、衰减/损耗，一般应在20db以内，超过25db不通。



