

第1章 计算机网络概论

笔记本: 网络工程师学习

创建时间: 2015/1/13 21:58

更新时间: 2015/1/21 11:41

URL: about:blank

计算机技术与通讯技术结合, 是信息收集、分发、存储、处理和消费的重要载体。

早期的计算机网络

计算机网络的特征:

(1) 资源共享; (2) 分散控制; (3) 分组交换; (4) 采用专门的通讯控制处理机; (5) 分层的网络协议。

点到点: 数据链路层

端到端: 传输层

早期的计算机网络多为终端系统。

计算机网络由通讯线路互相连接的许多计算机技术与通讯技术结合, 是信息收集、分发、存储、处理和消费的重要载体。

早期的计算机网络

计算机网络的特征:

(1) 资源共享; (2) 分散控制; (3) 分组交换; (4) 采用专门的通讯控制处理机; (5) 分层的网络协议。

点到点: 数据链路层

端到端: 传输层

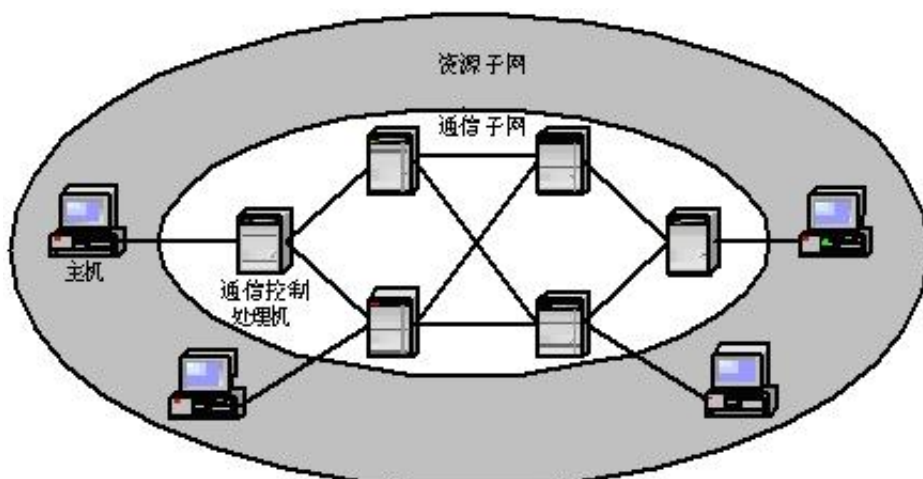
早期的计算机网络多为终端系统。

计算机网络由通讯线路互相连接的许多自主工作的计算机构成。自主工作计算机是为了区分多终端分时系统。在计算机网络中的各个计算机(工作站)本身拥有计算资源, 能独立工作, 能完成一定的计算任务。

比计算机网络更高级的系统是**分布式系统**。

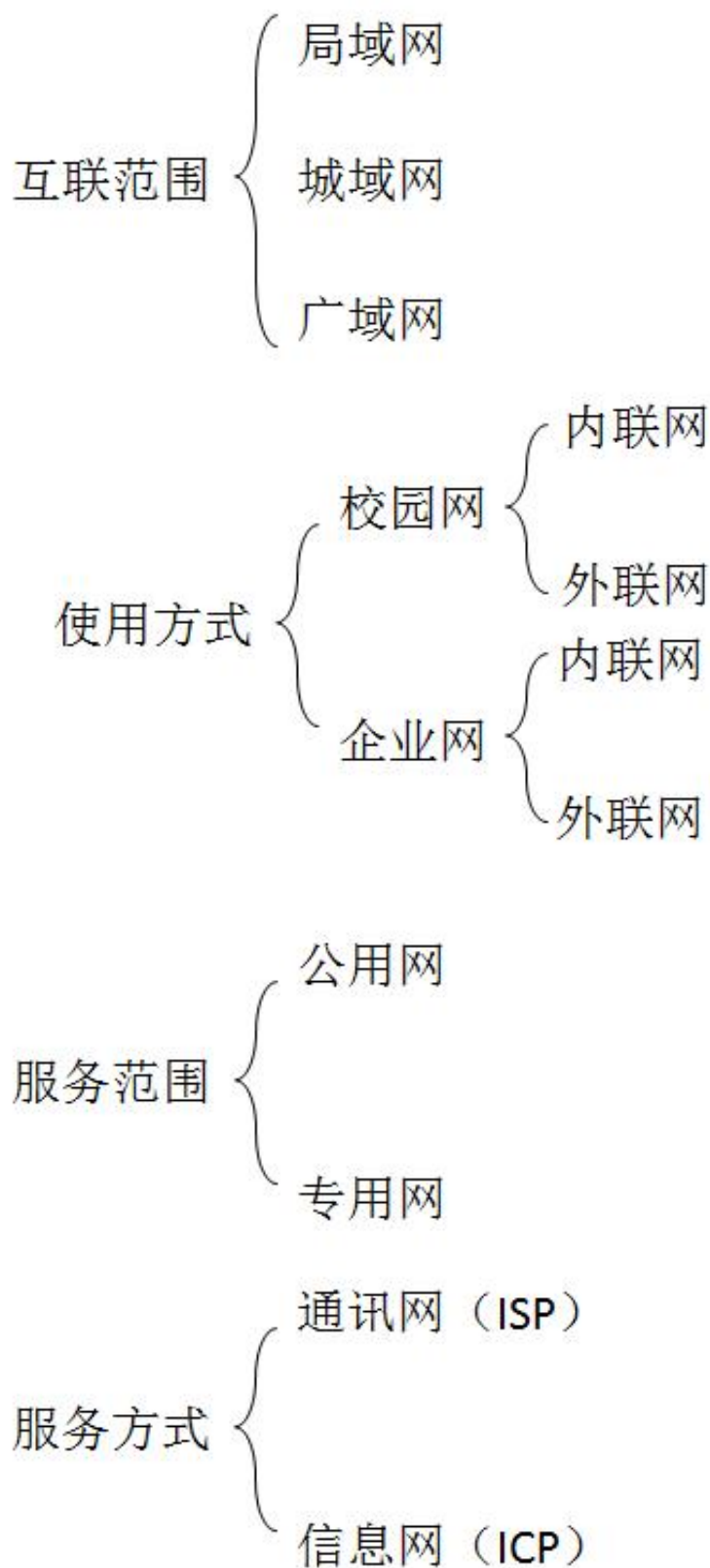
与计算机网络类似的另一种系统是**多机系统**。是同一机房中的许多大型主机互联组成的功能强大, 高速并行处理的计算机系统。

通讯子网与资源子网:



IMP (接口信息处理机 (通讯控制处理机)) 是专门用于通讯的计算机, 这些IMP之间直接连接, 有些IMP直通过其他IMP连接, 这种通讯方式叫做存储转发通讯。在广域网中的通信一般都采用这种方式, 另

局域网 (LAN): 使用分组广播
城域网 (MAN): 使用分组广播
广域网 (WAN): 使用分组交换



网络应用:

1、办公自动化

- 2、电子数据交换
- 3、远程教育
- 4、电子银行
- 5、证券和期货交易
- 6、娱乐和在线游戏

1987年9月20日 在北京发出第一封电子邮件。

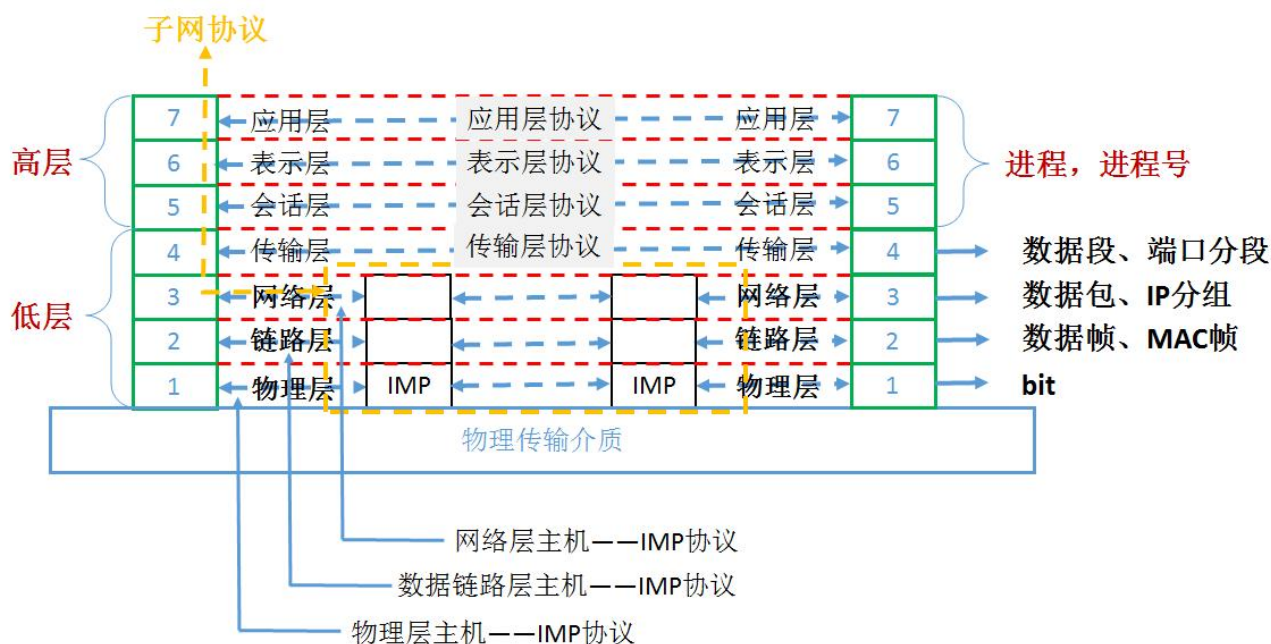
把系统组织成分层的体系结构, 即把很多相关的功能分解开来, 逐个予以解释和实现, 在分层体系机构中有明确定义的相互作用的集合, 即对等协议, 层之间相互作用称为接口协议。

计算机通讯有一个特点, 即间歇性或突发性。

计算机网络的功能之一是对传输的信息流进行**分组**, 加入**控制信息**, 并把分组**正确地**传送到目的地。

加入分组的控制信息主要有**两种**: 一种是接收端用于验证是否正确接收的**差错控制信息**; 另一种是指明数据包的发送端和接收端的地址信息。网络必须具有**差错控制功能**和**寻址功能**。

对等网络之间按规定的协议通讯, 相邻之间按接口关系提供服务和接受服务。把实现复杂的网络通信过程的各种功能划分成这样的层次结构, 就是网络的分层体系结构。



分层的基本想法是每一层都在它的下层提供的服务基础上提供更高级的增值服务, 而最高层提供能运行分布式应用程序的服务。

传输层在网络层服务的基础上增加了端到端的控制功能。

OSI/RM网络体系七层协议主要功能:

1、应用层

OSI的最高层。这一层协议直接为端用户服务, 提供分布式处理环境。包括系统启动、维持和终止, 一个应用是由一些合作的应用进程组成的。(类似物流把快递包裹送到用户手里)。

2、表示层

提供应用层选择的服务集合, 有统一的数据编码、数据压缩格式和加密技术等。(类似物流把订单号统一编码、压缩、加密、定规则)

3、会话层

实体结合在一起, 或者分开, 这叫会话管理。控制实体间的数据交换过程, 例如分段, 同步等, 这叫会话服务。一段一段的进行, 如果一段传错了, 可以回到分界限的地方重新传输。(类似物流快递员打电话联系送货)

4、传输层

传输层用多路复用或分流的方式优化网络的传输效率。

例如**TCP**: 传输层的服务可以提供一条无差错按顺序的端到端连接。

例如**UDP**: 不保证顺序的独立报文传输, 或多个目标报文广播。

传输层协议是真正的源端到目标端的协议, 它由传输连接两端的传输实体处理。

(类似物流司机开车传输配送货物)

5、网络层

可以是固定不变的, 也可以是根据网络的负载情况动态变化的。防止网络中出现局部的拥挤或全面的阻塞。此外网络层还应有记账功能。使异构网络能够互联互通。例如: **RIP**和**OSPF**的互通。(类似物流司机通过导航或地图进行路径选择)

6、数据链路层

各帧按照顺序传送, 并通过接收端的校验检查和应答保证可靠的传输。并把流量控制和差错控制合在一起进行。

7、物理层

这一层规定通信设备机械的、电气的、功能的和过程的特性, 用于建立、维持和释放数据链路实体间的连接。

X.25包括了通信子网最下边的3个逻辑功能层, 即物理层, 链路层和网络层, 与**SNA**的下面三层对应。

OSI协议集

1、物理层协议

在物理层, **OSI**采用了各种现成的协议: **RS-232**、**RS449**、**IEEE802.3**等。。。

2、数据链路层协议

在链路层, **OSI**的协议集也采用了当前流行的协议: **HDLC (X.25)**、**LAP-B**、**IEEE802**的协议。

3、网络层协议

提供了两种服务, 即面向连接的服务和无连接服务。

4、传输层协议

5、会话层协议

6、表示层协议

7、应用层协议

第2章 数据通讯基础

笔记本: 网络工程师学习

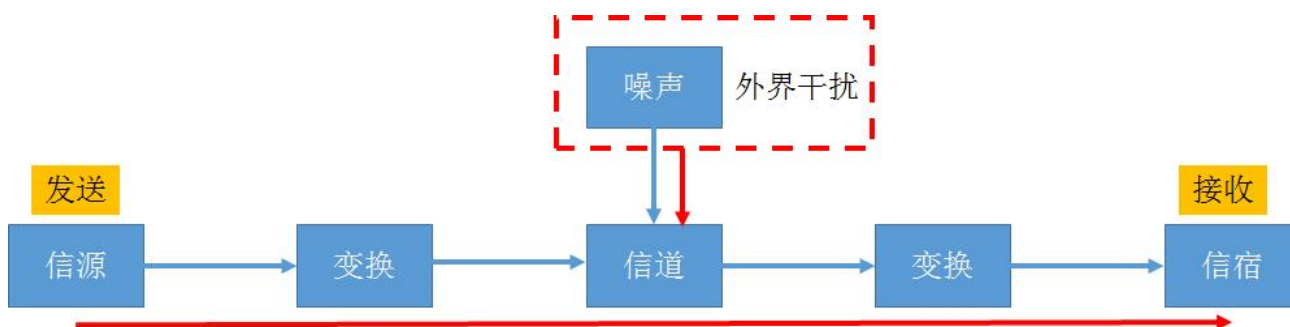
创建时间: 2015/1/21 11:38

更新时间: 2015/1/21 11:41

URL: about:blank

计算机采用数据通信方式传输数据（0和1），与语音通信和无线电广播通信不同。

通信中产生发送信息端叫信源，接收信息端叫信宿，信息在传输中会受到外界干扰，叫噪声。



通讯模式	信源	信道
模拟通信	模拟信号	模拟信道
数字通信	模拟信号	数字信道
数据通信	数字或模拟信号	数字或模拟信道

①模拟信道的带宽：信道带宽 $W = f_2 - f_1$ ， f_2 代表信道能通过的最高频率， f_1 代表信道能通过的最高频率。两者都是由信道的物理特性决定的。

②数字信道是一种离散信道，传送离散值的数字信号。信道带宽决定了信道传输脉冲序列的最高速率。一个数字脉冲为一个码元（ $T=1$ 个码元变化所用的时间），码元速率的单位叫波特（Baud），也叫波特率。

无噪声的极限波特率称为尼奎斯特定理。

$$B = 2W(\text{Baud})$$

由物理信道决定的，不可能超过奈奎斯特极限传送脉冲。

码元携带的信息量 n (位)与码元的种类 N 有如下关系：

$$n = \log_2 N \quad (N = 2^n)$$

N =离散值 n =信息量

$$R = Bn$$

$$R = B \log_2 N = 2W \log_2 N (\text{bps})$$

R为数据速率 B=码元速率

数据速率和波特率是两个不同概念: 仅有当码元取两个离散值时两者才相等, 例如: 普通电话线路, 带宽为3000Hz, 最高波特率为6000Baud。

香农定理 (有噪声信道的极限速率):

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

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 (因取值较大, 通常使用分贝数表示dB)。

分贝与性噪比的关系:

$$dB = 10 \log_{10} \frac{S}{N}$$

例如: 当S/N=1000是, 信噪比为30dB, 无论用什么调制, 只要给定信噪比, 则单位时间内最大信息传输量就确定了, 例如息道带宽为3000Hz, 信噪比为30dB, 最大速率为:

$$C = \frac{3000}{W} \log_2 \left(1 + \frac{1000}{1 + \frac{S}{N}} \right) \approx 3000 \times 9.97 \approx 30000 \text{bps}$$

$\approx 1024 = 2^{10}$

≈ 10

在模拟信道, 带宽按照公式 $W = f_2 - f_1$ 计算。

在数字信道, 带宽为信道能够达到的最大数据速率。(尼奎斯特定理/香农定理)

电缆中的传播速度一般为光速的77%, 即200m/us (200000km/s)。

500m同轴电缆实验大约是2.5us

卫星信道的时延大约为270ms。

双绞线分为屏蔽双绞线和无屏蔽双绞线, 常用的无屏蔽双绞线 (UTP) 和屏蔽双绞线 (STP) 外有铝箔包裹。

同轴电缆

细缆, 50欧姆, 传输数字信号 (基带)。助记: “基本很细50欧”

粗缆, 75欧姆, 传输模拟信号 (CATV)。宽带同轴电缆。

光缆

多模光纤: 多种模式传播, 有不同电磁场分布, 不同传播路径。(粗低短)

单模光纤: 直径小到光波波长大小, 成为波导, 无反射沿直线传播。(细高长)

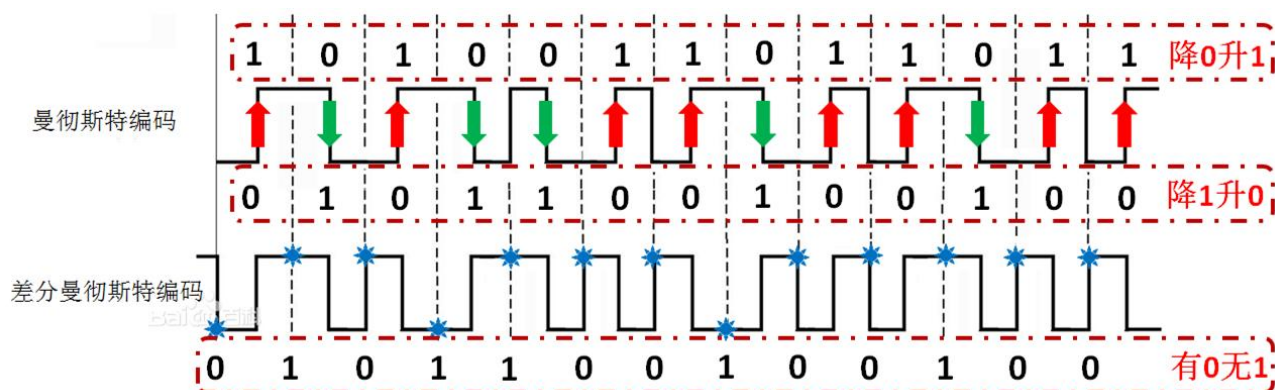
有线信道包括: 双绞线、同轴电缆、光纤等。

数据编码

1、单极性码: +电压表示0, 0电压表示1

2、极性码: +电压表示0, 负电压表示1

3、双极性码: 数据流中遇到1时使电平在正和负之间交替翻转。遇到0时则保持零电平, 与二进制码相比抗噪声特性更好。



曼彻斯特编码: 效率50%, 主要用于以太网中。

差分曼彻斯特编码: 效率50%, 主要用于令牌环网中。

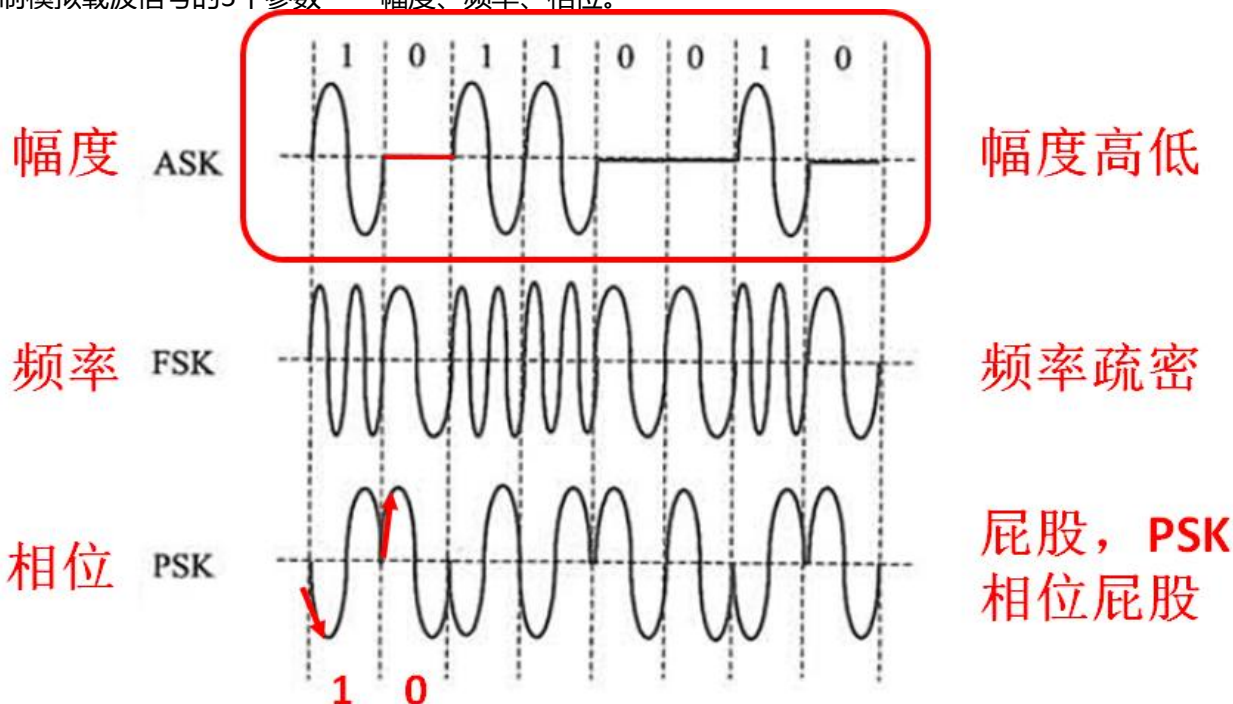
4B/5B编码: 效率80%。

数字调制技术 (数模转换)

数字数据**不仅**可以用方波脉冲传输, 也可以用个模拟信号传输。

数字数据调制模拟=数字调制

调制模拟载波信号的3个参数——幅度、频率、相位。



正交幅度调制 (QAM), 把**两个幅度相同, 但相位相差90度**的模拟信号合成一个模拟信号。

取样速率大于模拟信号最高频率两倍:

编码将量化后的样本值变成相应的二进制代码, 一个二进制代码可以一个脉冲串(4位)来表示, 代表了经PCM编码的模拟信号。

例如: 话音最高频率4KHz, 所以采样速率是8KHz。用128个量化等级, 用7位2进制表示, 速率 $7 \times 8000 = 56\text{Kbps}$ 。

$$\log_2 128 = 7$$

单工通信: 例如电视、广播。

半双工通信: 例如对讲机。

全双工通信: 电话, 手机。

异步传输: 字符分开传, 插入同步信息, 具有远距离、数据少的特点。异步类火车站出口, 同步类似火车站大门

同步传输: 同步传输在传送连续数据块更有效。距离近, 数据大。

交换方式: 电路交换、报文交换和分组交换3种。

电路交换: 一系列链路直接连通(物理线路), 电话交换系统采用。

报文交换: 含有目标节点的地址, 节点接收整个报文。

分组交换: 有固定的长度, 通过数据报(类似报文交换), 虚电路(类似电路交换)建立逻辑连接。

虚电路适合于交互式通信, 这是它从电路交换那里继承的优点, 数据报方式更适合于单向地传送短消息。

多路复用技术: 把多个低速通道组合成一个高速通道的技术。

频分多路复用: 子信道之间留有一定宽度的隔离频带。CATV电缆1000MHz, 可传送多个频道的电视节目, 每个频道两边都留有一定的警戒频带, 防止相互串扰。(不同频率子信道叠加到一个信道上传输)

时分多路复用: 子通道按时间片轮流占用整个带宽。

波分多路复用: 不同子信道用不同波长光波承载。

贝尔系统的**T1载波**, 1.544Mbps。

ITU-T的**E1载波**, 2.048Mbps

E2载波由4个E1载波组成, 速率8.448Mbps。E3载波由4个E2载波组成, 34.368Mbps。E4载波由4个E3载波组成, 速率为139.264Mbps。E5载波由4个E4载波组成, 数据速率为565.148Mbps。

同步数字系列, 光纤线路的多路复用标准有两个, 美国标准: 同步光纤网络(Synchronous Optical

Network, SONET)。ITU-T以SONET为基础制订出的国际标准叫做同步数字系列 (Synchronous Digital Hierarchy, SDH)，基本速率155.52Mbps。

OC-3 155.520Mbps, OC-9=OC-3*3
SDH STM-1 155Mbps。STM-3=STM-1*3

差错控制：差错有两大类：随机错误（热噪声引起），突发错误（冲击噪声（外界电磁干扰）引起）。通信线路中的热噪声是由电子的热运动产生的。

检错码

奇偶校验是最常用的检错方法。

海明码：可检错和纠错。

m位的数据增加k位的冗余位。

$$m + k + 1 < 2^k$$

循环冗余校验码 (CRC)

很强的检错能力，而且容易用硬件实现，在局域网中有广泛应用。

第3章 广域通信网

笔记本: 网络工程师学习

创建时间: 2015/1/21 11:39

更新时间: 2015/1/21 11:39

URL: about:blank

公共交换电话网 (PSTN)

用户电话通过一对铜线连接到最近的局端, 通常1~10km。

4个技术特性: 机械特性, 电气特性, 功能特性, 和过程特性。

机械特性, 物理特性, 如: 外形, 尺寸, 大小 (几何形状, 尺寸大小, 引线数, 引线排列方式及锁定装置)

RS-232-C大多使用9针 (附录建议使用25针D型连接器)

电气特性, V.28标准电路, 信号源产生3~15V的信号, 速率20K, 距离15m。

采用V.10和V.11, V.11是平衡接口, V.10是非平衡输出。

功能特性, 功能给出定义, 数据线、控制线、定时线和地线。TS-232-C采用V.24标准。

过程特性, 操作顺序/操作过程/操作规程。

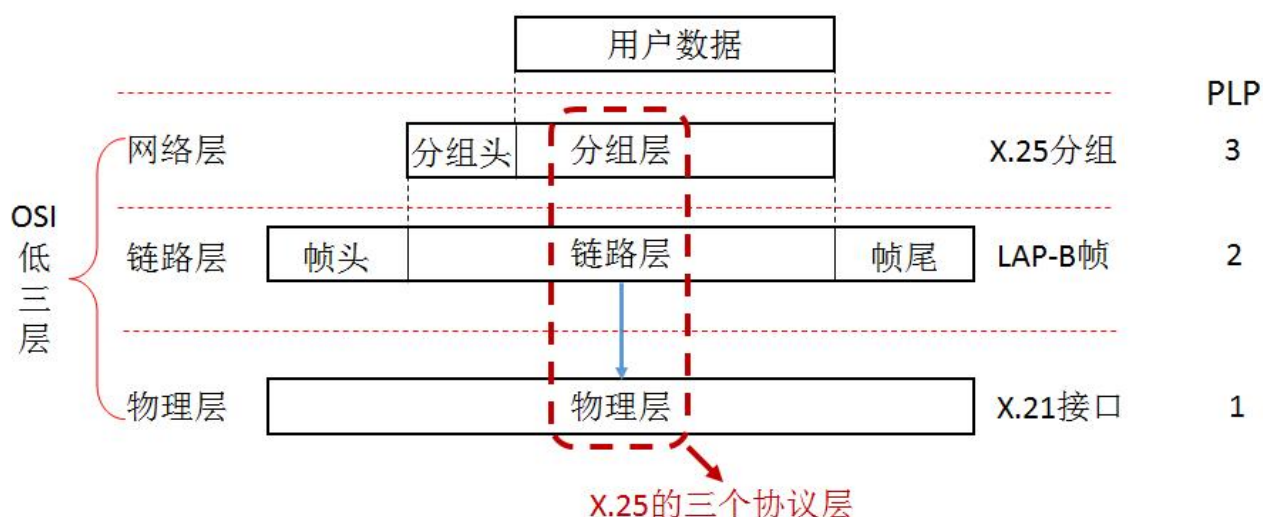
调制解调器 (Modem), 数模/模数 转换。

高速Modem采用格码调制 (TCM) 技术 (V.32)。

56Kbps的Modem, 形成了ITU的V.90建议

V.28(电路电气特性) V.24 (功能特性) V.32 (格码调制) V.90 (速率)

X.25公共数据网, 访问分组交换网的协议标准, 分为3个协议层, 物理层, 链路层, 分组层, 对已ISO/OSI 参考模型的低三层。



流量控制和差错控制 (拥塞控制, 调节速度流量)

流量控制是协调发送站接收站工作步调的技术, 避免发送过快, 使得接收站来不及处理而丢失数据。在没有传输错误下。

1、停等协议 (发送数据、等待回应信号) —— 打报告 (发出), 等领导签字 (应答)

工作原理: 发送站发出一帧, 待应答信号到达后再发送下一帧

2、滑动窗口协议 允许连续发送多个帧而无需等待应答。(ATM存钱 (发送多个) 无需银行同意 (无需应答))

3、差错控制 (检测并纠正错误)

①等停ARQ协议, 发出一帧后, 等待应答信号, 收到肯定应答信号ACK后继续发送, 在一定时间间隔内没有收到应答信号也必须重发 (超时重发)

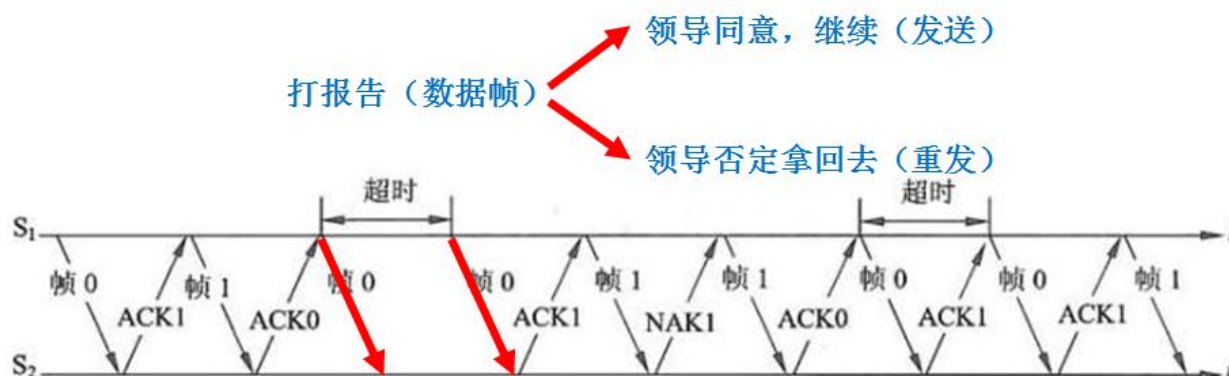
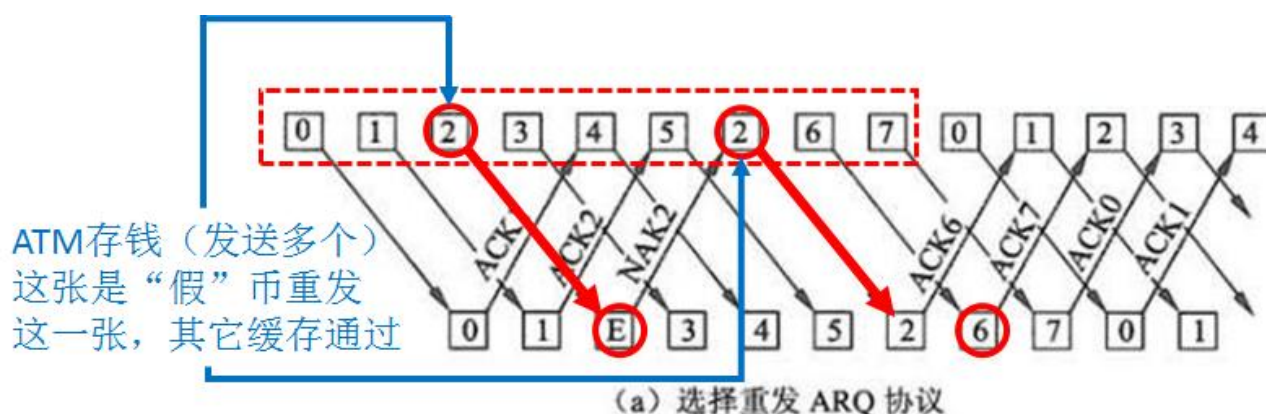


图 3-14 停等 ARQ 协议

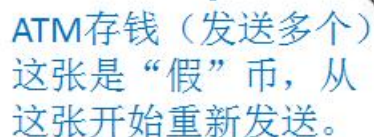
②选择重发ARQ协议, 其中第2帧出错, 随后的3、4、5帧被缓存。先缓存正确的, 待纠错完成后在按顺序向上提交。(选择: 单发)



重发ARQ协议, 即

$$W_{\text{发}} = W_{\text{收}} \leq 2^{k-1}$$

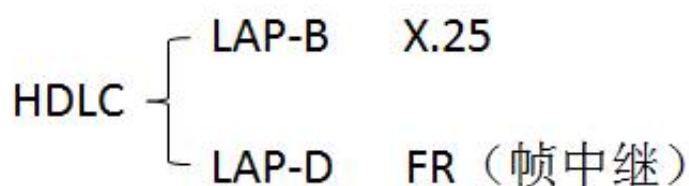
③后退N帧ARQ协议 (从发现错误处向后全部重发, 后退: 多发)



编号字段位数 k ，发送窗口大小为 W

(1从上边退下来啦~)

数据链路控制协议，面向位的协议以位（比特）作为传输的基本单位，它的传输效率高，广泛用于公共数据网上，面向位的数据链路控制协议。

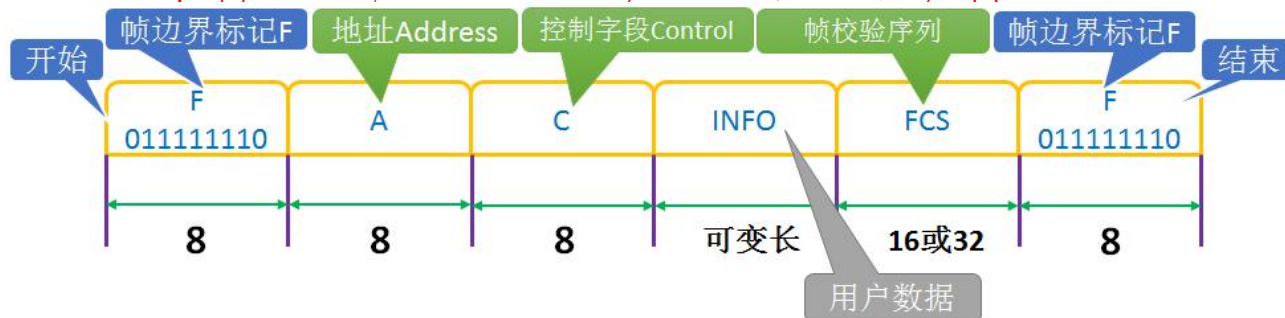


- (1) 主站 (控制链路, 发送命令帧)
- (2) 从站 (受主站控制, 发送响应帧)
- (3) 复合站 (具有主站从站的双重功能, 可发命令, 也可发响应)

平衡配置，仅用于点对点链路，由两个复合站组成。

异步响应方式 (ARM)

HDLC帧结构（MAC帧，VLAN帧）



X.25 PLP协议

X.25的分组层提供虚电路服务, 一种是交换虚电路 (SVC), 一种是永久虚电路 (PVC)。

X.25默认的窗口大小是2, X.25的差错控制采用后退N帧ARQ协议。



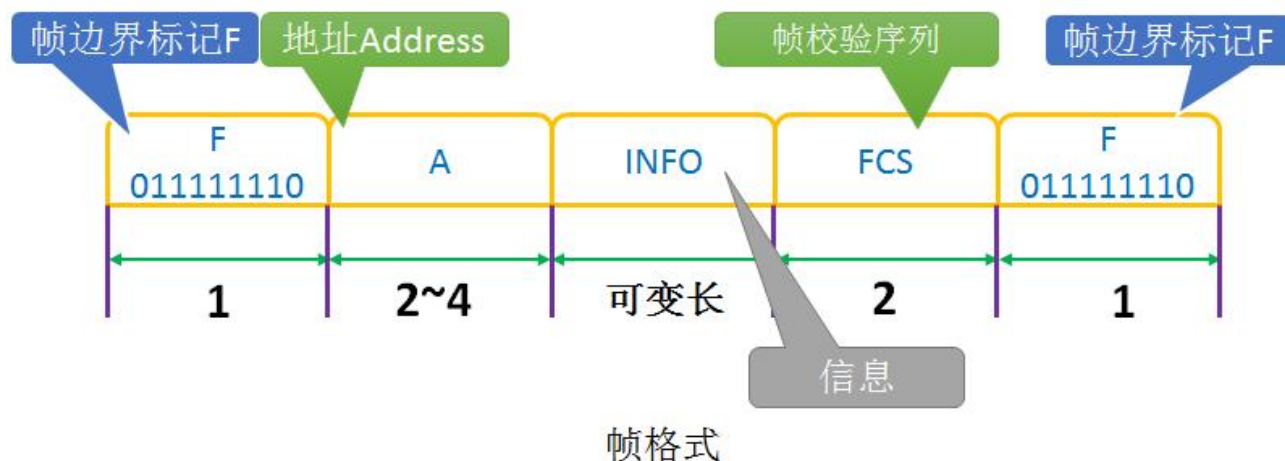
帧中继网 (FR frame relay)

帧中继在第二层建立虚电路, FR的帧层比HDLC操作简单, 只检错, 不重传, 没有滑动窗口式的流控, 只有拥塞控制。(效率高)

帧中继网络提供虚电路业务, 虚电路是端到端的连接, 连接标识符 (DLCI)

帧中继网上, 用户的数据速度可以在一定范围内变化, 从而既可以适应流式业务, 又可适应突发试业务。

LAP-D(Q.921)



LAP-B X.25 链路层协议

LAP-D 帧中继的链路协议

大部分中继网络仅提供永久虚电路服务, 即只能通过网络管理建立永久虚电路, 用户终端按照网络管理人员的指示预定DLCI进行通信。

帧中继远程连网的主要优点如下:

- (1) 基于分组(帧)交换的透明传输, 可以提供面向连接的服务
- (2) 帧长可变, 长度1600~4096字节, 可承载各种局域网数据帧。
- (3) 速率很高, 达2~45Mbps。
- (4) 可按需提供带宽, 也可以应付突发数据传输。
- (5) 没有流控和重传, 开销小。

帧中继的缺点如下:

- (1) 不适合对延迟敏感的应用(例如声音、视频)
- (2) 不保证可靠的提交。
- (3) 数据的丢失与否依赖运营商对虚电路的配置。

综合业务数字网

ISDN分为窄带ISDN(N-ISDN), 和宽带ISDN(B-ISDN)。

ISDN系统主要提供两种用户接口: 基本速率2B+D和基群速率30B+D, B信道是64Kbps, D信道是16Kbps或者64Kbps的信令信道。

$2B+D=2*64+16=144Kb/s$ $30B+D=30*64+64=1.984Mb/s$, 30B+D(接近2.048Mbps)的接口速率

B: 数据信号 D: 控制信号。

TCP/IP		表 3-4 B-ISDN 各层的功能		
层 次	子 层	功 能	与 OSI 的对应	
4层	高层	对用户数据的控制	高层	5,6,7层
3层	ATM 适配层	汇聚子层	第四层	4层
		拆装子层		
2层	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	3层
1层	物理层	传输汇聚子层	第二层	2层
		物理介质子层	第一层	1层

B-ISDN的关键技术是异步传输模式, 采用5类双绞线或光纤传输, 数据速率可达155Mbps。

同步传输模式(STM)。按顺序。

异步传输模式(ATM)。随机的, 它把用户的数据组成53字节长的信元(cell)

信元不仅是传输的信息单元, 而且也是交换的信息单元, 由于信元的53字节的固定长度, 可高速交换处理。

ATM的典型数据速率为150Mbps, 每秒钟每个信道上有36万个信元来到。

ATM是面向连接的。

ATM虚电路

ATM的网络层以虚电路提供面向连接的服务, 即虚通路(Virtual Path)和虚信道(Virtual Channel)

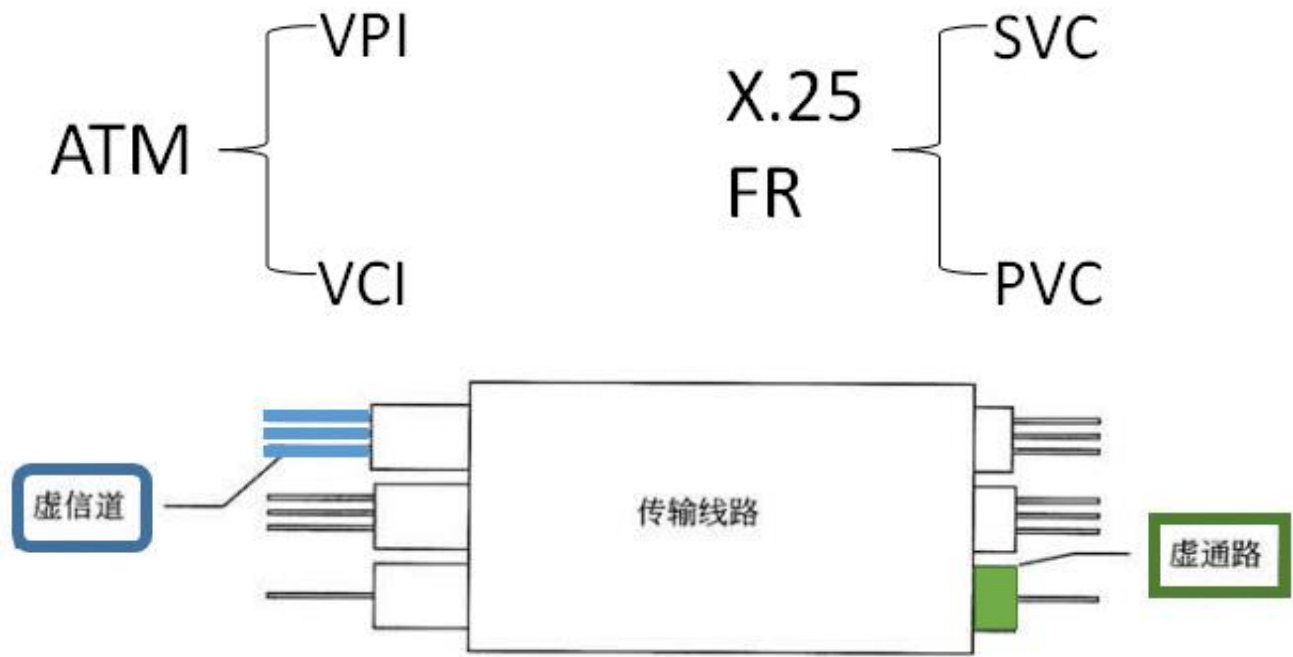


图 3-35 ATM 的虚通路和虚信道

- (1) CBR (Constant Bit Rate), 固定比特率业务。适用于交互式话音和视频流。
- (2) VBR (Variable Bit Rate), 可变比特业务。实时性, 交互式压缩视频信号 (MPEG)。非实时性, 例如多媒体电子邮件。
- (3) ABR (Available Bit Rate), 有效比特率业务, 用于突发式通信。租用线路连接各个办公室, 可以使用这类业务。
- (4) UBR (Unspecified Bit Rate), 不定比特率通信, 可用于传送IP分组。文件传输, 电子邮件, 和 USENET新闻是这类业务。

第4章 局域网与城域网

笔记本: 网络工程师学习

创建时间: 2015/1/21 11:40

更新时间: 2015/1/21 11:40

URL: about:blank

传统局域网是**分组广播式**网络, 这是与**分组交换式**的广域网最主要的区别。

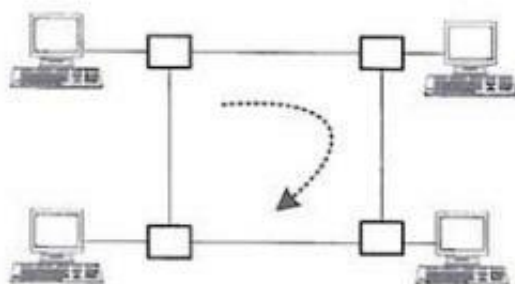
拓扑结构和传输介质**决定**了各种LAN的特点, **决定**了他们数据速率和通讯效率, 也**决定**了适合于传输的数据类型, 甚至**决定**了网络的应用领域。

总线是一种多点广播介质, 所有站点都通过接口硬件连接到总线上。由于总线共享介质, 多个站点同时发送数据时会发生冲突。

基带系统, 以太网使用特性阻抗为 50Ω 的同轴电缆。

宽带系统, 使用特性阻抗为 75Ω 的CATV电缆。

环形拓扑由一系列收尾相连的中继器组成, 每个中继器连接一个工作站。



(b) 环型

星型拓扑中有一个中心节点, 所有站点都连接到中心节点上。用星型拓扑结构也可以构成分组广播式的局域网。



(c) 星型

IEEE802标准。

目前有20多个分委员会

(1) 802.1研究局域网体系结构、寻址、网络互联、和网络管理 (802.1q (VLAN)、802.1X (安全认证))

(2) 802.2研究逻辑链路控制子层 (LLC) 的定义。

(3) 802.3研究以太网介质访问控制协议CSMA/CD及物理层技术规范。

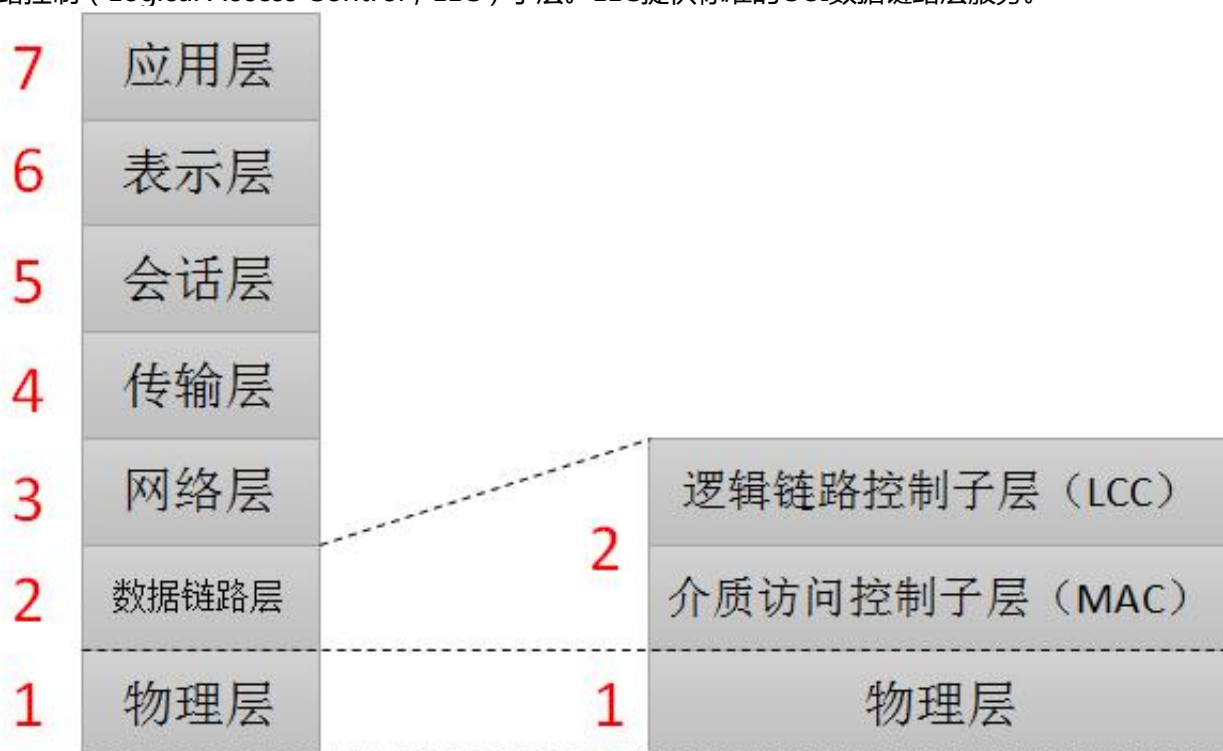
(11) 802.11研究无线局域网 (WLAN) ，包括802.11a/b/g/n/ac。

(13) 802.14研究采用线缆调制解调器 (Cable Modem) 的交互式电视介质访问控制协议及物理层技术规范。

(14) 802.15研究采用蓝牙技术的无线个人网 (Wireless Personal Area Network , WPAN)

(15) 802.16宽带无线接入工作组 (4G WMAN)

物理介质相关的部分叫做介质访问控制 (Media Access Control , MAC) 与物理介质无关的部分较逻辑链路控制 (Logical Access Control , LLC) 子层。LLC提供标准的OSI数据链路层服务。



逻辑链路控制子层规范包含在IEEE802.2标准中，这个标准与HDLC是兼容的。

LLC提供了以下3种服务。

LLC1 (1) 无确认无连接的服务。

大广播

LLC2 (2) 连接方式的服务

打电话

LLC3 (3) 有确认无连接的服务

打专线

LLC1型操作支持无确认无连接的服务。

LCC2型操作支持连接方式的服务。

LLC3型操作支持有确认无连接的服务

CSMA/CD (载波侦听多路访问/冲突检测) ， CSMA的基本原理是，站在发送数据之前，先监听信道上是
否有别的站发送的载波信号。若有，说明信道忙，否则说明信道是空闲的，然后根据预定的策略决定：空
闲是否发送，忙是否继续监听。

(1) 非坚持型监听算法。

①若信道空闲, 立即发送, 否则转②

②若信道忙, 则退后一个随机时间, 重复① (退回屋里等一会)

(2) I-坚持型监听算法

①信道空闲, 立即发送, 否则转②

②信道忙, 继续监听, 直到信道空闲后立即发送, (站在楼梯急等)

(3) P-型坚持型监听算法。

①信道空闲, 以概率P发送,

②信道忙, 继续监听直到信道空闲, 转①

③如果发送延迟一个单位时间t, 则重复①

整个发送期间将检测不到冲突。

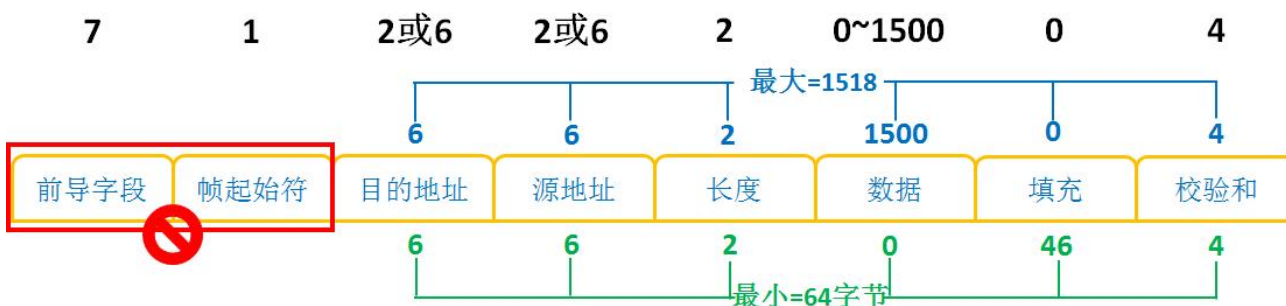
最小帧长 $L_{\min}$

$$L_{\min} = 2R \times d/v$$

R是网络数据速率, d为最大段长, v是信号传播速度。

以太网指示802.3标准中的一种。

MAC帧结构 (802.3的帧格式)



802.3的帧格式 (MAC帧格式)

长度字段说明**数据字段的长度**, 802.3规定最小帧长为64字节, 这个帧长是指从目标地址到校验和的长度。如果帧的长度不足64字节, 要加入最多46字节的填充位。

两个字节表示的数字范围是0~65535 (2^16), 长度字段最大值是1500, 因此1501~65535之间的值都可以用来标识协议类型。

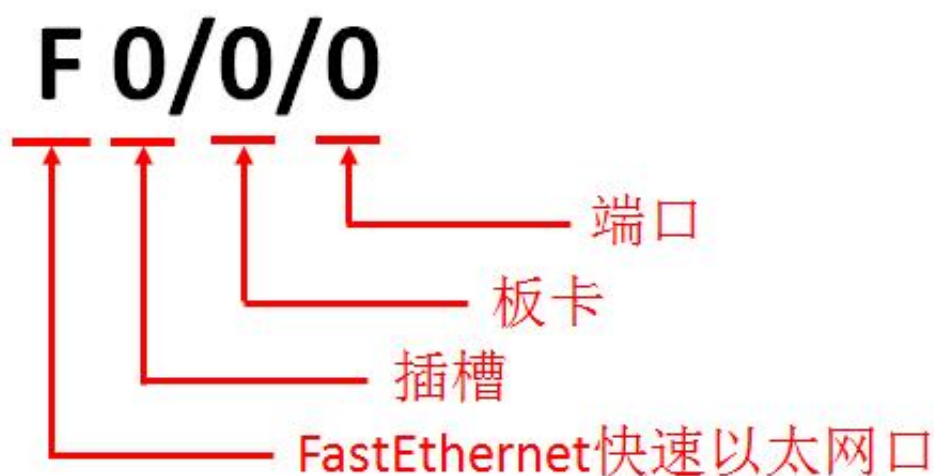
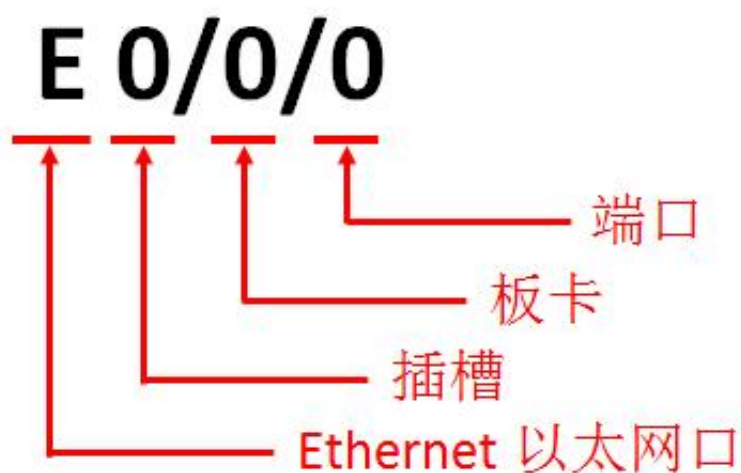
若检测到冲突, 发送8个十六进制数的序列55555555, 协议规定的阻塞信号。

Ethernet规范 10Base 5, 这里10表示数据速率为10Mbps, Base表示基带, 5表示最大段长为500m。

标准规定网络最大跨度为2.5km, 有5段组成, 最多含有4个中继器, 其中3段位同轴电缆。

5-4-3规则, 5段, 4中继, 3电缆

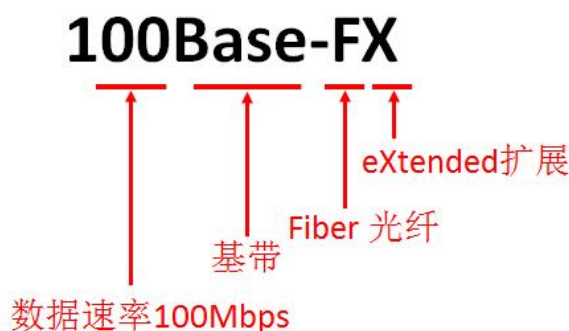
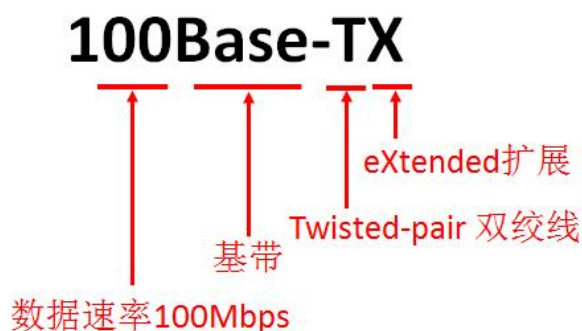
交换式以太网



快速以太网, 100Mbps, IEEE802.3u。

100Base-TX 两对5类UTP, 最大段长100m

100Base-Fx 一对单模光纤SMF, 最大段长40km



快速以太网的速率提高了10倍, 而最小帧长没有变, 所以冲突时槽缩小为5.12us

$$slot = \frac{2S}{0.7C} + 2t_{phy}$$

S表示网络的跨距。0.7C表示, 0.7倍光速, t_{phy}表示工作站物理层时延。

计算快速以太网跨距的公式:

$$S = 0.35C \left(\frac{L_{min}}{R} - 2t_{phy} \right)$$

千兆以太网

802.3z工作组, IEEE802.3ab已经成为千兆以太网的正式标准。

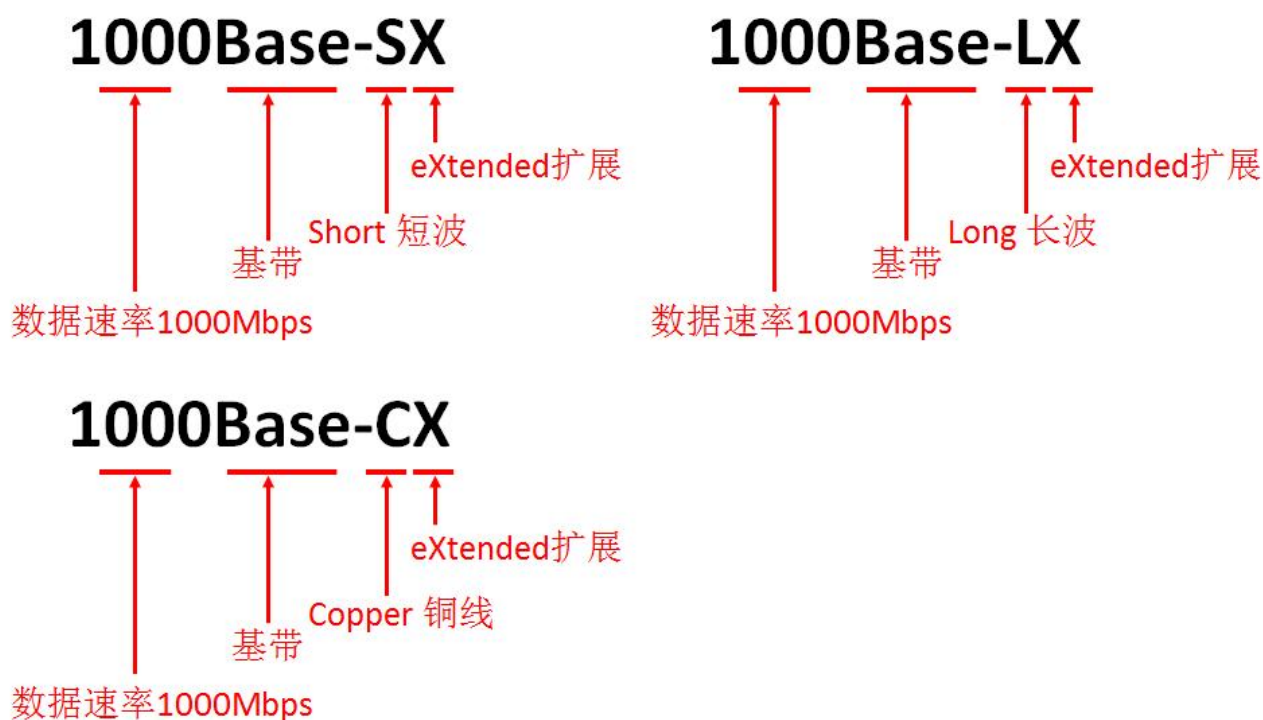
802.3z 1000Base-SX 短波光纤, 最大段长550m

1000Base-LX 长波光纤, 最大段长5000m

1000Base-CX 两队STP, 最大段长25m

802.3ab 1000Base-T 四对UTP, 最大段长1000m

802.3z还定义了一种帧突发方式 (frame bursting), 使得一个站可以连续发送多个帧。使用了4B/5B或8B/9B编码。



万兆以太网 IEEE802.3ae标准, 支持10Gbps, 没有冲突检测, 载波监听和多路访问技术也不在重要, 千兆以太网和万兆以太网采用与传统以太网**同样的帧结构**

10Gbase-S (Short) 50um多模, 300m, 62.5um, 65m。

10Gbase-L (Long) 单模光纤, 10km。

10Gbase-E (Extended) 单模光纤, 40km。

10Gbase-LX4, 单模光纤, 10km, 50um多模, 300m, 62.5um, 300m。

虚拟局域网与物理局域网有想相同的属性。

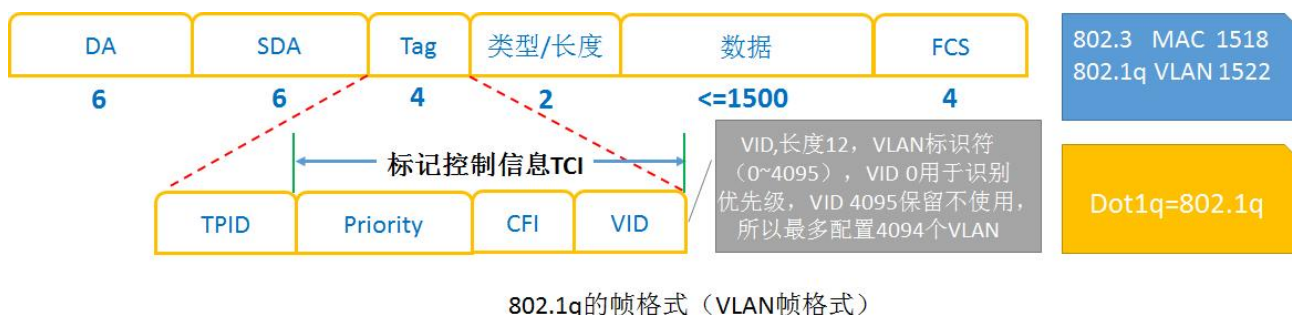
静态分配VLAN, 基于端口的划分。

动态分配VLAN, 可以根据MAC地址、网络层地址、IP广播域或管理策略来划分。根据MAC划分应用最多。

划分VLAN的好处:

- ①控制网络流量, 有利于控制广播风暴, 减小冲突域, 提高网络带宽的利用率。
- ②提高网络的安全性。提供广播过滤、安全和流量控制等。
- ③灵活网络管理。突破地理位置的限制。

VLAN中端口连接分两种: 接入链路连接 (Access Link Connection), 和中继链路连接 (Trunk-Link Connection)



局网提供网桥互联, 一种是802.1d的透明网桥, 另一种是802.5标准中定义的源路由网桥

生成树 (Spanning Tree) 网桥是一种完全透明的网桥, 这种网桥插入电缆后就可以自动完成路由选择功能, 无须有用户装入路由表或设置参数, 网桥的功能是自己学习获得的。

生成树算法 (自动寻找路径——车载导航)

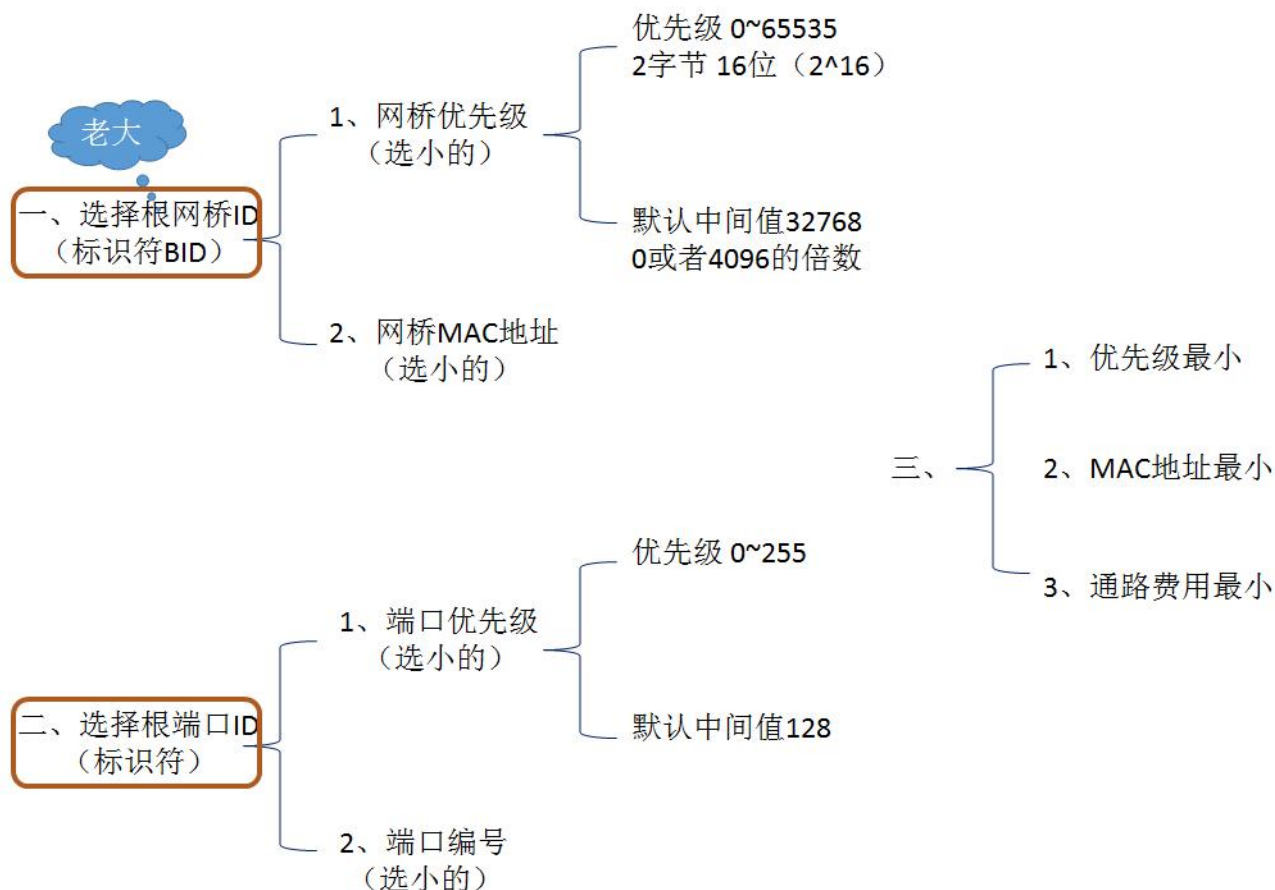
由环路引起的循环转发破坏了网桥的数据库, 使得网桥无法获得正确的转发信息。需要一种算法, 使得各个网桥之间通过交换信息自动阻塞一些传输端口, 从而破坏所有的环路并推导出因特网络的生成树。

MAC地址, 和唯一优先级, 地址和优先级构成网桥标识符 (BID/ID)

跟桥

通路费用, 通路费用与有关LAN的通讯速率联系起来 (一般为反比关系)

根端口



802.1w标准, 定义了快速生成树协议 (Rapid Spanning Tree Protocol, RSTP) 加快了收敛速度。

802.1D-2004对RSTP进行了改进, 并作废了原来的STP标准, 原标准需要30~50s才能响应拓扑改变, 新的快速生成树协议缩短3倍, 默认6s。

IEEE802.1d (生成树) 和IEEE802.1t (生成树补充)。

源路由网桥的核心思想是有帧的发送者显式地指明路由信息, 路由信息由网桥地址和LAN标识符的序列组成, 包含在帧头中。每个收到帧的网桥根据帧头中的地址信息可以知道自己是否在转发路径中, 并可以确定转发方向。

在这种方案中, 网桥无须保存路由表, 只需记住自己的地址标识符和它所连接LAN标识符, 就可以根据帧头中的信息做出路由决策。

城域以太网论坛 (MEF)

①以太网专用线 (EPL)

②以太网虚拟专线 (EVPL)

③以太网局域网服务 (E-LAN Services)

其中第③种技术被认为是最有前途的解决方案, 提供E-LAN服务的基本技术是802.1q的VLAN帧标记。

用户以太网, C网, 运营商城域以太网, S网, 当不同C网要互相通信, 插入S-VLAN字段, 用于标识传输服务, 用户VLAN帧标记 (C-VLAN) 保持不变。

802.1ad的运营商网桥协议 (Provider Bridge Protocol) 中, 被称为Q-in-Q技术。

Q-in-Q实际上是把用户VLAN嵌套在城域以太网VLAN中传送。

IEEE802.1ah标准提出了运营商主干网桥 (Provider Backbone Bridge , PBB) , 这种技术被称为MAC-in-MAC技术。

被认为是城域以太网最终解决方案, IEEE802.1ah标准正在完善之中。

弹性分组环 (Resilient Packet Ring , RPR) RPR支持数据速率可达10Gbps

RPR关键技术:

- (1) 业务类型
- (2) 空间复用
- (3) 拓扑发现
- (4) 公平算法
- (5) 环自愈保护, RPR和SDH一样能保证业务的倒换时间少于50ms

第5章 无线通信网

笔记本: 网络工程师学习

创建时间: 2015/1/21 11:42

更新时间: 2015/1/21 11:42

URL: about:blank

无线通信网包括面向语音 (1G , 2G , 3G) 及面向数据 (4G)

1G

高级移动电话系统 (Advanced Mobile Phone System , AMPS) , 采用频分双工 (FDD) 技术, 建立第一代蜂窝移动电话系统。

2G

第二代数字蜂窝电话, 主要有GSM (Global System for Mobile) 和码分多址 (CDMA系统)

全球移动通信系统GSM , TDMA (Time Division Multiple Access) 时分多路复用。

码分多址技术 (CDMA), 对不同用户分别不同的码片序列, 使得彼此不会造成干扰。

2.5G (第二代通信升级版)

通用分组无线业务GPRS, 理论上的分组交换速度大约是170Kbps, 二十几速度只有30~70Kbps

增强型数据速率的GSM演进 (EDGE) , EDGE有称为增强型GPRS (EGPRS) , 被认为是2.75G技术, 支持20~200Kbps的高速数据传输。

3G (第三代移动通信系统)

速度大约为2000Kbps (即2Mbps)

W-CDMA, 属于频分双工模式。

CDMA-2000, 属于频分双工模式。

中国提出的TD-SCDMA, 属于时分双工模式。

EDGE

EDCT

WiMAX (无线城域网技术)

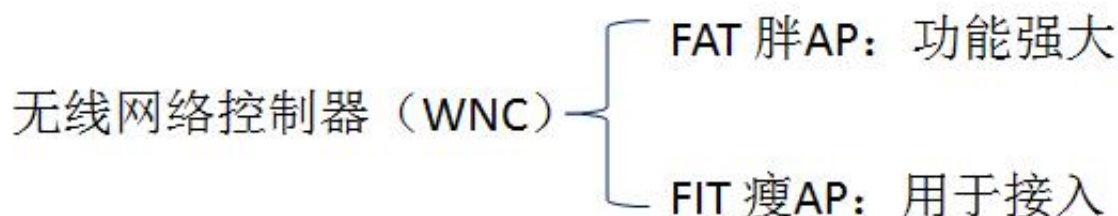
4G的传输速率应该达到100Mbps, 可以把蓝牙个域网、无线局域网 (WiFi) 和3G技术结合在一起。

WLAN

无线局域网 (Wireless Local Area Networks , WLAN) , 两大阵营, IEEE802.11标准和

HIPERLAN (High Performance Radio LAN)

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	2007年	2.4GHz ISM频段 5GHz U-NII频段	MIMO OFDM	300Mbps 600Mbps
802.11ac	2012年	5GHz U-NII频段	MIMO OFDM	500Mbps 1Gbps



IEEE802.11定义了两种无线网络拓扑结构,一种是基础设施网络 (Infrastructure Networking),另一种是特殊网络 (Ad Hoc Networking),在基础设施网络中,无线终端通过接入点 (Access Point, AP) 访问骨干网络设备,接入点如同一个网桥,它负责在802.11和802.3MAC协议之间进行转换。Ad Hoc 网络是一种点对点连接,不需要有线网络的接入点的支持,终端设备之间通过无线网卡可以直接通信,这种拓扑结构适合于移动情况下快速部署网络。

无线网主要有3种通信技术:红外线、扩展频谱和窄带微波技术。

红外线 (IR),首先红外线频谱是无限的,因此有可能提供极高的数据速率。其次红外线频谱在世界范围内不受管制,而有些微波频谱则需要申请许可证。另外,红外线与可见光一样,可以被浅色的物体漫反射,这样就可以用天花板反射来覆盖整间房间。红外线网络的另一个优点是它的设备相对简单而且便宜。红外线网络的缺点:室内环境可能因阳光或照明而产生强光线,这将成为红外线接收器的噪音,使得必须用更高能量的发送器,并限制了通讯范围。

IR通信分为3种技术:①定向红外光速,定向红外光束可以用于点对点链路。

②全方向广播红外线。全向广播网络包含一个基站。

③漫反射红外线,脉冲幅度调制 (PAM),脉冲位置调制 (PPM) 和脉冲宽度调制 (PDM)。

IEEE802.11规定采用PPM技术作为漫反射IR的介质和物理层标准,数据速率分别为1Mbps和2Mbps。

扩展频谱通讯,其主要想法是将信号散布到更宽的宽带上来减少阻塞的干扰的机会。频率跳动扩展频谱 (Frequency—Hopping Spread Spectrum, FHSS),更新的版本是直接序列扩展频谱 (Direct Sequence Spread Spectrum, DSSS)。

用于工业,科学研究和微波医疗方面,这些频段无须许可证,2.4GHz为各国共同的ISM频段,有些设备 (如无绳电话,无线麦克风,业余电台)的工作频率为900MHz。还有些设备运行在2.4GHz上,典型例子就是微波炉,它使用久了会泄露更多的射线。

窄带微波通信,使用微波无线电频段 (RF)

(1) 申请学科证的窄带RF。

(2) 免许可证的窄带RF。

MAC层分为MAC子层和MAC管理子层。MAC子层负责访问控制和分组拆装,MAC管理子层负责ESS漫游、电源管理和登记过程中的关联管理。物理层分为物理层会聚协议 (Physical Layer Convergence Protocol, PLCP)、物理介质相关 (Physical Medium Dependent, PMD) 子层和PHY管理子层。PLCP主要进行载波监听和物理层分组建立,PM D用于传输信号的调制和比编码,而PHY管理子层负责选择物理信道和调谐。

数据链路层	LLC		站 管 理
	MAC	MAC 管理	
物理层 PHY	PLCP	PHY 管理	
	PMD		

图 5-12 WLAN 协议模型

MAC子层的功能提供访问控制机制，它定义了3种访问控制机制：CSMA/CA支持竞争访问，RTS/CTS和点协调功能支持无竞争的访问PCF

CSMA/CA类似802.3的CSMA/CD。这种访问控制机制叫做载波监听多路访问/冲突避免协议。所谓隐蔽终端问题。采用冲突避免的办法可以解决**隐蔽终端**的问题。

RTS/CTS协议（Request To Send/Clear To Send）即请求发送/清除发送协议。
 RS232标准中的RTS与CTS：即请求发送/清除发送，用于半双工时的收发切换。

分布式协调功能

802.11 MAC层定义的分布式协调功能（DCE）利用了CSMA/CA协议，在此基础上有定义了点协调功能（PCF）。DCF是数据传输的基本方式，作用于**信道竞争期**。PCF工作于非竞争期。

3种帧间隔（IFS），以便提供基于优先级的访问控制。

DIFS（分布式协调IFS）：最长的IFS，优先级最低，用于异步帧竞争访问的时延

PIFS（点协调IFS）：中等长度的IFS，优先级居中，在PCF操作中使用。

SIFS（短IFS）最短的IFS，优先级最高，用于需要立即响应的操作。

点协调功能，所谓点协调就是有AP集中轮询所有终端，为其提供无竞争的服务，这种机制适用于时间敏感的操作。

802.11又定义了一个称为**超级帧**的时间间隔。有点协调功能向所有配置成轮询的终端发出轮询。

MAC管理子层功能是实现登记过程、ESS漫游、安全管理和电源管理功能。

①登记过程，信标是一种管理帧，有AP定期发送，用于时间同步。信标还用来识别AP和网络，其中包括基站ID，时间戳、睡眠模式和电源管理等信息。

②移动方式，IEEE802.11定义了3种移动方式，无转移方式是指终端是固定，BSS转移是指终端在同一个ESS内部的多个BSS之间移动；ESS转移是指从一个ESS移动到另一个ESS。

③安全管理，IEEE802.11提供了有线等效保密（Wired Equivalent Privacy, WEP）技术，又称无线加密协议（Wireless Encryption Protocol）

802.11i，密钥交换协议TKIP，高级加密标准AES。

④电源管理，IEEE802.11允许空闲站处于睡眠状态，在同步时钟的控制下周期性的唤醒处于睡眠态的空闲站。

WPA是Wi-Fi Protected Access（Wi-Fi保护接入）

WPA2是第二代更高级的加密

移动Ad Hoc网络

Ad Hoc 网络是由无线移动节点组成的对等网, 无须网络基础设施的支持, 能够根据通信环境的变化实现动态重构, 提供基于多跳无线连接的分组数据传输服务。每一个节点是主机, 有是路由器, 他们之间相互转发分组, 形成一种自组织的MANET (Mobile Ad Hoc Network) 网络。

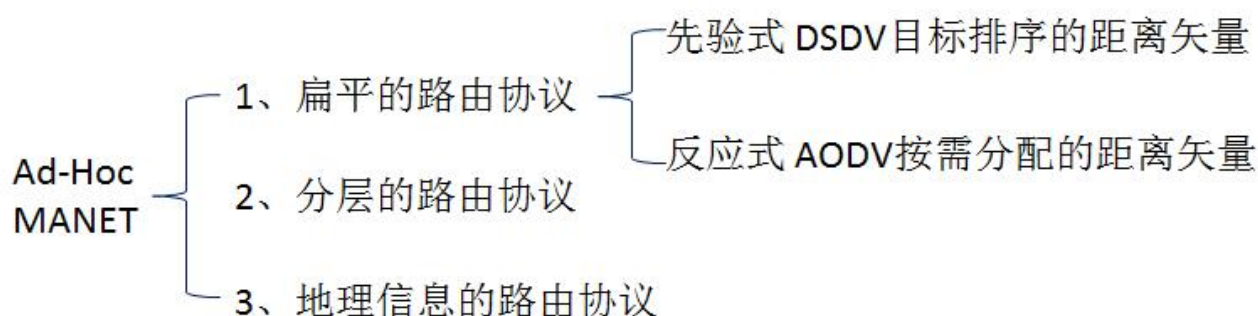
在战场网络、传感器网络、灾难现场和车辆通信等方面有着广泛的应用。

无线移动自组织网络中还有一种特殊现象, 这就是隐蔽终端和暴露终端问题。

路由算法是MANET (自组织网络) 中重要部分。

MANET中的路由协议。

根据路由策略分为: 表驱动的路由协议和源路由协议; 根据网络结构分为扁平路由协议、分层的路由协议和基于地理信息的路由协议。



(1) 扁平路由协议 , 参与路由过程的**各个节点**所起的作用都是相同的。

①先验式/表驱动路由 (先期检验) , 通过周期地交换路由信息, 每个节点可以保存完整的网络拓扑结构图。链路生命周期短, 路由开销较大。先验式路由协议适合于节点移动性较小, 而数据传输频繁的网络。

②反应式 / 按需分配路由 (触发反应) , 移动节点只是在需要通信时才发送路由请求分组, 以此来减少路由开销。

(2) 分层路由协议。

例如: 集群头网关交换路由协议 (CGSR) 把移动节点聚集成不同集群 (Cluster) , 每一个集群选出一个群集头。 (集群领头)

(3) 地理信息路由协议

利用地理坐标信息来设计Ad Hoc 路由协议, 这使得搜索目标节点的过程更加直接和有效。 (地理信息)

DSDV协议

目标排序的距离矢量协议 (Destination-Sequenced Distance Vector , DSDV) 是一种扁平式路由协议, 算法改进的距离矢量协议, 利用序列号机制解决了路由环路问题。

DSDV节点周期性地广播路由公告, 但是在出现新链路或者老链路断开时立即触发链路公告, 一种是广播全部路由表项, 称为**完全更新** (完全备份) , 另一种是只发送最近改变了的路由表项, 叫做**递增式更新** (增量备份) 。

排除路由环路想象。

DSDV要解决的另外一个问题是**路由波动问题**。

AODV协议

按需分配的距离矢量协议 (AODV) 也是一种扁平式路由协议, 但是采用了反应式路由策略, 利用类似 DSDV 的序列号机制解决路由环路问题, 但他只是在需要传送信息时才发送路由请求, 从而减少了路由开销。AODV 适合于快速变化的 Ad Hoc 网络环境, 用于路由信息交换的处理时间和存储开销较小。

AODV 是一种按需分配的路由协议, 当一个节点需要发现到达某个目标节点路由时就广播路由请求 (Route Request, RREQ) 报文。

IEEE802.11的新进展

SSID访问控制。

设置不同的 SSID (Service Set Identifier), 一般路由都提供 “允许 SSID” 广播功能, 应修改成个性化的 SSID 名字。

物理地址过滤

MAC 地址过滤访问控制。

MAC 地址可以伪造, 所以这个级别比较低的认证功能。

有线等效保密

有线等效保密 (Wired Equivalent Privacy, WEP) 使用 RC4 协议进行加密。使用 CRC-32 校验数据。

WPA (Wi-Fi Protected Access)

WPA 还采用了可以动态改变密钥的临时密钥完整性协议 TKIP (Temporary Key Integrity Protocol)

加强版本的 WPA, WPA2。

临时密钥完整性协议 TKIP 仍然使用 RC4 加密方法。

重新制定了新的加密协议, 称为 CBC-MAC 协议的计时器模式 (Counter Mode With CBC-MAC Protocol, CCMP)。基于高级加密标准 AES (Advanced Encryption Standard)。

无论使用 TKIP 还是 CCMP 进行加密, 身份证都是必要的。802.1x 是一种基于端口的身份认证协议。

WLAN的传输速率。

IEEE802.11n 标准达到 300Mbps, 甚至 600Mbps。

正交频分复用 (OFDM)

多入多出 (MIMO)

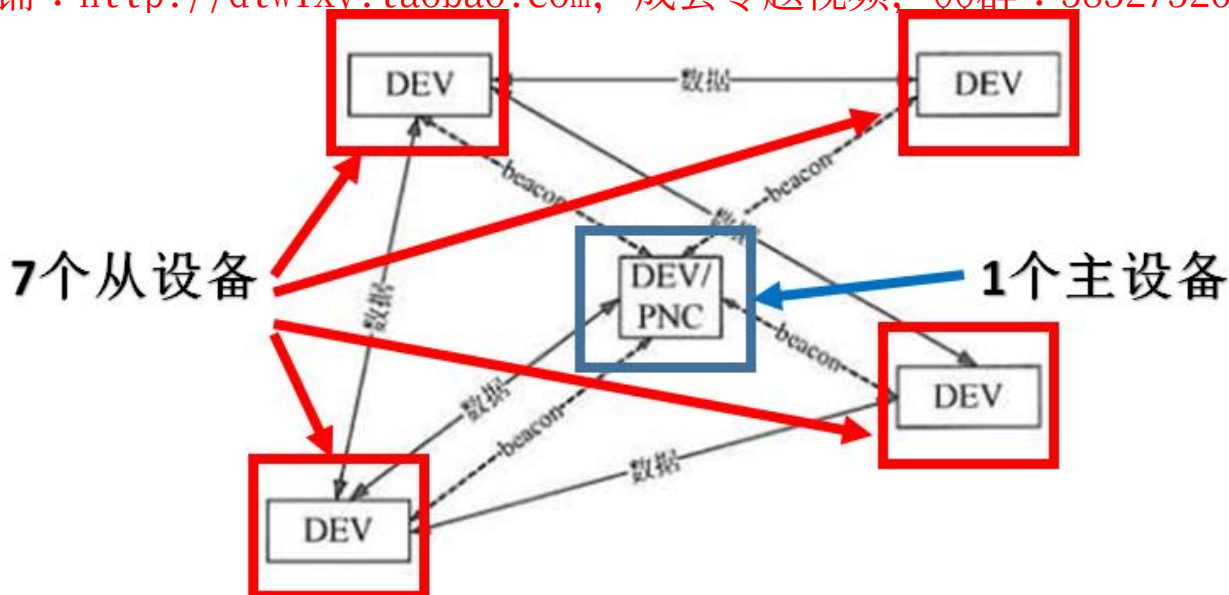
802.11n 采用的智能天线技术还扩大了覆盖范围, 还采用了一种软件无线电技术。

无线个人网

IEEE802.15 工作组负责制定无线个人网 (Wireless Personal Area Network, WPAN) 的技术, 这是一种小范围的无线通讯系统, 覆盖半径仅 10m 左右, 可用来代替计算机、手机、PDA、数码相机等智能设备的通信电缆, 或者构成无线传感器网络和智能家庭网络等。

802.15.1 (蓝牙网)

802.15.3 (微微网), 在人手可及的范围内, 多个电子设备可以组成一个无线 Ad Hoc 网络, 802.15 把这种网络叫做 piconet, 通常翻译为 微微网。各个电子设备 (DEV) 可以独立互相通信, 其中一个设备可以作为通信控制的协调器 PNC (piconet coordinator), 负责网络定时和向 DEV 发放令牌 (beacon), 获得令牌的 DEV 才可以发送通信请求。PNC 还具有管理 QoS 需求和调节电源功耗的功能。

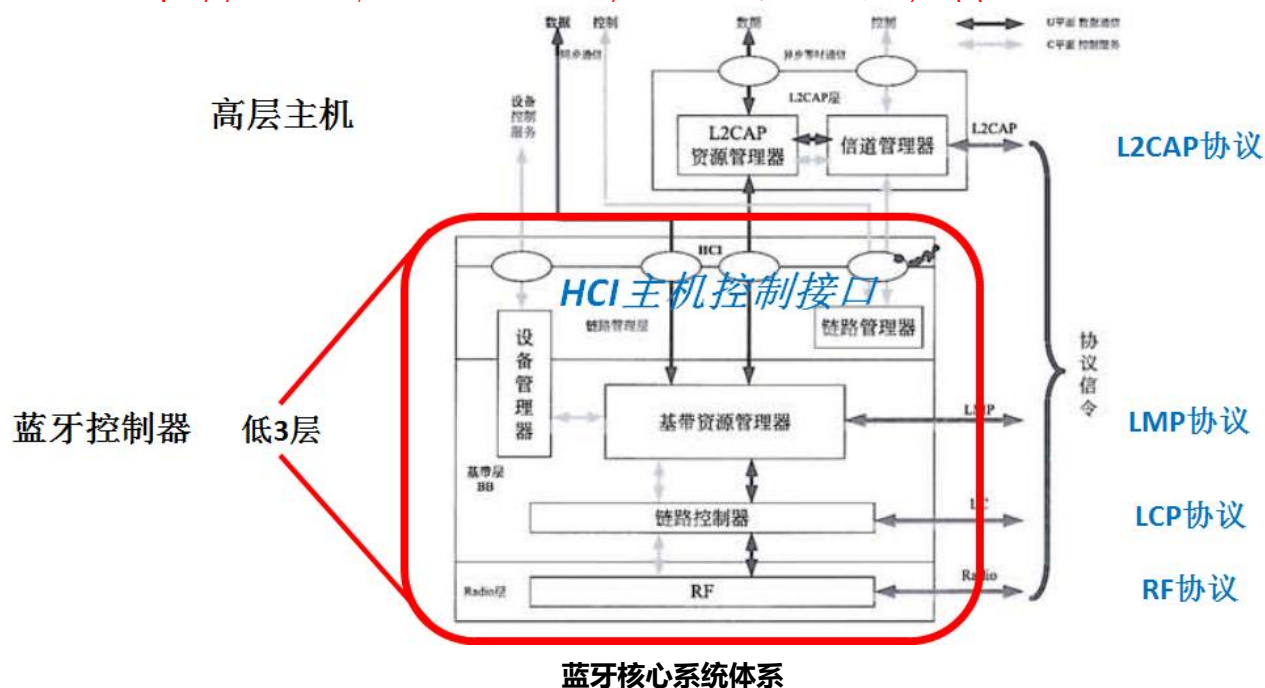


801.15.4 (ZigBee网) 瞄准了速率更低、距离更近的无线个人网, 适合用于固定的、手持的或移动电子设备, 主要由ZigBee联盟来做, 所谓Zigbee是指蜜蜂跳 “之字型舞蹈, 蜜蜂用跳舞来传递信息, 高速同伴蜜源的位置。” ZigBee “形象的表达了通过网络节点互相传递, 将信息从一个节点传输到远处另一个节点的通信方式。



蓝牙技术, 公元10世纪的丹麦国王, 史称蓝牙王, 爱吃蓝草莓, 牙齿变蓝, 统一了丹麦、挪威和瑞典。建立了强大的维京王国。接”统一“的含义, 诞生了”蓝牙“(Bluetooth)。

提供同步参照点的设备叫做主设备, 其他设备则是从设备。以这种方式取得同步的一组设备构成一个微微网, 这是蓝牙技术的基本组网模式。



逻辑链路控制和自适应协议L2CAP

核心系统只包含4个低层功能及其有关的协议。最下面3层通常构成了蓝牙控制器，而上面L2CAP以及更高层的服务都运行在主机中。

设备互操作通过核心系统协议实现，主要协议有RF（Radio Frequency，无线电频率）协议、链路控制协议LCP（Link Control Protocol）、链路管理协议LMP和L2CAP协议。

核心功能模块：

- (1) 信道管理器
- (2) L2CAP资源管理器
- (3) 设备管理器
- (4) 链路管理器（LM）
- (5) 基带资源管理器
- (6) 链路控制器
- (7) RF（Radio Frequency）

Zigbee技术

Zigbee是基于IEEE802.15.4开发，Zigbee联盟则对网络层协议、安全标准和应用构架（Profile）进行了**标准化**。

802.15.4定义的低速无线个人网（Low Rate-WPAN）包含了两类设备，即全功能设备（Full-Function Device，FDD）和简单功能设备（Reduced-Function Device，RFD）。FDD有三种工作模式，作为一般设备、协调器（Coordinator）或者PAN协调器，而RFD功能简单，智能作为设备使用，FDD可以与RFD或者其他FDD通信，而RFD只能与FDD通信，RFD之间不能互相通信。

	全功能	简单功能
	FFD	RFD
胖AP 全功能	通信	通信
瘦AP 简单功能	通信	不能通信

星型网络可用于家庭自动化、PC机外设管理、玩具和游戏，以及个人健康护理等网络环境。

点对点网络与星型网络不同，点对点拓扑可以构成更复杂的网络，工业控制和监控，无线传感器网络、库房管理和资产跟踪网络、智能农业网络和安全监控网络等，都可以通过点对点拓扑来构建。

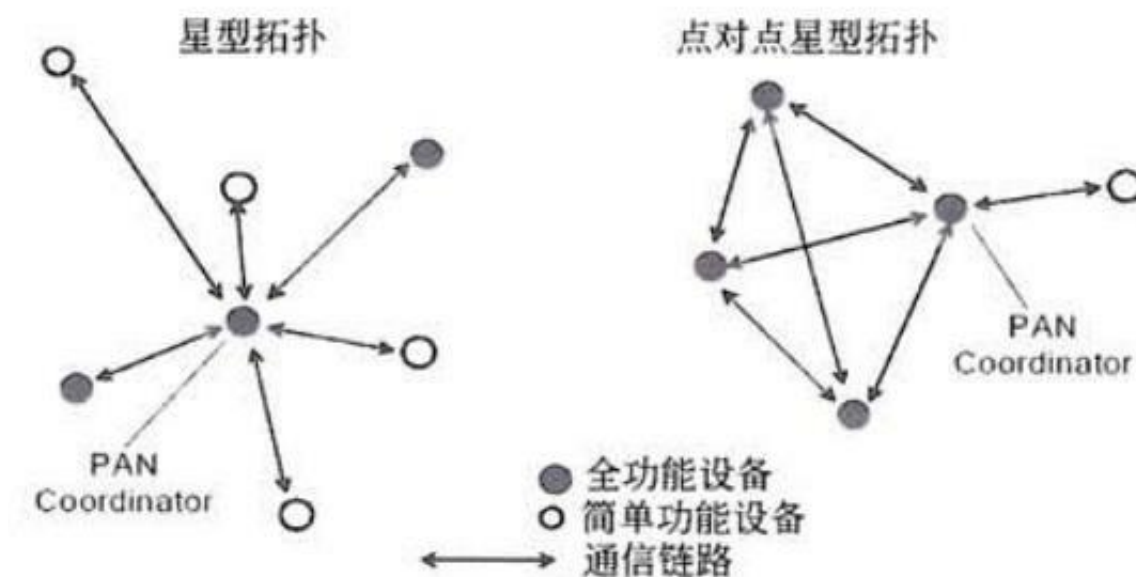


图 5-37 LR-PAN 拓扑结构

单个簇是最简单的簇集数，大型网络可能由互相领接的多个簇构成一个网状机构，网络中的第一个PAN协调器可以知道其他设备变成新簇的PAN协调器。

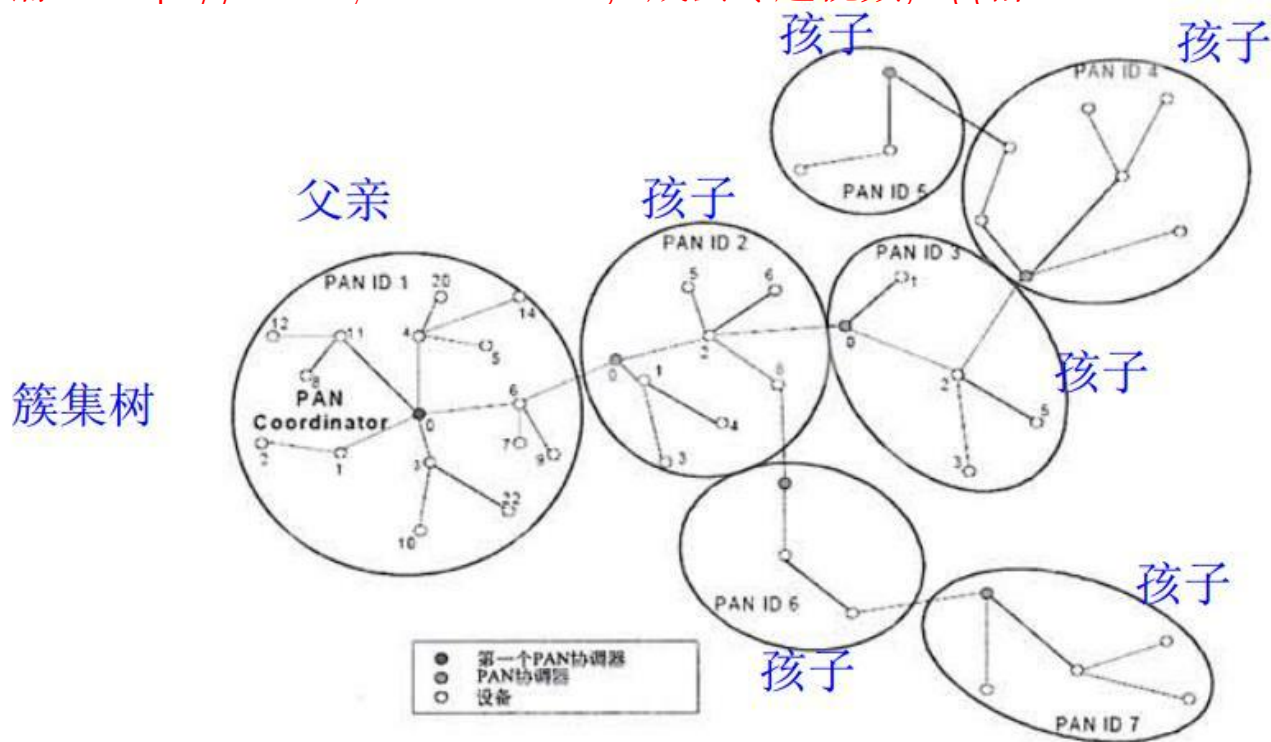


图 5-38 簇集树网络的网状结构

802.15.4-2006标准定义的4种物理层如下：

工作频率	扩频	调制	速率
868/915 MHz	直接序列扩频（DSSS）	二进制相移键控（BPSK）调制	20bps/40Kbps
868/915 MHz	直接序列扩频（DSSS）	偏置正交相移键控（O-QPSK）调制	100Kbps/250Kbps
868/915 MHz	并行序列扩频（PSSS）	二进制相移键控（BPSK）调制和幅度键控（ASK）调制	250Kbps
2.450 GHZ	直接序列扩频（DSSS）	偏置正交相移键控（O-QPSK）调制	250Kbps

基于竞争的访问方式应用了CSMA/CA后退算法。

Zigbee采用路由算法是按需分配的距离矢量协议AODV。

无线城域网

IEEE 802.16无线城域网技术

WiMAX (World Interoperability for Microwave Access)

目前比较成熟的标准有两个，一个是802.16d，无线固定接入，也叫固定WiMAX。

802.16e增加了对移动性支持，所以也称为移动WiMAX。

WiMAX比Wi-Fi的覆盖范围更大，数据速率也更高，同时WiMAX比Wi-Fi具有更好的可扩展性和安全性，从而能够实现电信级的多媒体通信服务。

Wi-Fi：无线热点，属于WLAN，基于802.11

WiMAX：无线城域网WMAN，基于802.16

802.16系统采用两个工作频段, 10~66GHz, 2~11GHz

1、802.16采用多路复用方式 OFDM/OFDMA。

2、为了进一步提高带宽利用率, 802.16还引入了多入多出技术MIMO。802.16系统以频分双工 (FDD), 或时分双工 (TDD) 方式工作。

MAC子层

802.16MAC层提供面向连接的服务, 各个连接通过唯一的连接标识符 (CID) 区分。

定义了完整的QoS机制

MAC定义的4中不同业务。

非请求的带宽分配义务

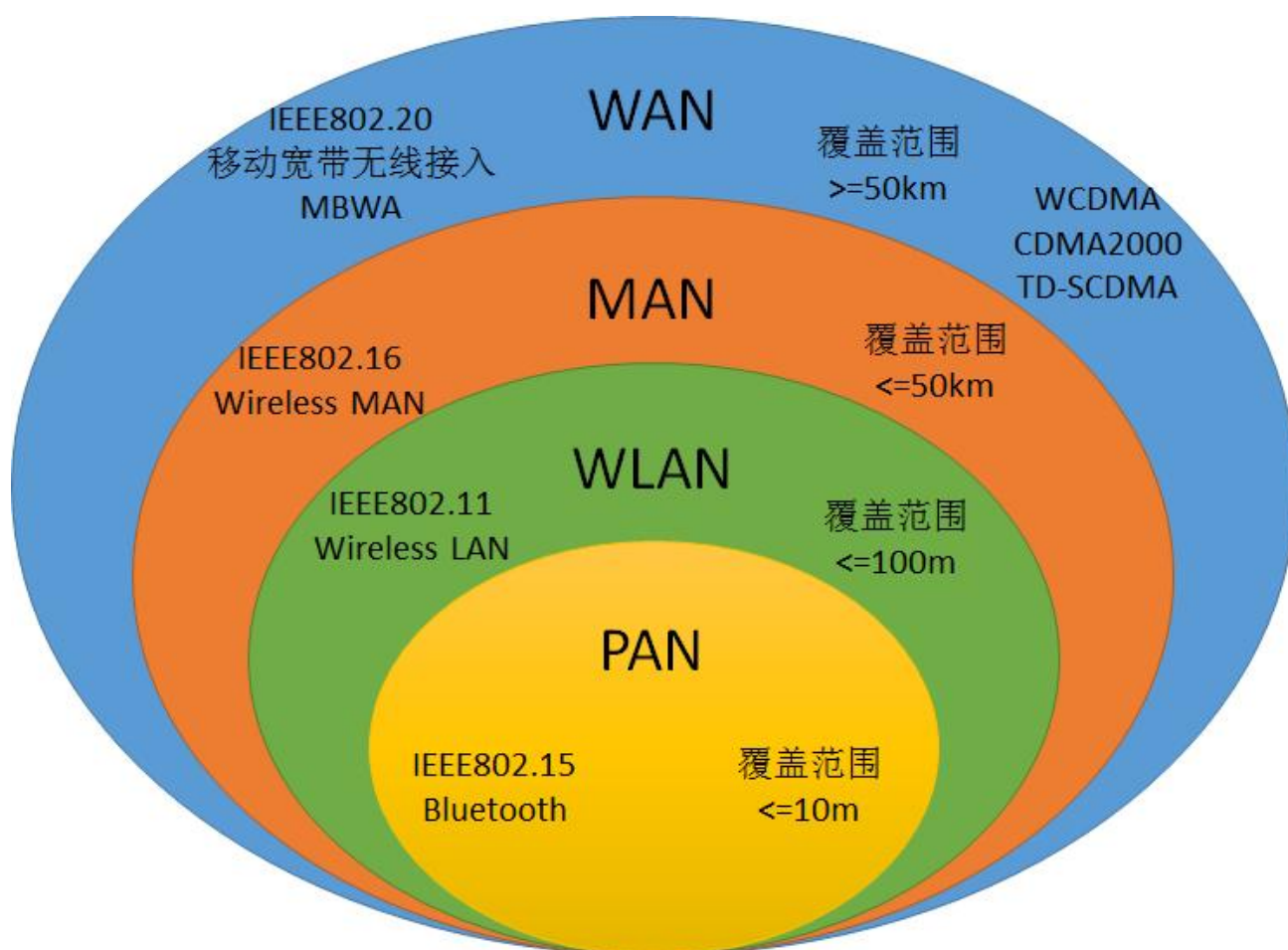
实时轮询业务

非实时轮训业务

尽力而为业务

向4G迈进

802.16d、802.16e



各种无线网络的作用范围

WiMAX II

最初候选的4G标准有3个, 即UMB (Ultra Mobile Broadband)、LET (Long Term Evolution) 和 WiMAX II (IEEE802.16m)。

1、超级移动宽带 (UMB)

2、长期演进 (LET)

第6章 网络互连与互联网

笔记本: 网络工程师学习

创建时间: 2015/1/21 11:44

更新时间: 2015/1/21 11:45

URL: about:blank

多个网络互相连接组成范围更大的网络叫做互联网 (Internet)

网络互相连接构成统一的通信系统, 实现更大范围的资源共享。

网络互连设备

中继器 (Repeater) 工作于物理层; 网桥 (bridge) 和交换机 (Switch) 工作与数据链路层; 路由器 (Router) 工作于网络层; 而网关 (Gateway) 工作于网络层以上的协议层。

比特流 (位) 1 0 bit

中继器的功能是对接收信号进行再生和发送。中继器不解释也不改变接收到的数字信息, 再生的信号与接收信号完全相同, 并可以沿着另外的网段传输到远端。

例如在以太网中, 限制最多使用4个中继器, 最多由5个网段组成。

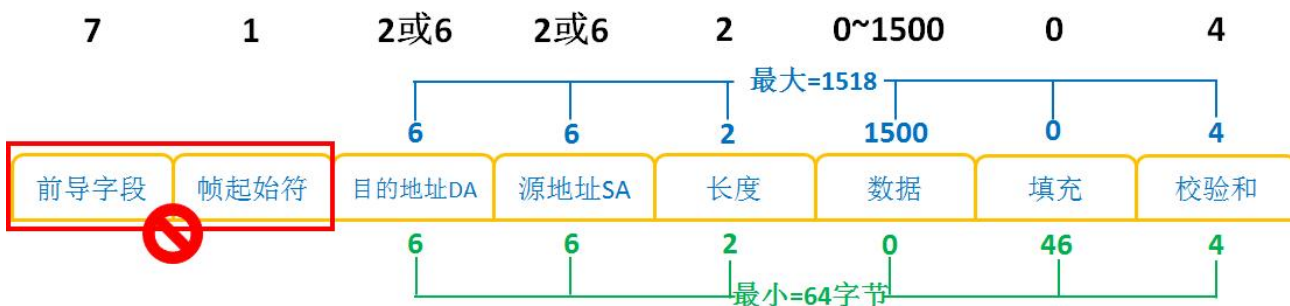
5-4-3规则: 5个网段, 4个中继器, 3个网段接PC

中继器工作于物理层, 只是起到扩展传输距离的作用。

集线器 (HUB) 工作原理上基本上与中继器相同。简单的说。集线器是一个多端口的中继器, 它把一个端口上收到的数据广播发送到其他所有端口上。

网桥

网桥也是连接两个局域网断, 但它工作于数据链路层。网桥要分析帧地字段, 以解决是否把收到的帧转发到另一个网段上。



802.3的帧格式 (MAC帧格式)

以太网中广泛使用的交换机是一种多端口网桥, 每一个端口都可以连接一个局域网 (二层) 。

路由器工作于网络层。通常把网络地址叫做逻辑地址 (IP地址), 把数据链路层地址叫做物理地址 (MAC地址) 。

由于路由器工作网络层, 它处理的信息量比网桥要多, 因此处理速度比网桥慢, 但路由器的互连能力更强, 可以执行复杂的路由选择算法。

路由器 (Routing Bridge) 路由器虽然能够运行路由器算法, 是属于工作在数据链路层的。

网关, 网关是最复杂的网络互连设备, 它用于连接网络层之上执行不同的协议的子网, 组成异构型因特网。网关能对互不兼容的高层协议进行转换, 翻译和变换。

最后, 有时不区分路由器和网关, 而是把网络层及其以上进行协议转换的互连设备统称为网关。

广域网互连

广域网的互连一般采用在网络层进行协议转换的办法实现。这里使用的互连设备叫做网关, 更确切的说, 是路由器。

面向连接的网际互连

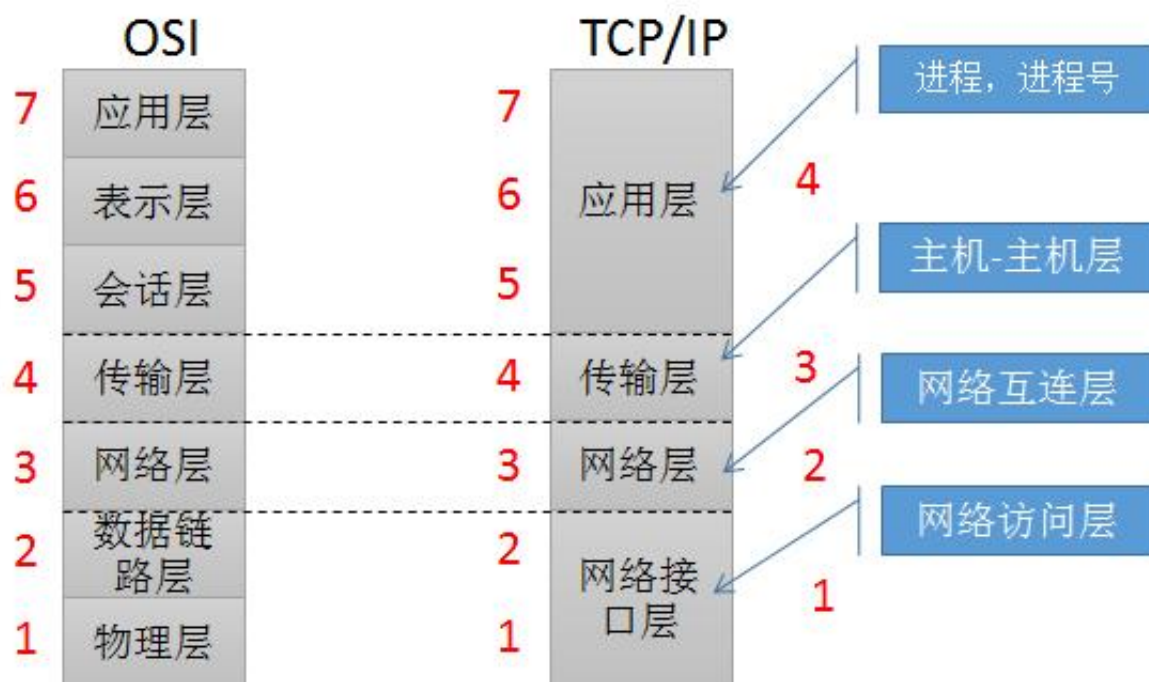
面向连接: 打电话
面向无连接: 广播

主要设备: 路由器

无连接的网际互连

因特网协议 (Internet Protocol, IP)

Internet 是今天使用最广泛的网络, 因特网中的主要协议是TCP和IP, 所以, Internet协议也叫TCP/IP协议簇。可以划分为4个层次。

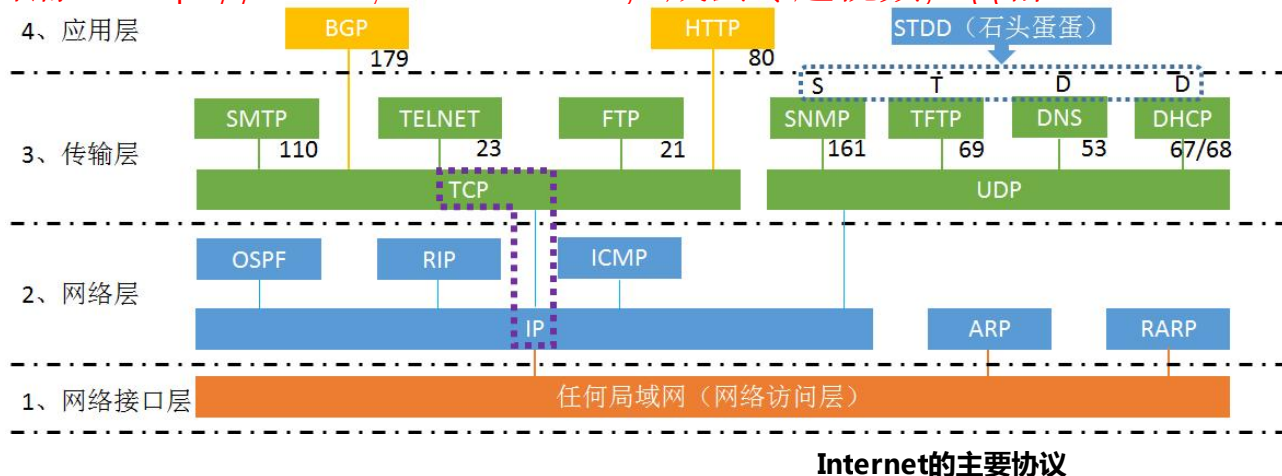


IP协议是Internet中的网络层协议, 作为提供无连接服务。

IP地址

IP网络地址采用“网络.主机”的形式。





IP地址格式：

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

地址类型	地址范围	网络数	子网掩码 (位数)	备注
A类	1.0.0.0~127.255.255.255	128	255.0.0.0 /8	
B类	128.0.0.0~191.255.255.255	64	255.255.0.0 /16	
C类	192.0.0.0~223.255.255.255	32	255.255.255.0 /32	
D类	224.0.0.0~239.255.255.255	16	不区分网络位和主机位	组播
E类	240.0.0.0~255.255.255.255	16	不区分网络位和主机位	科研

A、B、C类地址为常用地址。IP地址的编码规定全0表示本地地址，及本地网络或本地主机；全1表示广播地址，任何网站都能接收。

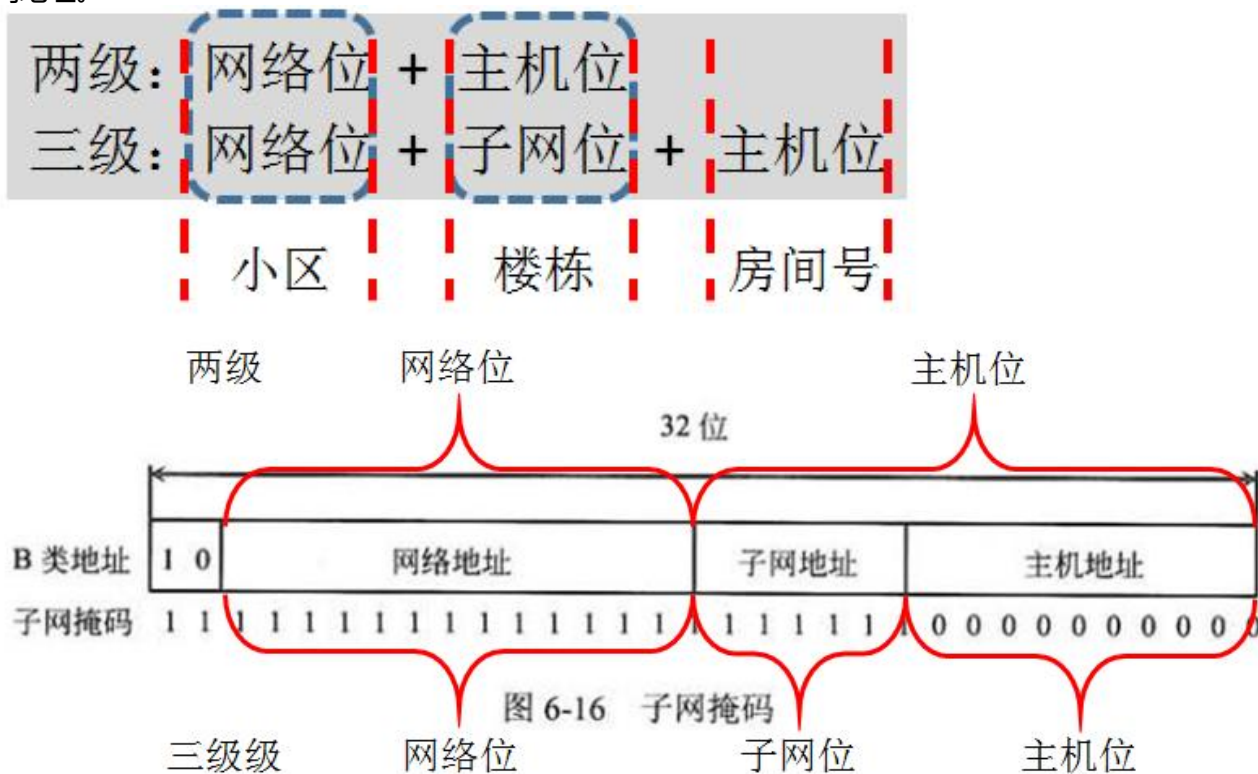
主机数 -2
 子网数 不-2

IP地址通常用十进制数表示, 即把整个地址划分为4个自己, 每个字节用一个十进制数表示, 中间用圆点分割, 根据IP地址的第一个字节, 就判断它是A类、B类还是C类地址。

点分十进制: 192.168.1.100

子网概念, 把主机地址部分再划分为子网地址和主机地址, 形成了**三级寻址结构**。

子网地址对网络外部是透明的, 边界路由把IP地址与子网掩码进行逻辑“与”(乘法)运算, 从而得到子网地址。



子网掩码

	网络地址	子网地址	主机地址
子网掩码	11111111.11111111.11111111.11111111	11111111	00000000.00000000
130. 47. 16. 254	10000010.00101111.00010000.11111110	00010000	11111110
130. 47. 17. 01	10000010.00101111.00010001.00000001	00010001	00000001
131. 47. 64. 254	10000010.00101111.01000000.11111110	01000000	11111110
131. 47. 65. 01	10000010.00101111.01000001.00000001	01000001	00000001

IP地址与子网掩码

可变长子网掩码 (VLSM)

D类地址是组播地址, 实现组播需要特殊的方法, 首先有识别组播地址的路由器, 其次主机要能发送组播数据报。主机哈需要能接收组播报文。

1、数据报生存期（TTL）

回路会造成数据包无休止地巡回。

经过的路由器的多少计数，每经过一个路由器，计数器加1。

2、分段和重装配

每个网络可能规定了不同的最大分组长度，需要对它进行分段，和重装配。

以太网MTU最大传输单元=1500。 802.3 MAC帧 MTU最大传输单元=1518 802.1q VLAN帧 MTU最大传输单元=1522

IP协议使用了4个字段处理分段和重装配问题。

3、差错控制和流控

无连接的网络操作**不保证数据报**的成功提交。把情况报告上层协议。

IP协议数据单元

版本号：（IPV4）

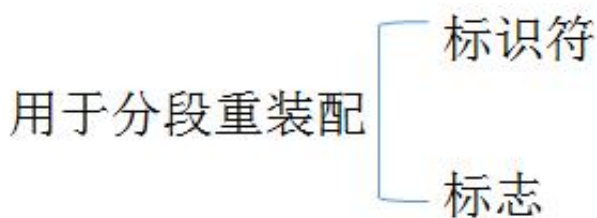
IHL：IP头长度，20个字节。

服务类型：区分不同可靠性、优先级、延迟和吞吐率的参数。

总长度：包含IP头的总长度（字节数）

标识符：唯一标识数据报的标识符

标志：包括3个标识，一个是M标志，用与分段（多段）重装配，另一个是D标识，禁止分段标志。第3个标志当前没有启用



段偏置值

生存期

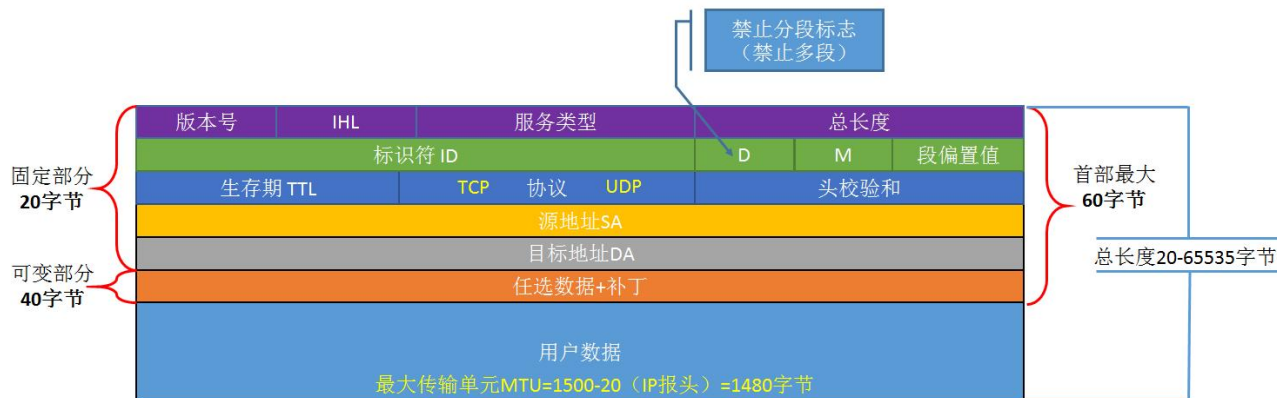
协议：上层协议（TCP或UDP）

头校验和：只校验数据报的首部，不包括数据部分。

源地址

目标地址

用户数据：以字节为单位，和IP头加在一起长度不超过65535字节。



IP协议格式

ICMP协议

因特网控制报文协议 (ICMP) 与IP协议同属于网络层。用于传送有关通信问题的消息。ICMP报文封装在IP数据报中传送, 因而不保证可靠的提交。校验和字段是关于整个ICMP报文的校验和。

ICMP相当于侦查员 (探子)



ICMP报文含义:

目标不可达 (类型3)

3拐了两个个弯, 不可达

超时 (类型11)

11类似, 超时

源抑制 (类型4)

4交通事故, 源抑制

路由重重定向 (类型5)

5拐了一个弯, 重定向

回声 (请求/响应, 类型8/0)

8喇叭口, 0没声音

时间戳 (请求/响应, 类型13/14)

1314, 一生一世

地址掩码 (请求/响应, 类型17/18)

18 B类掩码

TCP和UDP协议

在TCP/IP协议簇中有两个传输协议, 即传输控制协议 (TCP) 和用户数据报协议 (UDP), TCP是面向连接的, 而UDP是无连接的。

TCP，字节流形式。

TCP的PDU，叫做TCP段（报头），段头（包头）（也叫TCP头或传输头）

$$2^{16} = 65536, 0 - 65535$$

源端口（16位）

目标端口（16位）

标志字段（6位）

URG：紧急指针有效。urgent

ACK：应答顺序号有效。acknowledge

PSH：推进功能有效。push

RST：连接复位位初始状态。reset

SYN：对顺序号同步，用于连接的建立。synchronous

FIN：数据发送完毕，释放。finish

IP 校验和检查IP包头，不检查数据
 TCP 校验和检查TCP包头和数据、伪段头
 ICMP 校验和检查ICMP包头和信息。
 UDP 校验和检查UDP包头和数据（任选）

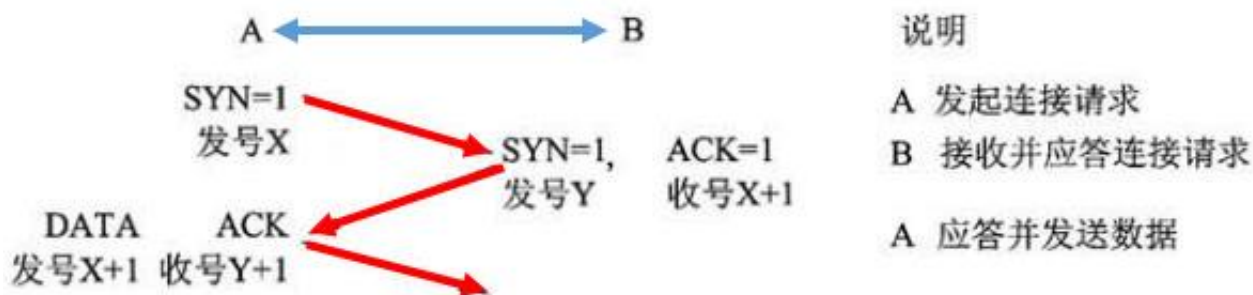
校验和（16位）



TCP传输头格式

同步标志SYN用于连接建立阶段。TCP三次握手过程建立连接。

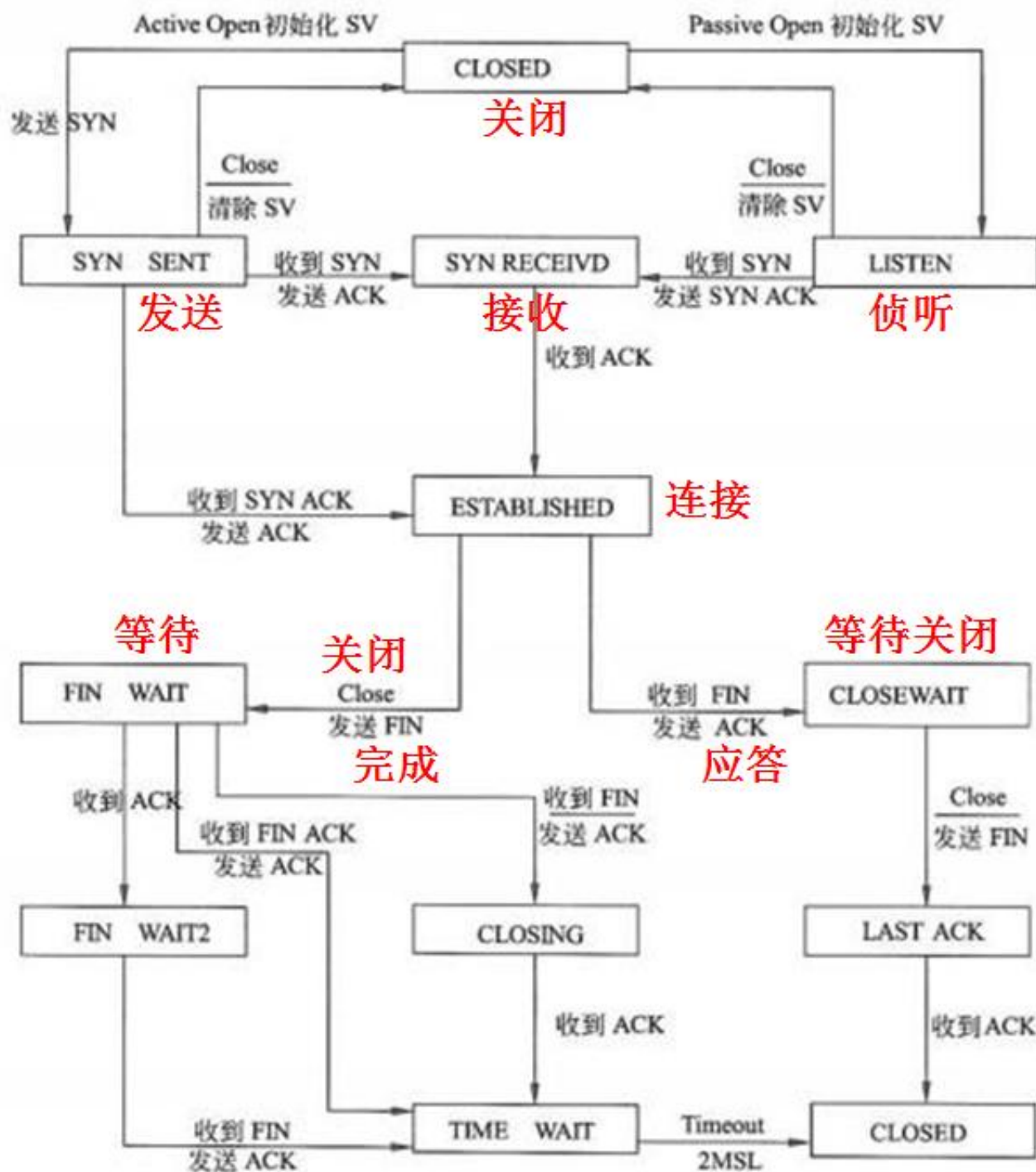
防止产生错误链接
 建立连接：三次握手
 释放连接：四次握手



TCP连接的建立

校验和的校验范围包括整个CP段和伪段头 (Pseudo-header) 。伪段头是IP头的一部分。

TCP头和IP头合在一起, 代表了传送一个数据单元的开销, 共**40个字节**



TCP连接状态图

TCP拥塞控制

重传及时器管理和窗口管理, 其目的是与流控机制配合, 缓解互联网中的通信紧张状况。

发送窗口缩小为原来的一半
 超时重传时间间隔扩大一倍

重传计时器管理, 用于确定网络传输时延和监视网络拥塞情况。通过观察最近一段时间的报文时延来估算当前的往返时间。

慢启动和拥塞控制

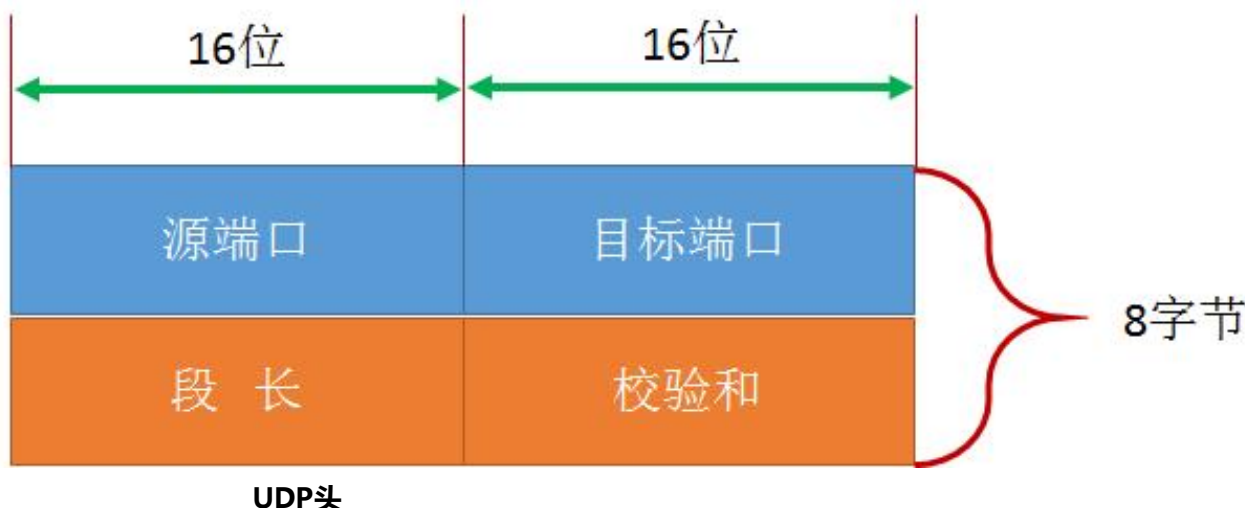
发送方实体在接收到确认之前逐步扩展窗口的大小, 而不是从一开始就采用很大的窗口, 这种方法称为慢启动过程。

发送窗口缩小为原来的一半
超时重传时间间隔扩大一倍

TCP: 有连接、可靠的、数据量大。
UDP: 无连接、不可靠、数据量小
高层解决排序、差错重传等。

TCP: 支持数据传输
UDP: 支持音频/视频传输

UDP也是常用的**传输层**协议, 他对应用层提供**无连接**的传输服务, 由于协议开销小, 特别是在**网络管理**方面, 大多使用UDP协议。



校验和与TCP相同, 但是任选的, 由于IP的校验和只作用于IP头, 并不包括数据部分。

Internet地址分为3级, 可表示为“网络地址.主机地址.端口地址”形式, 网络 and 主机地址即IP地址; 端口地址就是TCP或UDP地址, 使用专用端口号, 小于1024, 而用户进程端口号一般大于1024。

45 / 241

主机地址 网络地址 端口

http://www.dtwlxy.com :8080/rk

或是IP地址 用户进程端口号>=1024

固定分配的专用端口号

端口号	描 述	端口号	描 述
20	FTP-Data，文件传输协议	118	SQL Services
21	FTP-Control，文件传输协议	156	SQL Services
22	SSH 远程登录	161	SNMP，简单网络管理些
25	SMTP	179	BGP，边界网关协议
53	DNS，域名系统	443	HTTPS
80	HTTP,超文本传输协议	546	DHCP，动态主机配置协议，客户端
110	POP3	547	DHCP，动态主机配置协议，服务器端

保留端口：1-1023	知名端口	保留指派给常用的协议
注册端口：1024-49151		不指派，需注册，防重复
动态端口：49152-65535		客户应用进程动态使用

用户希望用名字来标识主机，从而便于记忆和使用。Internet的域名系统（DNS）就是为这种需要开发的。

DNS的逻辑结构是一个分层的**域名树**。

根域。根域没有名称，用句号“.”表示，但经常是省略的。

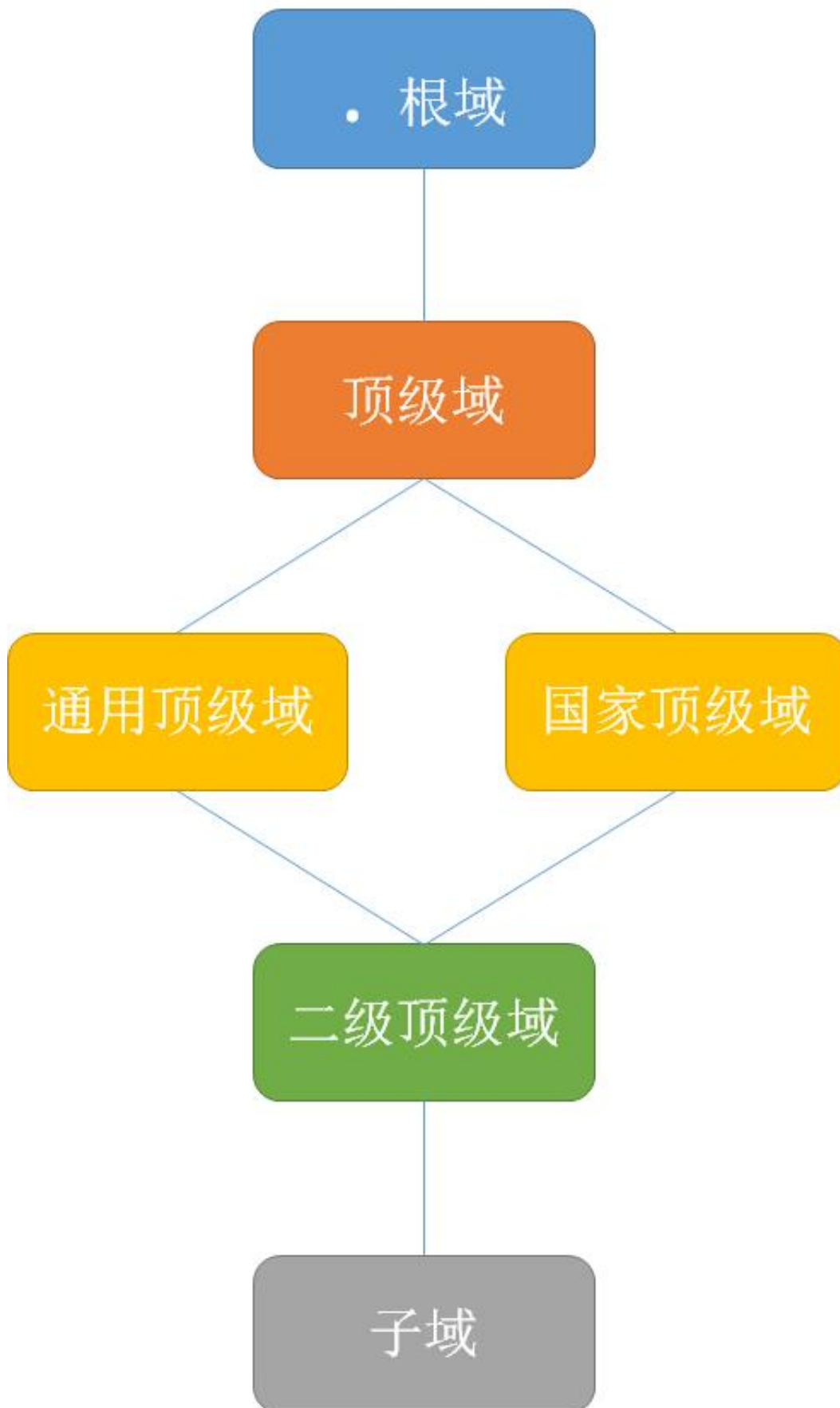
根域下面是**顶级域**（Top-Level Domains，TLD），分为**国家顶级域**（Country conde Top Level Domain，ccTLD）和**通用顶级域**（Generic Top Level Domain，qTLD）。

国家顶级域包含243个国家和地区的代码，**例如**：cn代表中国，uk代表英国等，最初的通用顶级域有7

表 6-4 通用顶级域名

域 名	使 用 对 象
com	商业机构等盈利性组织
edu	教育机构、学术组织和国家科研中心等
gov	美国非军事性的政府机关
mil	美国的军事组织
net	网络信息中心（NIC）和网络操作中心（BIC）等
org	非盈利性组织、例如技术支持小组、计算机用户小组等
int	国际组织

个。



顶级域下面是二级

域, 这是正式注册给组织和个人的唯一名称。在二级域之下, 组织机构还可以划分子域。

域名到IP地址的变换有DNS服务器来实现。客户端/服务结构（C/S结构）

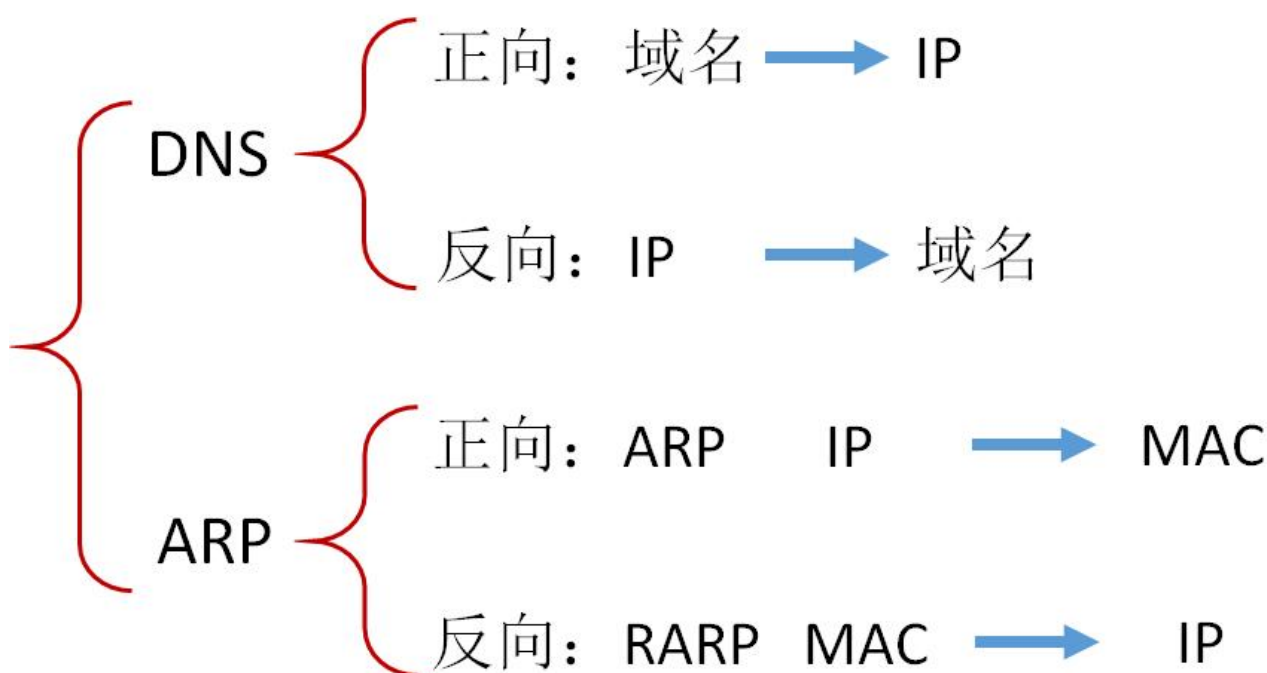
TCP 53端口
 UDP 53端口

IP地址是分配给主机的逻辑地址，还必须考虑主机的物理地址问题。由于有两种主机地址，因此需要一种映像关系把这两种地址对应起来。在Internet中使用地址分解协议（ARP）来实现逻辑地址知道物理地址映像的。

协议类型：发送方使用的协议，0800H表示IP协议。

发送方使用的
 协议，0800H
 表示IP协议

硬件类型		协议类型
硬件地址长度	协议地址长度	操作
发送节点硬件地址		
发送节点协议地址		
目标节点硬件地址		
目标节点协议地址		



- 1) 查本地内存ARP地址映像表。
 - 2) 如果ARP表查不到, 就广播一个ARP请求分组。
- 所谓代理ARP (Proxy ARP), 就是路由器“假装”目标主机来回答ARP请求。

(PDF 227页有个关于ARP的图, 重听了视频再补充)

RARP (Reverse Address Resolution Protocol) 是反向ARP协议。由硬件地址查找逻辑地址。多用于无盘工作站。

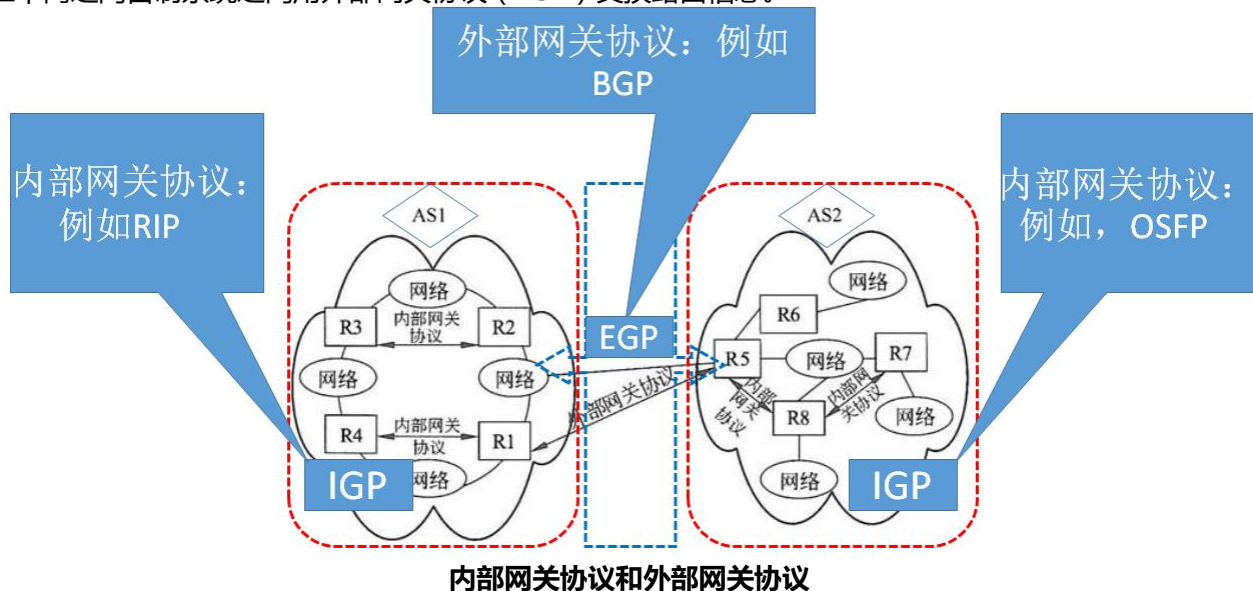
MAC查找IP

网关协议, Internet中的路由器叫做IP网关。网关协议就是用于网关之间交换路由信息的协议。

自治系统, 自治系统是由同构型的网关连接的因特网, 自治系统内部的网关之间执行内部网关协议

(IGP), 互连系统, 为特定的应用服务, 在自治系统之外是无效。

在不同之间自治系统之间用外部网关协议 (EGP) 交换路由信息。



最新的外部网关协议叫做BGP (Border Gateway Protocol)。BGP4已经广泛使用在ISP的网络间。

BGP4+ 可以用于IPV6

BGP4是一种动态路由发现协议, 支持无类别域间路由CIDR。BGP的主要功能是控制路由策略, BGP的4种报文。这些报文通过TCP (179端口) 连接传送。

表 6-6 BGP 的 4 种报文

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

内部网关协议, 网关协议也叫做路由协议 (Routing Protocol), 是路由器之间实现路由信息共享的一种机制, 它允许路由器之间通过交换路由信息维护各自的路由表。

常用的内部路由协议包括路由信息协议 (RIP); 开放最短路径优先协议 (OSPF); 中间系统到中间系统的协议 (IS-IS); 内部网关路由协议 (IGRP) 和增强的IGRP协议 (EIGRP) 等。最后两种是思科公司的

常用的是RIP（小网络）和OSPF（大网络）

路由信息协议

RIP适用于小型网络，因为它允许的跳步不超过**15步**。

（笔记07 PDF 231页）

RIPv1

- 1) RIPv1使用本地**广播**地址255.255.255.255发布路由信息，默认路由更新周期为30s，如果在180s内没有收到某邻居的路由更新报文，则认为该邻居已不存在。
- 2) RIP以**跳步计数**（Hop Count）来度量路由费用。
- 3) RIPv1是**有类别**的协议（Classful Protocol），不能把C类网络掩码255.255.255.0，用于B类网络，172.16.0.0。
- 4) RIP可以实现等费用通路的**负载均衡**。

RIPv2

RIPv2是增强了的RIP协议，有3方面改进：（1、2为一方面）

- 1、首先它使用**组播**而不是广播来传播路由更新报文。
- 2、采用触发更新（Triggered Update）机制来加速路由收敛。
- 3、是一个无类别协议（Classless Protocol），可以使用可变长子网掩码（VLSM），也支持无类别域间路由（CIDR）。
- 4、RIPv2支持认证，使用经过散列的口令字来限制路由更新信息的传播。

路由收敛：指网络的拓扑结构发生变化后，路由表重新建立到发送再到学习直至稳定，并通告网络中所有相关路由器都得知该变化的过程。也就是网络拓扑变化引起的通过重新计算路由而发现替代路由的行为。

路由收敛和水平分割

相邻的路由器之间**周期性**地交换路由表，并通过逐步交换把路由信息扩散到网络中所有的路由器。

解决路由环路问题可以采用水平分割法（Split Horizon）。一条路由信息不会被发送给该信息的来源。

借钱后不还了

带有**反毒化**的水平分割方案（Split Horizon with Poisoned Reverse），“把从邻居学习到的路由费用设置为无限大，并立即发送给那个邻居”

借钱后，在无限期之后还

触发更新技术也能加快路由收敛。

我有事了，要还钱

RIP报文格式

RIPv2报文封装在**UDP数据报**中发送，占用端口号**520**

OSPF协议

OSPF (RFC 2328 , 1998) 是一种链路状态协议, 用于在自治系统内部的路由器之间交换路由信息。

OSPF 具有支持大型网络, 占用资源少, 路由收敛快等优点。**很重要的地位。**

链路状态协议从各个路由器收集链路状态信息, 构成网络拓扑结构图, 使用Dijkstra的最短通路优先算法 (shortest Path First , SPF) 计算到达各个目标的最佳路由。

距离矢量是周期性的发布路由信息, 而链路状态协议是在网络拓扑发生变化时才发布路由信息, 而且OSPF采用TCP连接发送报文, 通信**更可靠**。

为了适应大型网络配置的需要, OSPF协议引入了“ 分层路由 ”的概念。所以典型的链路状态协议都把网络划分成较小的区域 (Area)。OSPF主干网负责在各个区域之间传播路由信息。主干网本身也是OSPF区域, 称为区域0 (Area 0), 主干网的拓扑结构对所有的跨区域的路由器都是可见的。

分层路由≈分区域

主干区域 Area 0

每个OSPF区域都指定了一个32位的区域标识符, 可以用点分十进制表示, 例如主干区域的标识符可表示为0.0.0.0。OSPF的区域分为以下**5种**:

1) 标准区域, 可接任何链路更新信息和路由汇总。

标准员工

2) 主干区域, 连接各个区域的传输网络。拥有标准区所有特性

技术骨干

3) 存根区域: 不接收自治系统以外的路由信息。

内定人员

4) 完全存根区域: 不接收自治系统以外的路由信息, 也不接收自制系统内的的路由汇总信息。(Cisco定义, 非标准)

不可救药

5) 不完全存根区域 (NSAA), 类似存根区, 但允许接收以**类型7**的链路状态公告。

内定, 除非领导7次安排

OSPF网络4种类型:

1) 点对网络, 例如一对路由器用64Kb的串行线路连接, 就属于点对点网络。

2) 广播多址网络: 例如**以太网**, **广播**路由信息给所有路由器。

3) 非广播多址网络 (Non-Broadcast Multi-Access , NBMA), 例如: **X.25**分组交换网。通过**组播**方式发布路由信息。

4) 点到多点网络。

路由器通过OSPF的**Hello协议**来**发现邻居**。在一个广播网络或者NBMA网络中要选一个**指定路由器** (Designated Router , **DR**), 其他的路由器都与DR建立毗邻关系, 把自己掌握的链路状态信息提交给DR, 由DR代表这个网络向外界发布。从而减少向外部发布路由的路由信息量。(备份服务器BDR)

OSPF路由器

- 1) 内部路由器
- 2) 主干路由器
- 3) 区域边界路由器ABR
- 4) 自治系统边界路由器 (ASBR)

链路状态公告

OSPF路由器之间通过链路状态公告 (LSA)

LSA有几种不同类型的报文。

表 6-7 LSA 类型

类型	名 称	发 送 者	传 播 范 围	描 述
1	路由器 LSA	任意 OSPF 路由器	区域内	路由器在区域内连接的链路状态
2	网络 LSA	DR	区域内	指定路由器 DR 在区域内连接的各个路由器
3	网络汇总 LSA	ABR	主干区域	ABR 连接的本地区域中的链路状态
4	ASBR 汇总 LSA	ASBR	主干区域	自治系统边界路由器 ASBR 的可到达性
5	外部 LSA	ASBR	除存根区之外的其他区	自治系统之外的路由信息
6	组播 LSA			用于建立组播分发树
7	NSSA LSA	连接到 NSSA 的 ASBR	不完全存根区 Not-So-Stub-Area	到达自治系统之外的目标的路由可以由 ABR 转换为类型 5 的 LSA

OSPF的**5种报文**，这些报文通过**TCP连接**传送。采用目标地址224.0.0.5代表所有的OSPF路由器。Hello协议用于发现邻居，建立毗邻关系，还用于选出区域内指定路由器**DR**和备份路由器**BDR**。

组播地址：224.0.0.5所有路由器
 224.0.0.6指定路由器

表 6-8 OSPF 的 5 种报文类型

类型	报 文 类 型	功 能 描 述
1	Hello 建立外交	用于发现相邻的路由器
2	数据库描述 DBD (DataBase Description) 外交书内容	表示发送者的链路状态数据库内容
3	链路状态请求 LSR (Link-State Request) 向对方请求外交	对方请求链路状态信息
4	链路状态更新 LSU (Link-State Update) 发送外交更新通告	邻居路由器发送链路状态通告
5	链路状态应答 LSAck (Link-State Acknowledgement)	对链路状态更新报文的应答

对外交更新的应答

OSPF的优缺点

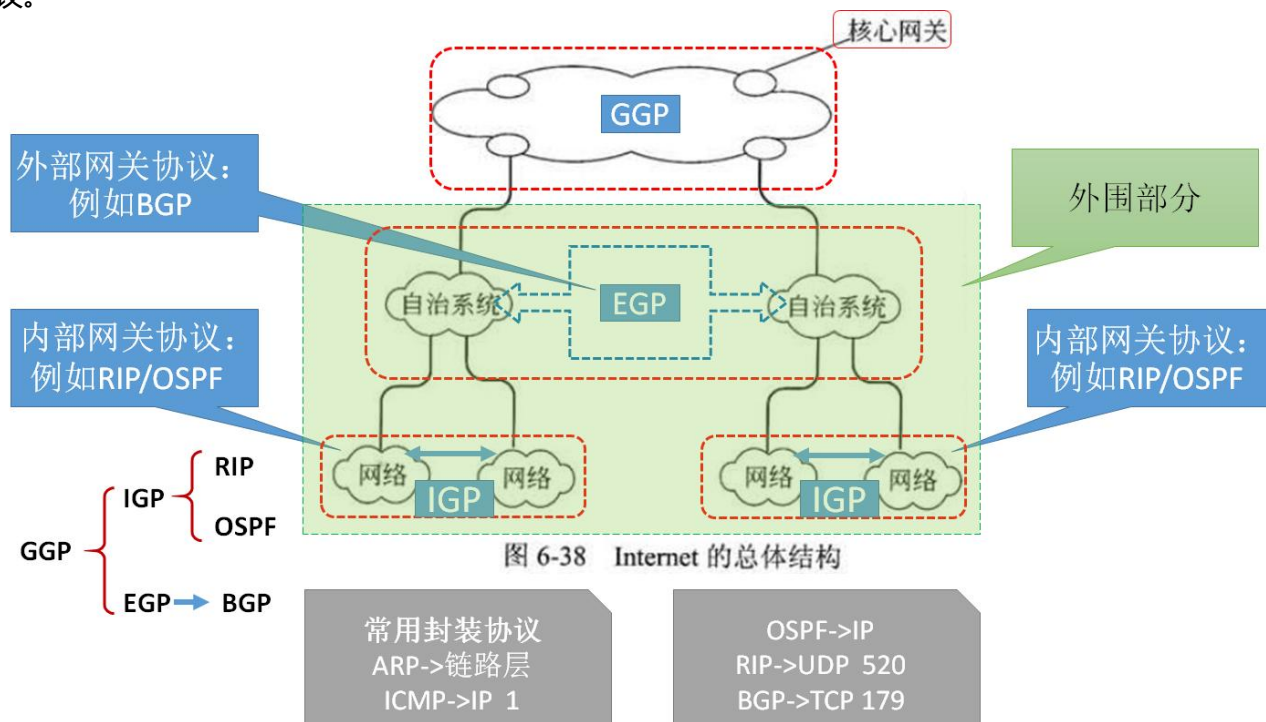
- 1) 链路状态协议使用了**分层的**网络结构，减小了LSA的传播范围，同时也减小了网络拓扑变化时影响所有路由器的可能性。**例如**：OSPF协议中，一个分区内部的拓扑变化不会影响其它分区。
- 2) 链路状态协议使用组播来共享路由信息，并且发布的是**增量式**的更新消息。使得网络带宽的利用和资源消耗更有效。
- 3) 链路状态协议支持**无类别**的路由和路由汇总功能，可以使用VLSM和CIDR技术，从而减少运行SPF算法的更新路由需要的CPU周期，也减少了路由器中的存储需求。

4) 使用SPF算法不会在路由表中出现环路。

链路状态有一个明显的缺点, 对CPU和存储器的要求更高, 链路状态协议需要维护更多的存储表。

核心网关协议

主干网中的网关叫核心网关。核心网关之间交换路由信息时使用核心网关协议 (Gateway to Gateway Protocol, GGP), EGP用于两个不同自治系统之间的网关交换路由信息, 而GGP是主干网中的网关协议。



GGP协议的报文格式与EGP类似。报文分为以下4类。

路由更新报文：发送路由信息。

应答报文：对路由更新报文的应答, 分肯定、否定两种。

测试报文：测试相邻网关是否存在。

网络接口状态报文：测试本地网络连接的状态。

因特网面临的另外一个问题是IP地址短缺问题。解决这个问题有所谓长期的或短期的两种解决方案, 长期的解决方案是具有更大地址空间的IPv6, 短期的解决方案有网络地址翻译 (NAT) 和无类别的域间路由技术 (CIDR) 等, 都在现有IPv4路由器中实现。

NAT技术主要解决IP地址短缺问题。

第一种应用是动态地址翻译 (Dynamic Address Translation)。可以把一个大的地址空间映射到一个小的地址空间。

另一种特殊的NAT应用是m:1翻译, 这种技术叫做伪装 (Masquerading), 因为用一个路由器的IP地址可以把子网中所有主机的IP地址隐藏起来。如果子网中有多个主机同时都要通信, 那么要对端口号进行翻译, 所以这种技术经常被称为网络地址和端口翻译 (Network Address Port Translation, NAPT)。

CIDR技术可以解决路由缩放问题, 所谓路由缩放问题, 1、对于大多数中等规模的组织没有适合的地址空间。2、路由表增长太快, 网络号占用一行, 路由表太大, 查找速度慢。

超网 (supernet)

小网合并为大网

子网

大网划分成多个小网

所谓三层交换, 是指利用第二层交换的高带宽和低延迟优势尽快的传送网络层分组的技术, 交换与路由不同, 前者用硬件实现, 速度快, 后者由软件实现, 速度慢。三层交换机的工作原理可以概括为: 一次路由, 多次交换。

三层交换机不但具有路由功能, 而且比通常的路由器转发得更快。

多协议标记交换 (MPLS) 可称为2.5层。



MPLS标记的标准格式

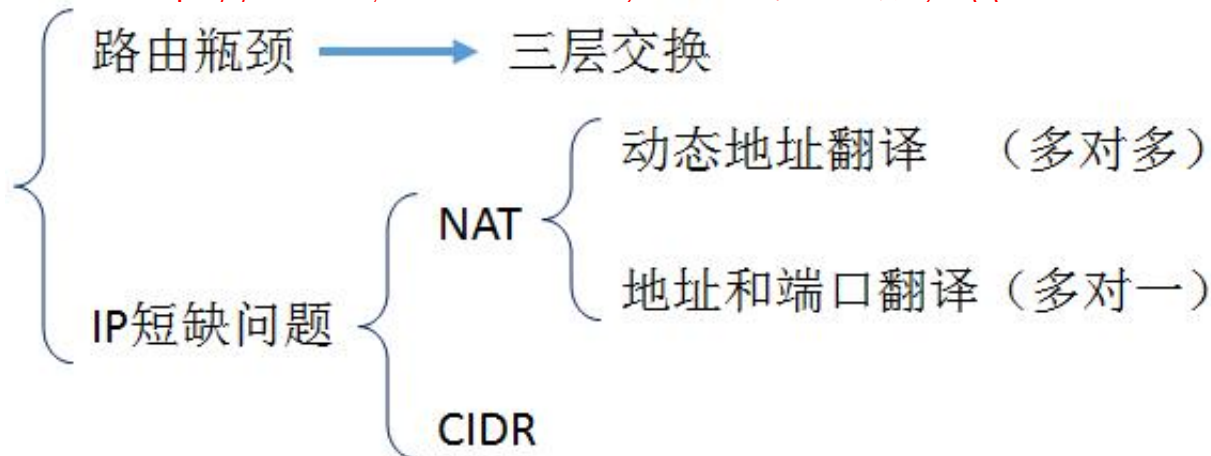
标记边缘路由器 (LER) 为其加上一个标记, 而且还引用了IP头中的源地址字段、传输层端口号和服务质量等。标记交换路由器 (LSR)

MPLS的工作原理: 为每个IP数据包提供一个标记, 并由此决定数据包的路径和优先级。



MPLS标记具有局部性, 一个标记只是在一定的传输域中有效。

MPLS转发处理简单, 提供显式路由, 能进行业务规划, 提供QoS保障, 提供多种分类粒度, 用一种转发方式实现各种业务的转发。MPLS具有可扩展性强、兼容性好、易于管理等优点。



新增内容：

一个IP地址代表一个主机，但**D类**IP地址指向网络中的一组主机。由一个源向一组主机发送信息的传输方式称为**组播**（Multicast），例如IPTV、网络会议、远程教育。

老师上课，喊某组人回答问题

IGMP（Internet Group Management Protocol）协议用于支持接受者**加入或离开**组播组。一旦有接受者加入一个组，就要为这个组在网络中构建一个**组播分布树**。生成和维护组播树的协议有许多种，例如独立组播协议PIM（Protocol Independent Multicast）等。

实现IP组播的前提是组播源和组成员支持组播。

支持的功能包括：

TCP/IP支持组播。

网络接口支持组播。

组管理协议，加入或离开组播。

第三层组播地址能映射到MAC地址。

软件支持IP组播功能。

成员间中间节点支持组播。

IP组播地址的分类。

1、224.0.0.0~224.0.0.255，用于路由协议，例如，224.0.0.1代表本地子网中的所有主机，224.0.0.2代表本地子网中的所有路由器，224.0.0.5代表所有OSPF路由器，224.0.0.9代表所有RIP2路由器，224.0.0.12代表DHCP服务器或中继代理，224.0.0.13代表所有支持PIM的路由器。

224.0.0.6

指定路由DR

2、224.0.1.0~238.255.255.255：用于**全球范围**的组播地址分配。

相当于公网IP

3、239.0.0.0~239.255.255.255：可以在本地子网中作为组播地址使用。

相当于内网IP

以太网组播地址

通常有两种组播地址, 一种IP组播地址, 另一种是以太网组播地址。

其映像方式是把IP地址的**低23位**复制到MAC地址的**低23位**。IANA保留一个以太网地址块**0x0100.5E00.0000**。

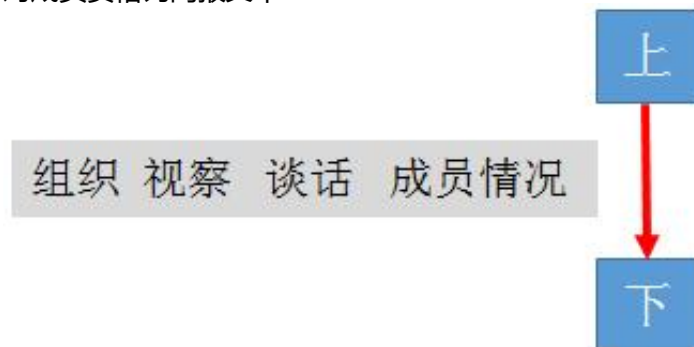
IGMP是在IPv4环境中提供组管理的协议, 以支持主机加入或离开组播组, 在IPv6环境中, 组管理协议已经合并到ICMPv6协议中, 不需要单独的组管理协议。

IGMPv3, 1、询问 2、报文 3、组记录

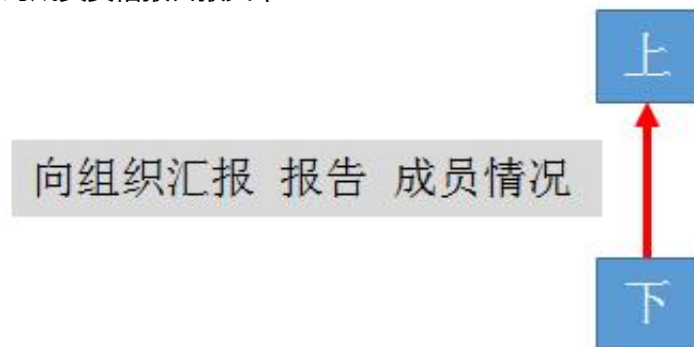
IGMP报文封装在IP数据报中传输。



对成员资格询问报文中:



对成员资格报告报文中:

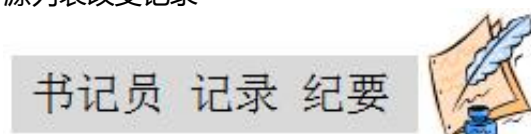


对组记录格式:

当前状态记录。

过滤模式改变记录

源列表改变记录



IGMP操作

1、加入一个组, 主机要发送成员则个**报告**报文。

加入组织

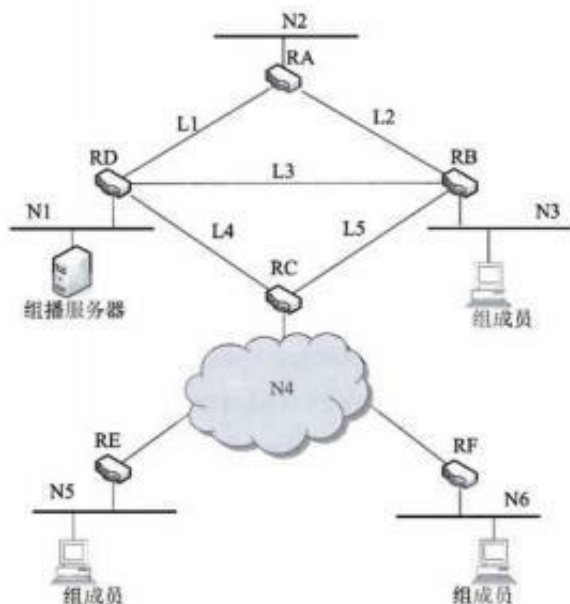
2、为了维护一个当前活动的组播地址列表, **周期性IGMP**通过**询问报文**, 封装在224.0.0.1 (所有主机)。组播路由器无须知道组播组中的每一个主机的地址, 对于一个组播组, 它只需要知道至少有一个组播成员处于活动状态就可以了。每个组只有一个成员对组播路由器的询问返回报告报文。

组织管理

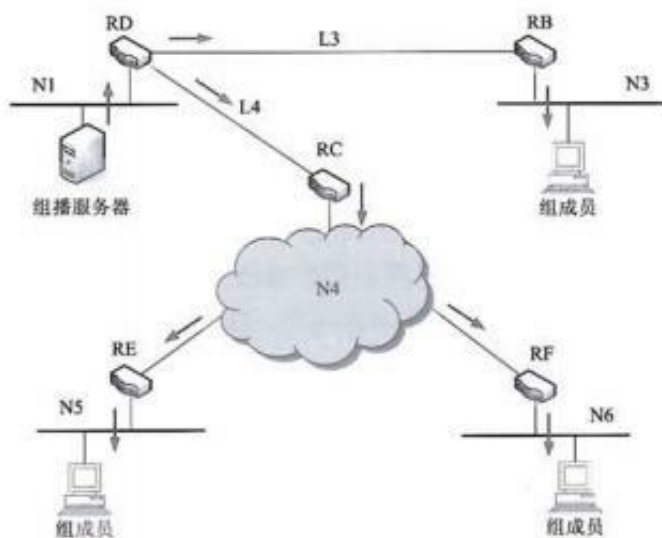
3、主要要离开一个组时, 它向所有路由器 (224.0.0.2) 发送一个组离开**报告**。

脱离组织

建立组播树是实现组播传输的关键技术, 是以组播源为树根的最小生成树 (Spanning Tree STP)



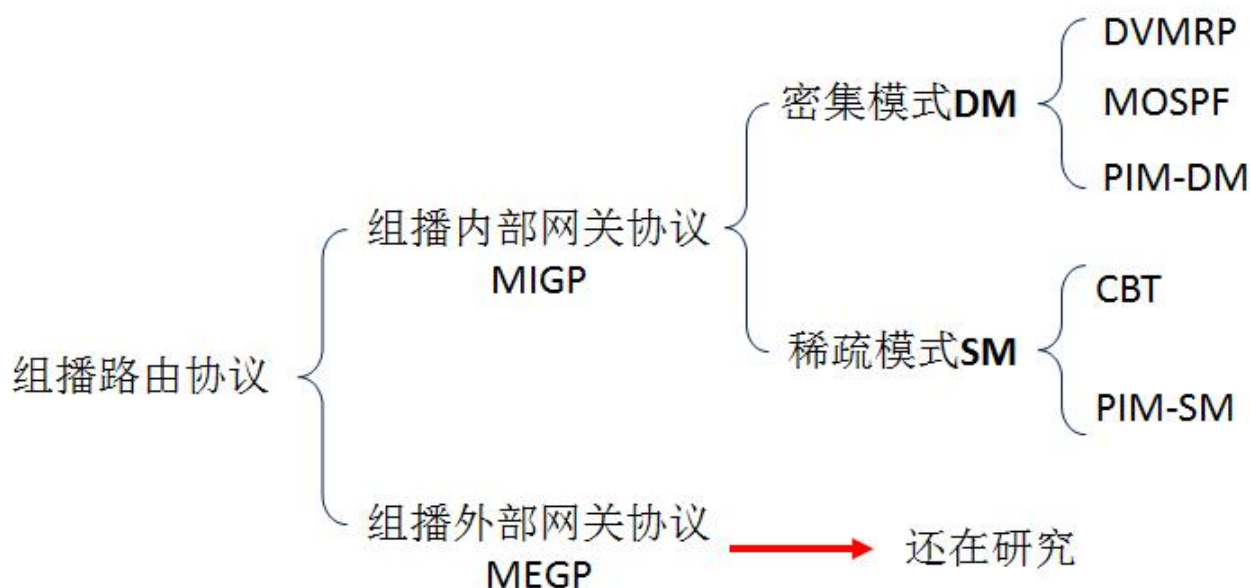
(a) 网络配置



(b) 对应的组播树

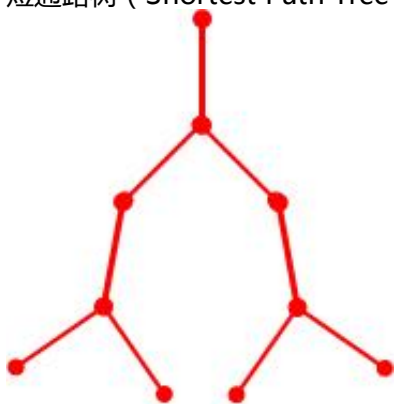
建立组播树要使用组播路由协议。组播内部网关协议 (MIGP), 包括了DVMRP、MOSPF、CBT、PIM-DM、PIM-SM。

组播外部网关协议 (MEGP) 还在研发中。



组播树分两种：

1、源专用树 (Source-Specific Tree) 是以每一个组播源为根建立最小生成树，PIM协议把这种树叫做最短通路树 (Shortest Path Tree, SPT)



生成树 树形

2、共享分部树。该方案利用了由 (一个或多个) 路由器组成的分布中心来生成一棵组播树，由这棵树负责所有组播的通信。PIM协议称这种树为约会点树 (Rendezvous Point Tree, RPT)



约会树 发散

密集模式路由协议 (Dense Mode Routing Protocols) 密集模式路由协议距离矢量组播路由协议 (Distance Vector Multicast Routing , **DVMRP**)、组播开放最短路径优先协议 (Multicast Open Shortest Path First , **MOSP**) , 以及密集模式的独立组播协议 (Protocol Independent Multicast-Dense Mode , **PIM-DM**) 等。

每一个PIM-DM路由器都要维护一个树信息库 (Tree Information Base , TIB) 其中保存着各个组播树的工作状态, 利用这些状态可以建立一个组播转发表, 以实现组播数据报的正确转发。

(笔记7 , PDF 256页)

首先是广播数据, 然后剪掉不需要的分支, 这一过程被称为泛洪-修剪循环, 这是所有密集模式协议中使用的**关键技术**。

稀疏模式路由协议 (Sparse Mode Routing Protocols) 适用于带宽小、组播成员分布稀疏的互联网。CBT (Core-Based Trees) 协议建立了一棵为所有组播会话服务的组播树, 独立组播协议PIM-SM (Protocol Independent Multicast Sparse Mode) 既可以为每个组播建立一个以约会点为树根的共享树, 也可以为每个组播源建立一棵最短通路树。通过这种方式建立SPT树, PIM除了密集模式和稀疏模式之外, 还有一种双向PIM协议 (Bi-directional PIM , BIDIR-PIM) , PIM控制报文封装在IP数据报中传送, 可以组播给所有PIM路由器, 也可以单播到特殊的目标。

IP QoS技术

QoS (Quality of Service , 服务质量)

网络流量 优先级 分出三六九等

- 1、继承服务体系结构 (Integrated Service Architecture , ISA)
- 2、区分服务 (Differentiated Service , Diffserv)

粗分: 网络质量分成三大类业务流, 提供网络服务

IETF集成服务 (IntServ) 3种类型:

- 1、保证质量服务 (Guaranteed Services)
- 2、控制负载服务 (Controlled-load Services)
- 3、尽力而为的服务 (Best-Effort)

资源预留协议 (Resource Reservation Protocol , RSVP) , RSVP是从源到目标单向预约的, 适用于点到点以及点到多点的通信环境。

区分服务 (DiffServ)

IP分组都要根据其QoS需求打上一个标记, 这种标记称为DS码点 (DS Code Point , DSCP) , 可以利用IPv4协议头中的服务类型 (Typy of Service) 字段, 或者IPv6协议头中的通信类别 (Traffice Class) 字段来实现, TOS。

细分: 把相同的业务汇聚成若干个业务流, 提供网络服务

流量工程 (Traffice Engineering , TE)

远程登录 (Telnet) , 通过TCP连接23端口, 定义了网络虚拟终端 (Network Virtual Terminal , NVT) , 采用C/S工作方式。

文件传输协议 (File Transfer Protocol , FTP) , 通过TCP21端口传送控制信息, TCP20端口传送文件内容。匿名FTP, 采用专门用户标识符 “anonymous” 。

简单邮件传输协议 (Simple Mail Transfer Protocol , SMTP) 远程服务进程使用TCP 25端口建立连接。

接收方从邮件服务器取回邮件要用到POP3 (Post Office Protocol 第3版) 协议。通过TCP 110端口建立连接, 下载邮件。

超文本传输协议 (Hyper Text Transfer Protocol , HTTP) 通过TCP 80端口 提供WEB服务, B/S机构。

浏览器通过统一资源定位器 (Uniform Resource Locators , **URL**) 例

如: <http://www.w3.org/welcome.html>是一个URL, 其中http是**协议名称**, www.w3.cog是服务器主机名, welcome.html是**网页文件名**

与WWW。有关的另外一个重要协议是公共网关接口 (Common Gateway Interface , CGI) 当Web用户要使用某种数据库系统时可以写一个CGI程序 (叫做脚本Script) , 作为Web与数据库之间的接口。CGI脚本程序跨越了不同服务器的界限, 可与运行在任何数据库管理系统上。

新增

P2P

点对点应用 (Peer-to-Peer , P2P) , 在这种模式中, 没有客户机和服务器的区别, 每个主机, 既是客户机, 又是服务器, 他们的角色是对等的, P2P是一种对等通信网络模型。

BitTorrent

没有服务中心, 也没有路由中心的网络称为 “纯” P2P网络, 有管理用户信息的索引服务器, 在索引服务器的引导下, 与其他对等方建立网络连接。BitTorrent是最早出现的P2P文件共享协议。

BitTorrent与Web浏览器不同:

- 1、BT在许多不同TCP端口上各自请求一小段数据, WEB在一个TCP端口上执行整个HTTP GET操作。
- 2、Bittorren下载是随机的, 实行稀有者优先 (rarest-first)下载的原则, 而HTTP是完全按照顺序下载的。

3、典型的BitTorrent下载是逐渐提升速度，并在下载完成后时又逐步下降速度，这些特点与HTTP服务器下载完全相反。

Kademlia算法

第一代P2P网络依赖中心跟踪器。

第二代P2P网络采用泛洪搜索法

第三代P2P网络使用分布式哈希表

当前主流的P2P软件大多采用分布式哈希表作为辅助检索协议，例如eMule、BitComet、Bitspirit、和Azureus。

运行Kademlia协议网络称为Kad网络。

第7章 下一代互联网

笔记本: 网络工程师学习

创建时间: 2015/1/21 11:47

更新时间: 2015/1/21 11:47

URL: about:blank

笔记09 PDF 275页

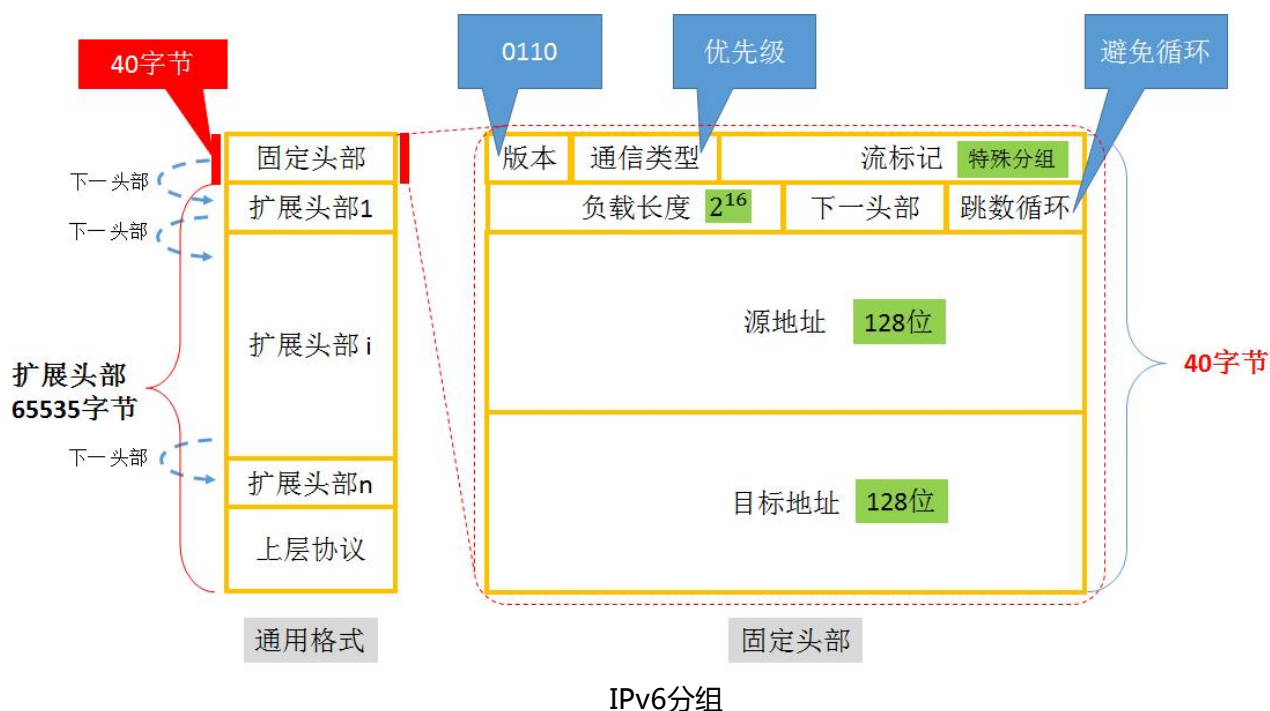
下一代互联网 (Next Generation Internet , NGI) , 我国下一代互联网 CNGI

IPv4主要问题:

- 1、网络地址短缺。
- 2、路由速度慢。
- 3、缺乏安全功能。
- 4、不支持新的业务模式。

下一代IP协议 (IPng)

整个IPv6分组由: 1) 一个固定头部, 2) 若干个扩展头部, 3) 上层协议的负载。



(09笔记, PDF, 276页)

通信类型: (8位): 用于区分不同的IP分组, 相当于IPv4中的**服务类型字段**。

跳数限制: (8位): 用于检测路由循环, 每个转发路由器对这个字段减1。

IPv6有6中扩展头部, **任选的**。

IPv6的扩展头部:

逐跳选项

目标选项

路由选择

分段

认证

封装安全负荷

如果一个IPv6分组包含多个扩展头, 建议采用下面的封装**顺序**:

- 1) IPv6头部
- 2) 逐跳选项头
- 3) 目标选项头
- 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
- 9) 上层协议头部。

IPv6地址扩展到128位。

IPv6地址采用冒号分割的十六进制表示。

冒分十六进制

- 1、每个字段前面的0可以省去, 后面的0不能省。例如0123, 可写为123。
- 2、一个或多个全0字段可以用一对冒号代替, 双冒号只能使用一次。
- 3、IPv4地址仍然保留十进制表示法, 只需要在前面加上1对冒号, 就成为IPv6地址, 称为IPv4兼容地址 (IPv4 Compatible), 例如: ::192.168.10.1
- 4、多个0压缩为1个0。

IPv6地址是一个或一组接口的标识符。IPv6地址分配到接口, 而不是分配给节点。

单播 (Unicast) 地址

教室里面的一位指定的学生

单播地址里两种特殊地址:

- 1) 不确定地址: 地址 0:0:0:0:0:0:0:0
- 2) 回环地址: 地址 0:0:0:0:0:0:0:1

任意播 (AnyCast) 地址

教室里面任意的一位学生

不能做源地址, 只能做目标地址

不能指定给IPv6主机, 只能指定给IPv6路由器。

组播 (MultiCast) 地址

教室里面的一组学生

IPv6中没有广播地址, 它的功能已被组播地址所代替。

笔记09 PDF 282页)

单播地址: 可聚合全球单播地址、链路本地地址、站点本地地址和其他特殊单播地址。

1、可聚合全球单播地址：这种地址在全球范围内有效，相当于IPv4公用地址。

格式前缀： 001

2、链路本地地址：相当于IPv4中的自动专用IP地址（APIPA）

格式前缀： 1111 1110 10

3、站点本地地址：相当于IPv4中的私网地址。

格式前缀： 1111 1110 11

IPv6组播地址

格式前缀： 1111 1111

任意播地址仅用作目标地址，且只能分配给路由器。

表 7-4 IPv4 和 IPv6 地址比较

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
续表	
IPv4 地址	IPv6 地址
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

IPv6有两种自动配置功能：

1) 全状态自动配置

2) 无状态自动配置

IPv4通过DHCP，IPv6通过全状态自动配置（Stateful Auto-Configuration）

下一代RIP协议（RIPng）是对原来RIPv2的扩展，使用UDP的521端口。

OSPFv3，用于支持IPv6，另外增加了八、九类LSA。

BGP4+

ICMPv6协议

ICMPv6新增加的邻居发现功能代替了ARP协议的功能。

对比IPv4，IPv6的改进：

1) 寻址能力方面的扩展。

2) 分组头格式得到简化。

3) 改进了对分组头部选项的支持。

4) 提供了流标记能力。

移动IP

解决用户因为不能在异地联网而感到苦恼。

移动主机能够在任何地方使用它的**家乡地址**进行联网。

移动主机配置一个**家乡地址** (home address) 赋予转交地址 (care-of address)。

1、保持网络连接

2、移动主机包括两类主机, 也就是说**移动主机**是指在离开**家乡网络**的远程站点**可以连网**工作的计算机。

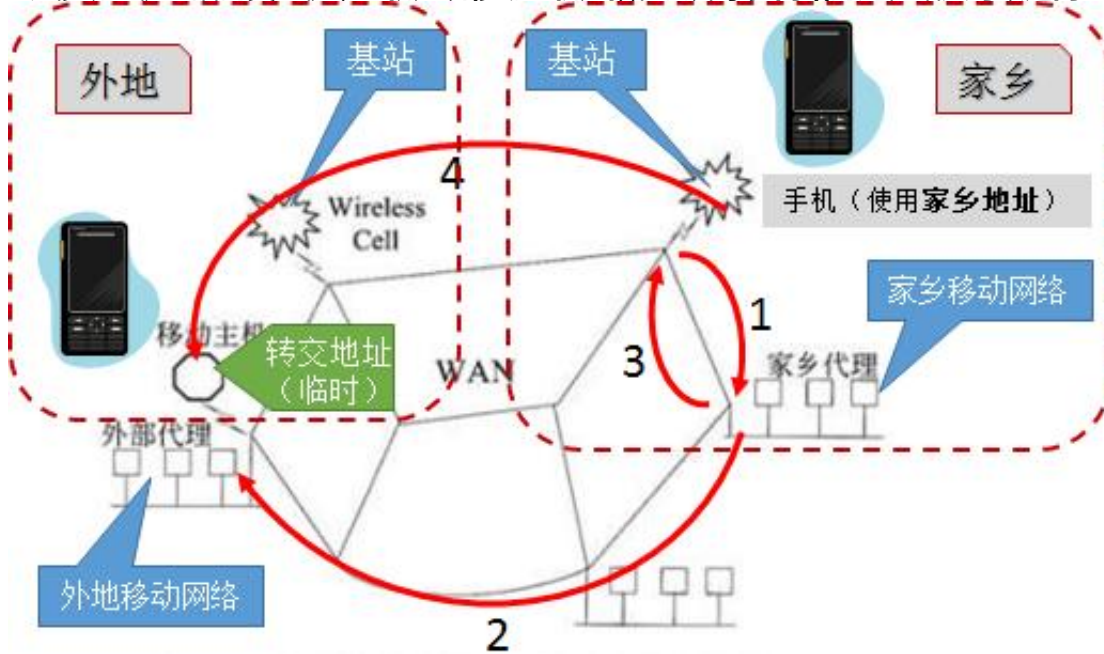


图 7-9 连接局域网和无线通信网的广域网

移动IP提供了两种获取转交地址的方式：

1) 外地代理转交地址 (Foreign Agent Care-of Address)

2) 配置转交地址 (Collocated Care-of Address)

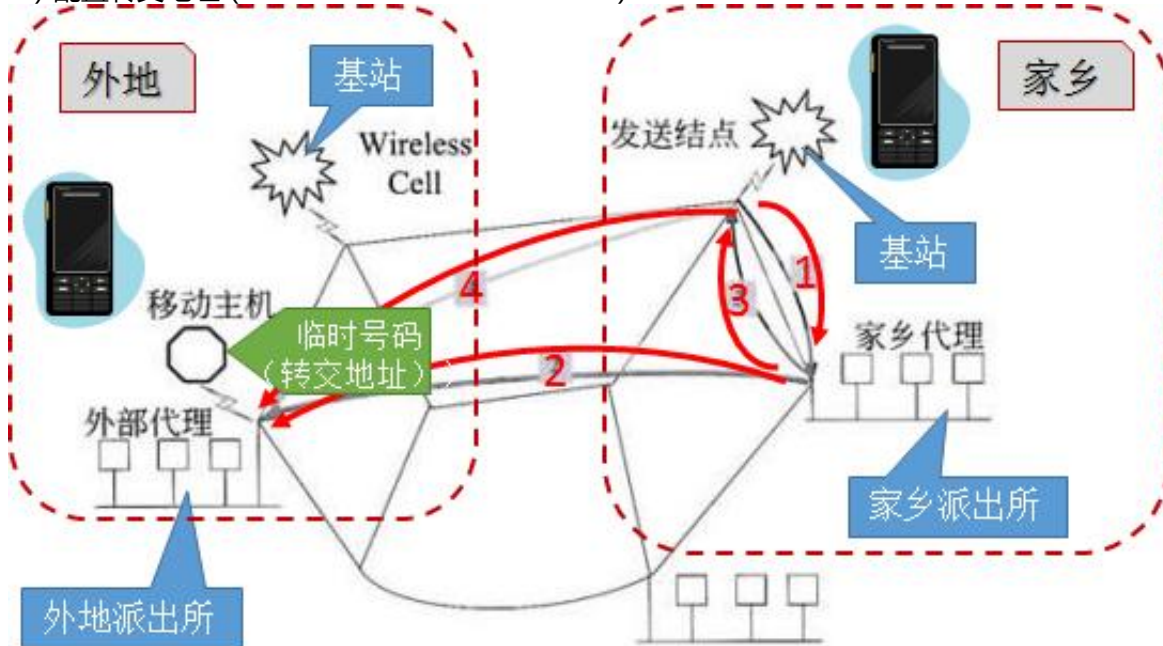


图 7-10 移动主机的通信过程

重要的是要认真区分转交地址和外地代理的功能。它可能是外地代理的地址 (foreign agent care-of address) , 也可能是移动主机获得的临时地址 (co-located care-of address) 外地代理与家乡代理一样, 都是为移动主机服务的**移动代理**。

IPv6对移动主机的支持功能, 定义的协议称为移动IPv6。

过渡技术可以归纳为以下**3种** :

1) 隧道技术

借助v4, 通过v6

2) 双栈技术

V4和v4, v6和v6

3) 翻译技术: 纯IPv6节点与纯IPv4之间。

纯v6和纯v4通信

所谓隧道技术, 就是把IPv6分组封装在IPv4分组中, 通过IPv4网络进行转发的技术。自动隧道技术



1、隧道中介技术

通过隧道服务器配置隧道端点。

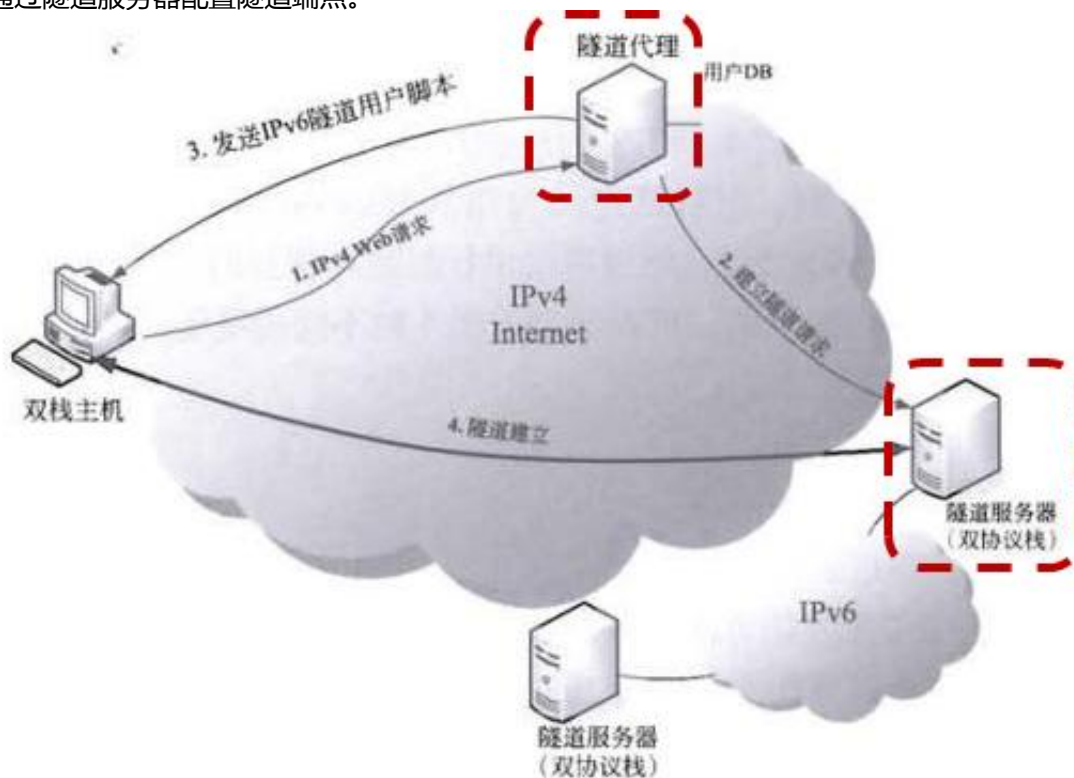


图 7-14 隧道中介

2、自动隧道

实现自动隧道的节点必须采用IPv4兼容的IPv6地址。

3、6to4隧道

6to4是一种支持IPv6站点通过IPv4网络进行通信的技术。

0x2002来表示6to4地址, 6to4前缀就是2002:000:022a::/48, 把16位前缀“2002”的IPv6地址称为6to4地址, 而把不使用这个前缀的IPv6地址称为原生地址(Native Address)。

6to4路由器应该配置双栈协议, 并能实现6to4地址转换。

由于不需要改变主机的配置, 只需要在路由器中进行很少的配置, 所以这种方法的主要优点是简单可行。

4、6over4隧道(地址)

6over4是一种由IPv4地址生成IPv6链路本地地址的方法, IPv6链路本地地址的格式前缀为FE80::/64。

6over4依赖于IPv4组播功能, 但是在很多IPv4网络环境中并不支持组播, 所以6over4技术在实践中受到一定的限制, 在有些操作系统中无法实现。另外一个限制条件是, IPv6主机连接路由器的链路应该处于IPv4组播路由范围之内。

5、ISATAP(地址)

通过IPv4地址自动生成IPv6站点本地地址或链路本地地址, IPv4地址作为隧道的端点地址, 把IPv6分组被封装在IPv4分组中进行传送。

协议翻译技术

协议翻译技术用于纯v6主机与纯v4主机之间的通信。

SIIT: 无状态的IP/ICMP翻译

NAT-PT: 网络地址翻译-协议翻译

SOCKS64: 基于SOCKS的IPv6/IPv4机制。

TRT: IPv6到IPv4的传输中继翻译器

1.SIIT

1) IPv4映射地址(IPv4-mapped), ::FFFF:w.x.y.z的形式, w.x.y.z是IPv4地址, 这种改地址仅用于支持IPv4的主机。

2) IPv4翻译地址(IPv4-translated), ::FFFF:0:w.x.y.z的形式, 这种地址可用于支持IPv6主机。

SIIT转换器规范描述了从IPv6到IPv4的协议转换机制, 包括IP头的翻译方法以及ICMP报文的翻译方法等。

2.NAT-PT

NAT-PT(Network Address Translator-Protocol Translator)是指定一个服务器作为NAT-PT网关, 并且要准备一个IPv4地址块作为地址翻译之用。

NAT-PT操作有3个变种: 基本NAT-PT、NAPT-PT和双向NAT-PT。

基本NAT-PT是单向的, 只允许IPv6主机访问IPv4主机。

NAPT-PT是网路地址端口翻译, 仍然是单向的, 但是扩展到了TCP/UDP端口的翻译, 也包括了ICMP询问标识符的翻译。

双向NAT-PT, 这意味着双向通道, 无论是IPv6主机还是IPv4主机, 都可以向对方发起会话。

协议翻译技术适用于IPv6孤岛与IPv4海洋之间的通信, 这种技术要求一次会话中的双向数据包都在同一个路由器上完成转换, 所以它只能适用于同一个路由器连接的网络。这种技术的优点是不需要进行IPv4和IPv6终端的升级改造, 只要求在IPv4和IPv6之间的网络转换设备上启用NAT-PT功能就可以了, 但是在实

双栈主机有下面两种方法:

BIS (Bump-In-the-Stack)

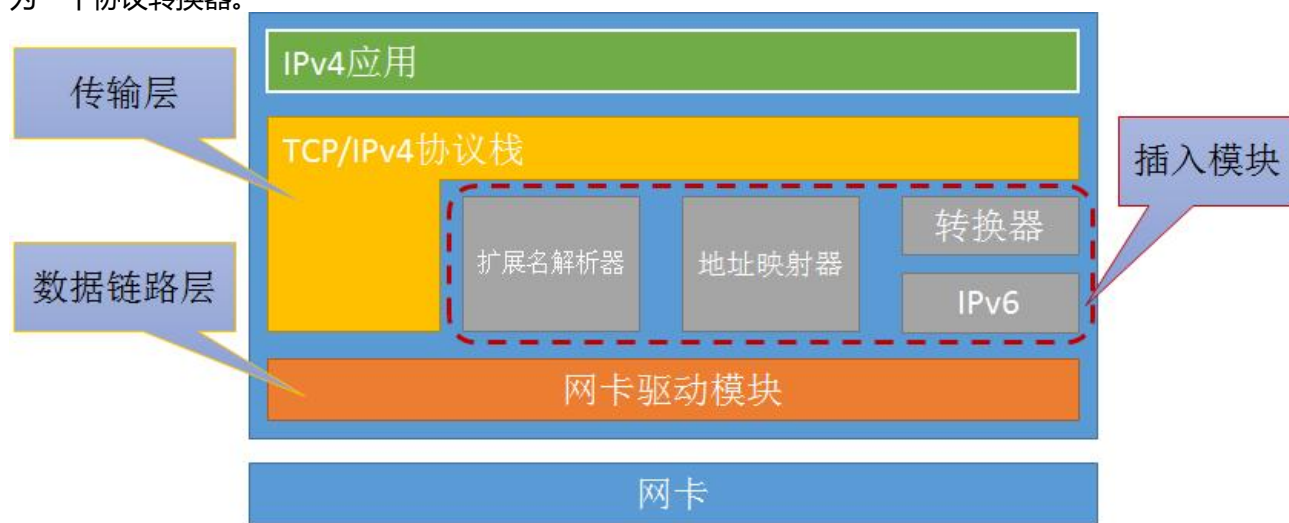
低层: 堆、栈

BIA (Bump-In-the-API)

高层: 应用程序接口

1.BIS

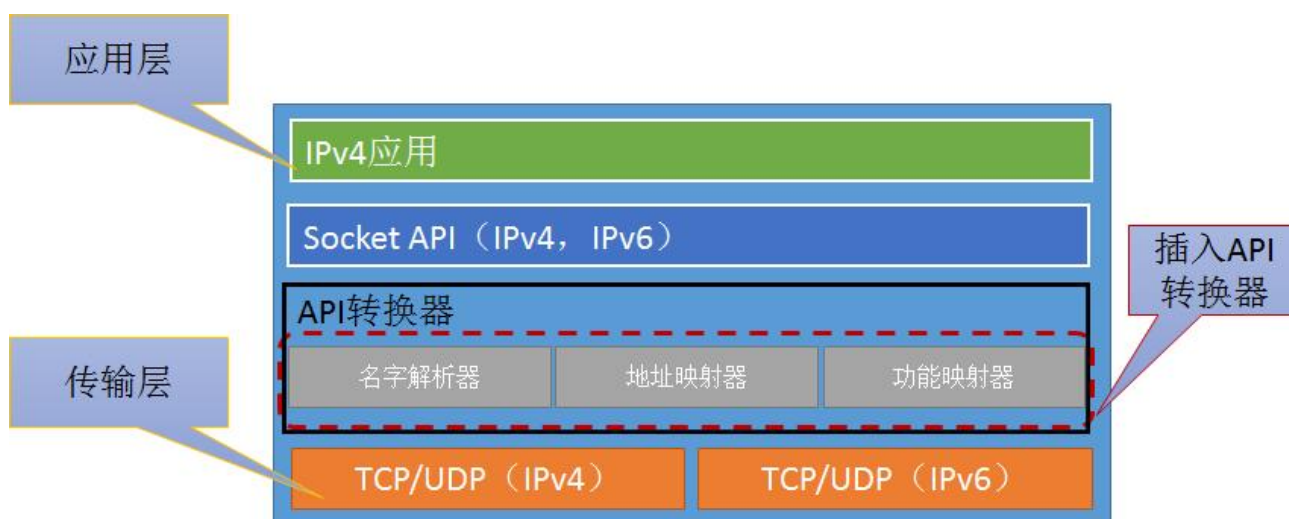
在主机的TCP/IPv4模块与网卡驱动模块之间插入一些模块来实现IPv4与IPv6分组之间的转换, 使得主机成为一个协议转换器。



双协议栈主机结构

2.BIA

BIA是在IPv4 Socket应用与IPv6 Socket应用之间进行翻译的技术。BIA要求在Socket应用模块与TCP/IP模块之间插入API转换器, 这样建立的双栈主机不需要在IP头之间进行翻译, 使得转换过程得到简化。



BIA双栈主机的体系结构

中国下一代互联网示范工程（CNGI）

由6个主干网、两个国际交换中心。CERNET2、中国电信、中国网通/中科院、中国移动、中国联通和中国铁通及国际交换中心。

CERNET2

CERNET2是CNGI中规模最大的主干网，也是目前世界上规模最大的，采用纯IPv6技术的下一代互联网。

GLORIAD，中美俄环球科教网正式开通。

第8章 网络安全

笔记本: 网络工程师学习

创建时间: 2015/1/21 11:49

更新时间: 2015/1/21 11:49

URL: about:blank

数据保密技术, 签名与认证技术, 网络安全的理论和解决方案。

网络安全威胁:

重放: 重复一份报文或报文的一部分, 以便产生一个被授权的效果。

拒绝服务: 当一个授权实体不能获得应有的对网络资源的访问或紧急操作。

基本安全措施: 数据加密、数字签名、身份认证、防火墙和入侵检测等。

- 1) 数据加密: 对信息的重新组合。
- 2) 数字签名: 证明消息是由发送者签发的。
- 3) 身份认证: 认证用户合法性。
- 4) 防火墙: 控制数据包的进出。
- 5) 内容检查。

信息加密技术:

- 1、对称密钥
- 2、非对称密钥
- 3、流密码加密

传统的加密系统是以密钥为基础的, 这是一种**对称密钥**, 也就是说, 用户使用同一个密钥加密和解密。而公钥则是一种**非对称密钥**加密方法, 加密者和解密者各自拥有**不同的密钥**。还有**流密码**等加密算法。

1、DES (Data Encryption Standard) 数据加密标准。

由**56位**的密钥, 最后产生**64位**的密文块。

2、三重DES (Triple-DES) 。

使用两把密钥对报文做三次DES加密, 第一层和第三层中使用相同的密钥, 有效长度**112位**的密钥。

3、IDEA (International Data Encryption Algorithm) , 国际数据加密算法。

128位密钥, 吧明文分成64位的块, IDEA可以用硬件或软件实现。比DES快

4、高级加密标准 (Advanced Encryption Standard , AES)

AES支持128、192和256位3种密钥长度。可以通过软件或硬件实现。

5、流加密算法和RC4

数据流与密钥生成二进制**比特流**进行异或运算的加密过程。

6、公钥加密算法

加密密钥和解密密钥是相同的, 称为公钥密钥算法或者对称密钥算法, 后有使用了不同的密钥进行加密和解谜的公钥加密算法。

用公钥加密, 私钥解密。用私钥加密, 公钥解密, 可实现数字签名。

公钥: 加密和认证

私钥: 解密和签名

7、RSA (Rivest Shamir and Adleman) 算法

选择两个大素数 p 和 q

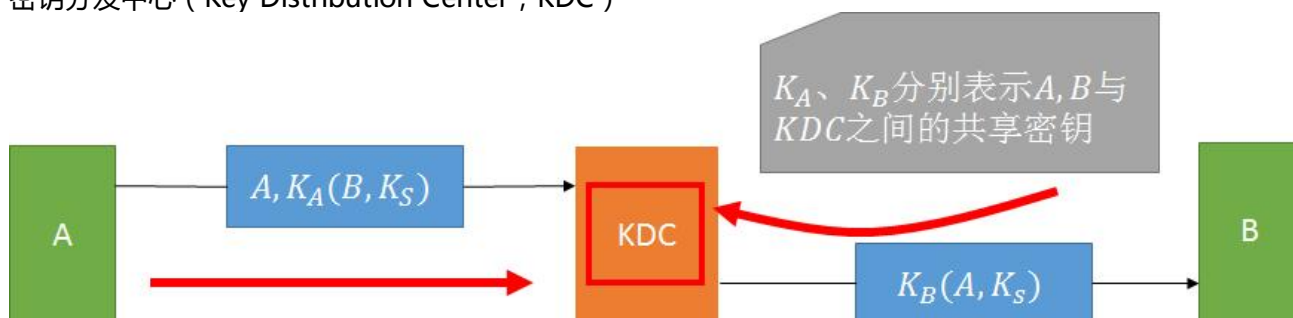
$$\text{令 } n = p * q, z = (p - 1) * (q - 1)$$

认证

证明身份、合法用户、防假冒

确认对方身份。

密钥分发中心 (Key Distribution Center , KDC)



Needham-Schroeder 认证协议 (N-S)

一种多次提问——相应协议, 可以对付**重放**, **随机数**在起作用。

基于公钥的认证

用对方公钥加密, 用各自私钥解密。

数字签名

防抵赖

证明发送者消息

公钥: 加密和认证

私钥: 解密和签名

A 向 B 发送签名的消息 P

1) B 可以验证消息 P 确实来源于 A。

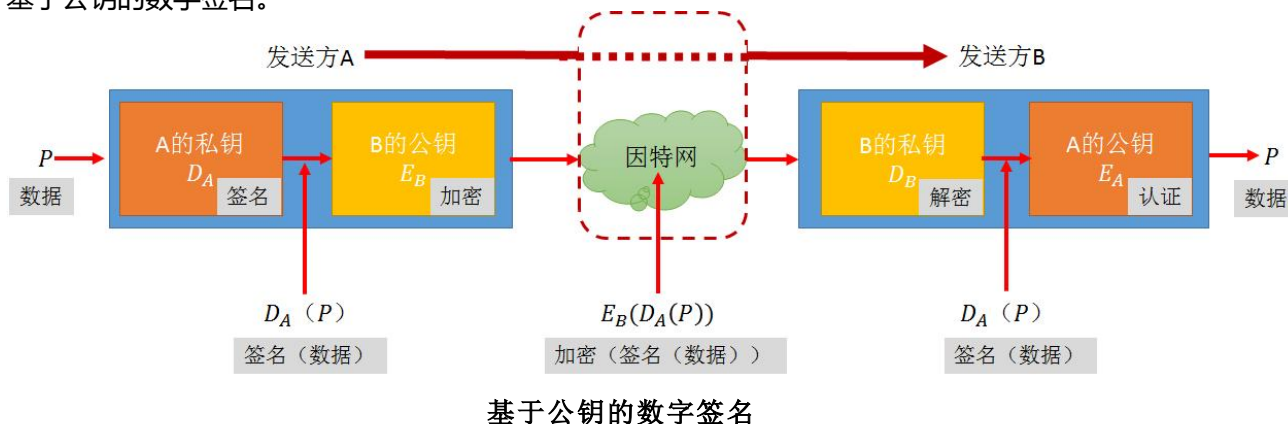
2) A 以后不能否认发送过消息 P。

3) B不能编造或改变消息P。

基于密钥的数字签名

设BB是A和B共同信赖的仲裁人。

基于公钥的数字签名。



报文摘要

防篡改

用于差错控制

报文摘要算法MD5, 产生128位的报文摘要。

安全散列算法 (The Secure Hash Algorithm, SHA), 产生160位的报文摘要。SHA算法的缺点是速度比MD5慢, 但是SHA的报文摘要更长, 更有利于对抗野蛮攻击。

散列式报文认证码 (Hashed Message Authentication Code, HMAC), 可以提供数据完整性数据源身份认证。

HMAC-MD5被指定为IPsec的验证机制, 提供数据认证和数据完整性保护。

电子证书的概念

电子交易

数字证书是各类终端实体和最终用户在网上进行信息交流及商务活动的身份证明。用户的数字证书由某个可信的证书发放机构 (Certification Authority, CA) 建立, 发放。

证书包含, 公钥: 有效的公钥及其使用方法。认证机构的签名: 用CA私钥对证书的签名。

证书的获取, 用户A从机构X1处获取证书, 用户B已从X2处获取证书。

证书链表示为:

《A》 X1 《X2》 X2 《B》

相反的。

《B》 X2 《X1》 X1 《A》

《A》 X 《W》 W 《V》 V 《U》 U 《Y》 Y 《Z》 Z 《B》

密钥管理

保存好密码

密钥管理, 密码自产生到最终销毁。包括初始化, 密钥产生、存储、恢复/备份、装入、分配、保护、更新、控制、丢失、吊销、销毁。

密钥管理体制主要有**3种**:

- 1) 适用于封闭网的技术, 以传统的密钥分发中心为代表的KMI机制;
- 2) 适用于开放网络的PKI机制;
- 3) 适用于规模化专用网的SPK技术。

KMI技术

内网

密钥管理基础结构 (Key Management Infrastructure , KMI) , 密钥分发中心 (KDC)

PKI技术

外网

在密钥管理中, 不依赖秘密信道的密钥分发技术。

公钥基础结构 (Public Key Infrastructure , PKI)

KMI和PKI两种密钥管理体制各有其**优缺点和适用范围**。KMI具有很好的封闭性, 而PKI具有很好的扩展性。

男人外面PK (I)

女人家里看门 (KMI)

KMI主内, PKI主外的密钥管理结构是比较合理的。

虚拟专用网 (Virtual Private Network , VPN) , 特点: 1、建立在公网上。2、虚拟性。3、专用性。

VPN的4种关键技术:

- 1) 隧道技术 (Tunneling)

- 2) 加密技术 (Encryption&Decryption)。
- 3) 密钥管理技术 (Key Management)
- 4) 身份确认技术 (Authentication)

VPN的3种解决方案：

- 1) 内联网VPN (Intranet VPN)，用于实现企业内各部门各个LAN之间的安全互连。

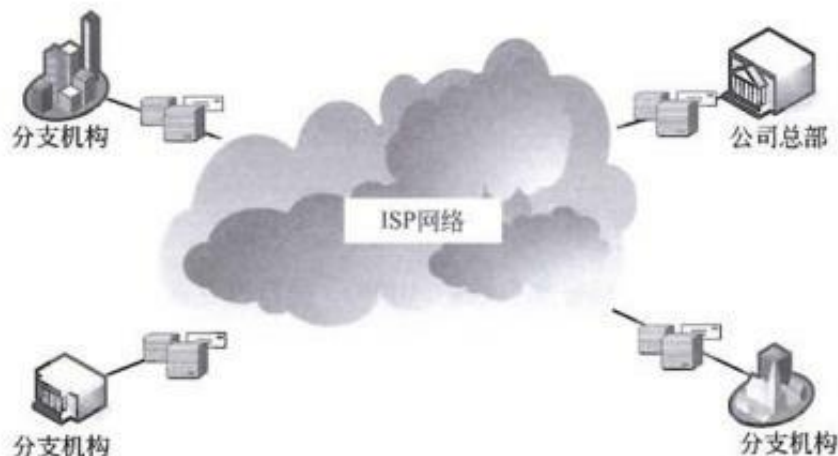


图 8-14 Intranet VPN

- 2) 外联网VPN (Extranet VPN)，用于实现企业与客户、供应商和其它相关团体之间的互连互通。



图 8-15 Extranet VPN

- 3) 远程接入VPN (Access VPN)，解决远程用户访问企业内部网络。

出差

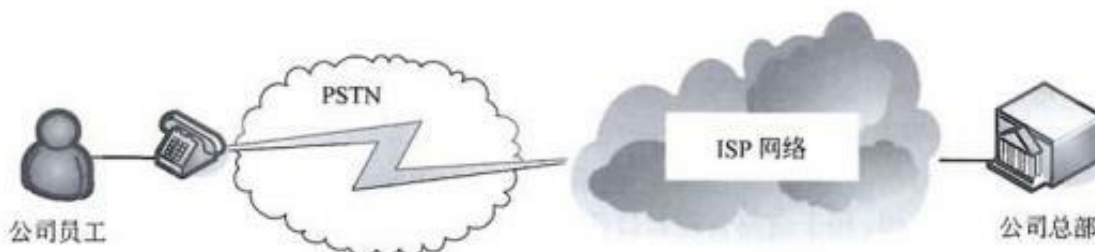


图 8-16 Access VPN

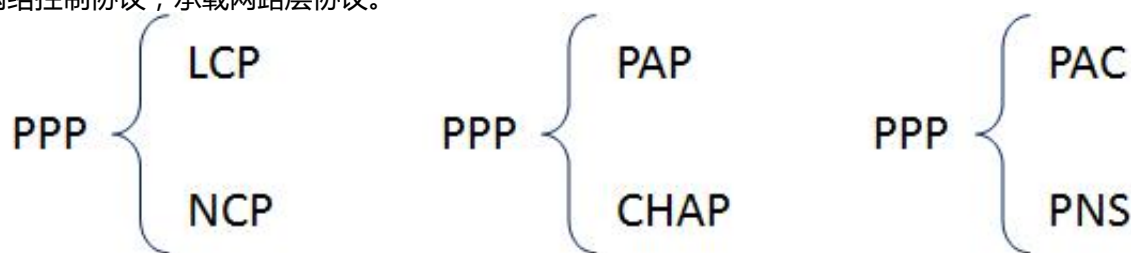
虚拟专用网可以通过第二层隧道协议，这些隧道协议（例如PPTP和L2TP）都是把数据封装在点对点协议（PPP）的帧中在因特网上传输的。

PPP协议, 点对点协议组

PPP协议 (Point-to-point Protocol) 可以在点对点链路上传输多种上层协议的数据包。PPP是数据链路层协议。

链路控制协议 (Link Control Protocol , LCP) 配置管理数据链路。

网络控制协议, 承载网路层协议。



口令认证协议 (Password Authentication Protocol , PAP) , 明文认证。

挑战——握手验证协议 (Challenge Handshake Authentication Protocol , CHAP) 采用**3次握手**, 不传密码, 传密码生成的散列值)

点对点隧道协议 (Point-to-Point Tunneling Protocol , PPTP)

PPTP接入集中器 (PPTP Access Concentrator , PAC)

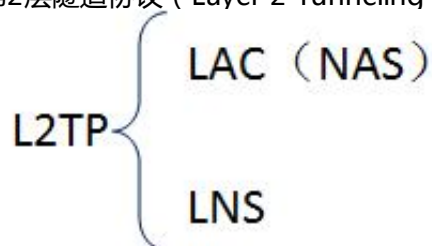
PPTP网络服务器 (PPTP Network Server , PNS)

PAC是负责接入的客户端设备。

PNS是ISP提供的接入服务器。

通用路由封装 (Generic Routing Encapsulation , GRE) 是在一种网络层协议上封装另外一种网路层协议的协议。

第2层隧道协议 (Layer 2 Tunneling Protocol , L2TP)



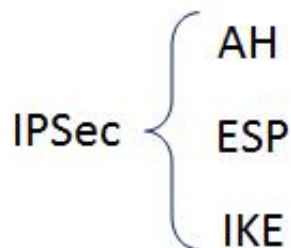
PPTP与L2TP的比较。

PPTP和L2TP都使用PPP协议对数据进行封装。

- 1) PPTP要求因特网络为**IP网络**, L2TP只要求隧道媒介提供面向数据包的对点连接。
- 2) PPTP只能在两端点间建立**单一**隧道, L2TP支持在两端点间使用**多个**隧道。
- 3) L2TP可以提供包头压缩。系统开销占用**4个**字节, 而在PPTP协议下要占用**6个**字节。
- 4) L2TP可以提供隧道验证, 而PPTP不支持隧道验证。

IPSec (IP安全性) (IP Security)

网络层, 3层



IPsec的功能可以划分为下面三类:

- 1) 认证头 (Authentication Header , AH)
- 2) 封装安全负荷 (Encapsulating Security Payload , ESP)
- 3) Internet密钥交换协议 (Internet Key Exchange ,IKE)

1、认证头 (AH) 提供了数据完整性和数据源认证, 但不提供保密服务。

IPsec有两种模式: 传输模式和隧道模式。

(笔记10 , PDF 344页)



2、封装安全负荷 ESP

IPsec封装安全负荷提供了数据加密功能。



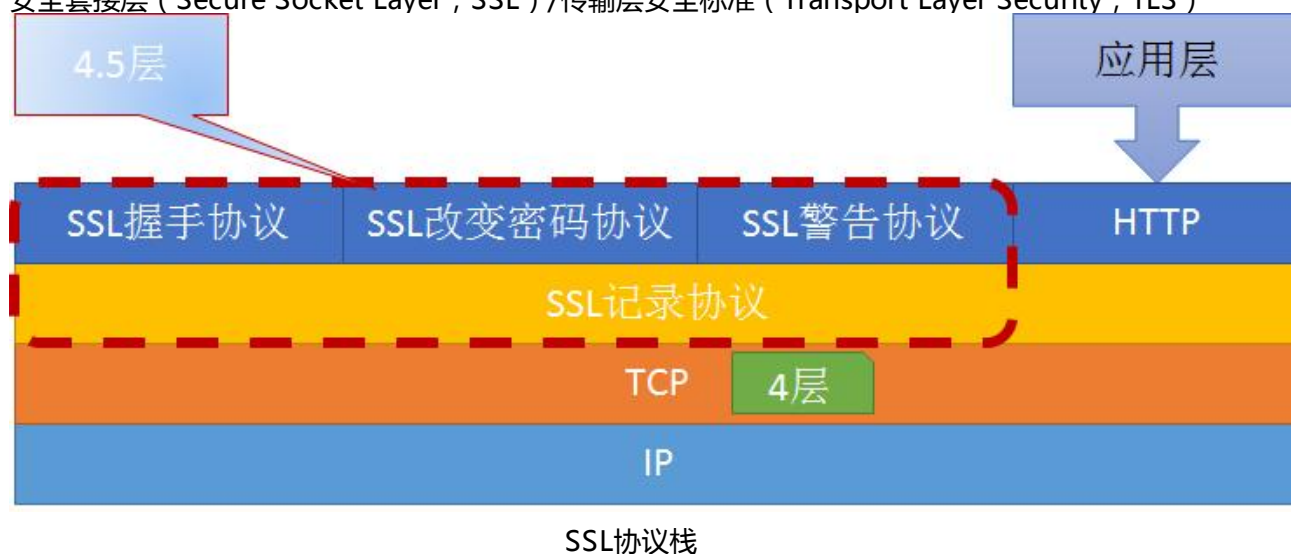
Internet密钥交换协议

IPSec传送认证或加密的数据之前, 必须就协议、加密算法和使用的密钥进行协商。

小结:



安全套接层 (Secure Socket Layer, SSL) / 传输层安全标准 (Transport Layer Security, TLS)



SSL和IPSec各有特点。SSL VPN与IPSec VPN一样, 使用RSA或D-H握手协议来建立隧道, SSL和IPSec都使用了预加密、数据完整性和身份认证技术, 两种协议区别是, IPSec VPN是在网络层建立安全隧道, 适用于建立固定的虚拟专用网, 而SSL的安全连接是通过应用层的WEB连接建立的, 更适合移动用户远程访问公司的虚拟专用网。

SSL/TLS在Web安全通信中被称为HTTPS。在虚拟专用网中, SSL可以承载TCP通信和UDP通信, 由于SSL工作在传输层, 所以SSL VPN的控制更加灵活, 既可以对传输层进行访问控制, 也可以对应用层进行访问控制。

HTTP 使用 80端口
HTTPS使用443端口

记录协议

1、划段。2、无损压缩。3、计算MAC。4、加密。5、发送

应用层安全协议

S-HTTP

安全的超文本传输协议 (Secure HTTP **S-HTTP**)

SSL基本取代了SHTTP。

PGP (Pretty Good Privacy) 电子邮件加密软件包。

S/MIME (Secure/Multipurpose Internet Mail Extensions) , 用于提供安全的电子邮件传输服务。

安全电子交易 (Secure Electronic Transaction , SET) 是一个安全协议和报文格式的集合。

Kerberos是一项认证服务, 它要解决的问题是: 在公开的分布式环境中, 工作站上的用户希望访问分布在网络上的服务器, 希望服务器能限制授权用户的访问, 并能对服务请求进行认证。

Kerberos 三头狗, 地狱守护者

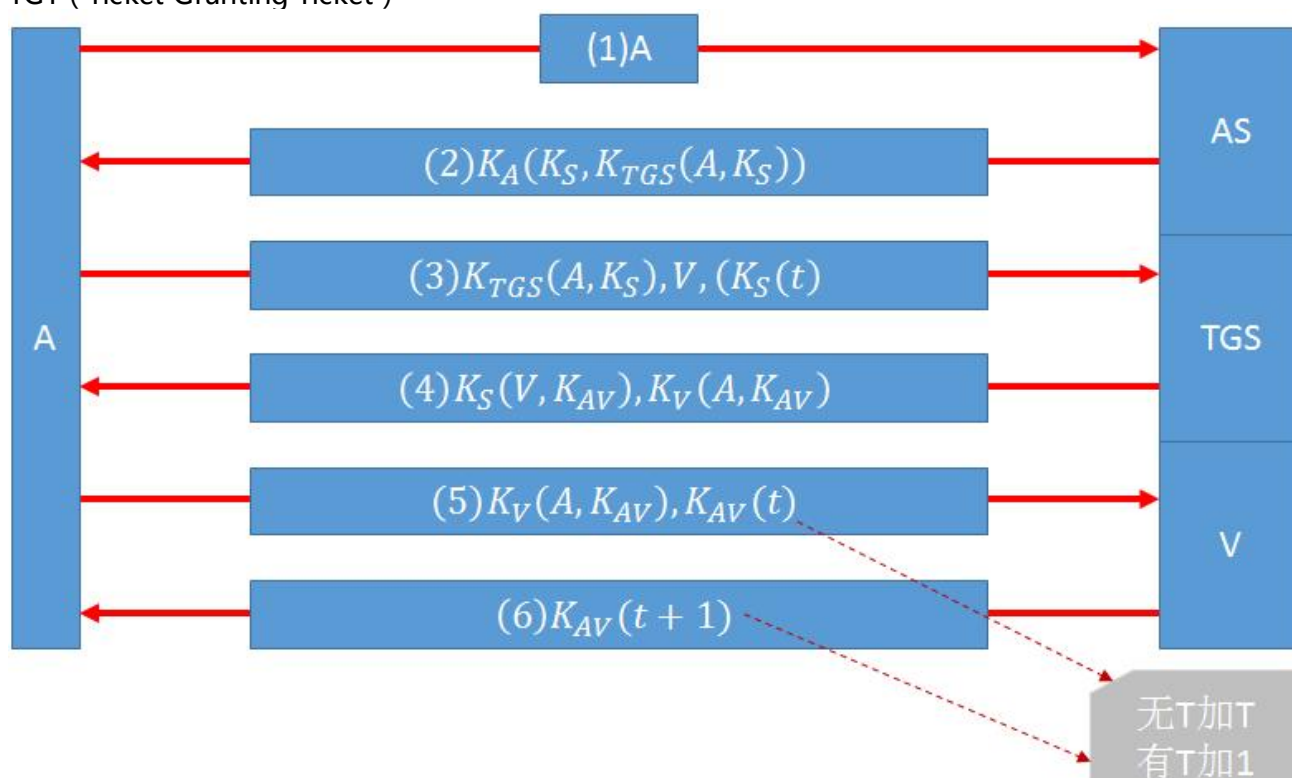
第4版还在广泛使用 (通过时间戳) , 第5版弥补了第4版的漏洞 (通过序列号) 。

AS (Authentication Server) : 认证服务器

TGS (Ticket Granting Server) : 票证授予服务。

V : 用户请求访问的应用服务器。

TGT (Ticket Granting Ticket)



可信任系统, 一个由完整的硬件及软件所组成的系统。

1、D级, 最低保护 (Minimal Protection) 个人计算机的系统虽未经过安全测试, D级并非没有安全保护功能, 只是太弱。

自己开发的系统或软件

2、C级, 自定式保护 (Discretionary Protection), 如系统管理员、用户和应用程序) 的自定义访问权。

自定义访问权限

3、B级, 强制式保护 (Mandatory Protection)

4、A级, 可验证保护 (Verified Protection)

例如: 微软的Windows NT 4.0有C2安全等级, 也就是说, 它的安全特性就在于自定式保护, NT未来可能提高到B2安全等级。Windows2000现已顺利获得认证。UNIX未经测试时, 一般认为是C1, 也有人认为是C2。

防火墙作为网络安全的第一道门户, 可以实现内部可信任网络与外部不可信任网络之间 (或是内部不同网络安全区域之间) 的隔离和访问控制。

1) 所有的从外部到内部或从内部到外部的通信都必须经过它。

2) 只有内部访问策略授权的通信才能被允许通过。

3) 系统本身具有很强的可靠性。

防火墙的类型:

1) 过滤路由器。分组过滤功能。

ACL访问控制列表

2) 双宿主网关。有两个网络接口的双宿主网关 (Dual-Homed Gateway) **代理服务器**。

3) 过滤式主机网关。过滤路由器和运行网关软件的主机。

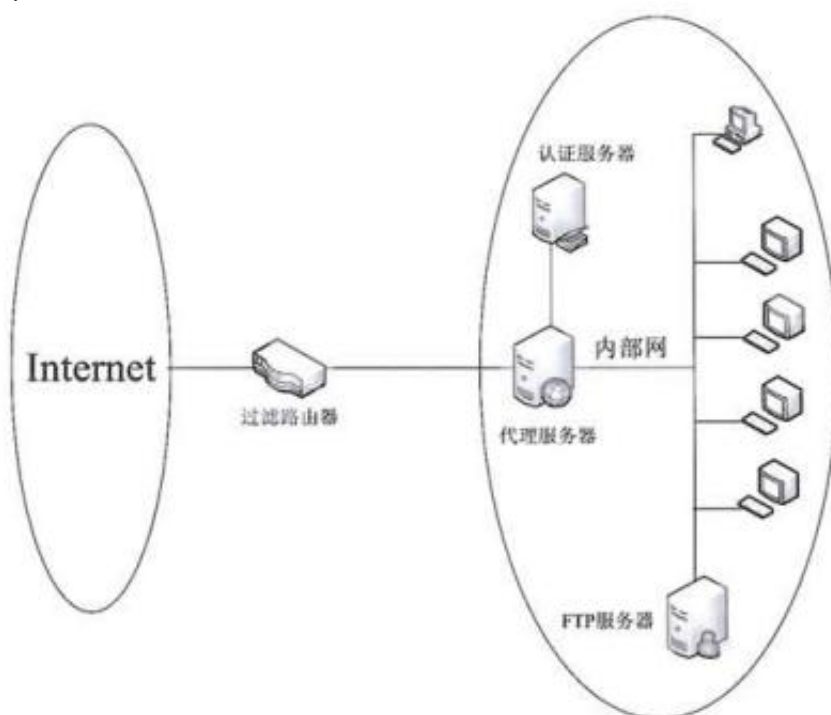


图 8-36 过滤式主机网关

4) 过滤式子网。

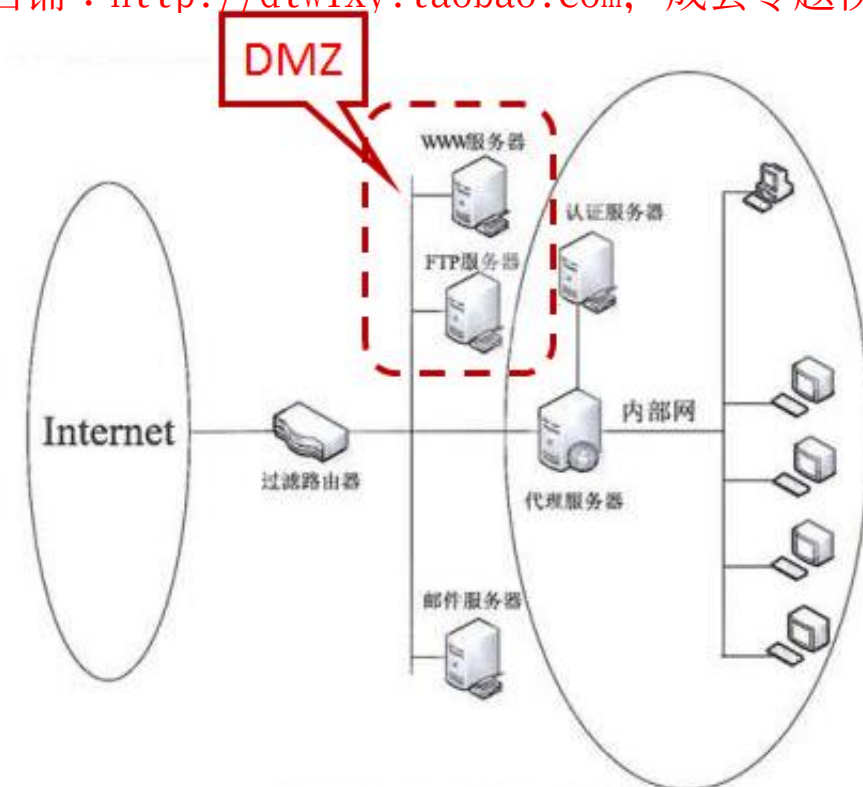


图 8-37 过滤式子网结构

5) 悬挂式结构。

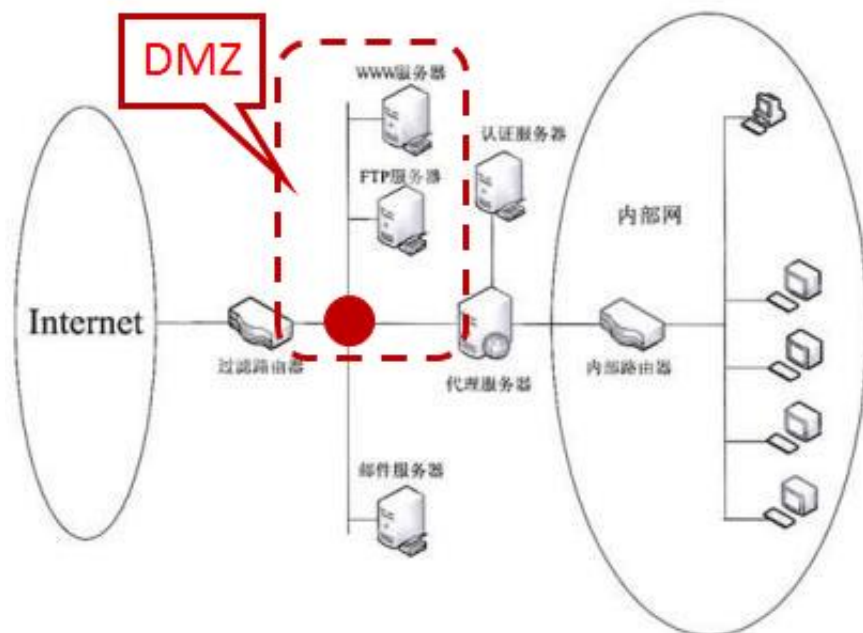


图 8-38 悬挂式网结构

病毒：是指一段可执行的程序代码，通过对其他程序进行修改，可以感染这些程序，使其含有该病毒程序的一个副本。

病毒的分类和命名规则：

- 1) 系统病毒：前缀 Win32、PE、Win95、W32、W95
- 2) 蠕虫病毒：前缀Worm
- 3) 木马病毒和黑客病毒：木马Trojan、黑客病毒Hack。
- 4) 脚本病毒：前缀，Script

5) 宏病毒: 前缀, Macro, 第二前缀, Word, Word97、Excel, Excel97.

6) 后门病毒: Backdoor

入侵检测

IPS: 入侵防御系统 (Intrusion-Preventionsystem)

串联、切断

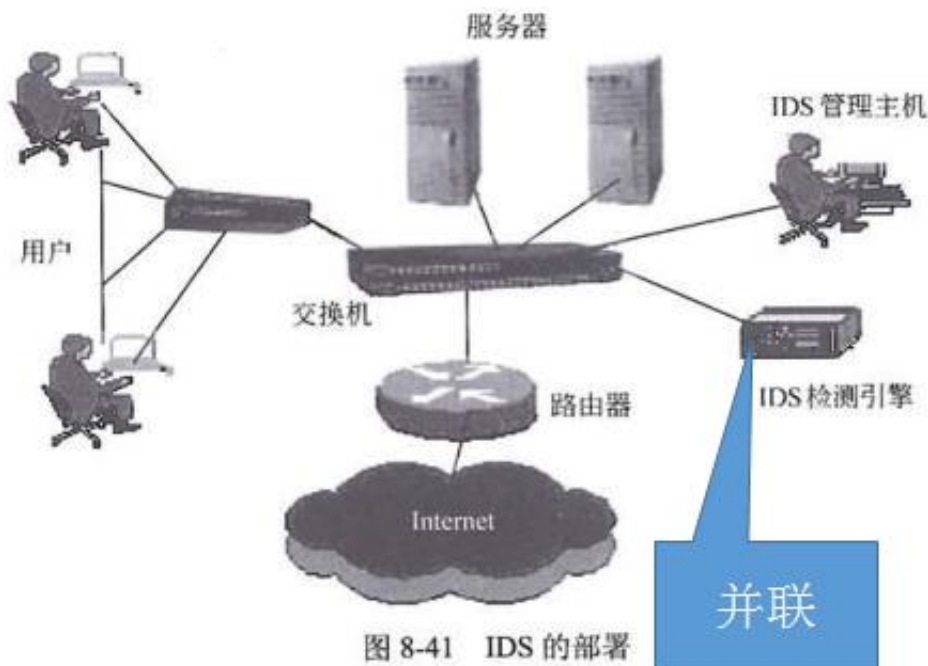
IDS: 入侵检测系统 (Intrusion Detection System)

并联、检测

IDS的主要功能包括: 监测与分析, 入侵检测通过实时地监控入侵事件, 在造成系统损坏或数据丢失之前**阻止**入侵者进一步的行动。

对IDS部署的**唯一要求**是应当挂接在所关注流量必须流经的链路上。**能靠近攻击源。**

- 1) 服务器区域的交换机上。
- 2) Internet接入路由器之后的第一台交换机。
- 3) 重点保护网段的局域网交换机上。



第9章 网络操作系统与应用服务器

笔记本: 网络工程师学习

创建时间: 2015/1/21 11:49

更新时间: 2015/1/21 11:49

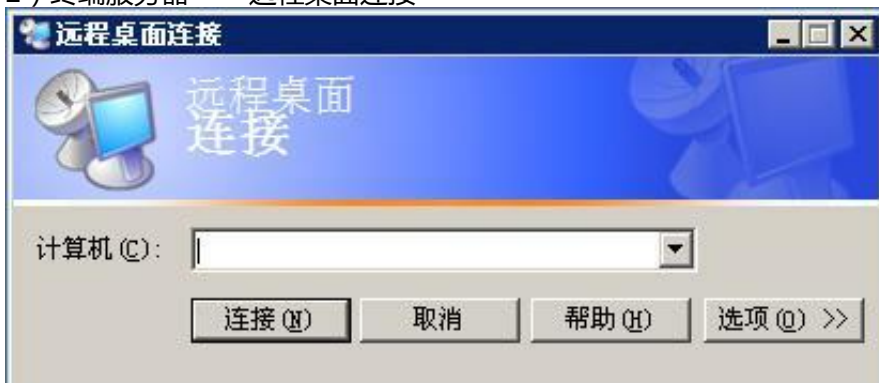
URL: about:blank

网络操作系统: Windows和Linux。

windows server 2003在server 2000基础上增加了:

1) 配置流程向导。

2) 终端服务器——远程桌面连接

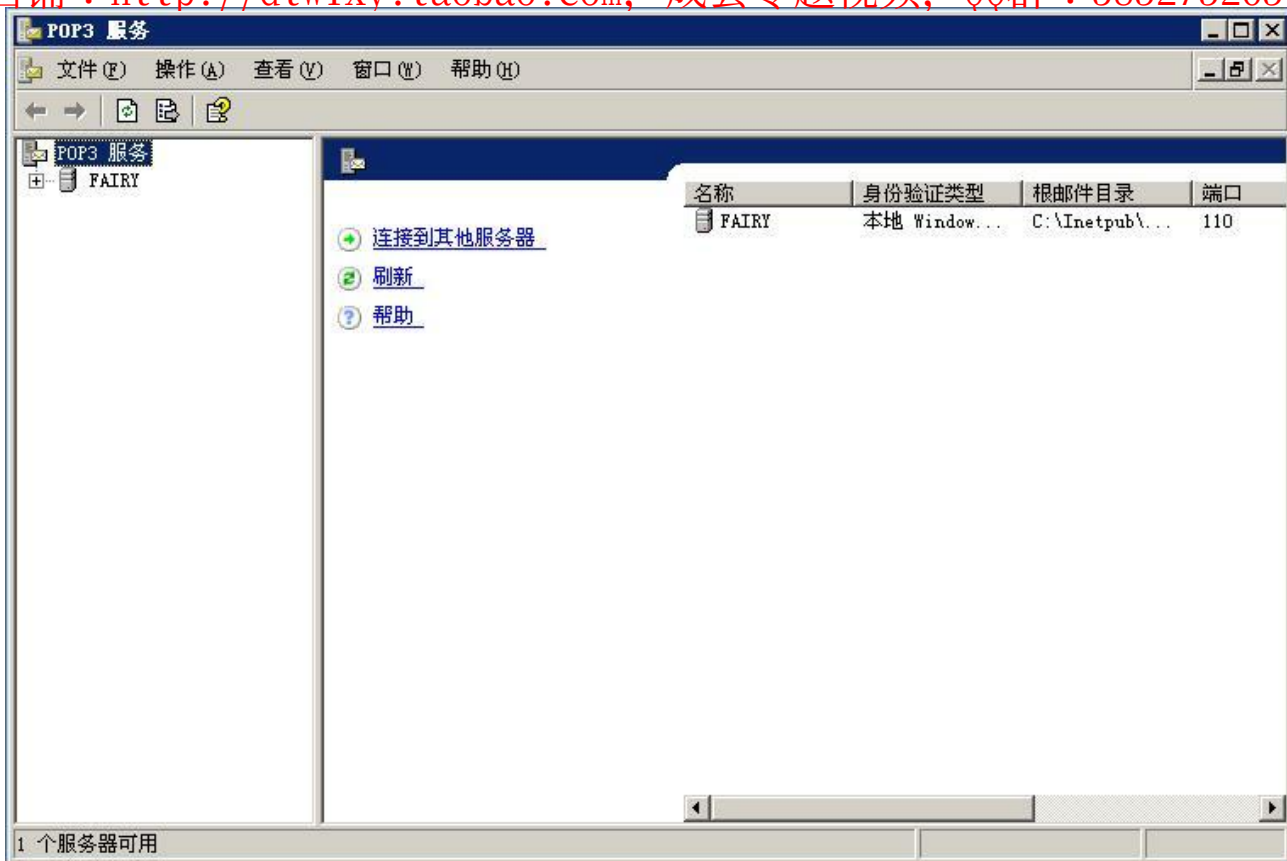


3) Internet信息服务6.0

增强了可靠性、方便性、安全性、扩展性。



4) 简单的邮件服务器



5) 流媒体服务器

WMS9在电影点播、电台播放、视频会议、远程教育/培训等方面有优势。



6) 系统关闭事件跟踪。



Linux系统简介。

Red Hat Linux是目前世界上使用最多的Linux操作系统家族成员，Red Hat Linux 9就是Red Hat Linux的一个较新版本。使用**RPM**模块安装应用软件包。

本地组与用户

用户：用户名、密码、说明、权限。

具有相同属性的用户归结，统一授权，形成**用户组**（Group）。

全局组，可通行所有域的组。

域：区域

本地组。

特殊组。

如INTERACTIVE组、NETWORK组、SYSTEM组、CREATOR OWNER组、EVERYONE组。

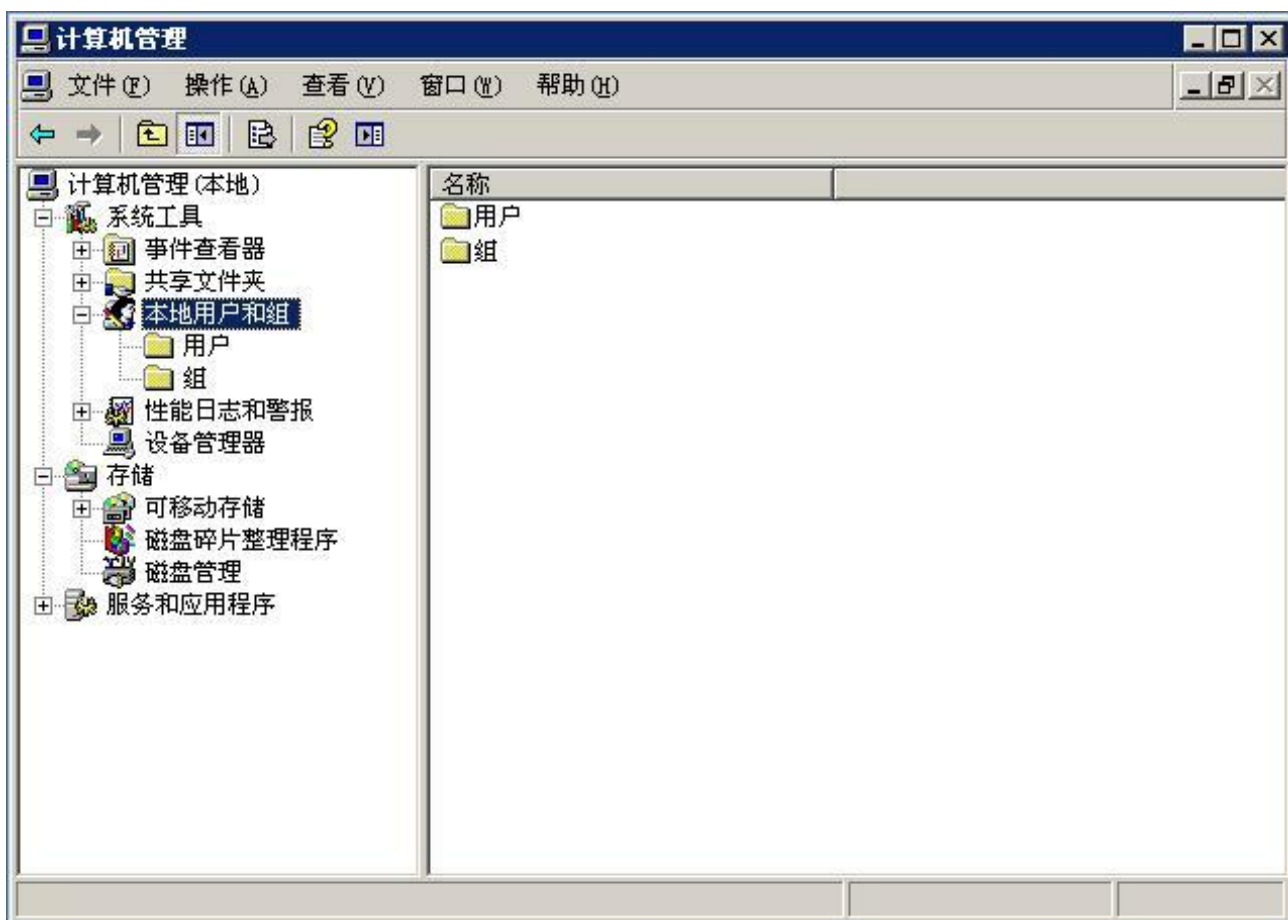
用户权限：

表 9-1 用户权限描述

名 称	权 限 描 述
<u>Administrators</u>	<u>管理员</u> 对计算机/域有不受限制的 <u>完全访问权</u>
<u>Backup Operators</u>	<u>备份操作员</u> 为了备份或还原文件可以替代安全限制
<u>Guests</u>	按默认值, <u>来宾</u> 和用户组的成员有同等访问权, 但来宾账户的限制更多
HelpServicesGroup	帮助和支持中心组
Network Configuration Operators	此组中的成员有部分管理权限来管理网络功能的配置
Performance Log Users	此组的成员可以远程访问以计划此计算机上性能计数器的日志
Performance Monitor Users	此组的成员可以远程访问以监视此计算机
<u>Power Users</u>	<u>高级用户</u> (Power Users) 拥有大部分管理权限, 但也有限制。因此, 高级用户可以运行经过验证的应用程序, 也可以运行旧版应用程序
<u>Print Operators</u>	成员可以 <u>管理域打印机</u>
<u>Remote Desktop Users</u>	此组中的成员被授予 <u>远程登录</u> 的权限
Replicator	支持域中的文件复制
TelnetClients	本组的成员可以访问此系统上的 Telnet 服务器
<u>Users</u>	<u>用户</u> 无法进行有意或无意的改动。因此, 用户可以运行经过验证的应用程序, 但不可以运行大多数旧版应用程序

使用“本地用户和组”管理用户与组

我的电脑=>右键=>管理=>本地用户和组



活动目录 (Active Directory) 是一个动态的分布式文件系统, 包含了存储网络信息的目录结构和相关的目录服务。

1、需要硬盘文件格式为NTFS

2、在活动目录中, 对象名字采用DNS域名结构, 所以安装活动目录需要DNS服务器的支持。
轻型目录访问协议 (Light Directory Access Protocol , LDAP) 。LDAPv3访问活动目录。

域是活动目录的核心单元, 是共享同一个活动目录的一组计算的**集合**。

域树 (Domain Tree) 是域的**集合**。

域林 (Domain Forest) 是域树的**集合**。

组织单元 (Organizational Unit , OU) 是域下面的容器对象, 是比域更小的管理边界。

组织单元是可以配置组策略或委派管理权限的最小单位, 组织单元类似于WindowsNT中的工作组。



域控制器, 域控制器存储着活动目录数据, 并管理用户域之间的各种交互作用, 包括用户登录、身份验证和目录搜索等过程。一个域可以有一个或多个域控制器。 (备份域控制器)

活动目录中的工作组 :

1) 全局组 (Global Groups) 可以达到域林中的任何信任域。全局组的成员来自生成该组的本地域。

校长组

2) 域本地组 (Domain Local Groups) : 域本地组的访问权限仅次于本地域, 域本地组的成员可以来自于任何域, 本地域中的资源。

年级组

3) 通用组 (Unicursal Groups) : 通用组的成员来自于域林中的任何域。 **域林中的任何域**。

巡考组



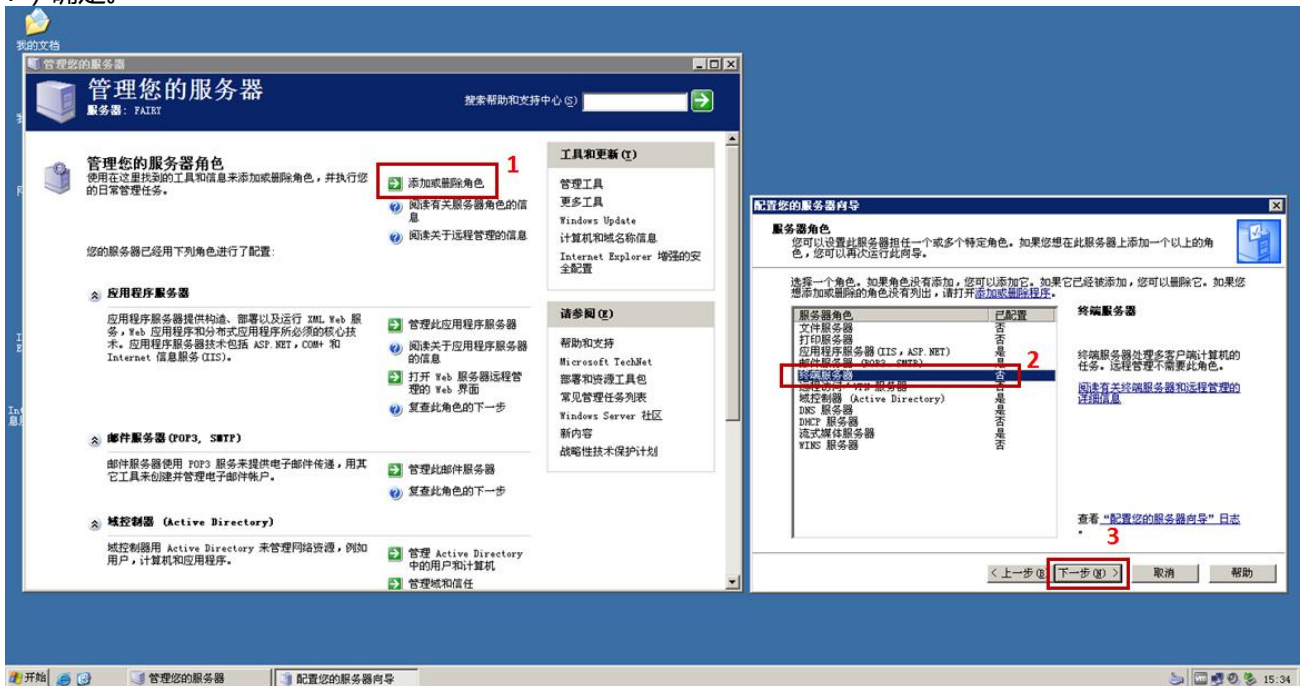
活动目录必须安装在Windows sever 2003的NTFS分区。并且必须安装DNS服务器。通过 “管理您的服务器” 窗口进入到 “Active Directory 安装向导” 对话框。

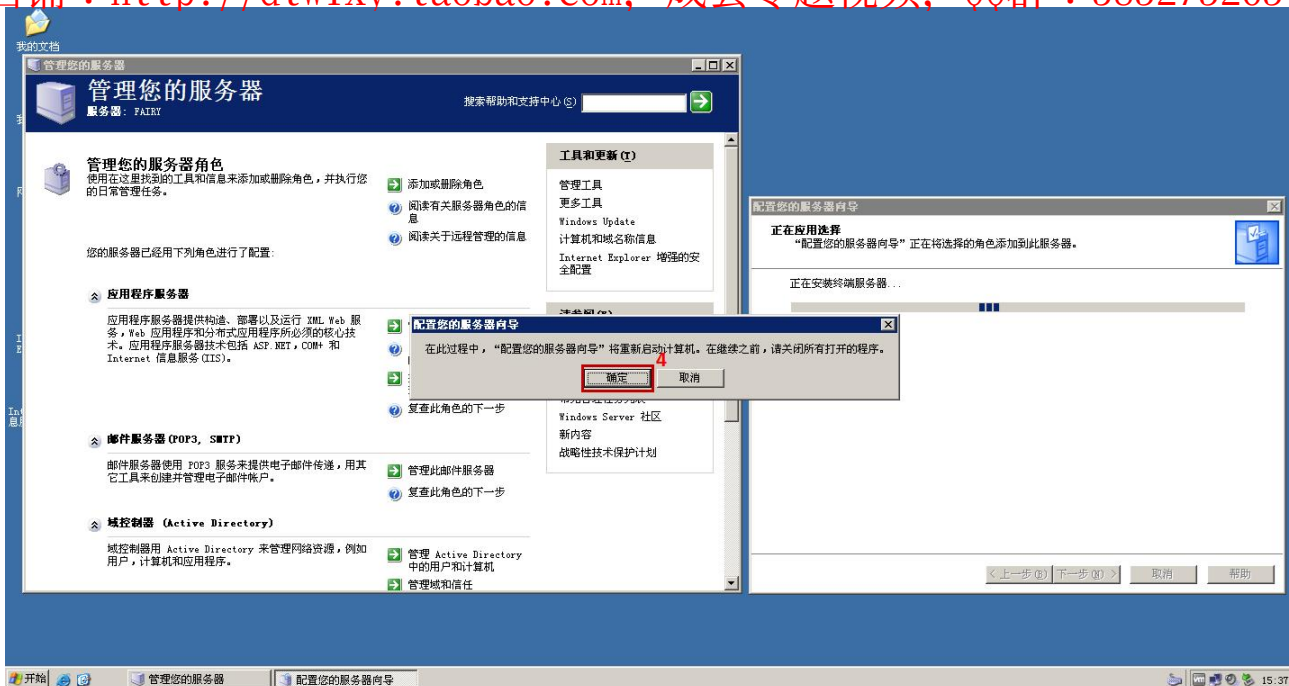


终端服务，多个远程访问服务器桌面。

终端服务器安装：

- 1) 单击开始=》管理工具=》配置您的服务器向导
- 2) 下一步，预备步骤。
- 3) 下一步，检测。。。
- 4) 下一步，“服务器角色”，选“终端服务器”
- 5) 下一步，选择总结
- 6) 下一步，开始安装。
- 7) 确定。

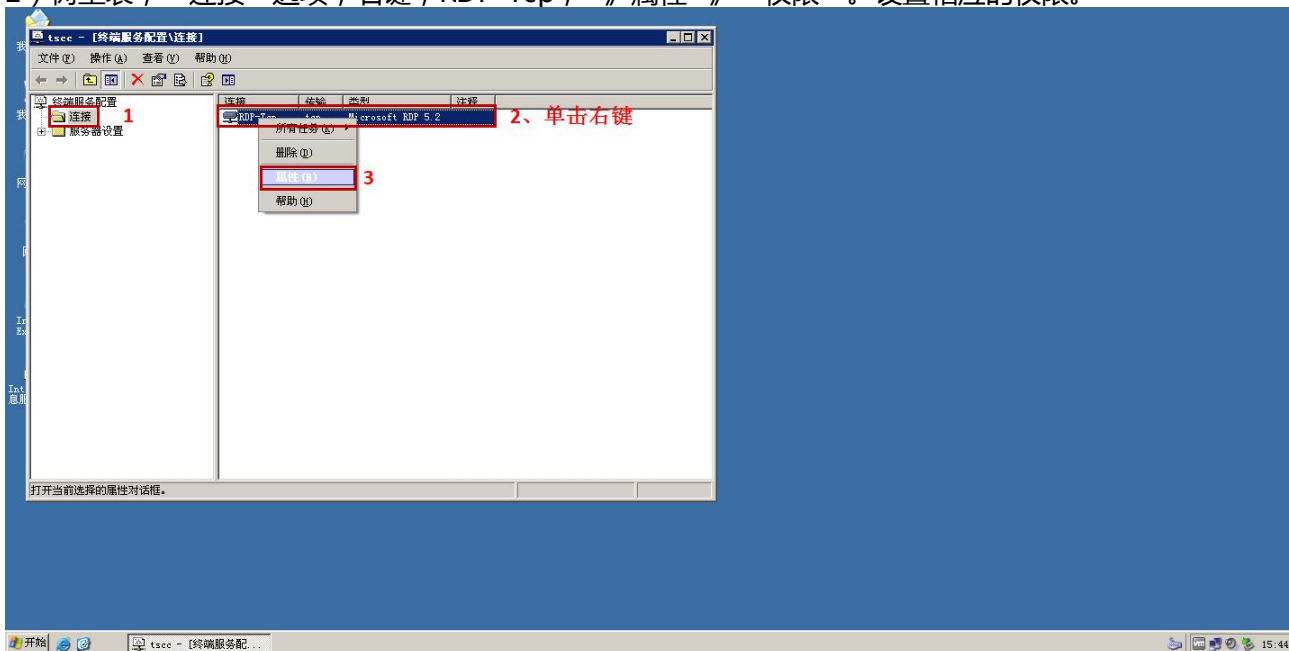




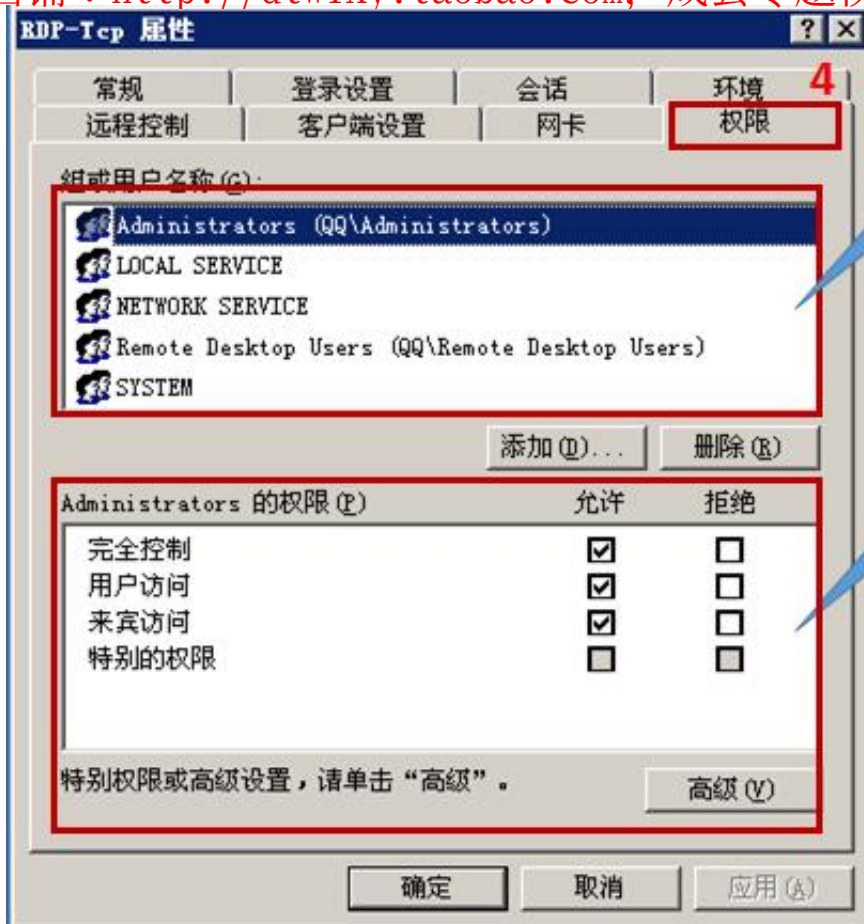
赋予用户权限。

1) 开始=》管理工具=》终端服务配置

2) 树型表, “连接” 选项, 右键, RDP-Tcp, =》属性=》“权限”。设置相应的权限。



管理员有“完全控制”、“用户访问”、“来宾访问”。



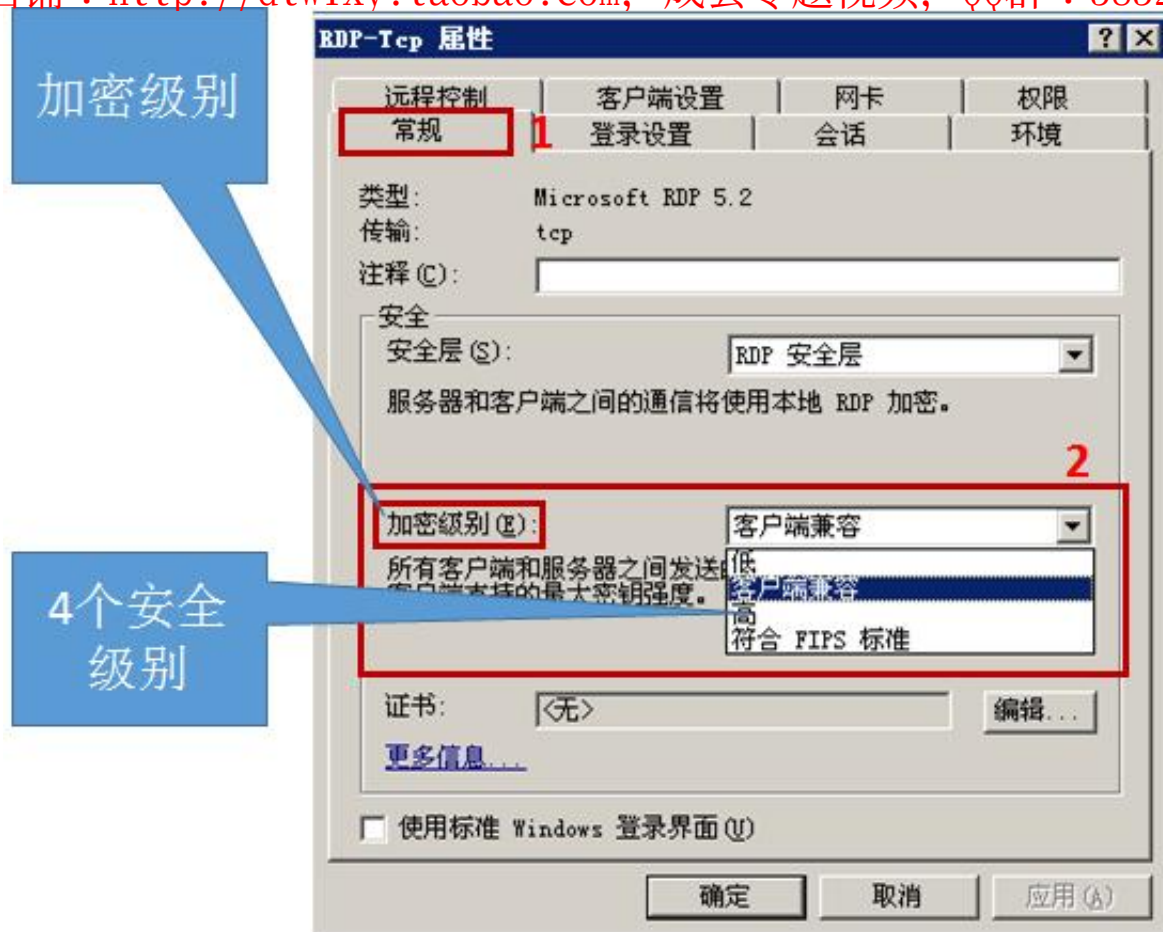
不同用户
和组

不同权限
设置

更改加密级别：

“常规”选项卡，在“加密”选项区域的“加密级别”有4种级别。

- ①低，使用 56位密钥。
- ②客户端兼容，使用客户端支持大长度密钥
- ③高，使用128为密钥的加强算法。
- ④符合FIPS标准。Microsoft加密模块。



允许用户自动登陆：

在“用户名”“密码”和“确认密码”文本框输入用户名密码。

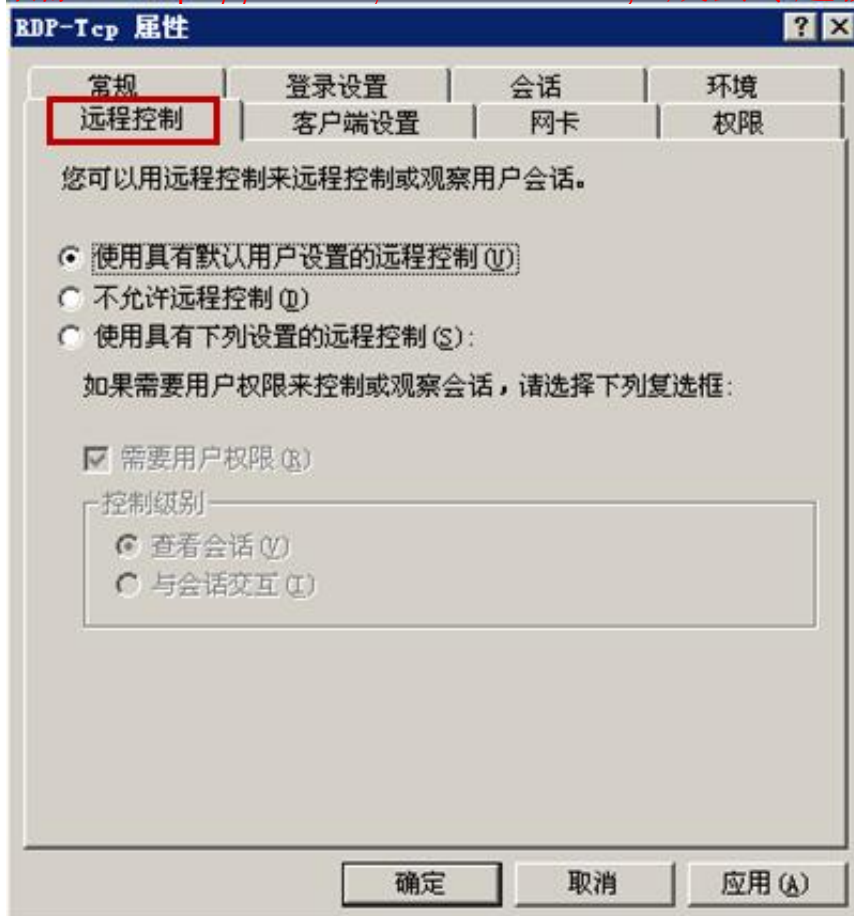


配置终端服务超时重连。

- ① “结束已断开的会话”
- ② 活动会话限制，设置的是**最长时间**
- ③ 空闲会话限制，设置的是**最长时间**。
- ④ 替代用户设置。



管理远程控制。



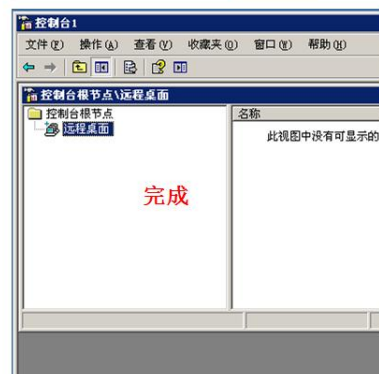
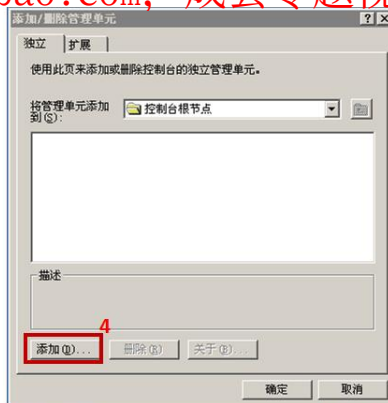
Windows2003远程管理的改进。

- 1) 管理远程桌面, 从2000中的“远程管理”模式中称为“终端服务”。
- 2) 远程协助。
- 3) 远程管理Web界面。
- 4) 远程安装服务的改进功能。“远程安装服务 (RIS)”

Microsoft管理控制台 (MMC)

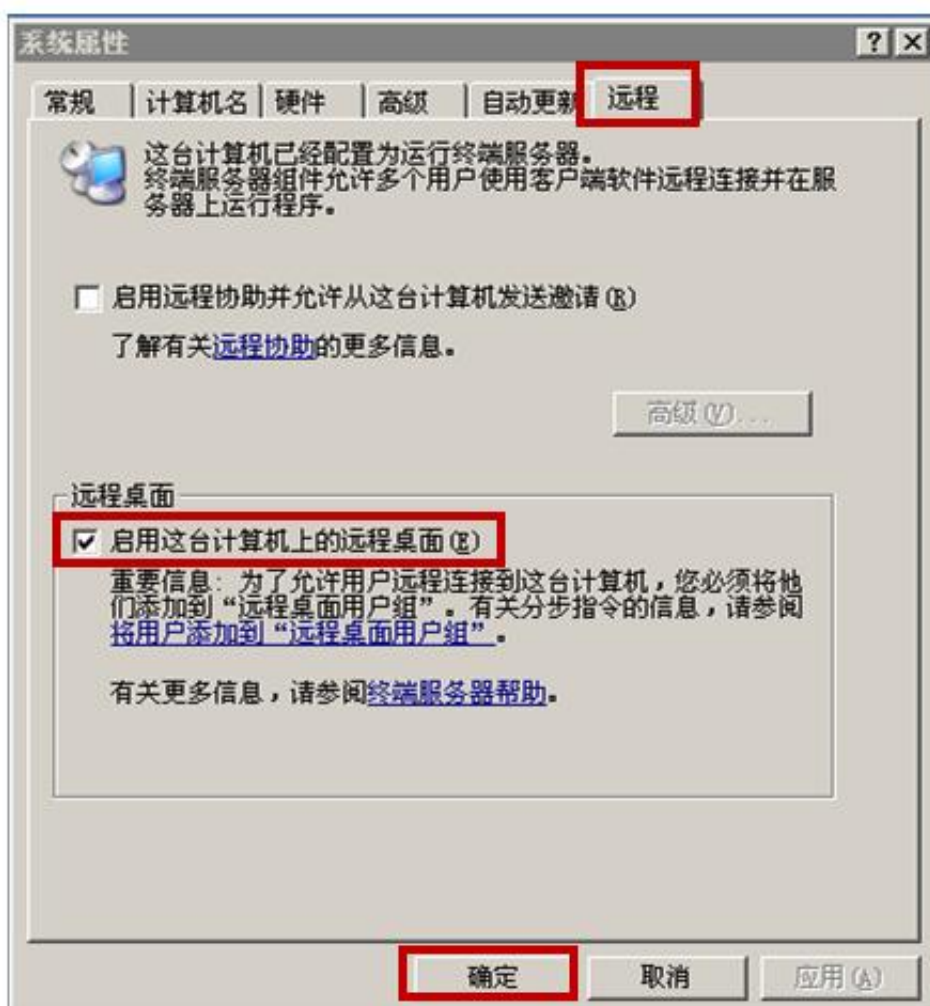
Microsoft管理控制台集成了用来管理网络、计算机、服务及其他系统组件的管理工具, 可以用MMC创建、保存并打开管理工具单元, 这些管理工具用来管理硬件、软件和Windows系统的网络组件。MMC可以运行在各种Windows 9X/NT操作系统上, 包括XP和2003。

1、开始=>运行



远程桌面连接是为Windows 2003系统提供的一种连接工具。

控制面板=>系统=>系统属性, “远程”选项卡



用鼠标右击“本地连接”=>“属性”=>“高级”

在“Internet连接防火墙”选项区域中取消选中“通过限制或阻止来自Internet的对此计算机的访问”。



“远程桌面连接”在“开始”=>“所有程序”=>“附件”=>“通讯”。

输入需要访问远程桌面的IP地址或域名



远程桌面选项：



LINUX网络配置。

文件脚本位于/etc目录下。

用#开头做注释。

/etc/sysconfig/network文件。服务器上的网络配置信息文件。

NEWNOK=yes/no：表示网络是否被配置。

HOSTNAME=hostname hostname：表示主机名

GATEWAY=gw-ip gw-ip：网关IP

FORWARD_IPV4=yes/no：开启IP转发功能。

GATEWAYDEV=gw-dev gw-dw：网关设备名称。

/etc/hostname文件，主机名称，完全域名。

/etc/sysconfig/network

/etc/hosts文件。/etc/hosts中包含了IP地址和主机名之间的映射。

```
127.0.0.1 pc1 localhost.localdomain localhost
192.168.0.100 pc7
192.168.0.101 otherpc otheralias
```

127.0.0.1	pc1	localhost.localdomain localhost
192.168.0.100	pc7	
192.168.0.101	otherpc	otheralias
IP	主机名	别名

/etc/host.conf。通过解析器来获得主机名对应的IP地址

Order hosts, bind DNS服务器

顺序	1	2
----	---	---

order：主机名查询顺序，先查询/etc/hosts文件，然后用DNS来解析域名。

multi：值为on表示允许/etc/hosts可以指定多个地址。

nospoof：值为on不是不允许进行IP地址欺骗。

/etc/resolv.conf配置DNS客户。

```
nameserver 210.34.0.14 首选DNS
nameserver 210.34.0.13 备用DNS
```

(笔记12，PDF 390页)

/etc/rc.d/init.d/network文件。网络主机地址、子网掩码和网关等参数的配置。

```
IP地址      IPADDR=192.168.0.100
子网掩码    NETMASK=255.255.255.0
广播地址    BROADCAST=192.168.0.255
网关        GATEWAY=192.168.0.1
```

网卡驱动存放目录 /lib/modules/(版本号)/net/ 下。

网络配置命令。

网络接口设置命令ifconfig。对TCP/IP网络参数进行设置。

功能等同于windows下的 ipconfig命令

开启关闭接口

ifconfig Interface-name ip-address up|down 。

使用不带任何参数的ifconfig命令可以查看当前系统的网络配置情况。

例如：

```
[root@localhost]#ifconfig eth0 192.168.0.5 netmask 255.255.255.0 up
```

若将网络接口“关闭”，则输入命令ifconfig eth0 down，不需要指定IP地址和网络掩码。

```
[root@localhost]#ifconfig eth0 查看接口信息
```

```
eth0 Link encap:Ethernet Hwaddr 00:20:5C:00:78:33
Inet addr:192.168.0.5 Bcast:192.168.0.255 Mask:255.255.255.0
UP BROADCAST RUNNING MULTICAST MTU :1500 Metric:1
RX packets:9625272 errors:0 dropped:0 overruns:0 frame:0
TX packets:6997276 errors:0 dropped:0 overruns:0 frame:0
collisions:0 txqueuelen:100
Interrupt:19 Base address:0xc800
```

配置路由命令route，设定主机或局域网的出口IP地址。

route[-选项]

del：删除一个路由表项。

add：增加一个路由表项。

target：配置目的网段或主机，可以是IP，也可以是网络或主机名

netmask Nm：路由表项的子网掩码

gw GW：网关

例如，运行不带参数的route命令：

查询路由

```
[root@localhost]#route
```

系统将显式内核路由表如下：

```
Kernel IP routing table
Destination Gateway Genmask Flags Metric RefUse Iface
127.0.0.0 127.0.0.1 255.0.0.0 U 0 0 0 lo
129.168.0.0 192.168.0.5 255.255.255.0 U 0 0 0 eth0
```

例如，可以用下列命令把路由192.168.0.1添加到网路配置中。

```
[root@localhost]#route add default 192.168.0.1 1（添加路由）
```

default用于目的地址，则创建默认路由。

网络测试命令 ping

ping命令用于查看网络上的主机是否在工作。

ping[-选项]

-t: 一直检测, 直到用户中断。

-a: 将地址解析为计算机名。

-n count: (次数) 发送完毕后结束, 默认值为4

-l length: (长度) 发送指定长度, 默认值为64字节, 最大字节为8192。

网络查询命令netstat, 用来显示内核路由表, 互动网络连接和状态和每个已安装网络接口的统计信息。

netstat[-选项][-参数]

-a: 显示所有连接 (all)

-i: 显示统计信息 (interface)

-r: 核心路由表 (route)

-n: 以数字格式形式显示地址。 (number)

[root@localhost]#netstat -nr

linux的文件系统为EXT2, 其他文件系统, EXT3、NTFS、NFS、SYSV、FAT16、FAT32.

Linux文件结构

树型结构最上层是根目录, 用 "/" 表示, Linux将所有软件、硬件都做为文件来管理, 每个文件被保存在目录中, 有几个分区, 就有几个树型结构, 它们之间的关系是并列的。无论操作系统管理几个磁盘分区, 这样的目录树只有一个。

Linux文件系统一般包括5种基本文件类型, 即普通文件、目录文件、连接文件、设备文件、管道文件。

linux的目录访问权限。

三级权限: 文件的所有者、与文件所有者同组的用户及其他用户。对文件主要三种处理: 读取、写入、执行。



cat命令, 在屏幕上滚动。

more命令, 每次显示一屏文本, 显示满屏后停下来。

less命令, 按页显示文件, 向前也可以向后翻阅。

文件复制命令cp,

-f 删除已存在的的目标文件而不提示。

-i 要求用户确认, 交互式复制

文件移动命令mv。

-i交互式操作。

-f 禁止交互操作

文件删除命令rm

-f : 忽略不存在文件, 不给提示。

-i 进行交互式删除。

创建目录命令mkdir

删除目录命令rmdir

改变目录命令cd

显示当前目录命令pwd

列出目录命令ls (list)

文件访问权限命令chmod

文件链接命令ln

13个命令 {

5个显示: cat more less pwd ls
=
2个增加: cp mkdir
+
3个删除: mv rmdir rm
=
2个改动: cd chmod
+
1个改动: ln

PDF 403页。

Linux用户和组管理

其中最重要的是超级用户, 即根用户root。

linux系统中其他的一些组群和用户都是由root来创建的。

用于用户管理的最重要的文件, 这个文件对所有用户都是可读的。

/etc/shadow文件是一个只有超级用户root能读的文件/etc/shadow

/etc/group文件, 管理用户组的基本文件是/etc/group

用户管理

增 删 改 密

1、useradd[-选项] username

增加用户账号就是在/etc/passwd文件中为新用户增加一条记录。

指定和修改用户口令的命令是passwd。

2、pass[-选项][username]

删除用户命令userdel

3、userdel[-选项]username

4、su[username]切换到的用户名。

用户组管理

增 删 改

1、groupadd[-选项]groupname

新建的组

2、删除一个已有用户组

groupdel groupname

3、修改用户组属性

groupmod[-选项]groupname

小结：

网络配置文件：（6个） /etc/sysconfig/network

/etc/hostname

/etc/hosts

/etc/host.conf

/etc/resolv.conf

/etc/rc.d/init.d/network

网络配置命令：（4个） ifconfig、route、ping、netstat

文件目录命令：（13个） cat、more、less、pwd、ls、cp、
mkdir、mv、rmdir、rm、cd、chmod、
ln

用户配置文件：（3个） /etc/passwd

/etc/shadow

/etc/group

用户管理命令：（4个） useradd、passwd、userdel、su

用户组管理命令：（3个） groupadd、groupdel、groupmod

IIS服务器的基本概念

因特网信息服务器 (Internet Infrmtion SERVER , IIS)

WWW服务, 可以传送文本信息, 还可以传送图形、图像、动画、声音和视频信息。 (HTTP使用80端口)

FTP服务, 两个远程计算机之间传送文件的协议。 (FTP服务连接使用21端口)

SMTP服务, 简单邮件传输协议在客户端应用程序和远程计算机的邮件服务器之间传送邮件信息。 (SMTP使用25端口)

POP3服务, POP3功能是存储和管理邮件, 能为用户提供账号、密码、身份验证。 (POP3服务使用110端口)

IIS是微软出品的, 假设Web、FTP、和SMTP服务器的一套整合软件。

FrontPage

Internet服务管理

SMTP Service

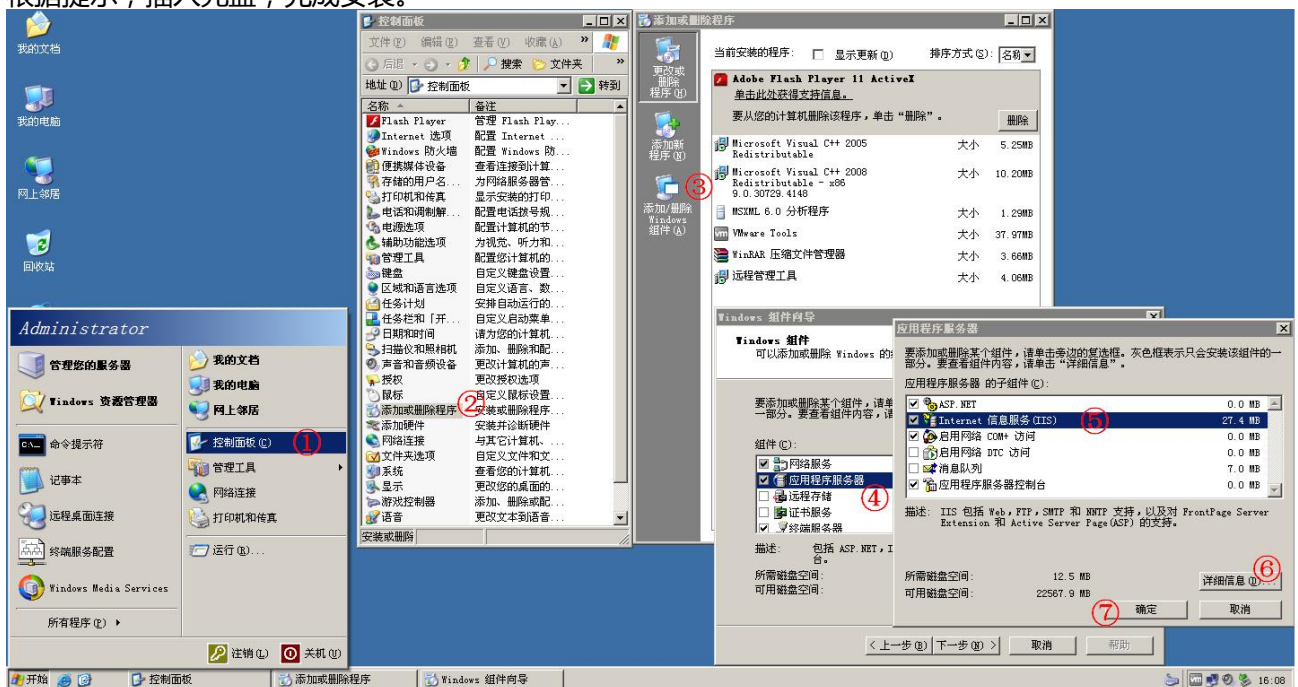
World Wide Web 服务器

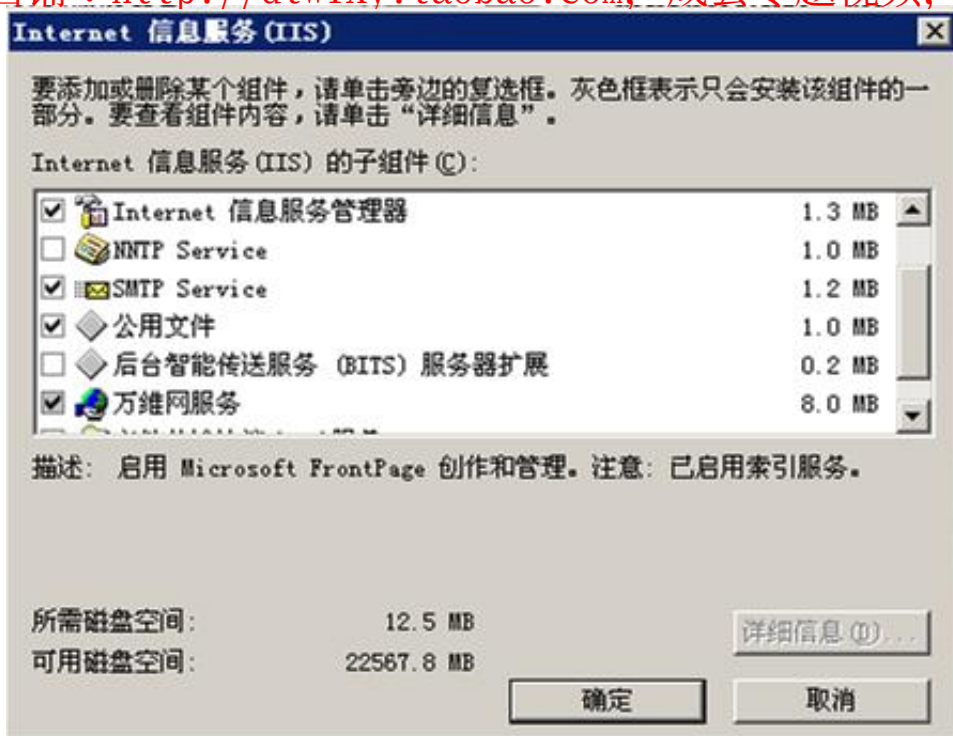
公用文件

FTP服务器

IIS的安装过程: 开始→控制面板→添加删除程序→添加删除windows组件→windows组件向导→组件→应用程序服务器→详细信息→应用程序服务器→Internet信息服务 (IIS) →详细信息, 这只Internet信息服务 (IIS) 的子组件。

根据提示, 插入光盘, 完成安装。





配置WEB服务器

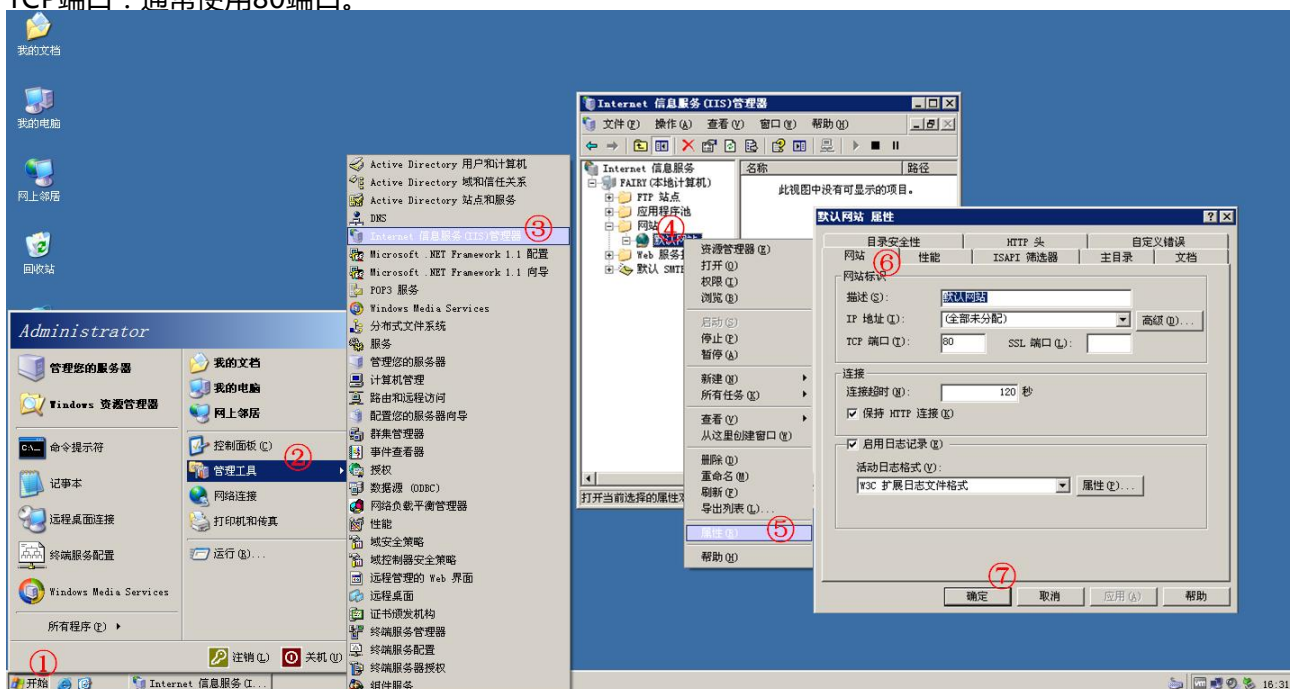
1、网站的基本配置

在控制面板中选择：管理工具→“Internet信息服务（IIS）管理器”→“默认网站”→右键菜单“属性”，进入“默认网站属性”对话框，“网站”选项卡。

网站表示：在“描述”文本框中输入网站的名称。

IP地址：为了安全起见，通常为Web站点分配一个IP地址。

TCP端口：通常使用80端口。



访问权限：“读取”权限。“写入”权限和“目录浏览”权限

日志访问：

脚本资源访问：

目录浏览：



默认网站属性 对话框中选择“文档”选项卡，设置默认网页文件，Default.htm、Default.asp、index.htm、iisstart.asp，任选。

(笔记13 PDF 412页面。)

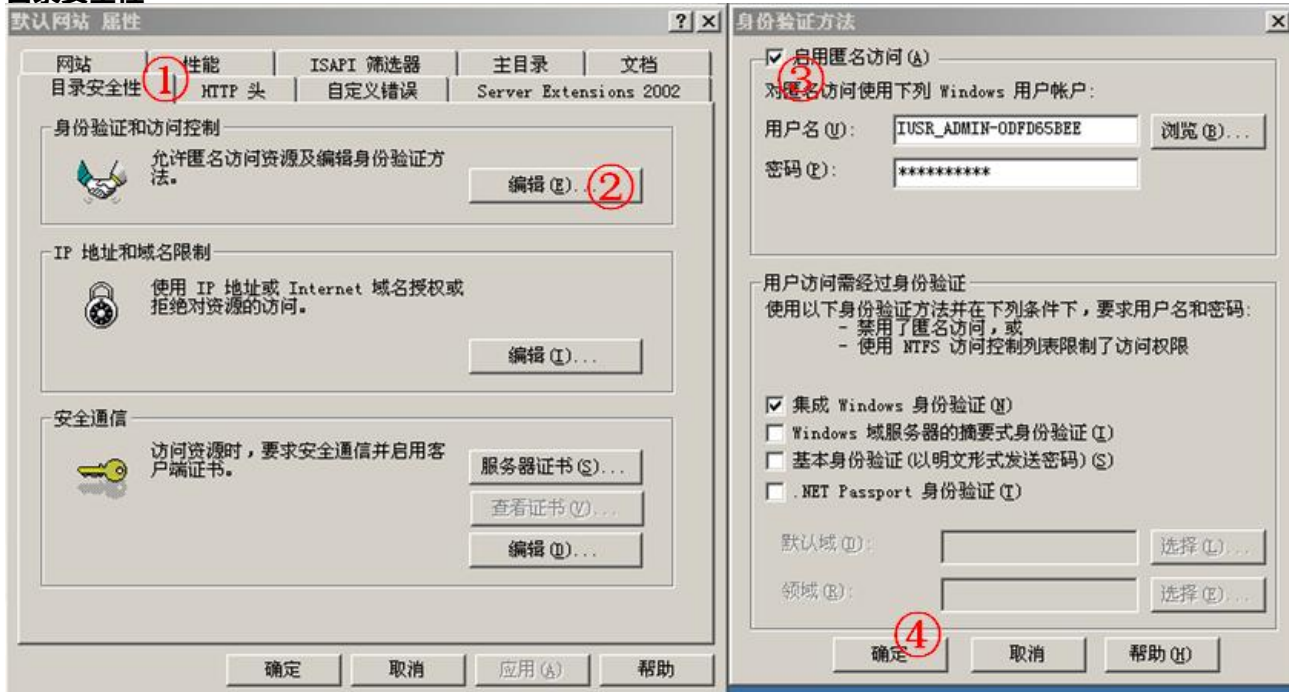
网站安全习性设置

“目录安全性”选项卡，1、进行身份验证和访问控制。2、IP地址和域名限制设置。(可以编辑“匿名访问和身份验证控制”。为了方便匿名访问，需要选中“允许IIS控制密码”复选框，这样用户不必输入账号和密码就可以访问网站。

文档



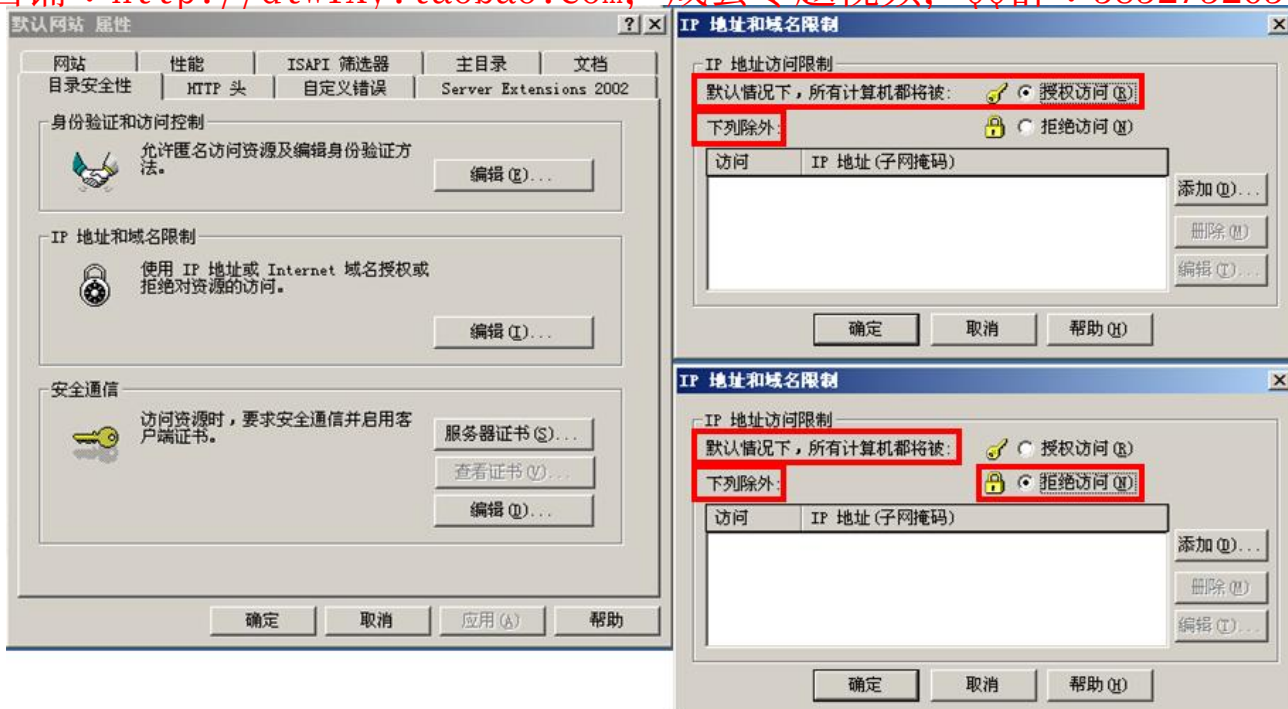
目录安全性



(1) 基本身份验证

(2) 继承windows身份验证, 用户名和密码在发送前要经过加密, (Kerberos v5身份验证)

IP地址和域名限制:



“安全通信”选项卡设置 Web 服务器证书向导。

FTP服务器

开始→管理工具→Internet信息服务 (IIS) 管理器 “

展开FTP站点, 选中“默认FTP站点”

单击鼠标右键, 进入“属性”

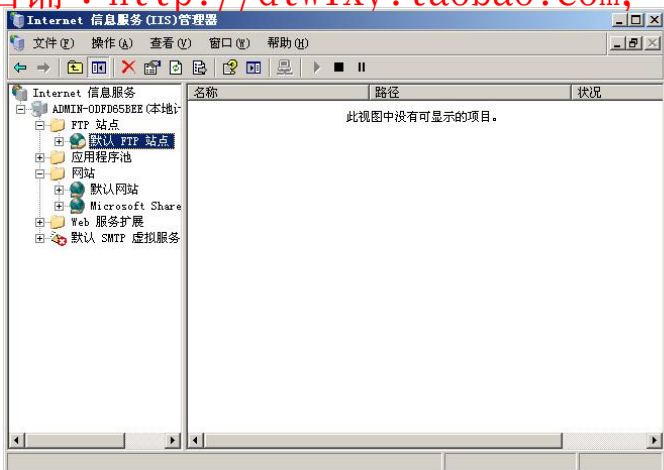
“FTP”站点选项卡。

IP地址、TCP端口等

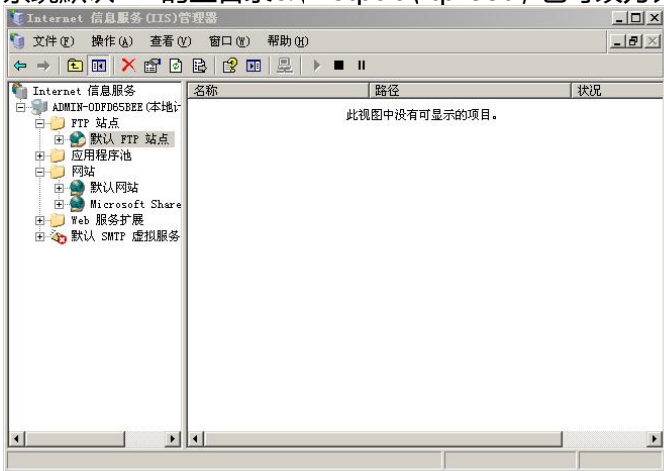
例如可以设置标识为MP3, IP地址为192.168.0.61, 端口号为21。

FTP站点连接:

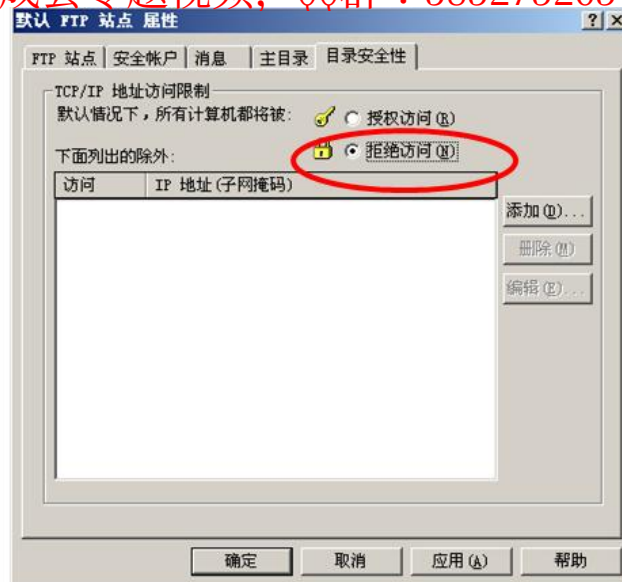
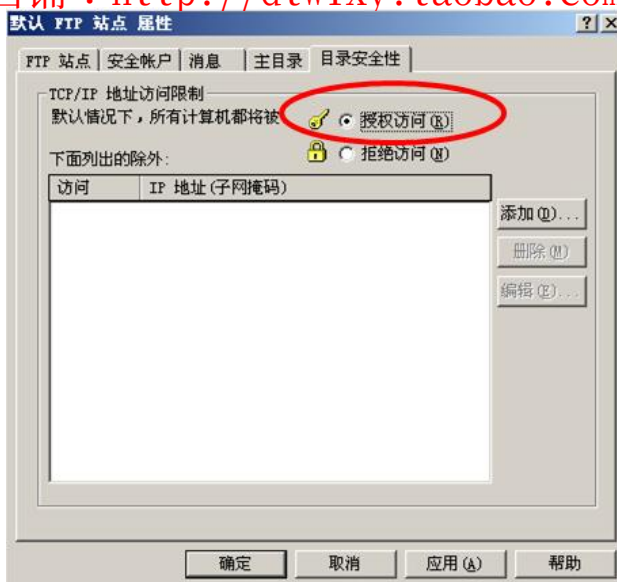
- 1) 不受限制
- 2) 连接限制为
- 3) 连接超时



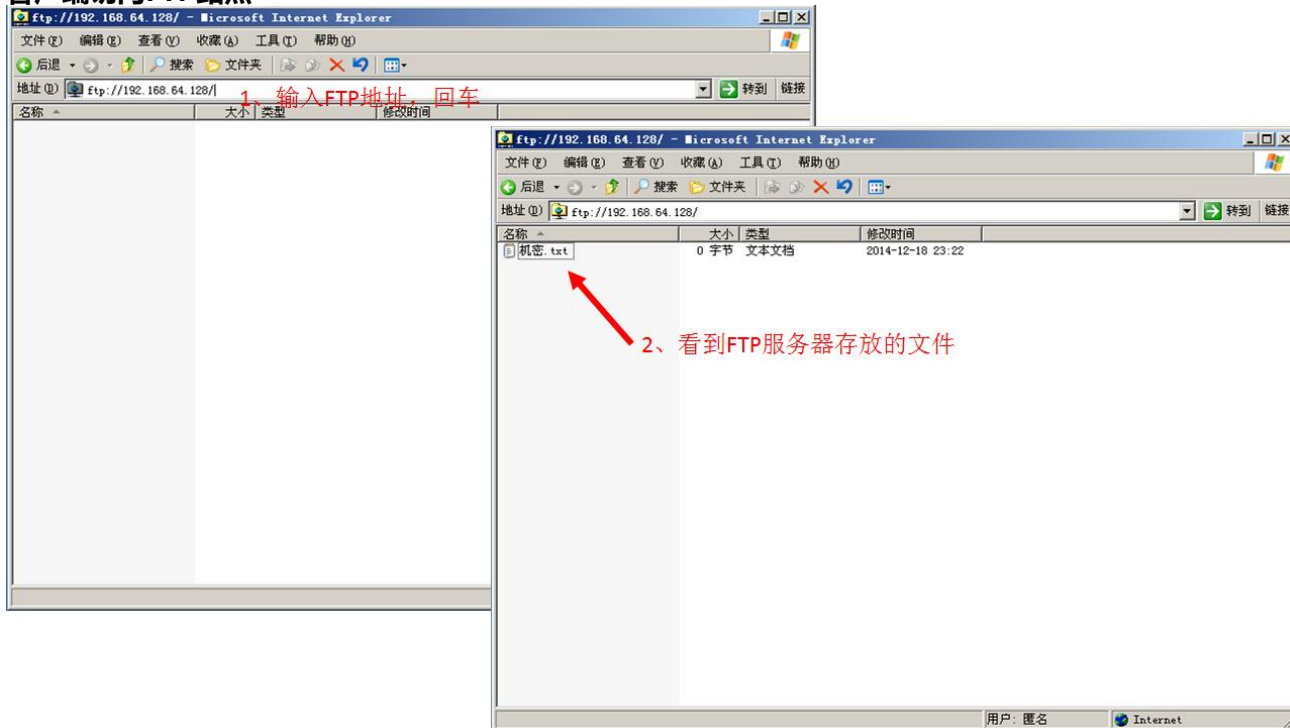
系统默认FTP的主目录c:\inetpub\ftproot，也可改为计算中的其它文件夹。



- (1) 禁止匿名访问, “安全账户”选项卡。
- (2) 限制IP地址, “目录安全性”选项卡



客户端访问FTP站点



FTP下的命令:

dir命令: 显示FTP服务器端有哪些文件可以下载。

get命令: 从服务器端下载一个文件。

! dir命令: 用来显示客户端当前目录中的文件信息。

put命令: 用来向FTP服务器上传一个文件。

lcd命令: 用来设置客户端当前的目录。

bye命令: 退出FTP连接。

Linux Apache (linux下的Web服务器)

Apache安装文件, apache-1.3.23-11.i386.rpm

Start Apache启动Apache服务器

Apply Changes 保存。

Stop Apache 停止。

httpd, Apache服务器的守护进程。

所谓虚拟主机服务, 是指在一台物理机器上提供多个Web服务。

Apache设置虚拟主机, 两种方案: 1、基于IP地址的虚拟主机。2、基于名字的虚拟主机。

基于域名的虚拟主机服务是目前应用比较广泛的一种方案。

基于IP地址的虚拟主机服务实现需要在机器上配置多个IP地址。因IP资源紧张, 很少使用这种方法。

Apache中的访问控制。

web网站常有这样的需要, 对某网站某部分内容进行简答的密码保护, 指允许授权的用户访问。

目录中默认名.htaccess配置文件。

AllowOverride

AuthName

DNS服务器配置。

1、名字解析服务

名字解析就是将**计算机名字**转换成**IP地址**的过程。在windows中使用两类名字: 主机名和NetBIOS名字。

DNS名字解析通过DNS服务器实现。

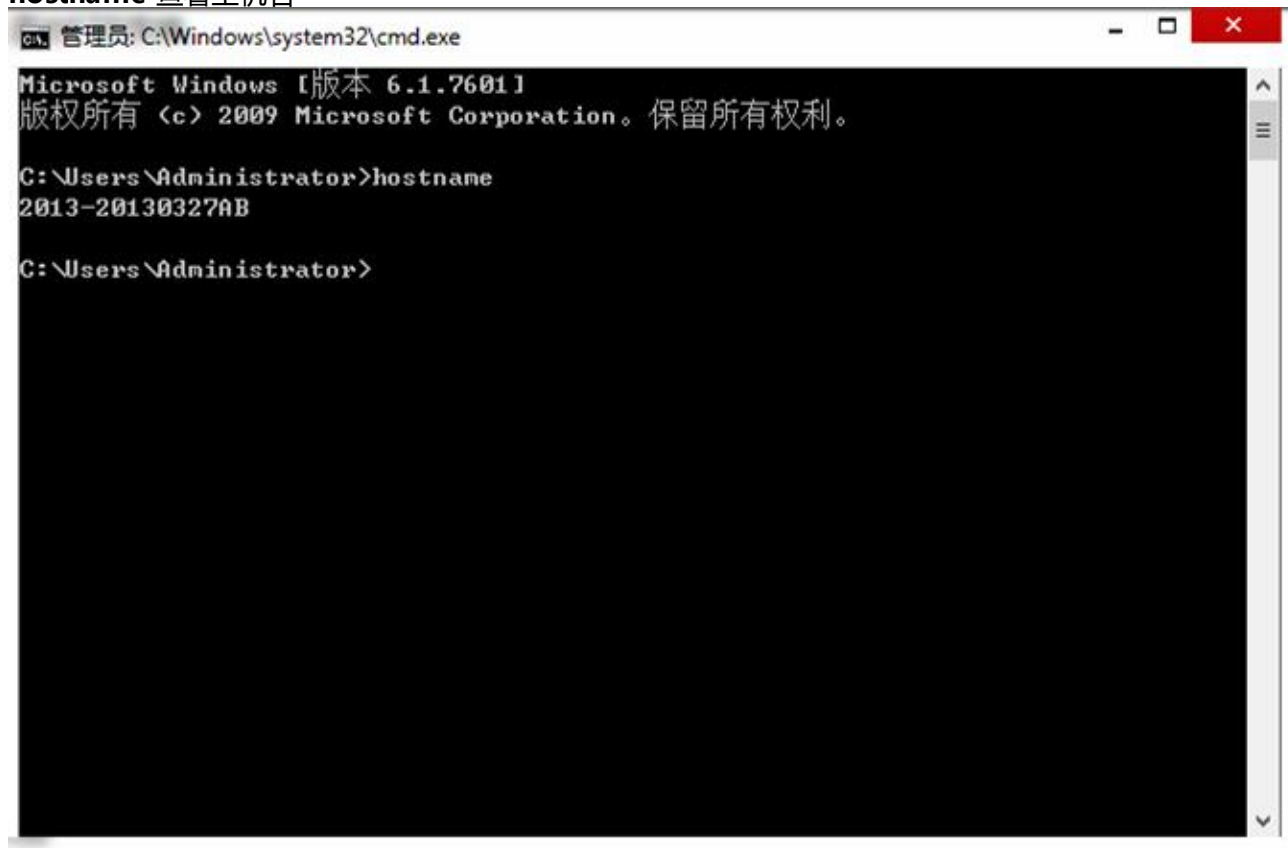
NetBIOS运行在网络层和应用层之间。

windows2000以后的计算机都使用DNS域名来实现大多数功能。

可以用hostname查看主机名, 也可以用ipconfig/all命令查看主机名。

使用nbtstat -n显示系统中注册的NetBIOS名字, 命令 nbtstat -c 。

hostname 查看主机名



```
管理员: C:\Windows\system32\cmd.exe
Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\Users\Administrator>hostname
2013-20130327AB

C:\Users\Administrator>
```

ipconfig/all 查看主机名和DNS后缀

```

管理员: C:\Windows\system32\cmd.exe

C:\Users\Administrator>ipconfig/all

Windows IP 配置

主机名 . . . . . : 2013-20130327AB
主 DNS 后缀 . . . . . :
节点类型 . . . . . : 混合
IP 路由已启用 . . . . . : 否
WINS 代理已启用 . . . . . : 否

以太网适配器 本地连接:

    连接特定的 DNS 后缀 . . . . . :
    描述 . . . . . : Realtek PCIe GBE Family Controller
    物理地址. . . . . : 90-FB-A6-8E-3C-3E
    DHCP 已启用 . . . . . : 是
    自动配置已启用 . . . . . : 是
    本地连接 IPv6 地址. . . . . : fe80::25a0:1006:7c59:c4e9%12<首选>
    IPv4 地址 . . . . . : 172.17.16.16<首选>
    子网掩码 . . . . . : 255.255.254.0
    获得租约的时间 . . . . . : Friday, December 19, 2014 08:41:01
    租约过期的时间 . . . . . : Friday, December 19, 2014 20:41:01
    默认网关 . . . . . : 172.17.16.1
    DHCP 服务器 . . . . . : 192.168.1.2
    DHCPv6 IAID . . . . . : 261159846
    DHCPv6 客户端 DUID . . . . . : 00-01-00-01-18-E4-6B-82-90-FB-A6-8E-3C-3E

    DNS 服务器 . . . . . : 192.168.1.2
                                202.203.144.33
    TCP/IP 上的 NetBIOS . . . . . : 已启用
    
```

nbtstat -n 系统注册的NetBIOS名字


```
管理员: C:\Windows\system32\cmd.exe

Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\Users\Administrator>nbtstat -n

本地连接:
节点 IP 地址: [172.17.16.16] 范围 ID: []

          NetBIOS 本地名称表

    名称                类型      状态
    -----
    2013-20130327AB<00>  唯一      已注册
    WORKGROUP           <00>      组        已注册
    2013-20130327AB<20>  唯一      已注册
    WORKGROUP           <1E>      组        已注册

C:\Users\Administrator>
```

nbtstat -c 显示NetBios缓存内容

```
管理员: C:\Windows\system32\cmd.exe

Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\Users\Administrator>nbtstat -c

本地连接:
节点 IP 地址: [172.17.16.16] 范围 ID: []

缓存中没有名称

C:\Users\Administrator>
```

DNS主机名解析

DNS主机名解析的查找顺序是: 1、先查找客解析程序缓存。2、后向DNS服务器发出解析请求。3、再用NetBIOS名字解析方法取得结果

可以用ipconfig/displaydns查看内容。

```
管理员: C:\Windows\system32\cmd.exe
Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\Users\Administrator>
C:\Users\Administrator>ipconfig/displaydns

Windows IP 配置

      sls.microsoft.com
-----
记录名称. . . . . : sls.microsoft.com
记录类型. . . . . : 1
生存时间. . . . . : 86400
数据长度. . . . . : 4
部分. . . . . : 答案
A <主机>记录 . . . . : 127.0.0.1

      sls.microsoft.com
-----
没有 AAAA 类型的记录

      genuine.microsoft.com
-----
记录名称. . . . . : genuine.microsoft.com
记录类型. . . . . : 1
生存时间. . . . . : 86400
数据长度. . . . . : 4
部分. . . . . : 答案
A <主机>记录 . . . . : 65.55.58.177
```

清除解析程序缓存的命令：ipconfig/flushdns



编辑HOST文件可以帮助DNS主机名解析。(c:\windows\system32\drivers\etc)

域名系统

域名系统 (Domain Name System , DNS) 通过层次结构的分布式数据库建立。

DNS的逻辑结构是一个分层的**域名树**。

根域。根域没有名称, 用句号“.”表示, 但经常是省略的。

根域下面是**顶级域** (Top-Level Domains , TLD) , 分为**国家顶级域** (Country conde Top Level Domain , ccTLD) 和**通用顶级域** (Generic Top Level Domain , gTLD) 。

国家顶级域包含243个国家和地区的代码, **例如**: cn代表中国, uk代表英国等, 最初的通用顶级域有7个。

顶级域下面是**二级域**。

在**二级域**之下, 组织机构还可以划分**子域**。

域名服务器

国际域名由13个根域服务器提供服务, 其中9个根域服务器放置在美国, 另外3个分别放置在英国, 瑞典、日本。中国有3个国际域名的镜像服务器。

域是名字空间的一部分, “区域”是存储的概念, 是存储空间的一部分。

SOA (Start of Authoritative) : 开始授权记录

A (Address) : 地址记录表示主机名到IP地址的映像。

正向DNS

PTR (Pointer) : 指针记录式IP地址到主机名的映射。

反向DNS

NS (Name Server) : 给出区域的授权服务器。

MX (Mail eXchanger) : 定义了区域邮件服务器及其优先级 (搜索顺序)

CNAME : 为正式主机名 (canonical name) 定义了一个别名 (alisa) 。

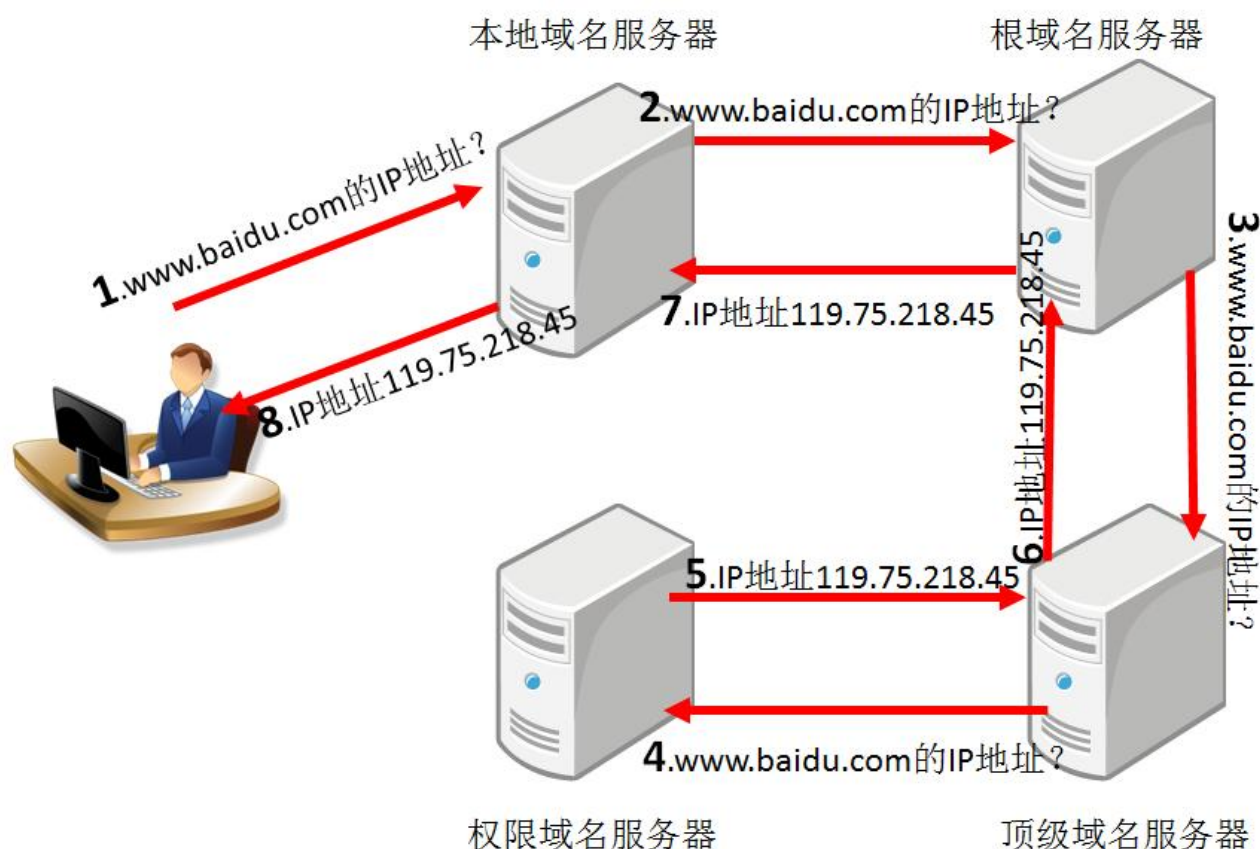
域名查询

DNS实现正反两个方向的查询, 正向查询是检查地址记录 (A)。反向查询时检查指针记录 (PTR)。

查询方式:

1、递归查询:

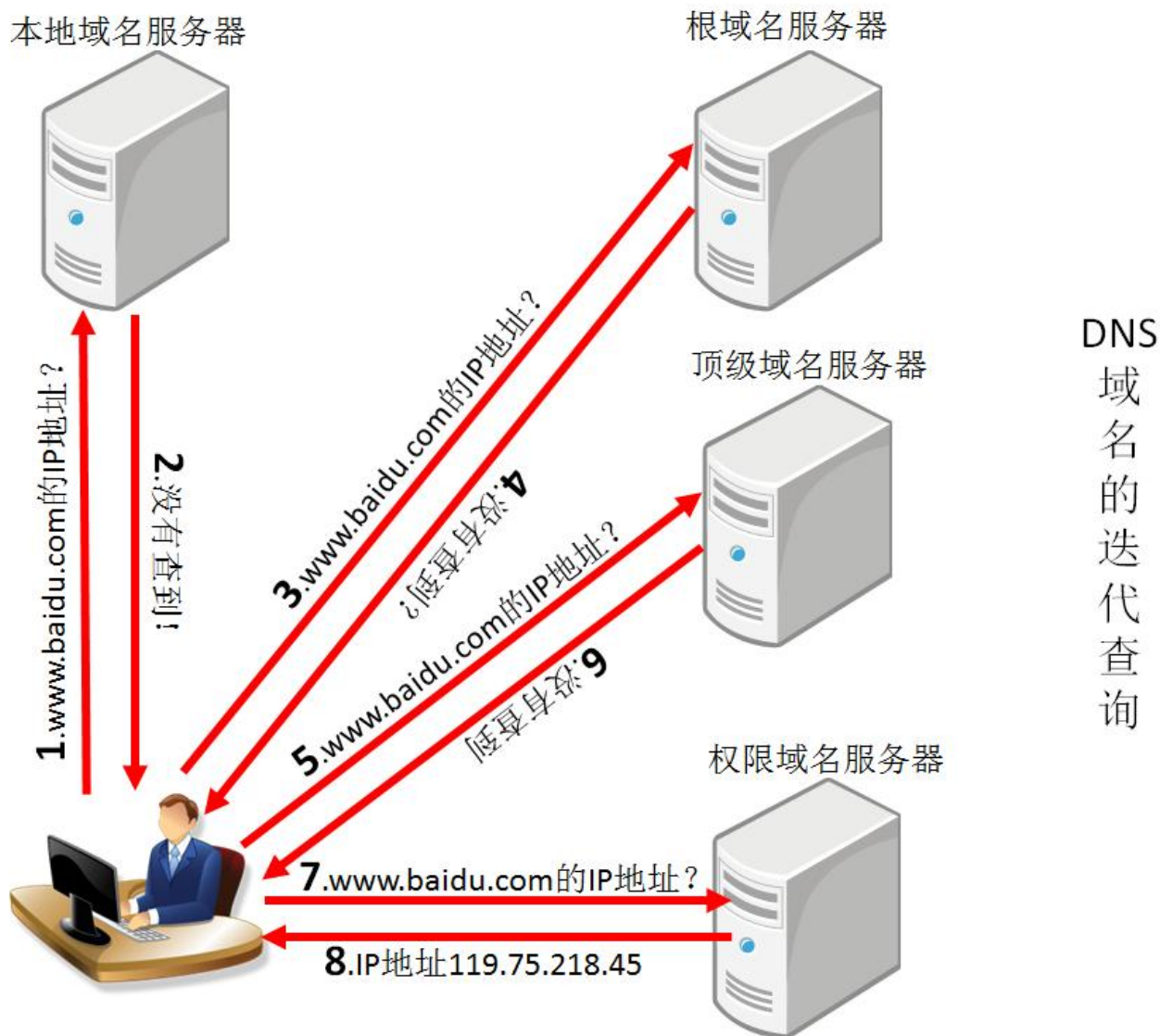
一次查询 (一个来回)



DNS域名的递归查询

2、迭代查询:

多次查询 (多个来回)



DNS服务器收到查询请求后, 1、首先在自己的区域文件中查找。2、再在高速缓存找。3、DNS服务器必须向其它服务器发送请求。

3个DNS命令
6个NS资源类型
2个查询方式
2个查询方向

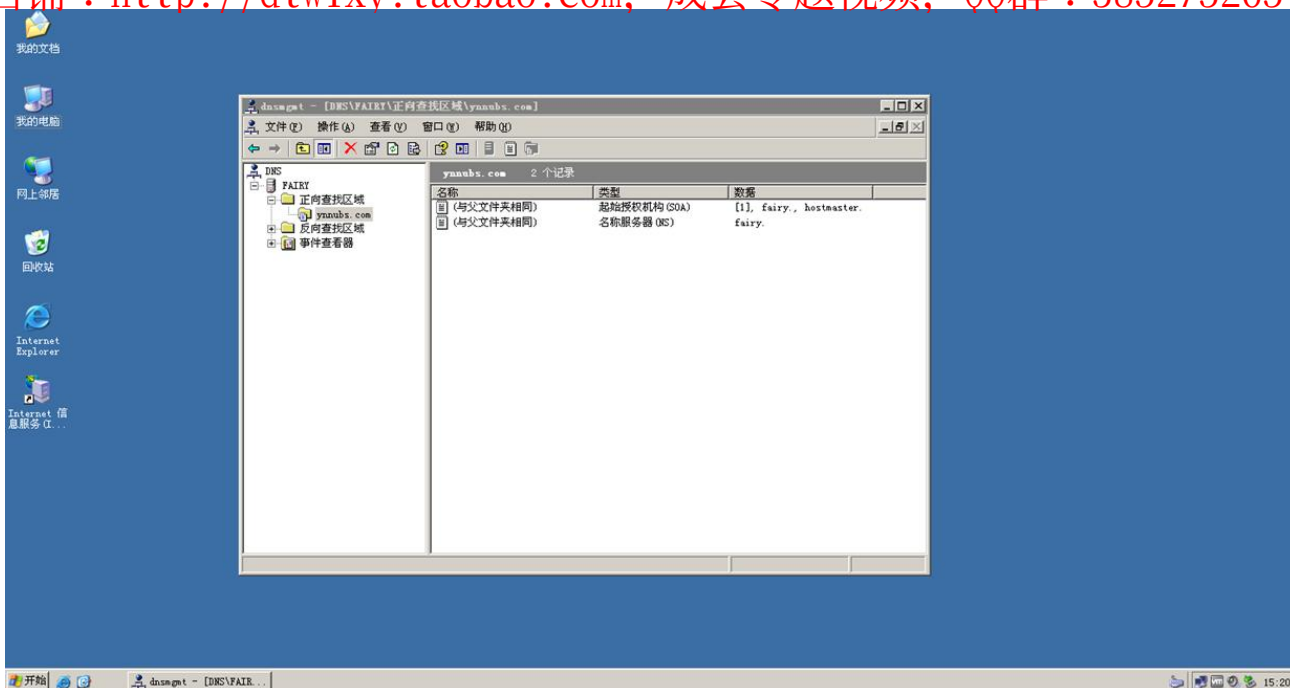
把一个区域的名字服务器分为**主服务器**和**辅助服务器**, 可以实现**冗余容错**功能。可以实现**负载分担**的功能。

服务器中复制全部资源记录, 区域信息改变时才复制部分资源记录。

前者叫**完全复制**, 后者叫**增量复制**。

DNS服务器的安装。

单击“开始”→“管理工具”→“配置您的服务器向导”命令, →下一步。进入“服务器角色”→DNS服务器→下一步→选择总结→安装DNS服务器。→运行配置DNS服务器向导来配置。提示时插入windows2003的安装盘。

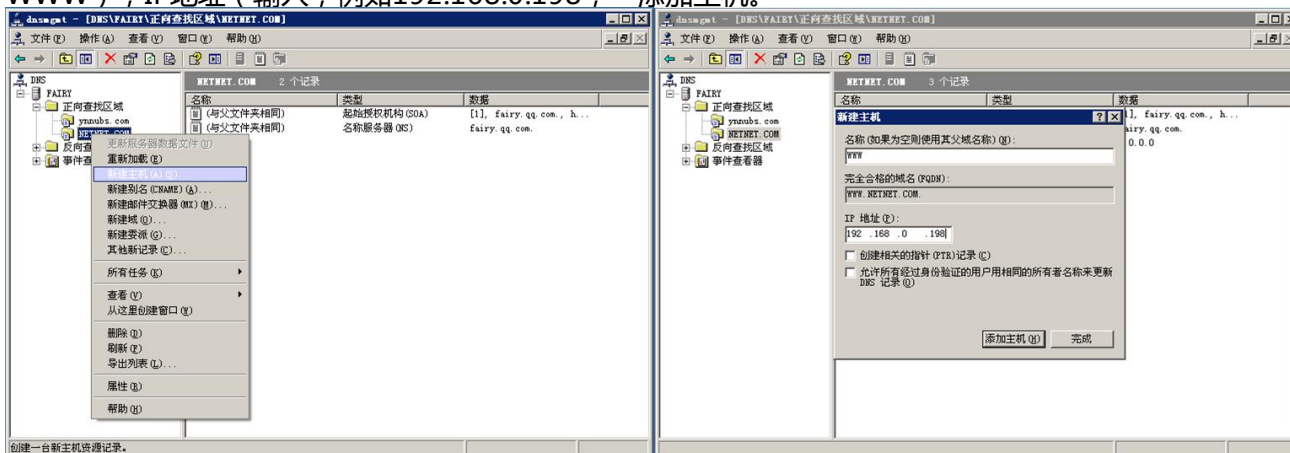


创建DNS解析区域

“配置DNS服务器向导” 下一步, 打开” 选择配置操作 “→创建正向查找 (适合小型网络) →主服务器位置→这台服务器维护该区域→区域名称→输入 (例如: xidian.cdu.cn)

创建域名

开始→管理工具→DNS→dnsmagmt控制台。→ServerName→正向查找区域→新建主机, →名称 (输入 WWW), IP地址 (输入, 例如192.168.0.198 , →添加主机。



设置DNS客户端

将windows下的DNS服务器地址设置正确。

linux BIND DNS服务器安装

BIND (Berkeley Internet Name Domain) 是在UNIX/Linux下试下域名解析的软件包, Red Hat Linux 上使用BIND建立DNS服务器。

安装bind软件包, 双击\RedHat\RPMS\bind-9.2.0-8.i386.rpm.

使用nslookup命令对BIND DNS服务器进行测试。

(笔记14 PDF 436页)

115/241

正向解析 (A)

#nslookup

> master.test.com /*测试正向解析地址记录, 查询主机master.test.com的IP地址*/

```
Sever: 192.168.1.114
Address: 192.168.1.114#53

Name:master.test.com
Address:192.168.1.114
```

反向解析 (PTR)

#nslookup

> 192.168.1.113/*测试反向解析地址记录, 查询IP地址为192.168.1.113的主机名称*/

```
Sever: 192.168.1.114
Address: 192.168.1.114#53

113.1.168.192.in-add.arpa  name=slave.test.com
```

定义别名 (CNAME)

#nslookup

> dns.test.com/*测试“名称别名”记录, 查询主机dns.test.com的别名*/

```
Sever: 192.168.1.114
Address: 192.168.1.114#53
dns.test.com  canonical name=master.test.com
Name:master.test.com
Address:192.168.1.114
```

NS (区域的授权服务器)

> set type=ns/*测试type为NS (Name Server 名称服务器) 记录*/

```
Sever: 192.168.1.114
Address: 192.168.1.114#53
test.com: nameserver=slave.test.com
test.com: namesserver=master.test.com
```

MX (区域邮件服务器)

> set type=mx/*测试类型为MX (Mail eXchanger邮件服务器) 记录*/

> test.com

115/241

Sever: 192.168.1.114
Address: 192.168.1.114#53
test.com: mail exchanger=**10** mail.test.com

优先级

DHCP服务器配置：

在大中型网络中使用DHCP (Dynamic Host Configuration Protocol) 的**好处**：

- 1) 管理员可以迅速验证IP地址和网络参数。
- 2) DHCP不会从一个范围里同时租借相同的IP地址。
- 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: 设置默认网关、DNS和WINS服务器地址)
- 4) 主机物理上被移动到了不同的子网上, 该子网上的DHCP服务器自动配置TCP/IP配置信息。
- 5) 方便了便携机用户, 当移动到不同的子网时不再需要为便携机分配IP地址。

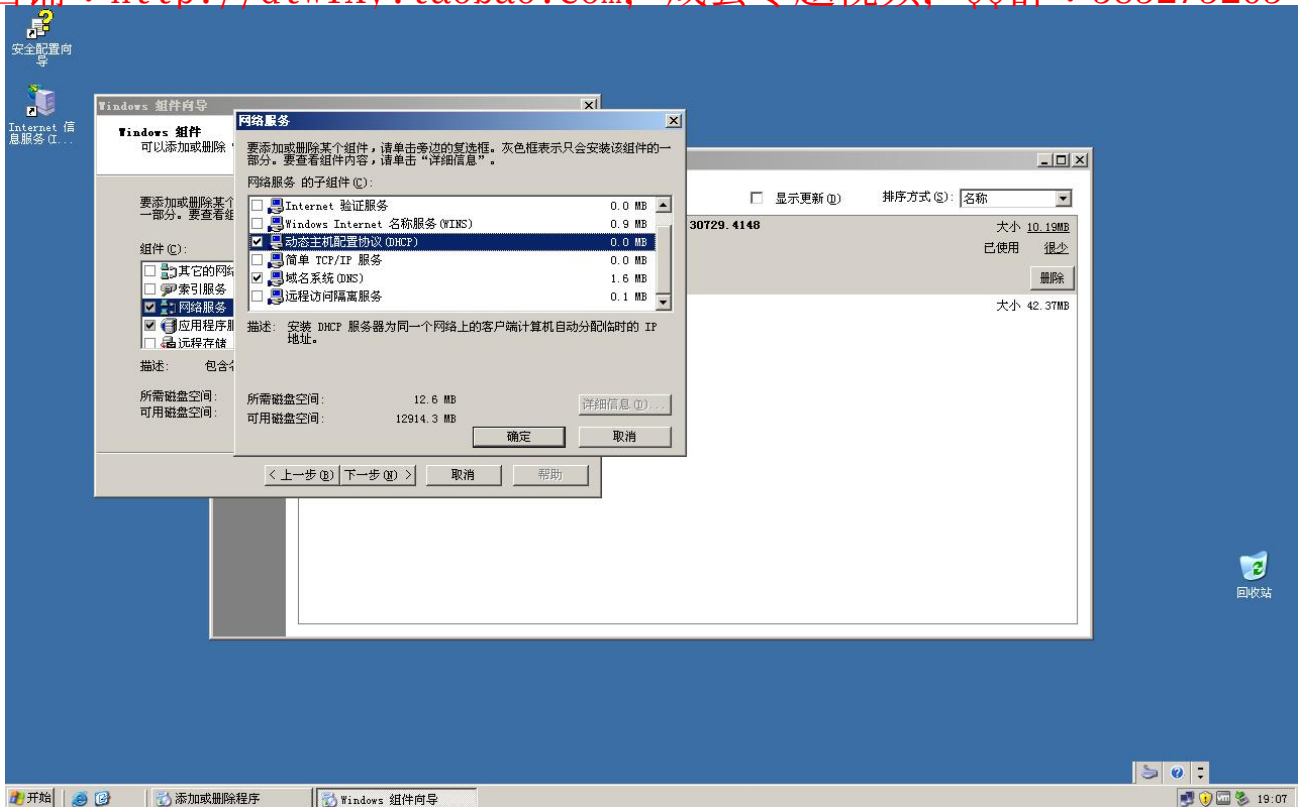
DHCP工作过程如下：

- 1) DHCP客户端首次启动, 向DHCP发送一个**Dhcpdiscover**数据包 (租用请求)
- 2) DHCP服务器收到后, 提供 (dhcpoffer) 一个未分配的IP地址。
- 3) DHCP服务器向客户端发送一个**确认** (dhcpack), (包括最初给的IP地址和租约信息) 租约默认**8天**。
- 4) 当租约过了**50%**, 客户端将和分配地址的DHCP服务器更新租约, 当超过**87.5%**时, 还没有得到更新, 将与其他DHCP联系, 如果没有其他DHCP服务器运行, 则**停止使用**这个IP, 并发送一个新的dhcpdiscover数据包, 重复过程。

电脑重启发送DhcpRequest

安装DHCP服务器：

控制面板→添加删除程序→添加/删除windows组件→windows组件向导→双击“网络服务”→动态主机配置协议 (DHCP) (复选框) →确定→下一步→完成。



创建DHCP作用域

确定一段IP地址范围。

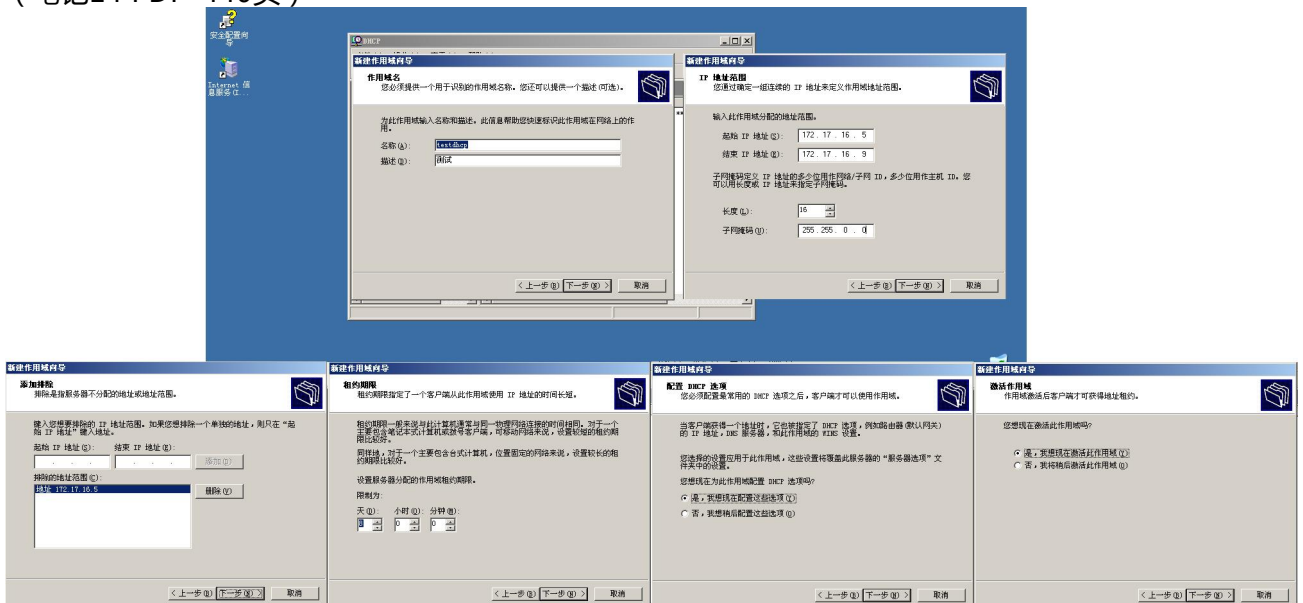
开始→管理工具→DHCP→右键DHCP服务器名称→新建作用域。

新建作用域向导，下一步→作用域名→名称（输入名称和描述）→IP地址范围→起始IP地址和结束IP地址（输入范围）。

添加排除向导

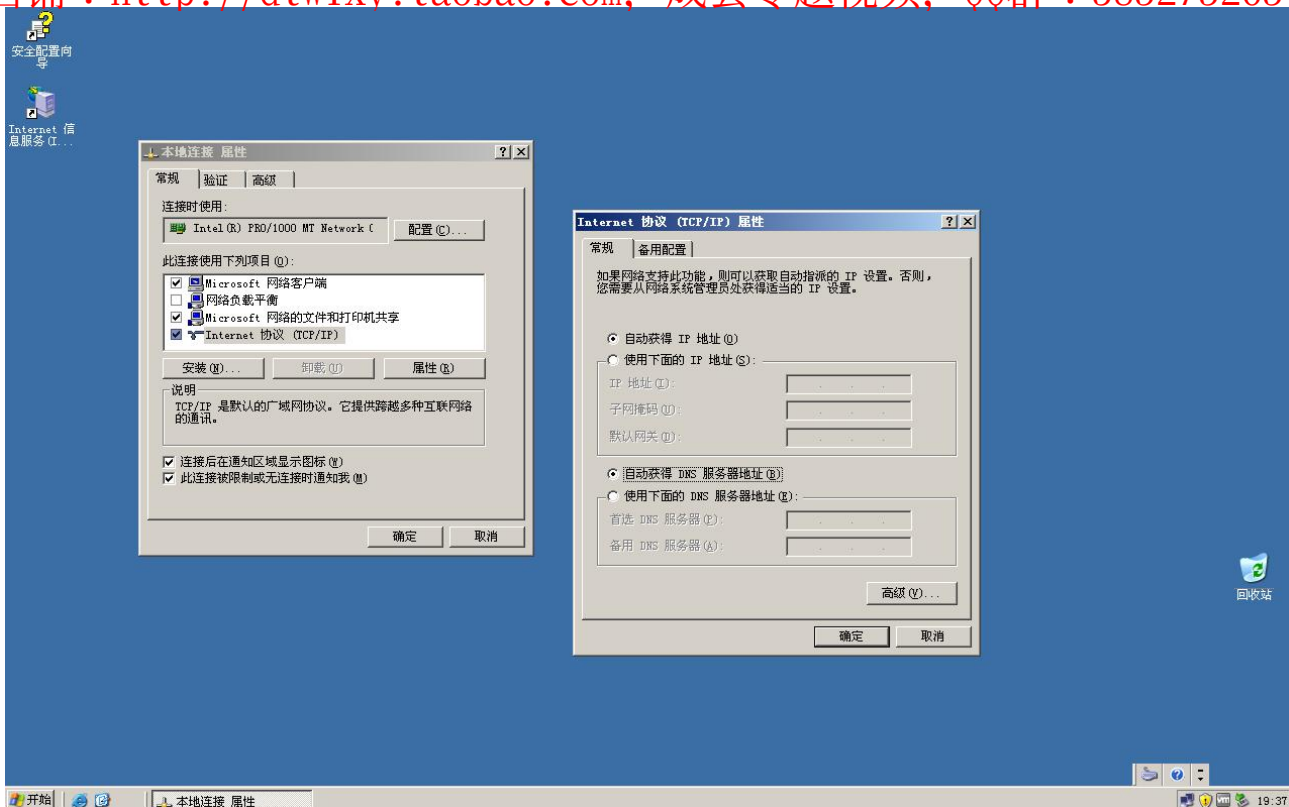
是，我想现在配置这些选项→下一步→“默认网关”（可以不填）→激活作用域→是，我想现在激活此作用域→下一步→完成。

（笔记14 PDF 440页）

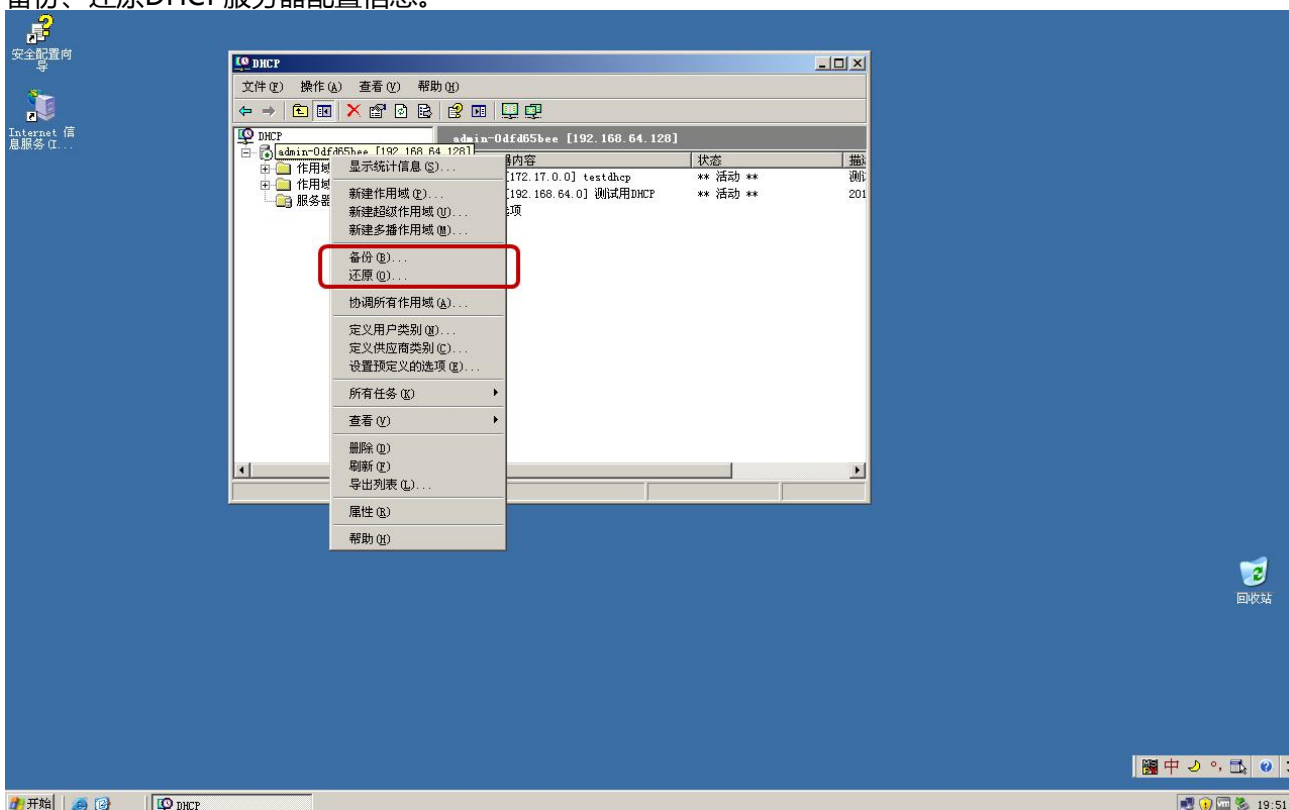


DHCP的客户端设置：

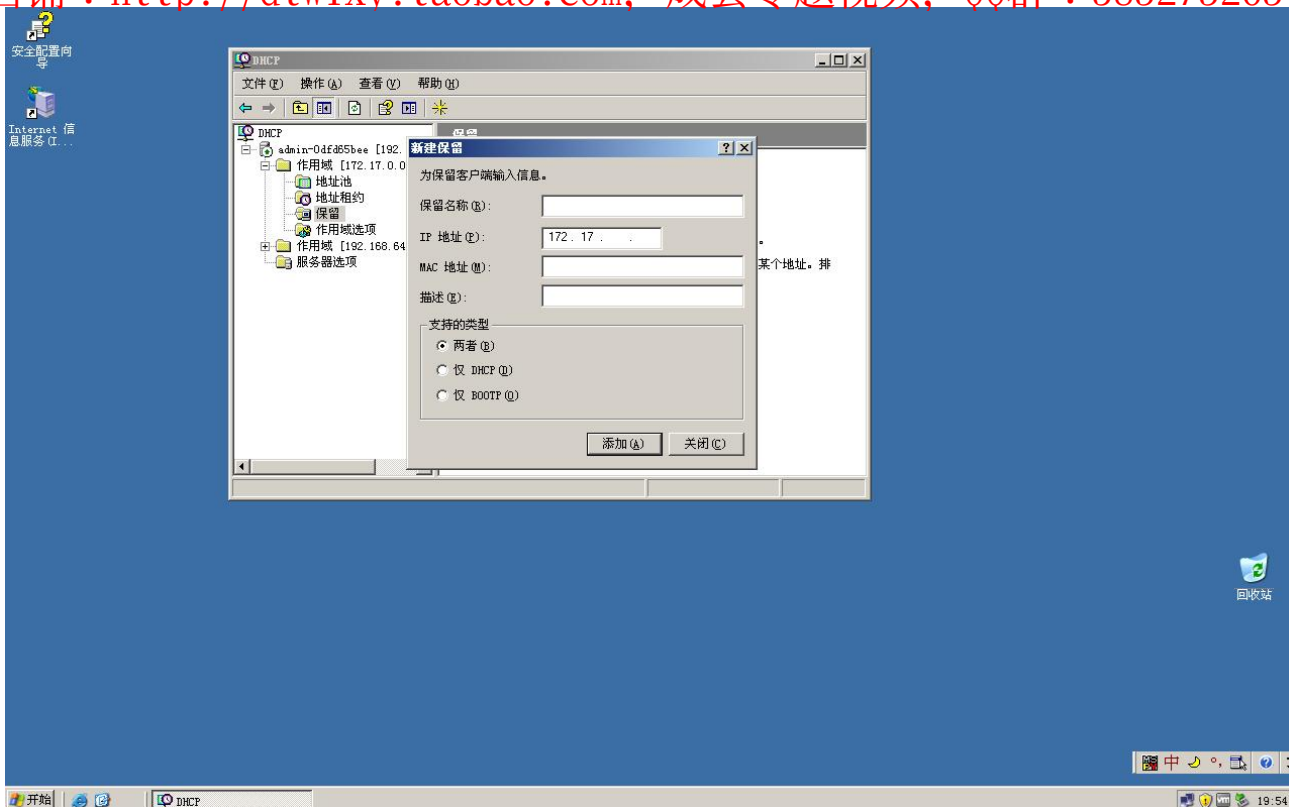
通过本地连接属性窗口，进入Internet协议TCP/IP，设置为自动



备份、还原DHCP服务器配置信息。



DHCP服务器的IP地址与MAC地址绑定策略，
右击保留选项，新建保留→名称（输入计算机名）→在IP地址。



Linux的DHCP服务器文件/etc/dhcpd.conf

DHCP服务的网络配置参数：

参数

ddns-update-style 更新模式，包括none、interim、ad-hoc

default-lease-time 默认租约时间，单位秒

max-lease-time 最大租约时间，单位是秒

hardware 接口类型和MAC地址。

server-name DHCP服务器名称。

fixed-address 分配给客户端一个固定地址。

declarations：用来描述网络布局、提供dhcp客户的IP地址分配策略。

subnet：子网

range：范围

host：主机

option（选项）：用来配置DHCP可选参数，全部用option关键字开始。

subnet-mask：子网掩码

domain-name：DNS名字

domain-name-server：DNS服务器IP地址

host-name：主机名称

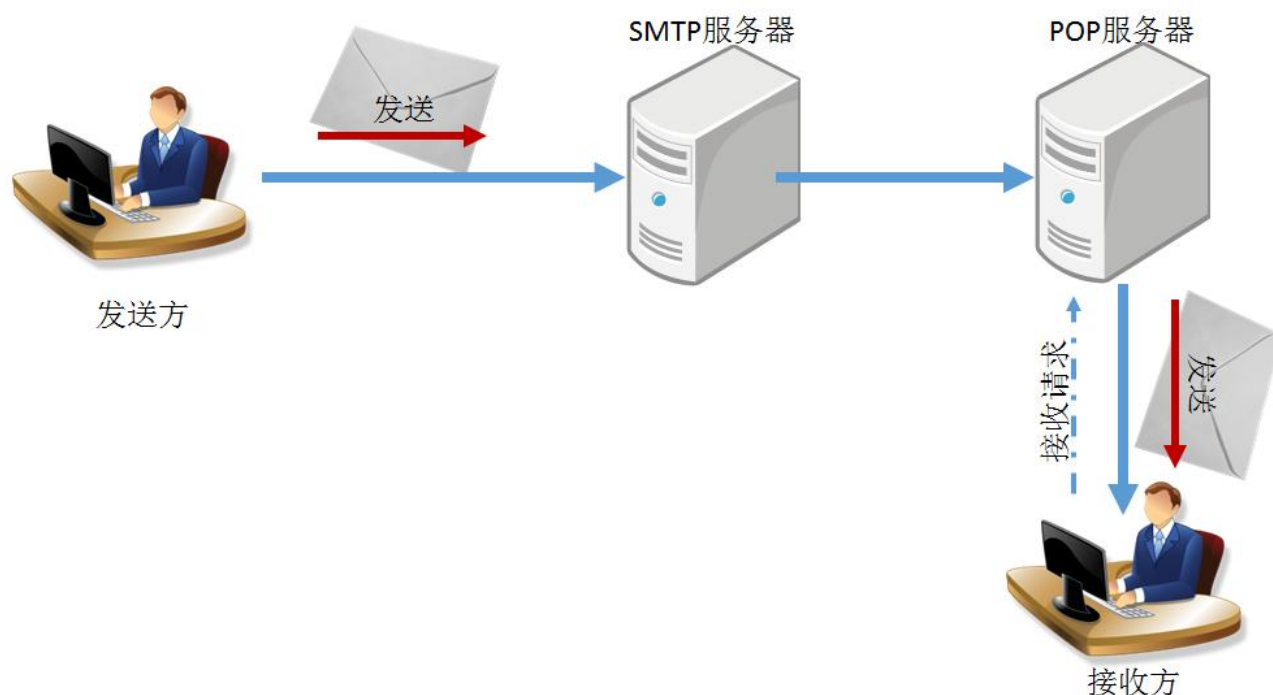
routers：默认网关。

*windows不需要host-name，linux采用Dhcp.conf配置文件进行说明。

```
ddns-update-style none;  
subnet 192.168.0.0 netmask 255.255.255.0  
range 192.168.0.200 192.168.0.254  
ignore clirnt-updates  
default-lease-time 3600  
max-lease-time 7200  
option routers 192.168.0.1  
option domain-name "test.org"  
option domain-name-servers 192.168.0.2  
hsot test1 {hardware Ethernet 00:E0:4C:70:33:65;fixed-address 192.168.0.8}
```

电子邮件服务器的配置。

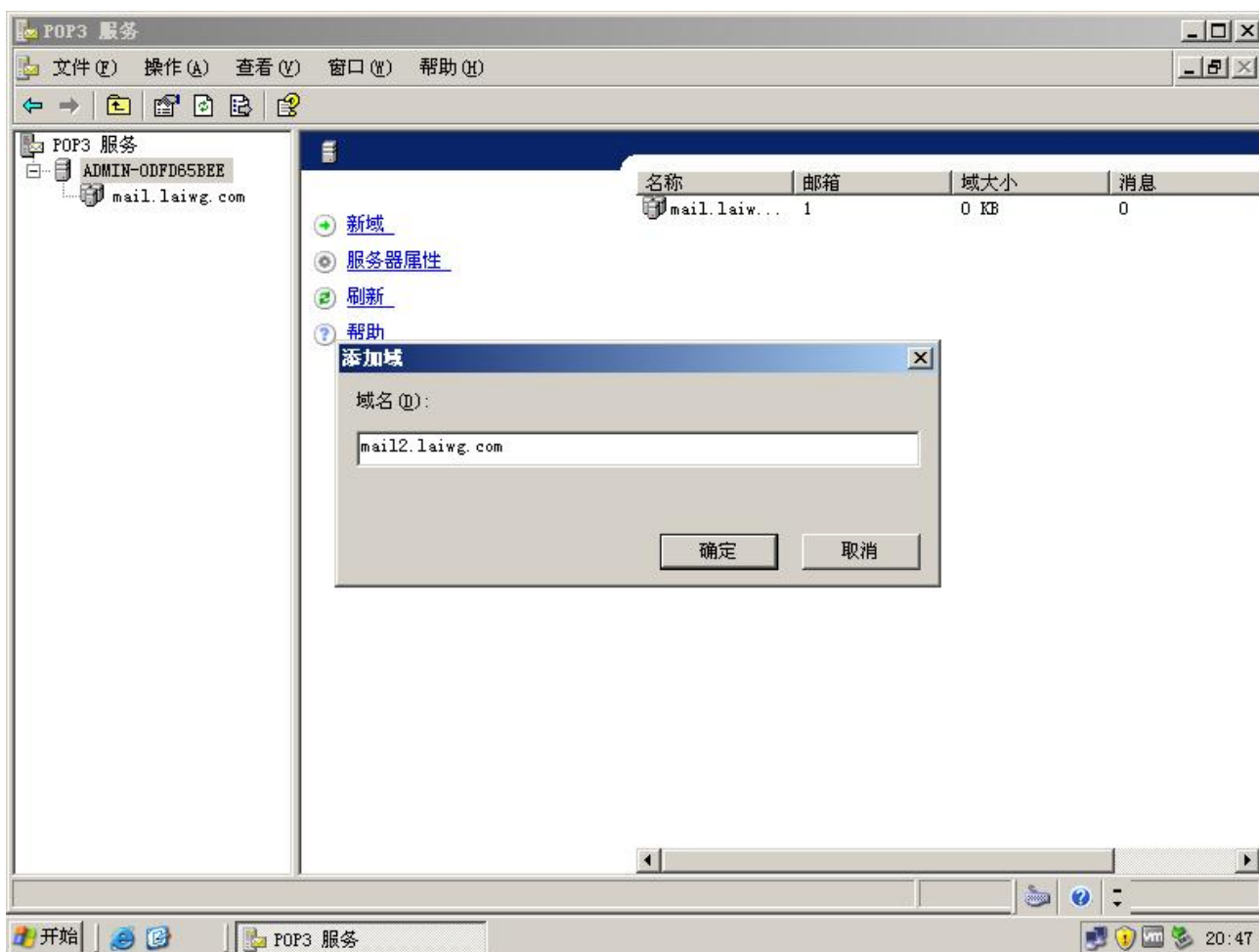
SMTP（发件）服务器和POP3（收件）服务器。

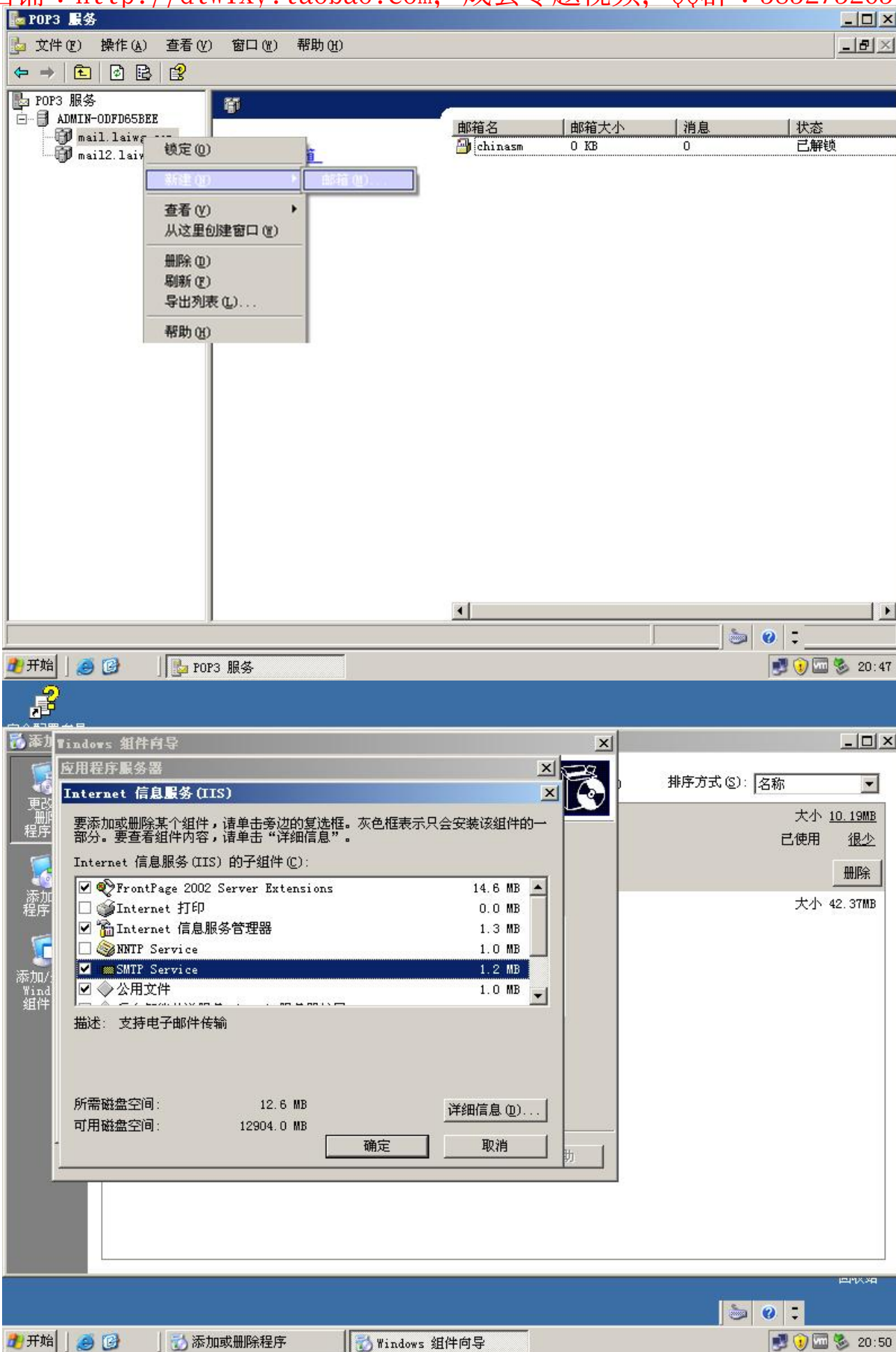


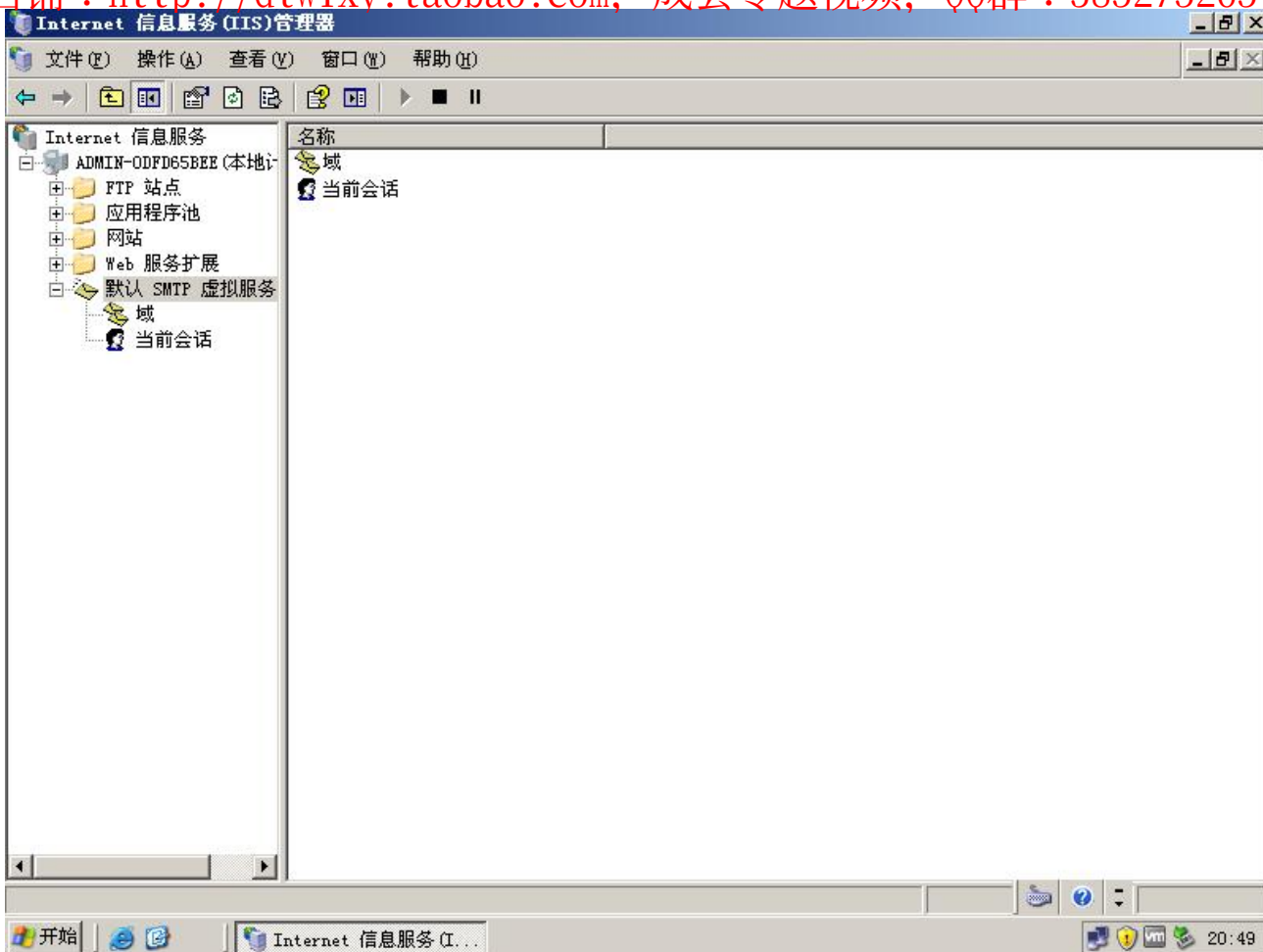
安装：

开始→管理工具→管理您的服务器→添加或删除角色→服务器角色（对话框）→选中“邮件服务器（POP3，SMTP）”。



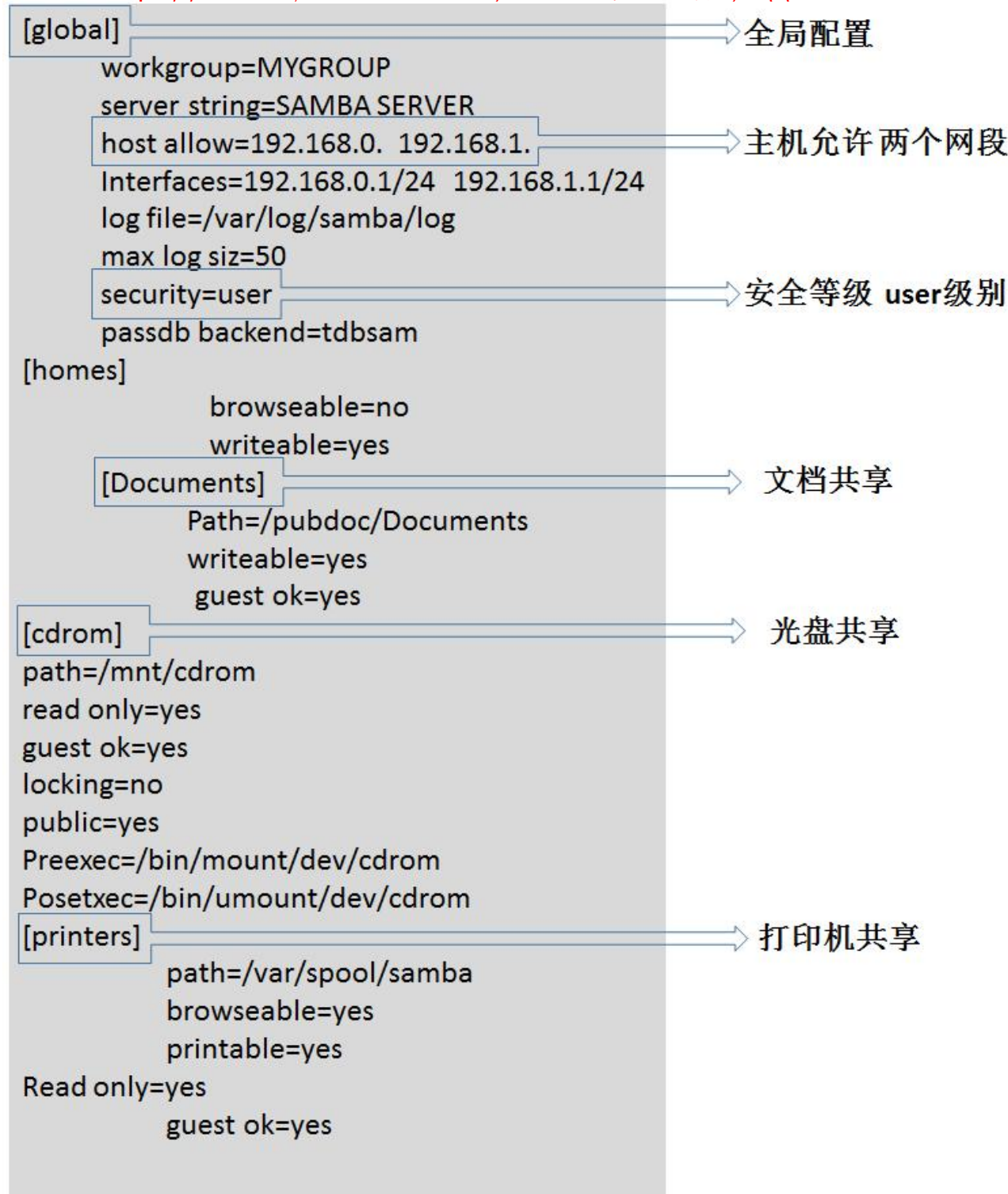






Samba服务器向Linux或windows系统客户端提供windows风格的文件和打印机共享服务，实现在Samba服务器上的打印机和文件系统的共享。

samba.conf典型配置：



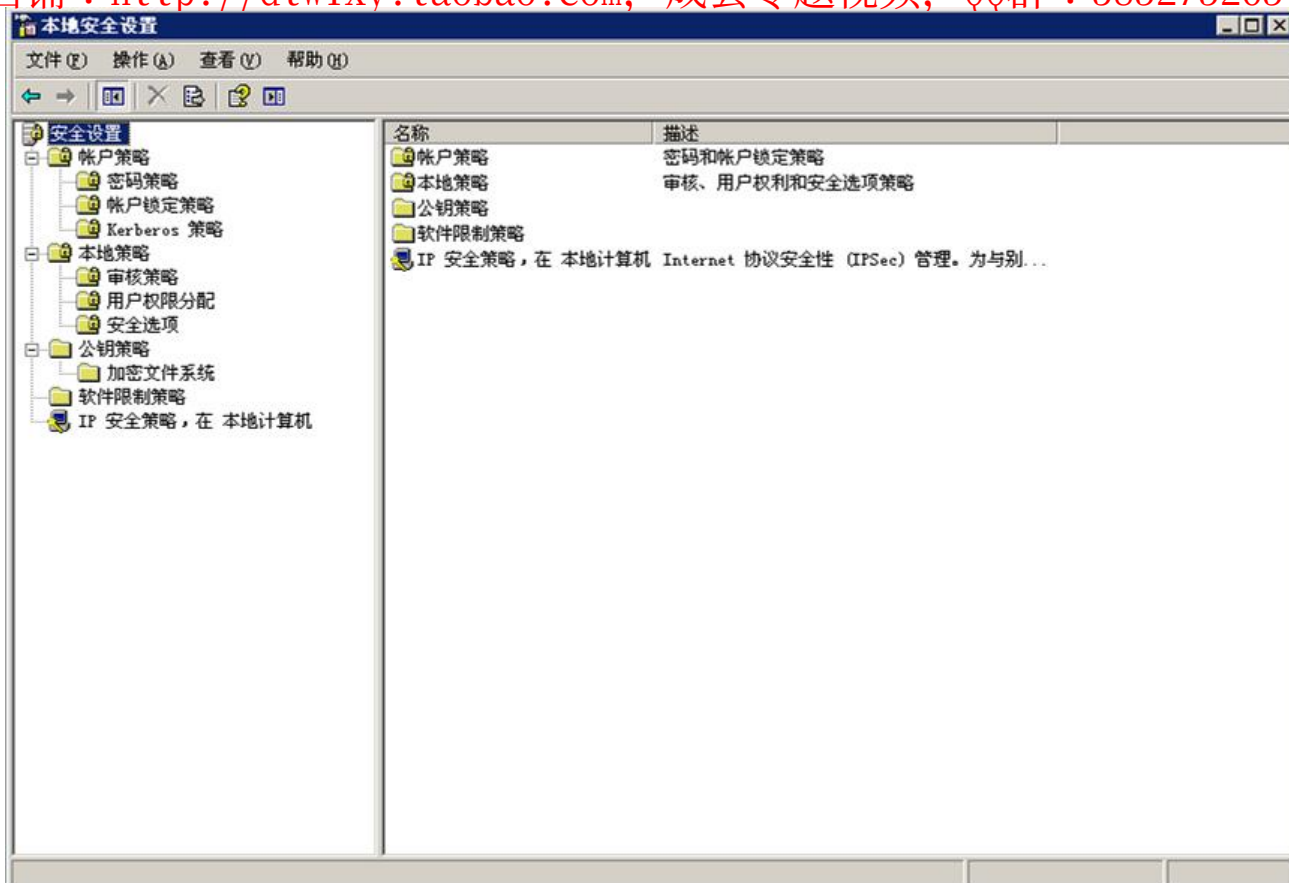
windows Server 2003安全策略 (新增章节, 重点)

安全策略是事先定义好的一系列应用计算机的行为准则。

在2003中安全策略分为：“本地安全策略”和“组策略”。

本地安全策略基于单台计算机。

组策略则在范围内实现。



本地安全策略, 可以修改计算机的账户策略、本地策略、公钥策略和IPSec策略。



IPSec策略

组策略定义了系统管理员需要管理的用户桌面环境的多种组件。

Windows Server 2003提供了组策略编辑器, **gpedit.msc**。



账户密码策略设置

步骤:

1、开始→管理工具→本地安全策略。(或者运行secpol.msc)

选择“帐户策略”下的“密码策略”, 已启用状态, 并满足一定的要求。

不包含全部或部分的用户帐户名

长度至少为6个字符。

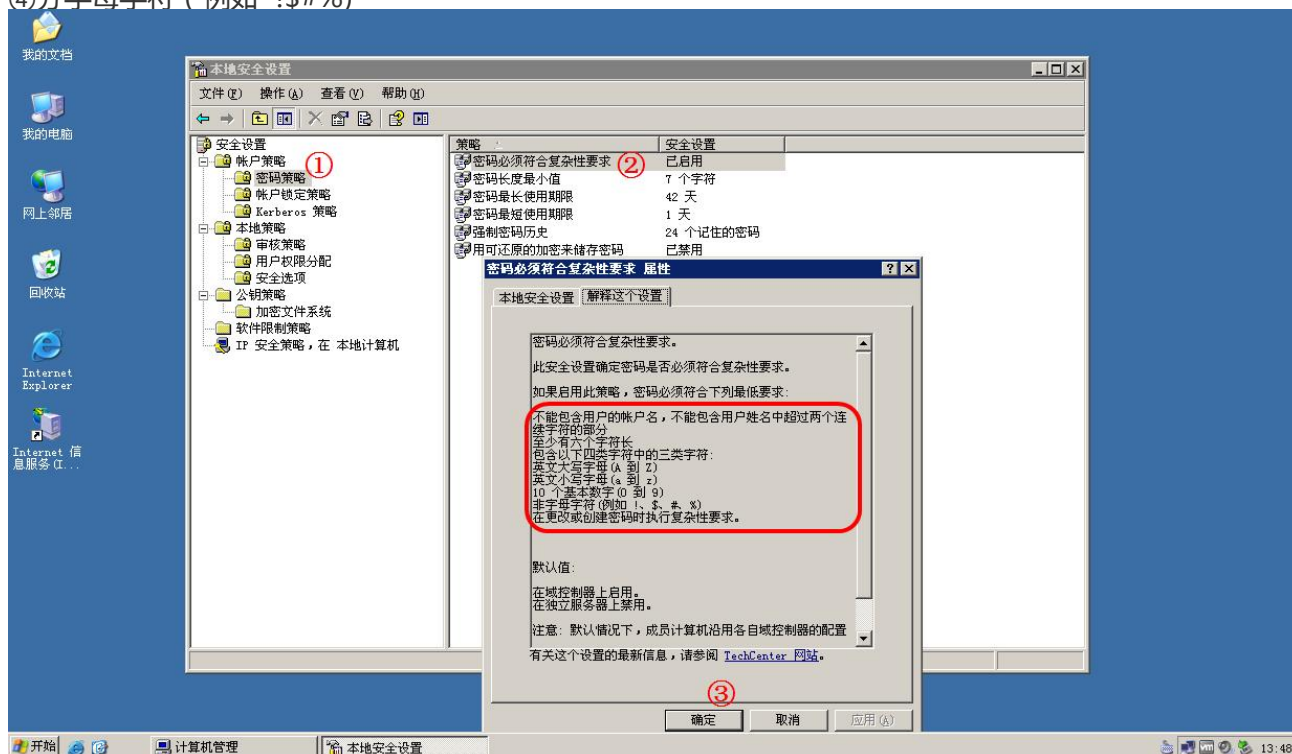
包含来自以下4个类比中的3个字符:

①英文大写字母(从A到Z)

②英文小写字母(从a到z)

③10个基本数字(从0到9)

④分字母字符(例如 !\$#%)



IPSec策略设置

配置一个IPSec包括: 1、创建IPSec策略。2、创建筛选器。3、配置隧道规则。4、进行策略指派。

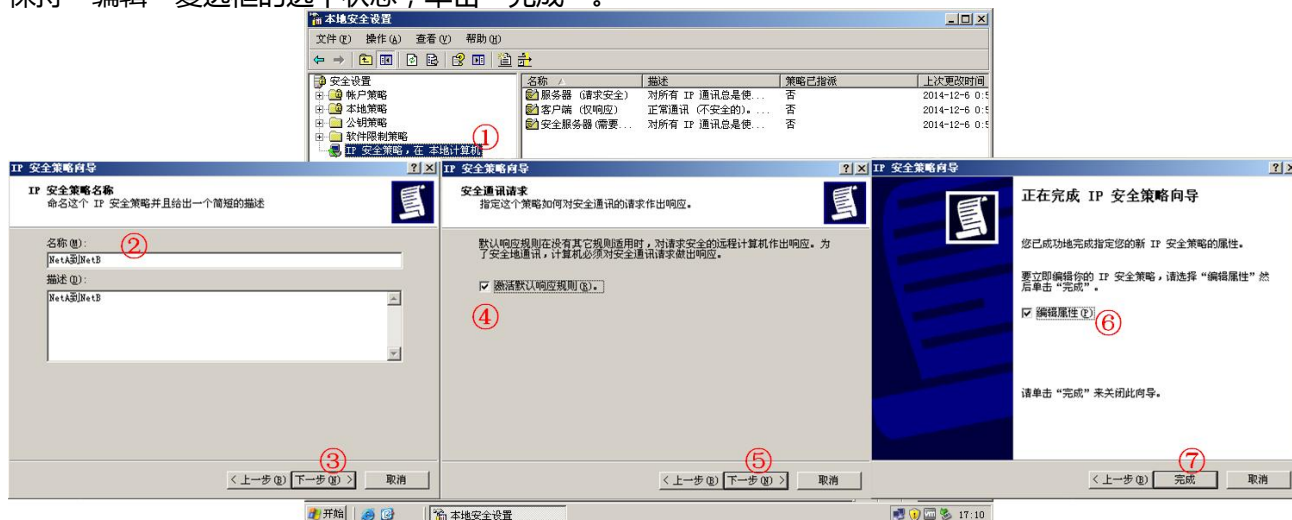
基本步骤:

右键单击“IP安全策略, 在本地计算机”选项, 单击“创建IP安全策略”

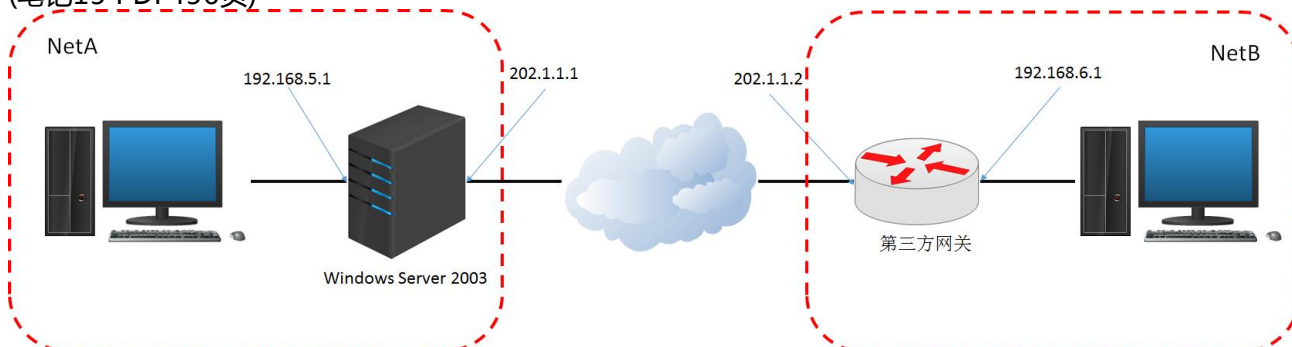
输入策略名称, 根据实际情况自定义。

清除“激活默认响应规则”复选框, 下一步

保持“编辑”复选框的选中状态, 单击“完成”。

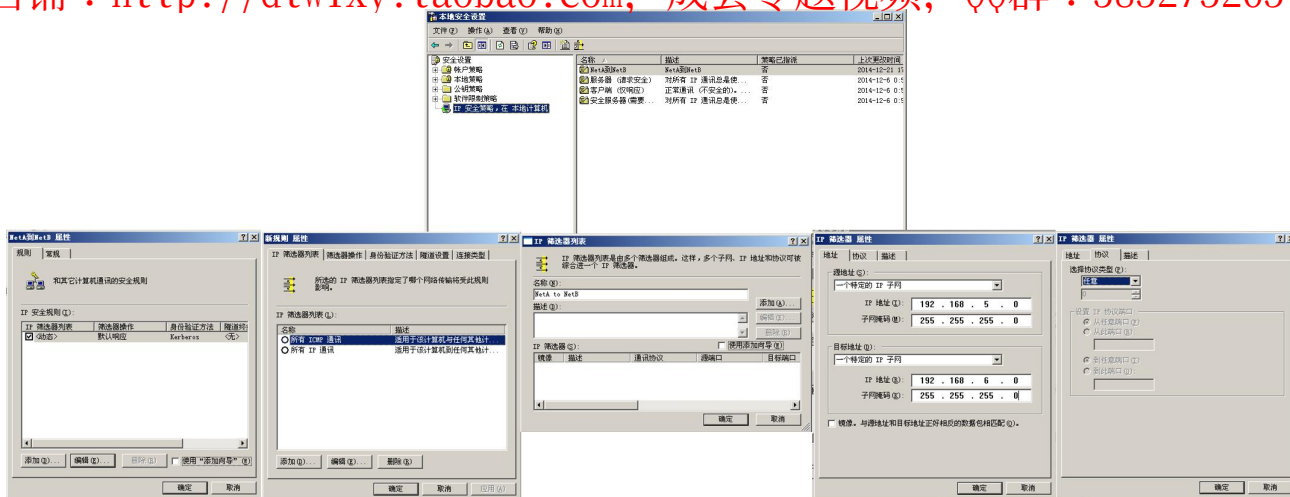


(笔记15 PDF456页)



需要建立两个筛选器, 一个用于匹配NetA到NetB (隧道1), 另一个用于匹配NetB到NetA (隧道2)

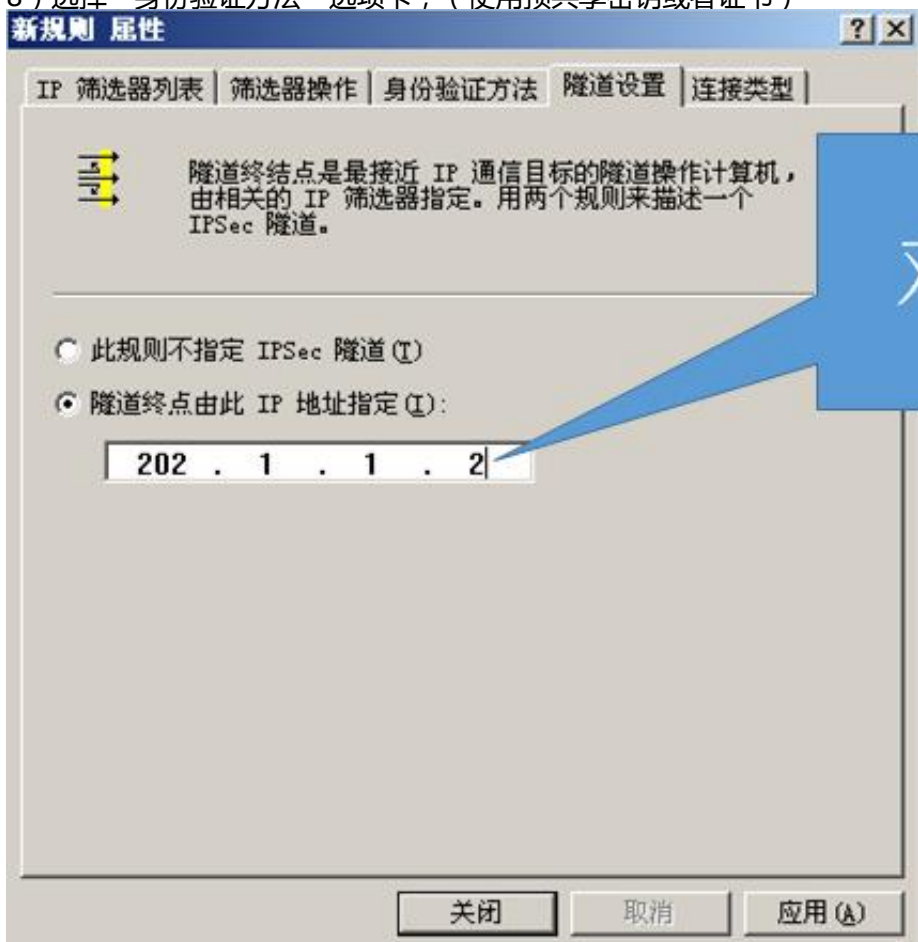
- 1) 在新隧道属性中清除“使用添加向导”的复选框, 单击“添加”按钮
- 2) 选择“IP筛选器列表”选项卡
- 3) 输入名称, 使用添加向导复选框, 并单击“添加”按钮, 弹出“筛选器属性”对话框。
- 4) 源地址: “一个特定的IP子网”, 输入192.168.5.0
- 5) 目标地址: “一个特定IP子网”, 输入192.168.6.0
- 6) 清除“镜像”
- 7) 选择“协议”, 使用协议类型设置为任意。

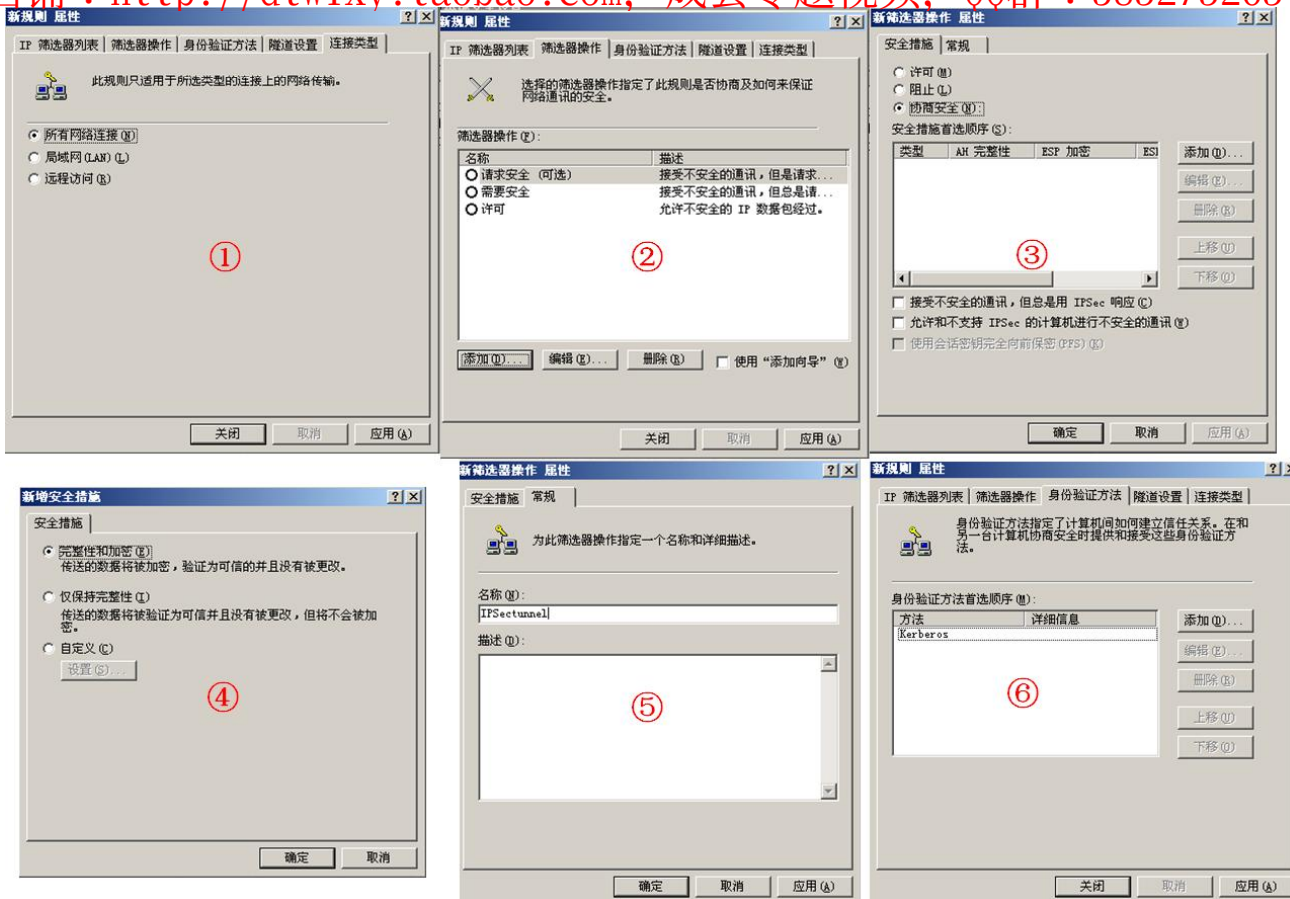


隧道规则

IPSec策略使用IKE主模式的默认设置创建, IPSec隧道由两个规则组成, 指定一个隧道终结点。

- 1) 选择"IP筛选器列表"选项卡。
- 2) 选择"隧道设置"选项卡, 单击"隧道终结点由此IP指定"。
- 3) 选择"连接类型", 选中"所有网络连接"
- 4) 选择"筛选器操作", 清除"使用添加向导", 单击"添加"按钮。弹出"新筛选器的属性"对话框。
- 5) 保持"协商安全", 清除"接受不安全的通信, 但总是用IPSec响应"复选框。
- 6) 添加一选中"安全性和加密" (也可以自定义)
- 7) 选择常规→输入名称。
- 8) 选择"身份验证方法"选项卡, (使用预共享密钥或者证书)



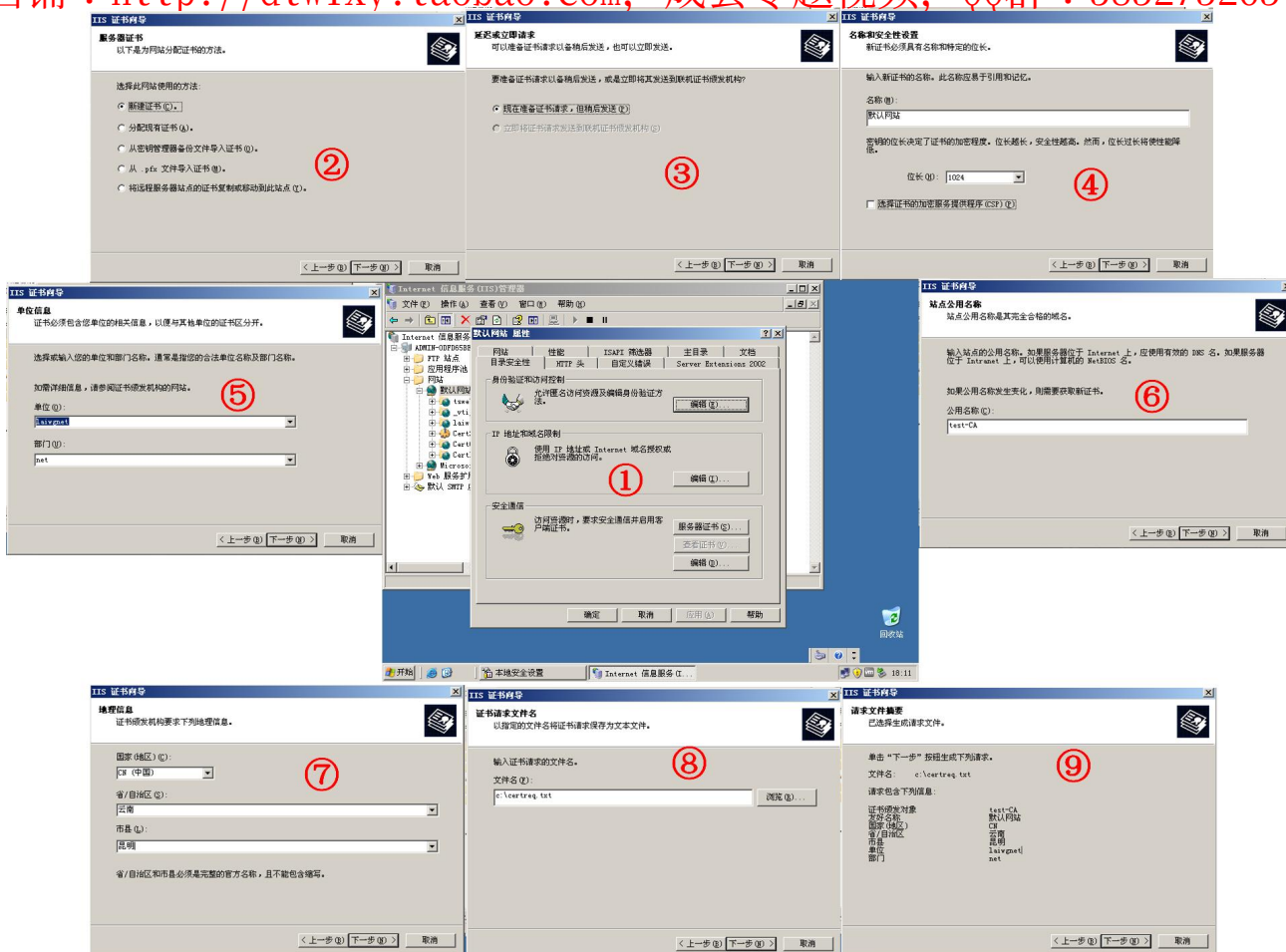


Web数字站点证书

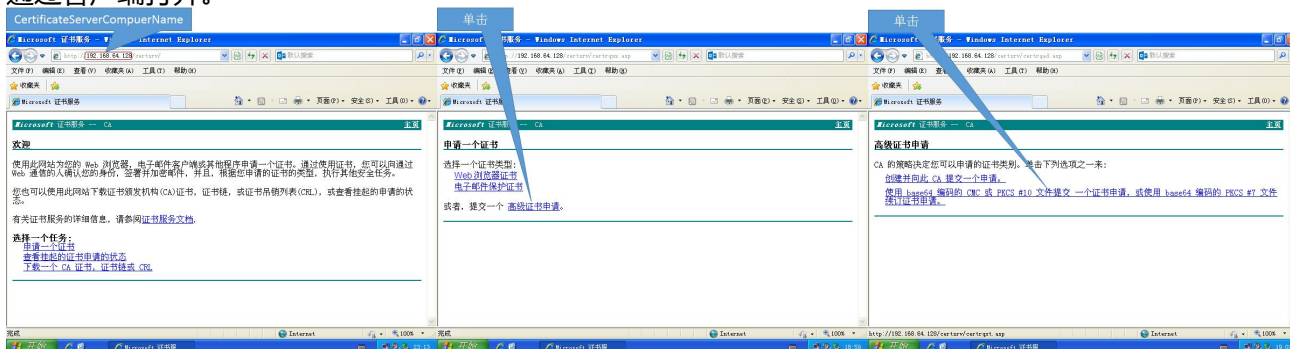
- 1) 申请数字证书
- 2) 下载数字证书
- 3) 安装数字证书

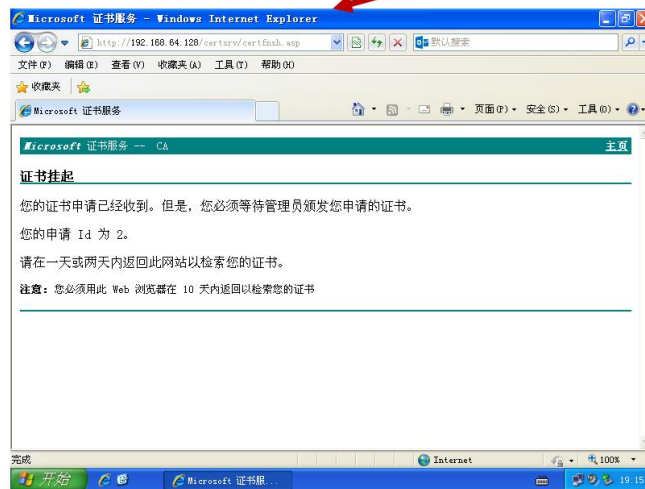
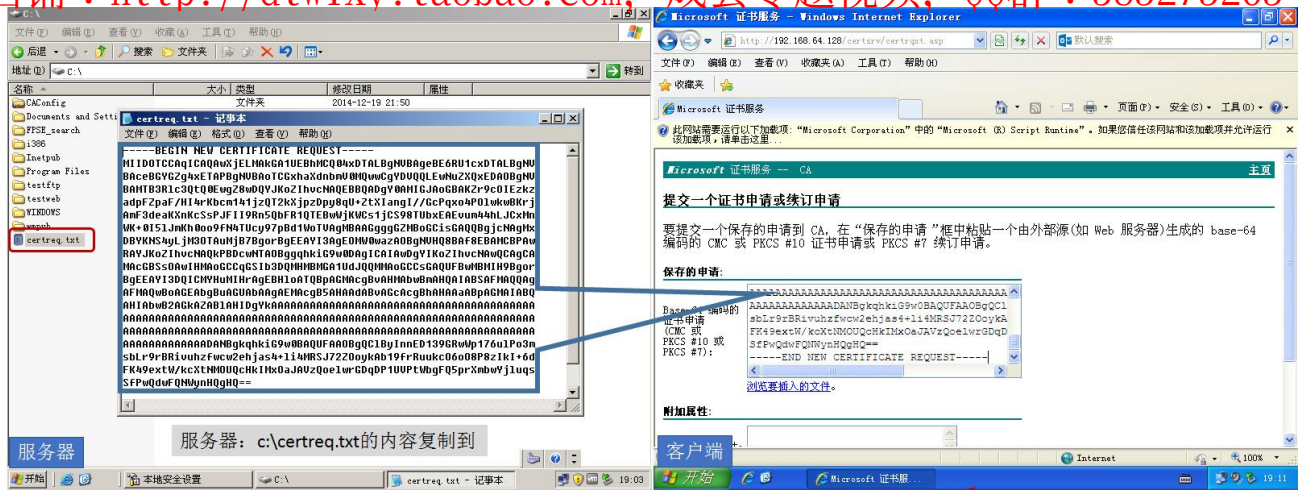
申请数字证书

- 1) 右击要申请的Web站点, 选择"属性"
- 2) 目录安全性→服务器证书
- 3) 下一步→新建证书→下一步
- 4) 延迟或立即请求→选择"现在准备证书请求, 但稍后发送"→下一步
- 5) 为证书设置名称、单位信息、站点公用名称、地理信息和证书请求文件名称。
- 6) 下一步→出现请求文件摘要。
- 7) 单击所有"完成"按钮
- 8) 启动IE输入 (<http://CertificateServerCompuerName/certsrv>) CertificateServerCompuerName是证书服务器名称。
- 9) 单击申请一个证书→高级证书申请→使用base64编码。
- 10) 打开c:\certreq.txt (证书请求文件), 将文件内容复制到"保存的申请"文本框, 单击提交。
- 11) 返回页面提示"证书挂起", 等待证书服务服务器批准后即可下载安装。

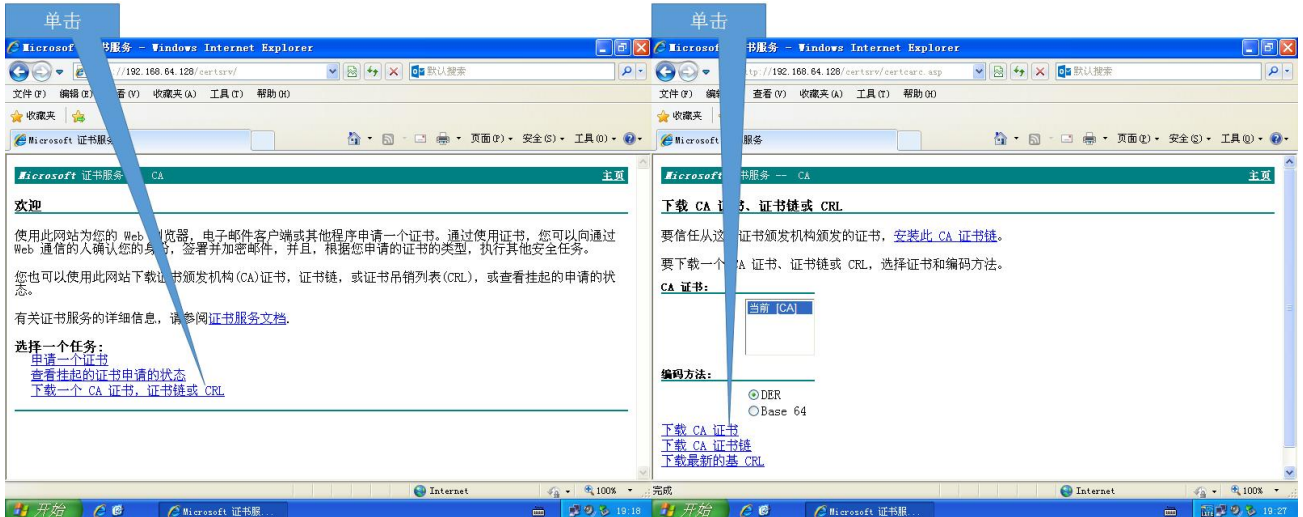


通过客户端打开。



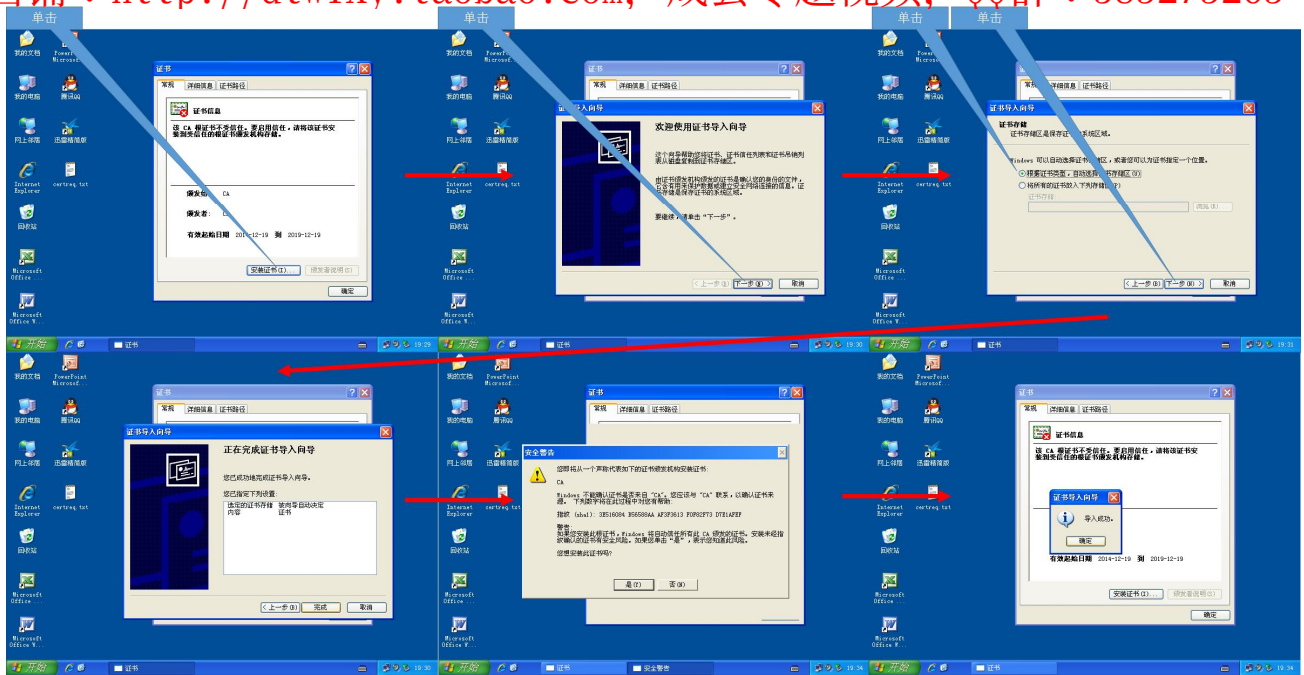


下载数字证书



安装数字证书

- 1) 找到下载的数字证书, 单击“打开”
- 2) 在证书对话框中单击“安装证书”
- 3) 单击“根据证书类型的证书自动选择存储区”
- 4) 单击“确定”确认导入。



第10章 组网技术

笔记本: 网络工程师学习

创建时间: 2015/1/21 11:50

更新时间: 2015/1/21 11:50

URL: about:blank

交换机分类:

1) 通过交换方式划分

存储转发式交换 (Store and Forward), 延时大, 但可以提供差错校验。主流的工作方式。

直通式交换 (Cut-through), 延迟小, 交换快, 没有检错能力。

碎片过滤式 (Fragment Free), 小于64字节就丢弃, 大于等于64就转发, 用于中低档交换机。

2) 根据交换协议层划分

第二层交换, 根据MAC地址交换。

第三层交换, 根据网络层地址 (IP地址) 交换

多层交换, 根据第四层端口号或应用协议进行交换。

3) 根据交换机结构划分

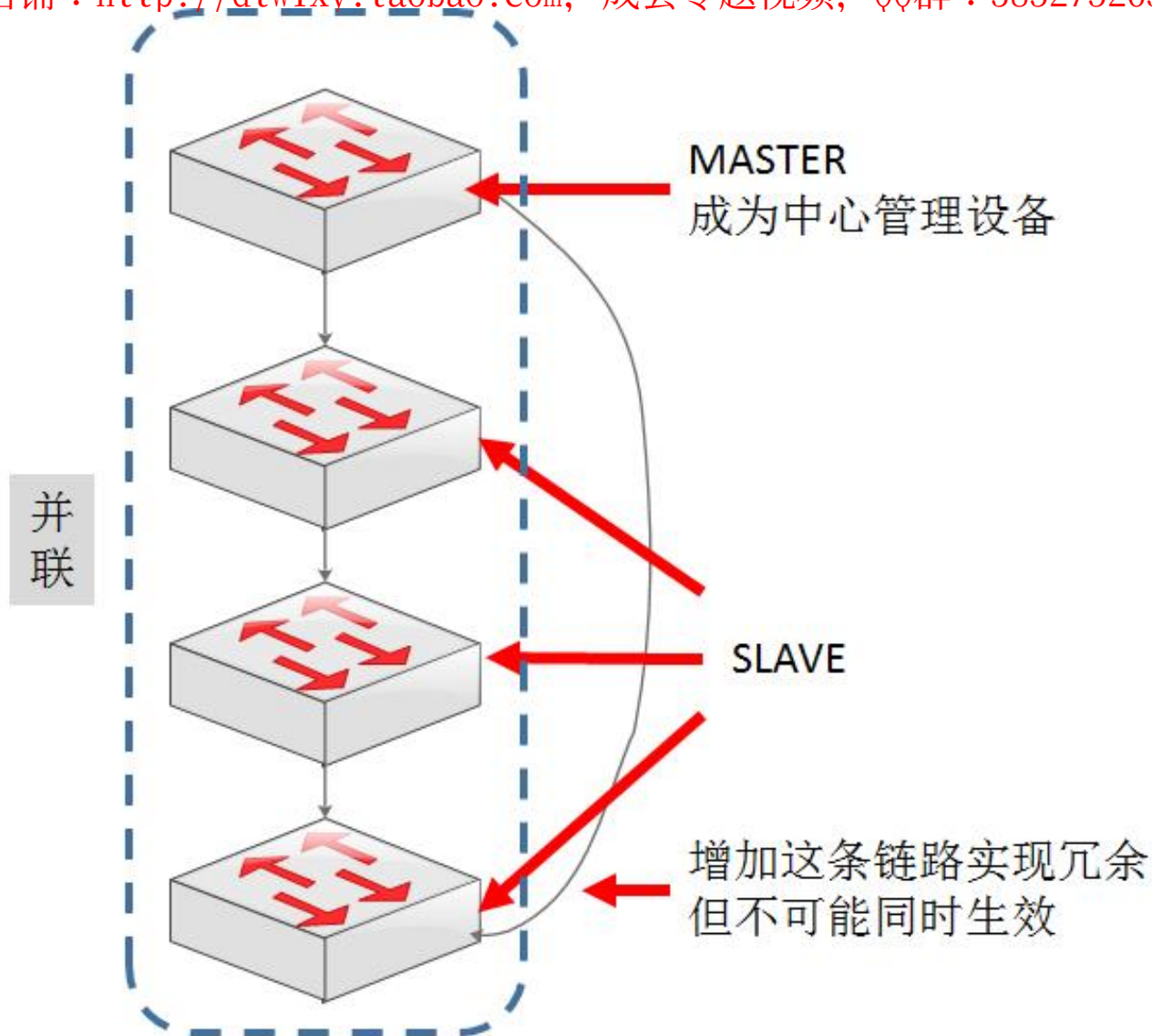
固定端口交换机。

模块化交换机

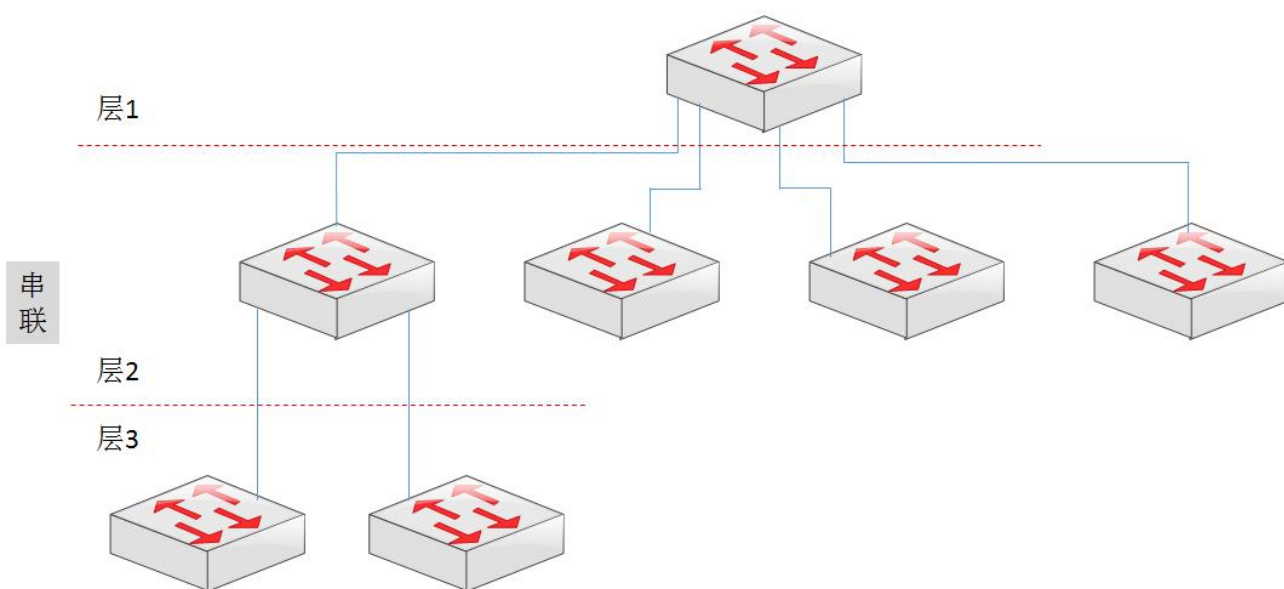
4) 根据配置方式划分

堆叠型交换机。提供堆叠端口, 可堆叠4~9层, 堆叠后的所有交换机可以当作一台交换机来管理。

非堆叠型交换机。通过级连方式进行扩充, 一般不超过4层。



交换机的堆叠



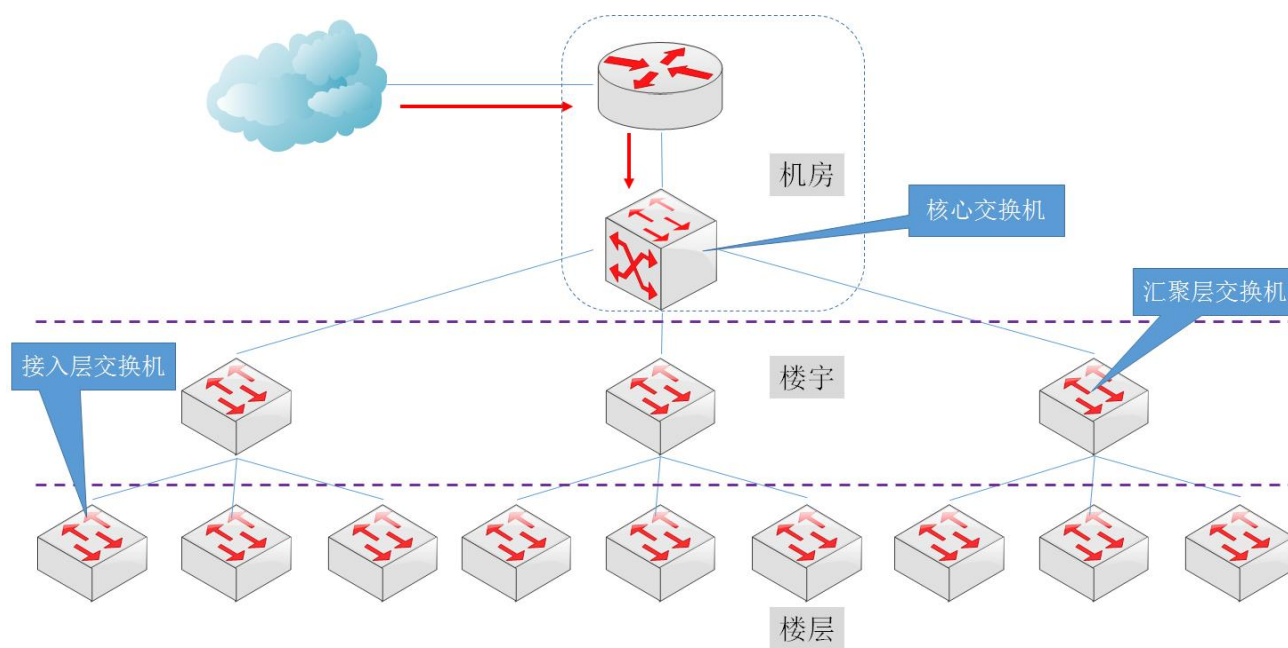
交换机的级连

5) 根据管理类型划分

网管型交换机, 支持简单网络管理协议 (SNMP) 和管理信息库 (MIB)。实现远程配置, 监控, 管理。

非网管型交换机, 不支持SNMP和MIB, 只能根据MAC地址交换。

智能型交换机, 基于WEB图形化管理和MIB-II, 提供QoS管理、VPN、用户认证。



分级网路结构

接入层交换机: 访问控制, 低成本高密度接入 (用户接入)

汇聚层交换机: 分组过滤, 服务质量 (QoS) 和速度限制, (ACL) 访问控制, 组播管理。 (策略控制)

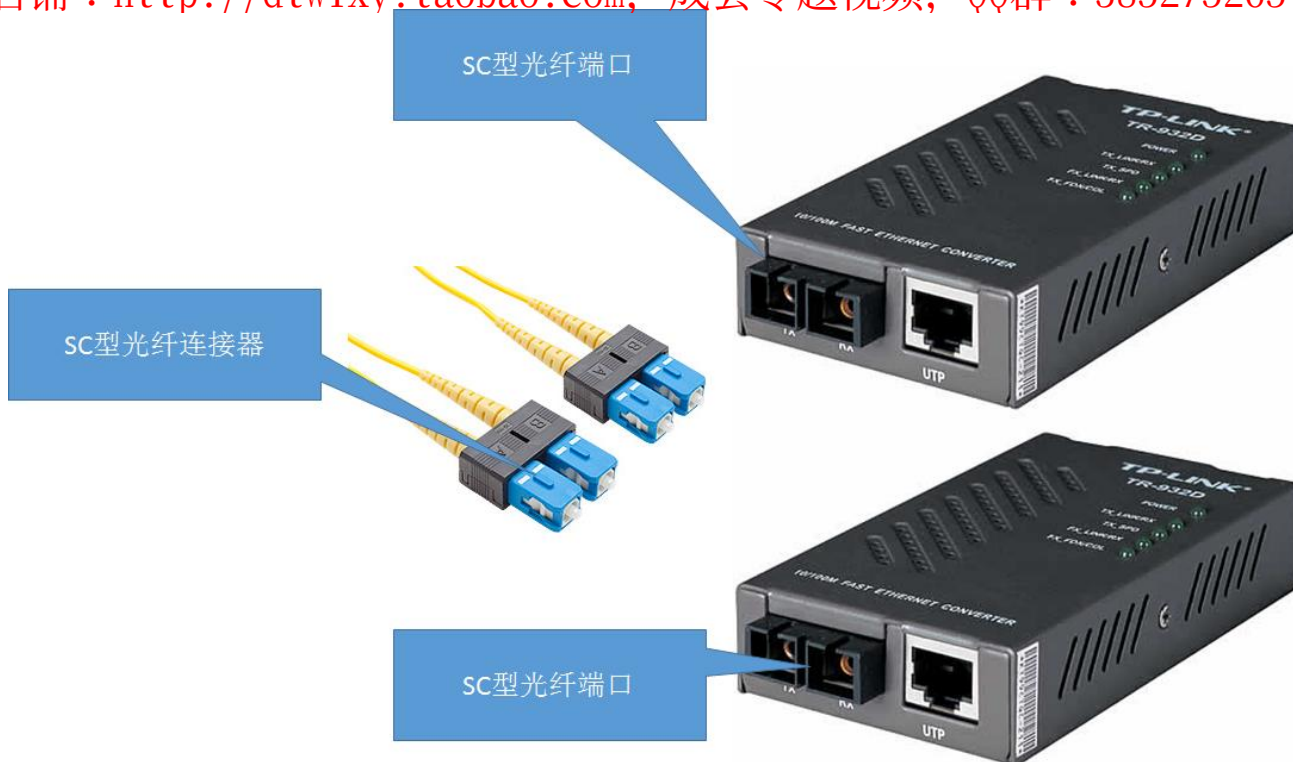
核心层交换机: 高性能交换机, 主干线路, 链路冗余, 路由冗余, VLAN中继和负载均衡。 (高速转发)

交换机的性能参数:

端口类型:

双绞线端口, 百兆端口用于连接工作站, 千兆端口用于级联。

光纤端口: **SC端口**。



GBIC端口：

图1 千兆位接口转换器

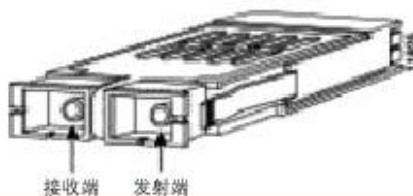


表1列出了现有的GBIC

GBIC	产品编号
短波长 (1000BaseSX)	WS-G5484
长波长/长距离 (1000BaseLX/LH)	WS-G5486
延伸距离 (1000BaseZX)	WS-G5487

SPF端口，小型机架可插拔设备 (Small Form-factor Pluggable , SFP) 是GBIC的升级版本。



包转发率：包转发率也称端口吞吐率，单位pps（package per second）（包/秒）单位时间内发送64字节数据包的个数。

包转发率计算方法：

$$1000\text{Mbps} \div 8\text{b} \div (64 + 8 + 12)\text{byte} = 1488095\text{pps}$$

64字节 8字节帧头 12字节的帧间开销

包转发率 = 千兆端口数 $\times$ 1.488Mpps + 百兆端口数 $\times$ 0.1488Mpps + 其余端口数 $\times$ 相应包转发数

背板带宽。

交换机背板带宽是指交换机端口处理的单位间最大数据量。

总带宽 = 端口数 $\times$ 端口速率 $\times$ 2（全双工模式）

（笔记16，PDF 468页）

交换机支持的以太网协议

标准	简要说明	规范
IEEE802.3i	以太网10M	两对UTP，RJ-45连接器，传输距离100m
IEEE802.3u	快速以太网100	TX，两对5类UTP，支持10,100M自动协商，FX，光纤
IEEE802.3z	以太网物理层规范1000M	SX,短波光纤 LX,长波光纤
IEEE802.3ab	双绞线1000M	TX，4对UTP。
IEEE802.3ad	LACP（链路聚合） 链路捆绑、以太网通道技术 EtherChannel（多个物理链路，形成一个逻辑链路）	链路汇聚技术可以将多个链路绑定在一起，形成高速链路，以达到更高带宽，实现链路备份和负载均衡。
IEEE802.3ae	万兆以太网物理层规范	
IEEE802.af	PoE供电	48V直流供电（通过双绞线）
IEEE802.1d	STP生成树	
IEEE802.1q	VLAN标记	定义以太网MAC帧标记。VLAN ID（12位）优先级（3位）
IEEE802.1p GARP GVRP GMRP	802.1p组播协议	
IEEE802.1s	多生成树	
IEEE802.1x	用户认证（端口认证）	
IEEE802.1w	RSTP快速生成树	

路由器分类

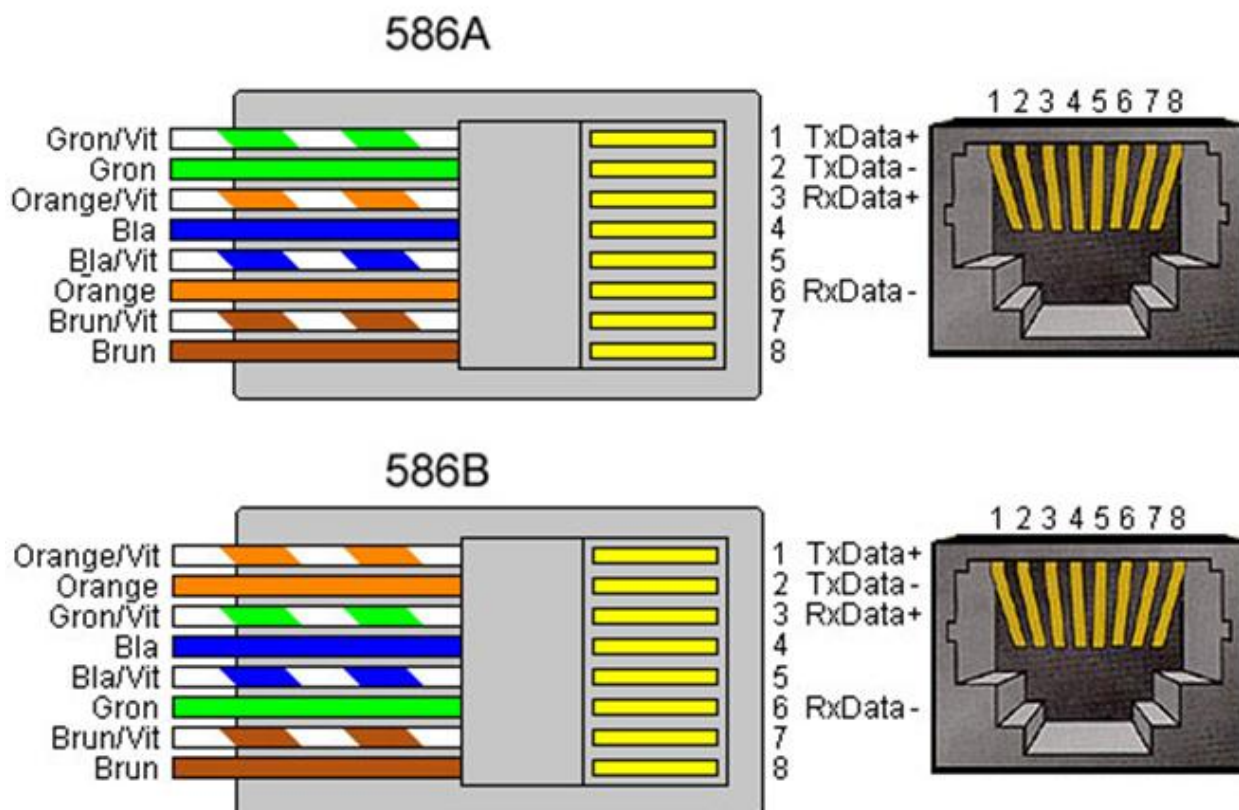
骨干路由器，主干网络互联。

企业级路由器，

接入级路由器，也叫边缘路由器。

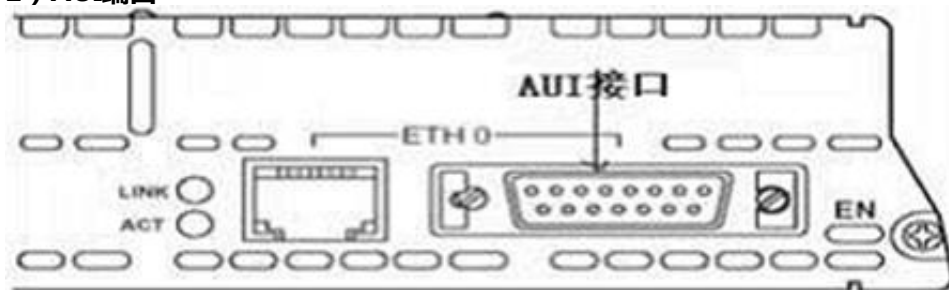
路由器的端口

1) RJ-45端口，这种端口通过**双绞线**连接以太网。

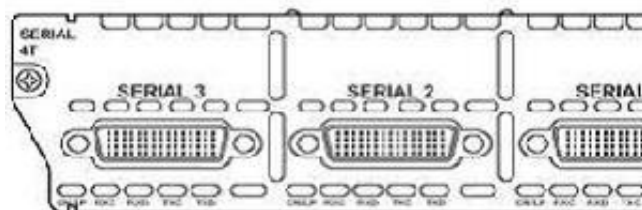


如果标识为ETH为10Base-T，表示为10/100TX为快速以太网自适应。

2) AUI接口



3) 高速同步串口，在路由器与广域网的连接中，应用最多的是高速同步串行口（Synchronous Serial Port），适用于DDN、帧中继、X.25和PSTN等，可高速进行数据传输。



4) ISDN BRI端口

5) 异步串口

6) Console端口

Console端口通过配置专用电缆连接至计算机串行口，利用终端仿真程序（如Windows中的**超级终端**）进行本地配置。



路由器操作系统

路由器有一个操作系统, 英特网操作系统 (Internetwork Operating System , IOS)

操作系统是由**配置文件** (configuration file或config) 控制的。

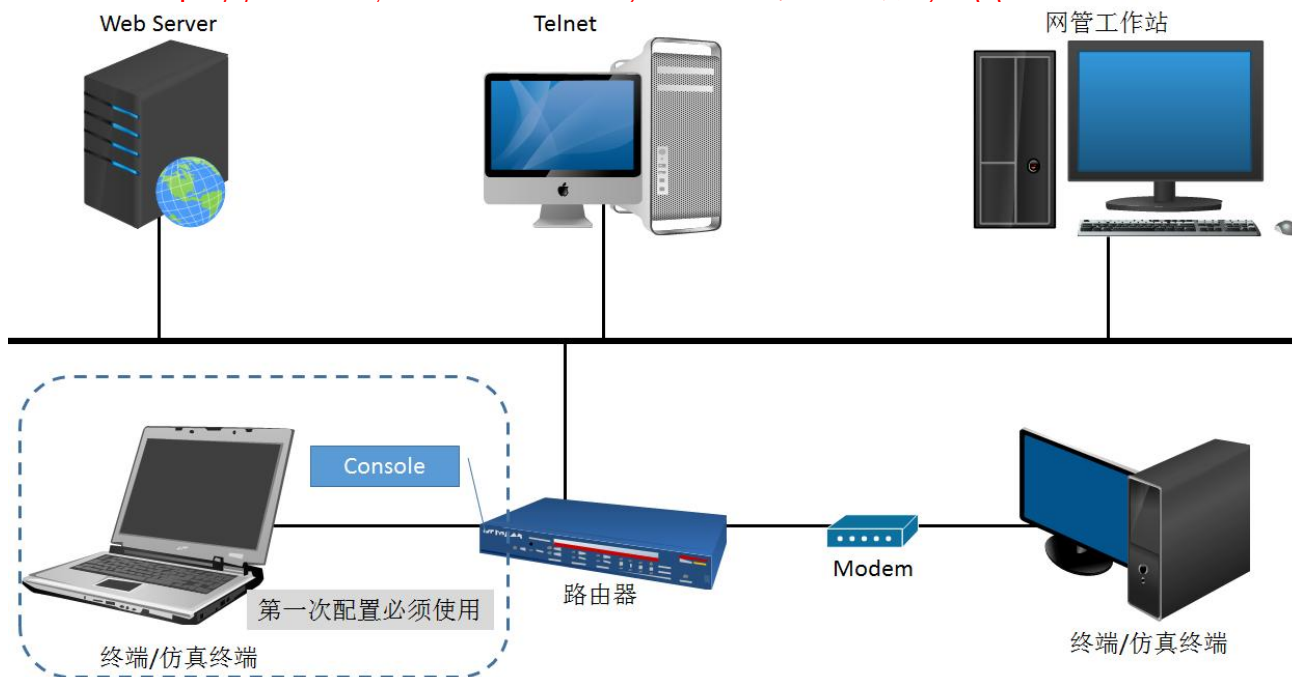
IOS命令通用, 使用命令行界面 (Command Line Interface , CLI)

IOS有3种命令模式, 用户模式 (User mode) , 特权模式 (Privileged mode) 和配置模式 (Configuration mode)

提示符:
用户模式, >
特权模式, #
配置模式, config

访问路由器或交换机

- 1) 通过Console
- 2) 通过AUX端口接Modem
- 3) 通过Telnet程序
- 4) 通过浏览器
- 5) 通过网管软件



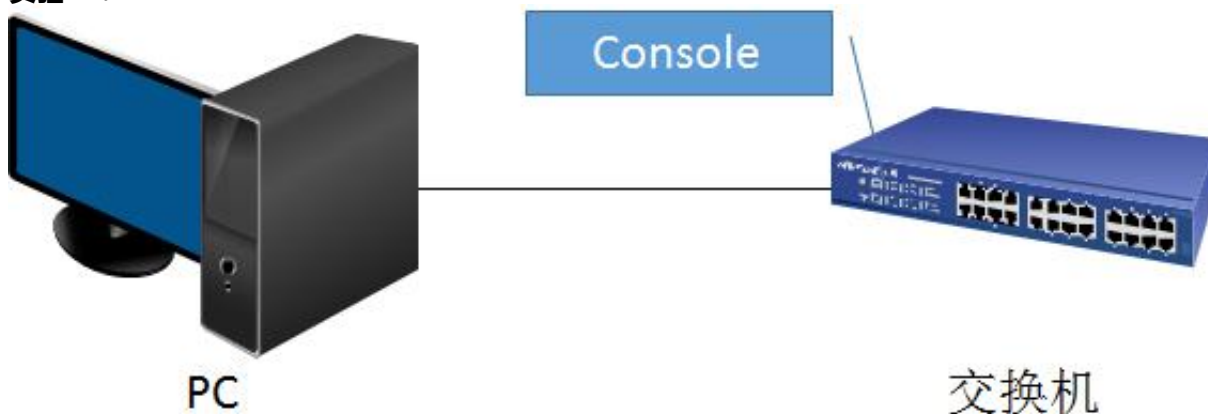
对设备的第一次设置必须通过第一种方法来实现。

连接Console端口的线缆称为控制台点电缆（Console Cable），一端接入网络设备的Console端口（RJ45），一端接入终端或PC的串行接口。

多层交换机，除了使用第二层MAC地址进行交换，还是用第三层网络地址，多层交换机也可以检查第四层信息，包括识别程序类型的TCP头。

交换机基本配置

实验一：



仿真终端与交换机的连接

交换机Console端口的默认参数如下：

端口速率：9600bps

数据位：8

奇偶校验：无

停止位：1

流控：无

8515

Windows超级终端，COM1口配置：



交换机启动：

IOS版本

```
C2950 Boot Loader (C2950-HBOOT-M) Version 12.1(11r)EA1 RELEASE SOFTWARE (fc1)
Compiled Mon 22-Jul-02 18:57 by miwang
Cisco WS-C2950G-24-EI starting... 型号EI增强型，可做镜像端口监控全网流量
Base ethernet MAC Address: 0002.1683.883B (基本MAC地址)
Xmodem file system is available.
Initializing Flash... (初始化Flash)
flashfs[0]: 1 files, 0 directories
flashfs[0]: 0 orphaned files, 0 orphaned directories
flashfs[0]: Total bytes: 64016384
flashfs[0]: Bytes used: 3058048
flashfs[0]: Bytes available: 60958336
flashfs[0]: flashfs fsck took 1 seconds.
...done Initializing Flash.
Boot Sector Filesystem (bs:) installed, fsid: 3
Parameter Block Filesystem (pb:) installed, fsid: 4
Loading "flash:/c2950-i6q4l2-mz.121-22.EA4.bin"...#####
##### [OK] (解压缩IOS文件)
File "flash:/c2950-i6q4l2-mz.121-22.EA4.bin" uncompressed and installed, entry point: 0x80010000
executing... (执行IOS文件)
```

WS - C 2950 G - 24 - EI - DC
交换机 Cisco 型号 吉比特 端口数 增强型 直流电

POST: System Board Test: **Passed** (系统板自检)
POST: Ethernet Controller Test: **Passed** (以太网控制器自检)
POST: FRONT-END LOOPBACK TEST: **Passed** (环路自检)

Model number: WS-C2950-24
System serial number: FOC0718Y0EA

其中, 部件号、序列号、和版本号是验货时非常重要的信息。

实验二:

在默认配置下, 所有端口都处于可用状态, 并且都属于VLAN1, 无须做特殊的配置。

1) 配置enable口令和主机名。配置使能口令 (enable password) 和使能密码 (enable secret), 口令是明文形式存储, 密码是以密文方式存储, 配置一个即可, 同时配置时密码生效。

```
Switch> (用户执行模式提示符)
Switch>en (进入特权模式)
Switch# (特权模式提示符)
Switch#config terminal (进入配置模式)
Switch# (配置模式提示符)
Switch(config)#enable password cisco (设置使能口令, enable password为cisco, 明文形式存储)
Switch(config)#enable secret cisco1 (设置使能密码, enable secret为cisco1, 明文形式存储)
Switch(config)#hostname c2950 (设置主机名为C2950)
c2950(config)#end (返回特权模式)
c2950#
```

2) 配置交换机的IP地址, 默认网关、域名和域名服务器。

```
c2950>enable 进入特权模式
c2950#config terminal 进入配置模式
c2950(config)#interface vlan 1 进入vlan 1 接口配置模式
c2950(config-if)#ip address 192.168.1.1 255.255.255.0 设置交换机IP地址
c2950(config-if)#exit 退出vlan 1接口配置模式
c2950(config)#ip default-gateway 192.168.1.254 设置默认网关
c2950(config)#ip domain-name cisco.com 设置域名
c2950(config)#ip name-server 200.0.0.1 设置域名服务器
c2950(config)#end exit退回一层 end (或ctrl+Z) 直接退回#特权模式
c2950#
```

3) 配置交换机端口属性。主要配置对象有速率、双工和端口描述信息。


```
c2950(config)#interface fastethernet 0/1
c2950(config-if)#speed ?
10 Force 10 Mbps operation
100 Force 100 Mbps operation
auto Enable AUTO speed configuration
```

进入接口0/1的配置模式
 查看speed命令的子命令
 显示结果

```
c2950(config-if)#speed 100
c2950(config-if)#duplex ?
auto Enable AUTO duplex configuration
full Force full duplex operation
half Force half-duplex operation
```

设置该端口速率为100Mbps
 查看duplex命令的子命令
 显示结果

```
c2950(config-if)#duplex full
c2950(config-if)#description TO_PC1
c2950(config-if)#^Z
c2950#show interface fastethernet 0/1
c2950#show interface fastethernet 0/1 switchport
```

设置端口为全双工
 设置该端口描述为TO_PC1
 按ctrl+Z组合，同end
 查看0/1的配置结果，结果略
 查看0/1的状态，结果略

4) 配置和查看MAC地址表。MAC地址表的配置有3个方面：①超时时间（超时时间默认为300s），②永久地址，③限制地址。静态MAC地址是永久存在，不会超时。限制性静态（restricted static）地址是在永久地址基础上同时限制源端口。

c2950(config)#mac-address-table ? 查看mac-address-table的子命令

```
aging-time Aging time do dynamic addresses
permanent Configure a permanent address
restricted Configure a restricted static address
```

显示结果
 模拟器仅支持static命令

c2950(config)#mac-address-table aging-time 100

设置超时时间为100s

c2950(config)#mac-address-table permanent 0000.0c01.bbcc f0/3

加入永久地址，目标，源

c2950(config)#mac-address-table restricted static 0000.0c02.bbcc f0/6 f0/7

目的 目标

加入限制静态地址，MAC和端口绑定

c2950(config)#end

c2950#show mac-address-table

查看整个MAC的地址表

Number of permanent address:1

Number of restricted static address:1

Number of dynamic addresses:0

Address	Dest Interface	Type	Source Interface List
0000.0C01.BBCC	FastEthernet 0/3	Permanent	All
0000.0C02.BBCC	FastEthernet 0/6	Static	F0/7

可以看到永久地址有一个，设置在F0/3端口上，限制性的有一个，设置为F0/6，源端口为F0/7。

c2950#clear mac-address-table restricted static 清除限制性地址

在使用配置命令的时候可以使用**缩写形式**。

例如用户模式（提示符>）下enable命令，en开头就这一个，可以缩写为en。

config Terminal 简写为conf t。

实验三：

VLAN的配置和管理，用于把物理上直接相连的网络从逻辑上划分为多个子网。每一个VLAN对应着一个广播域，处于不同VLAN上的主机不能进行通信，不同VLAN之间的通信要引入第三层交换技术才可以解决。对虚拟局域网的配置管理主要涉及VTP、VLAN、中继和VLAN的配置。

- 1、VLAN中继 (VLAN Trunk) 使得属于不同VLAN的数据帧都可以通过这条中继链路进行传输。
- 2、VLAN中继协议 (即VTP协议) 可以维护VLAN的信息全网一致性。

VTP有3种工作模式:

服务器模式: VLAN信息进行添加、删除、修改等操作。

VLAN信息的增删改、广播

客户模式: 管理员不能进行任何操作, 只接收服务器模式交换机广播的VLAN配置信息, 并应用到本地

接受VLAN

透明模式: 可以对VLAN信息进行增删改, 但不广播, 不接受服务器模式的配置信息到本地。而直接转发。

VLAN信息的增删改、独立、转发。

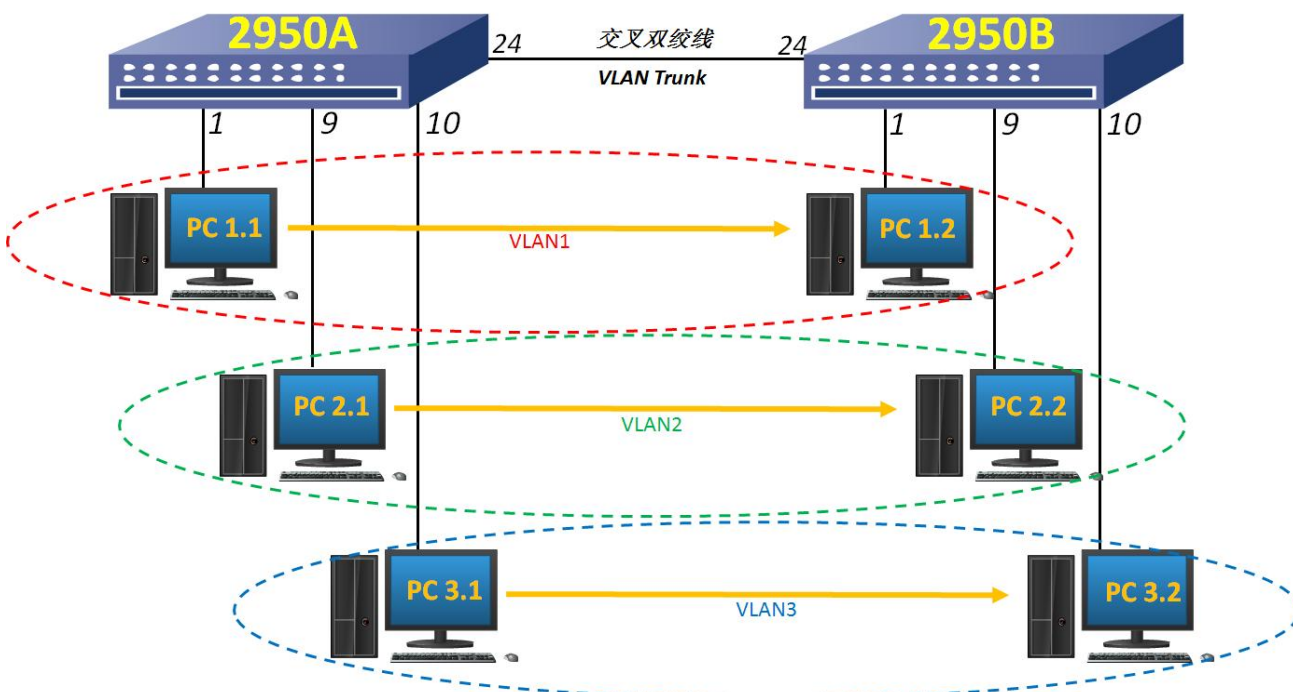
交换机的初始状态是工作在服务器模式, 有一个默认的VLAN (vlan 1), 所有的端口都属于这个VLAN。

划分VLAN的方法, 实现形式有3种: 即静态端口分配、动态虚拟局域网和多虚拟局域网端口配置。

- 1、静态虚拟网的直接设置交换机端口。
- 2、对于支持动态虚拟局域网的端口。通过MAC地址、逻辑地址或协议类型来确定从属。
- 3、多虚拟网端口配置支持。

第一步:

完整网络结构图:



配置2950交换机为服务器模式。


```
Switch>enable      进入特权模式
Switch#config Terminal  进入配置模式
Switch(config)#hostname 2950A  修改主机名
2950A(config)#interface f 0/24  进入f0/24端口配置模式
2950A(config-if)#switchport mode trunk  设置为中继模式
2950A(config-if)#exit
2950A(config)#vtp ?  查看VTP的配合命令
    domain  Set the name of the VTP administrative domain.
    mode    Configure VTP device mode
    password Set the password for the VTP administrative domain
    version Set the adminstrative domain to VTP version
2950A(config)#vtp mode ?
    client   Set the device to client mode.
    server   Set the device to server mode.
    transparent Set the device to transparent mode.
2950A(config)#vtp mode server  设置为Server模式
Device mode already VTP SERVER.
2950A(config)#vtp domain vtpserver  设置域名
Changing VTP domain name from NULL to vtpserver
2950A(config)#vtp password cisco  设置VTP域口令
Setting device VLAN database password to cisco
2950A(config)#vtp pruning  启动修剪功能 模拟器不支持
2950A(config)#exit  退出VLAN配置模式
```

(笔记16 PDF 483页)

完成以上配置后, 查看VTP协议状态:

2950A#show vtp status 查看VTP设置信息
VTP Version : 2
Configuration Revision : 0 配置版本号为0
Maximum VLANs supported locally : 255
Number of existing VLANs : 5 当前交换机所拥有的VLAN个数为5
VTP Operating Mode : Server
VTP Domain Name : vtpserver
VTP Pruning Mode : Enable
VTP V2 Mode : Disabled
VTP Traps Generation : Disabled
MD5 digest : 0xA1 0x13 0xBF 0x5B 0x94 0xF0 0x24 0x91
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Local updater ID is 0.0.0.0 (no valid interface found)
2950A#

配置2950B交换机为客户端模式，则它会从服务器（2950A）那里学习到VTP的其他信息及VLAN信息。

Switch>en 进入特权模式
Switch#conf t 进入配置模式
Switch(config)#hostname 2950B 修改主机名
2950B(config)#interface fastEthernet 0/24 进入f0/24端口配置模式
2950B(config-if)#switchport mode trunk 设置为中继模式
2950B(config-if)#exit
2950B(config)#vtp mode client 设置为客户端模式
Setting device to VTP CLIENT mode.
2950B(config)#vtp password cisco 设置VTP域口令
Setting device VLAN database password to cisco

查看VTP协议状态：


```
2950B#show vtp status 查看VTP设置信息
VTP Version : 2
Configuration Revision : 0 配置版本号为0
Maximum VLANs supported locally: 255
Number of existing VLANs : 5 当前交换机所拥有的VLAN个数为5
VTP Operating Mode : Server
VTP Domain Name : vtpserver
VTP Pruning Mode : Enable
VTP V2 Mode : Disabled
VTP Traps Generation : Disabled
MD5 digest : 0xA1 0x13 0xBF 0x5B 0x94 0xF0 0x24
0x91
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Local updater ID is 0.0.0.0 (no valid interface found)
2950B#
```

```
2950A#conf t
2950A(config)#interface f0/24
2950A(config-if)#switchport trunk allowed vlan all 设置允许从该端口交换数据的VLAN
2950A(config-if)#
2950A#
```

这条命令一般不用设置

将端口加入到某个VLAN中。

```
2950A(config)#vlan 2 建立VLAN 2
2950A(config-vlan)#exit
2950A(config)#vlan 3 建立VLAN 3
2950A(config)#interface f0/9 进入端口9 配置模式
2950A(config-if)#switchport mode access 设置端口为静态VLAN访问模式
2950A(config-if)#switchport access vlan 2 将端口9 分配给vlan2
2950A(config-if)#exit
2950A(config)#interface f0/10 进入端口10 配置模式
2950A(config-if)#switchport mode access 设置端口为静态VLAN访问模式
2950A(config-if)#sw
2950A(config-if)#switchport access vlan 3 将端口10 分配给vlan3
```

配置后的VLAN信息: 2950A#show vlan

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/11, Fa0/12, Fa0/13, Fa0/14 Fa0/15, Fa0/16, Fa0/17, Fa0/18 Fa0/19, Fa0/20, Fa0/21, Fa0/22 Fa0/23
2	VLAN0002	active	Fa0/9
3	VLAN0003	active	Fa0/10
1002	fddi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	

2950B已经学习到vlan划分

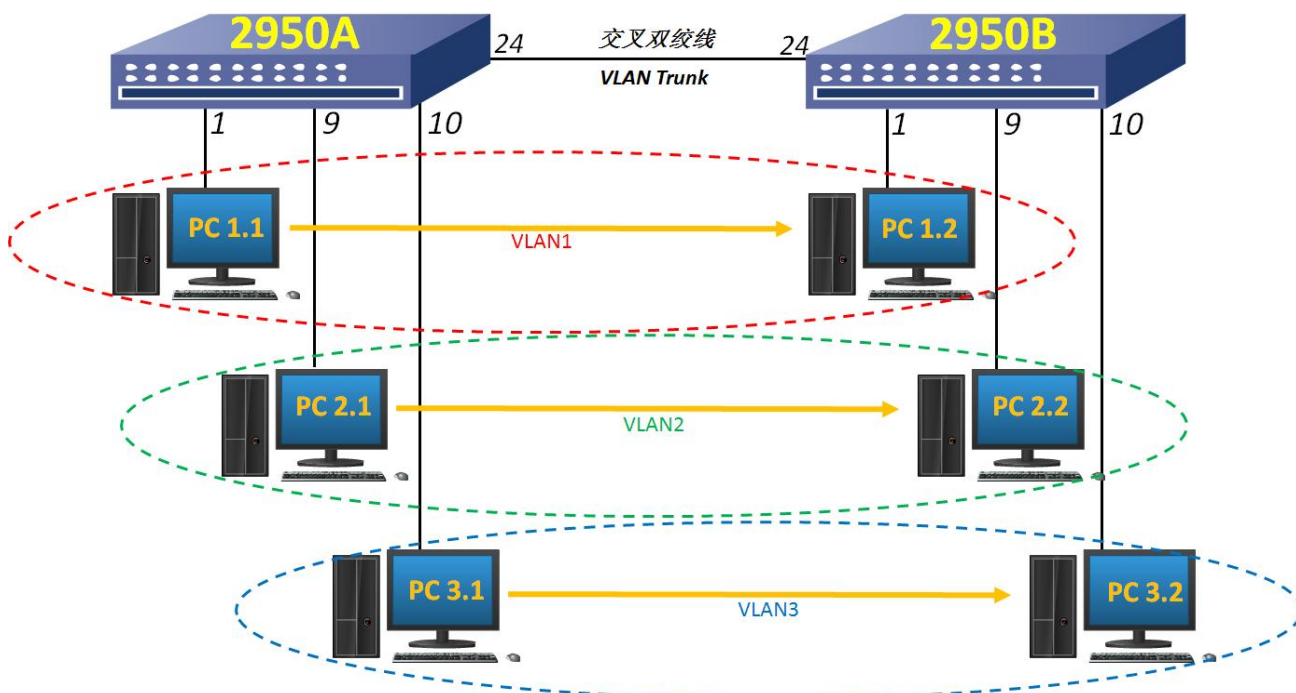
通过命令将f0/9和f0/10划分到已经学习到的vlan 2 和 vlan 3中

```
2950B(config)#interface f0/9
2950B(config-if)#switchport mode access
2950B(config-if)#switchport access vlan 2
2950B(config-if)#exit
2950B(config)#interface f0/10
2950B(config-if)#switchport mode access
2950B(config-if)#switchport access vlan 3
2950B(config-if)#end
2950B#
```

2950B#show vlan

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/11, Fa0/12, Fa0/13, Fa0/14 Fa0/15, Fa0/16, Fa0/17, Fa0/18 Fa0/19, Fa0/20, Fa0/21, Fa0/22 Fa0/23
2	VLAN0002	active	Fa0/9
3	VLAN0003	active	Fa0/10
1002	fddi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	

完整网络结构图：



配置完毕：

PC1.1地址192.168.1.1与PC1.2地址192.168.1.4，同属于vlan1 (default) 可以通信。

```
PC>ping 192.168.1.4

Pinging 192.168.1.4 with 32 bytes of data:

Reply from 192.168.1.4: bytes=32 time=24ms TTL=128
Reply from 192.168.1.4: bytes=32 time=1ms TTL=128
Reply from 192.168.1.4: bytes=32 time=0ms TTL=128
Reply from 192.168.1.4: bytes=32 time=0ms TTL=128

Ping statistics for 192.168.1.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 24ms, Average = 6ms

PC>
```

PC2.1地址192.168.1.2与PC2.2地址192.168.1.5，同属vlan 2 (vlan0002) 可以通信。

```
PC>ping 192.168.1.5

Pinging 192.168.1.5 with 32 bytes of data:

Reply from 192.168.1.5: bytes=32 time=12ms TTL=128
Reply from 192.168.1.5: bytes=32 time=0ms TTL=128
Reply from 192.168.1.5: bytes=32 time=1ms TTL=128
Reply from 192.168.1.5: bytes=32 time=0ms TTL=128

Ping statistics for 192.168.1.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 12ms, Average = 3ms

PC>
```

但PC3.1地址192.168.1.3与PC1.2地址192.168.1.2, 同在一台交换机, 但分别属于vlan3 (vlan0003) 和vlan 2 (vlan0002), 不能通信。

```
PC>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

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

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>
```

实验四: (实际使用较少, 作为了解)

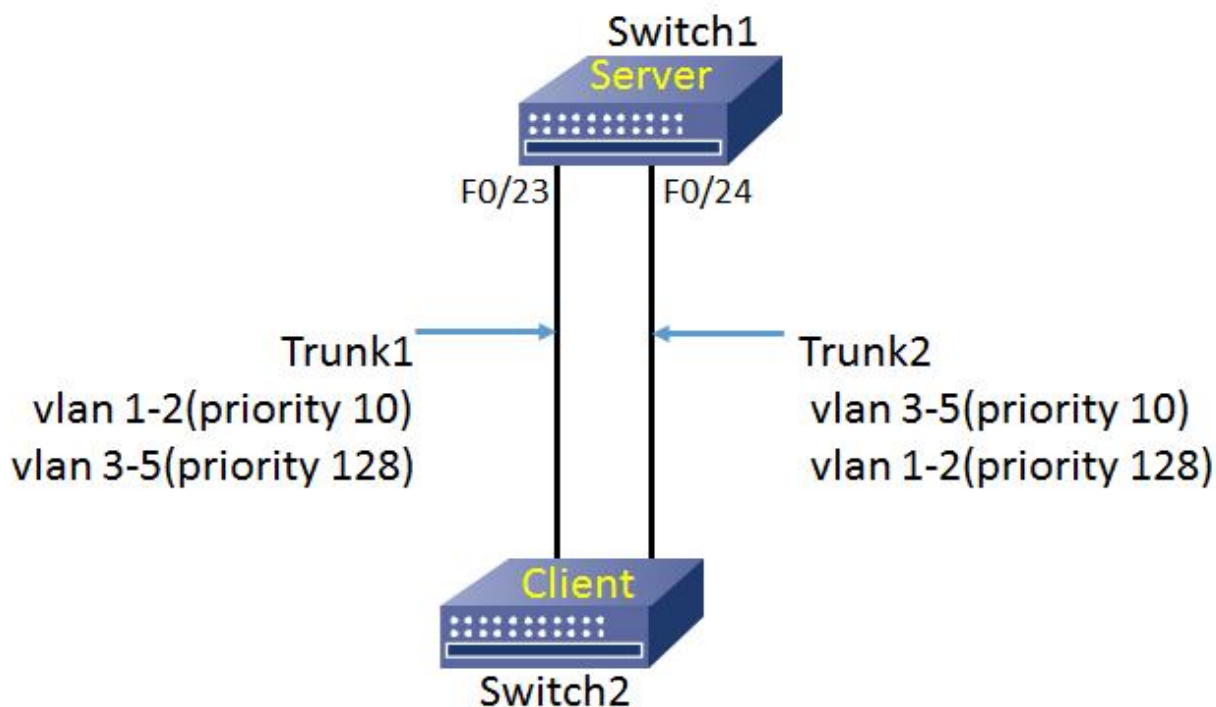
生成树协议, 目的在实现交换机之间的冗余连接的同时避免网络环路的出现, 实现网络的高可用性。

当交换机之间有多个VLAN时Trunk线路负载会过重, 这时需要设置多个Trunk端口, 但这样会形成网络环路, 使用STP协议可以解决这个问题。

使用STP端口权值实现负载均衡

有较高优先级的端口 (数字较小的) VLAN处于转发状态, 假设有5个VLAN, Trunk1将发送和接收vlan 1-2的数据, Trunk2将发送和接收vlan3-5的数据。

(笔记16, PDF 487页)



用端口f0/23做Trunk1，用端口f0/24做Trunk2：

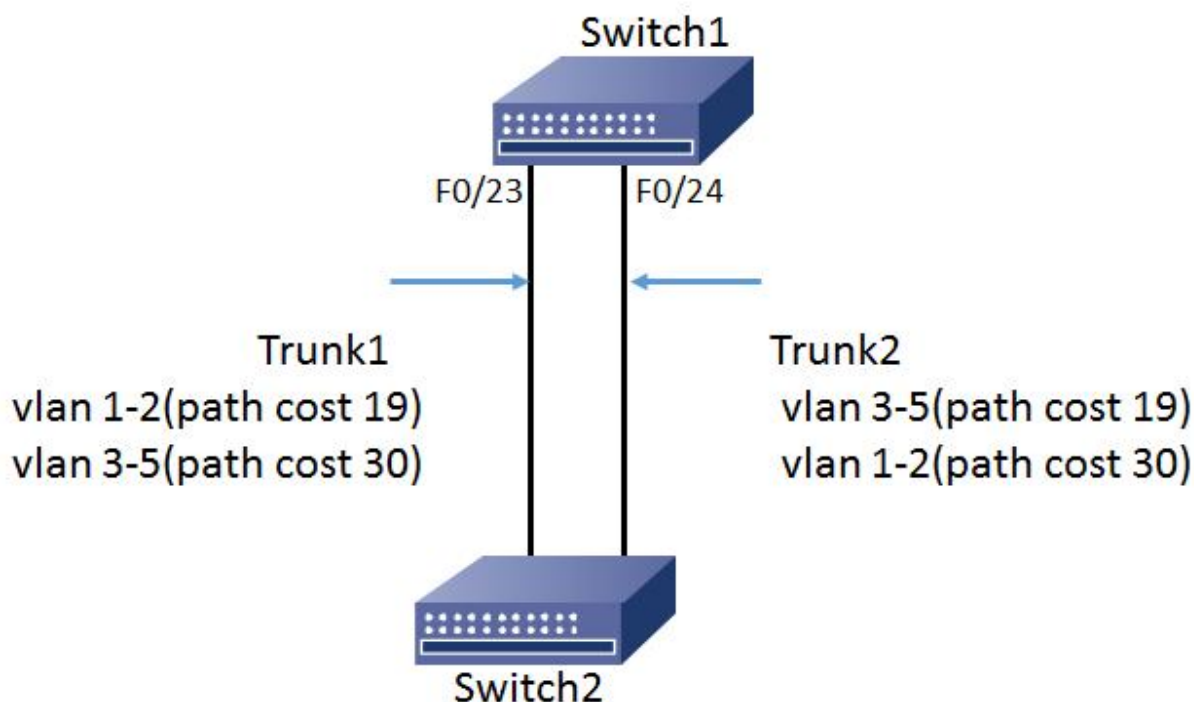
```
Switch#config terminal
Switch(config)#vtp mode server 设置本交换机为Server模式
Device mode already VTP SERVER.
Switch(config)#vtp domain vtpserver 设置域名
Switch(config)#exit
Switch#
Switch#show vtp status
VTP Version          : 2
Configuration Revision : 0
Maximum VLANs supported locally : 255
Number of existing VLANs : 5
VTP Operating Mode    : Server
VTP Domain Name       : vtpserver
VTP Pruning Mode      : Disabled
VTP V2 Mode           : Disabled
VTP Traps Generation  : Disabled
MD5 digest            : 0x83 0xDB 0x02 0xC0 0x52 0x03 0x6B
0x45
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Local updater ID is 0.0.0.0 (no valid interface found)
Switch#config terminal
Switch(config)#hostname Switch1
Switch1(config)#interface f0/23
Switch1(config-if)#switchport mode trunk
Switch1(config-if)#exit
Switch1(config)#interface f0/24
Switch1(config-if)#switchport mode trunk
Switch1(config-if)#end
Switch1#
```

```
Switch1(config)#interface f0/23 进入23口配置模式, (Trunk1)
Switch1(config-if)#spanning-tree vlan 1 port-priority 10 将vlan1的权值设置为10
Switch1(config-if)#spanning-tree vlan 2 port-priority 10
Switch1(config-if)#spanning-tree vlan 3 port-priority 128 将vlan3的权值设置为128
Switch1(config-if)#spanning-tree vlan 4 port-priority 128
Switch1(config-if)#spanning-tree vlan 5 port-priority 128 权值较大的不通过, 较小的通过。
Switch1(config-if)#exit
Switch1(config)#interface f0/24 进入24口配置模式, (Trunk2)
Switch1(config-if)#spanning-tree vlan 1 port-priority 128 将vlan1的权值设置为128
Switch1(config-if)#spanning-tree vlan 2 port-priority 128
Switch1(config-if)#spanning-tree vlan 3 port-priority 10 将vlan3的权值设置为10
Switch1(config-if)#spanning-tree vlan 4 port-priority 10 权值较小的通过, 较大的不通过
Switch1(config-if)#spanning-tree vlan 5 port-priority 10
Switch1(config-if)#end
Switch1#copy runnin-config startup-config 保存配置文件, 可以用wr命令代替。
Destination filename [startup-config]?
Building configuration...
[OK]
```

由于分别设置了不同Trunk上不同vlan的权值, 默认情况下权值为128.

端口: 0-255,	中间值128
网桥: 0-65535	中间值32768

配置STP路径值。




```
Switch1#config terminal
Switch1(config)#interface f0/23
Switch1(config-if)#spanning-tree vlan 1 cost 19
Switch1(config-if)#spanning-tree vlan 2 cost 19
Switch1(config-if)#spanning-tree vlan 3 cost 30
Switch1(config-if)#spanning-tree vlan 4 cost 30
Switch1(config-if)#spanning-tree vlan 5 cost 30
Switch1(config-if)#exit
Switch1(config)#interface f0/24
Switch1(config-if)#spanning-tree vlan 1 cost 30
Switch1(config-if)#spanning-tree vlan 2 cost 30
Switch1(config-if)#spanning-tree vlan 3 cost 19
Switch1(config-if)#spanning-tree vlan 4 cost 19
Switch1(config-if)#spanning-tree vlan 5 cost 19
Switch1(config-if)#end
Switch1#
```

设置vlan 3 生成树路径值为19

模拟器不支持cost。
Cost默认值19.

希望阻断的VLAN生成树路径设大, STP协议会阻断该VLAN从该Trunk上通过, 从而可以把负载均衡到多个Trunk端口上。

路由器

路由器是(典型的网络层设备)用于多个逻辑上分开的网络, 路由器具有判断网络地址和选择路径的功能。

一般来说, 异种网络互联与多个子网互联都采用路由器来完成。

路由器的主要工作就是为经过的每个数据报寻找一条最佳的传输路径, 并将该数据有效地传送到目的站点。

最佳路径选择策略(路由算法), 路由器中保存着路由表(Routing Table)

事先设置号的路由表称为**静态**(static)路由表。

根据网络系统的运行情况而自动调整的称为**动态**(Dynamic)路由表。

路由器的基本配置:

提示符:
用户模式, >
特权模式, #
配置模式, config

配置模式又分为:

- 1.全局配置模式
- 2.接口配置模式
- 3.路由协议配置模式
- 4.线路配置模式

Router>看到连接状态，可以访问其他网络和主机。不能看到和更改路由器的设置内容

Router#特权模式，执行所有用户命令，可以看到更改设置的内容

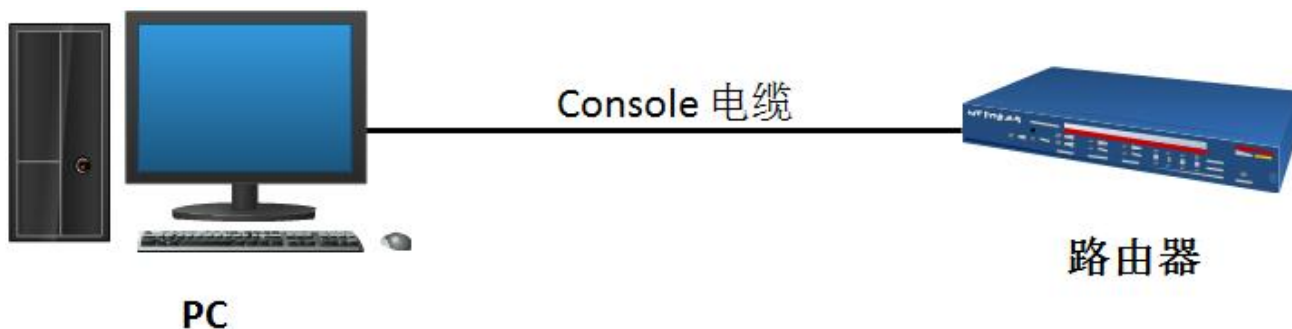
Router(config)#全局配置（配置）模式，设置全局参数

Router(config-if)#，Router(config-line)#，Router(config-router)#处于局部设置状态，设置某个局部参数。

基本配置：

配置enable口令、enable密码和主机名。

```
Router(config)#enable password 123456
Router(config)#enable secret 123456
```



```
Router>enable
```

```
Router#config t
```

```
Router(config)#interface fastEthernet0/1
```

```
Router(config-if)#ip address 192.168.1.11 255.255.255.0
```

设置接口IP地址

```
Router(config-if)#no shutdown
```

激活接口

```
Router(config-if)#
```

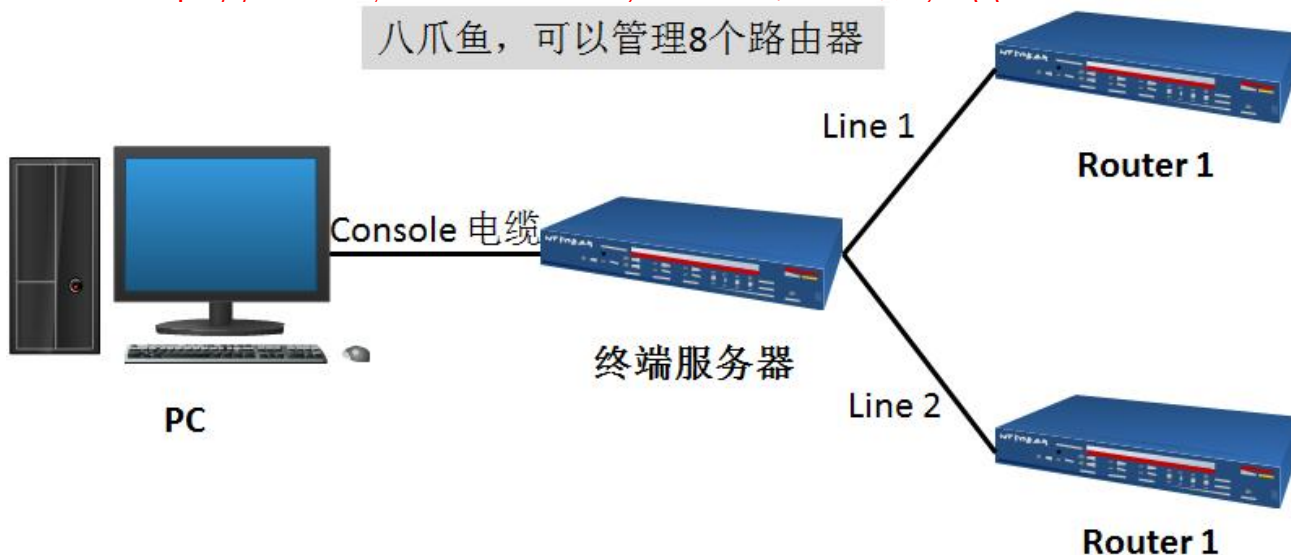
```
Router(config-if)#end
```

```
Router#
```

```
Router#show running-config
```

查看配置结果

（非重点，作为一边了解）配置终端服务器，通过配置终端服务器（Terminal Server）来实现用一台PC同时访问多个网络设备。常称为“八爪鱼”。为了访问其他路由器，可以配置主机表。



终端服务器路由器配置命令:

```
Router#config terminal
Router(config)#hostname Term_Server
Term_Server(config)#enable password 2600
Term_Server(config)#enable secret cisco
Term_Server(config)#ip host router1 2001 10.1.1.1
Term_Server(config)#ip host router2 2002 10.1.1.1
Term_Server(config)#interface loopback 0
Term_Server(config)#ip address 10.1.1.1 255.255.255.255
Term_Server(config)#line con 0
Term_Server(config-line)#no exec-timeout
Term_Server(config)#line vty 0 4
Term_Server(config-line)#password user11
Term_Server(config-line)#end
Term_Server#
```

(笔记16 PDF493页)

```
Term_Server#
Term_Server#router1
Trying router1(10.1.1.1,2001)...Open
Router>enable
Router#config t
Router(config)#hostname router1
Router1(config)#end
Router1#
```

（会话切换命令Ctrl+Shift+6后接x，即先同时按下Ctrl+Shift+6组合键，然后再按下X键）

```
Term_Server#router2
Trying router2(10.1.1.1,2002)...Open
Router>enable
Router#config t
Router(config)#hostname router2
Router2(config)#end
Router2#
```

（会话切换命令Ctrl+Shift+6后接x）

```
Term_Server#show sessions 查看终端服务器会话
```

Conn	Host	Address	Byet	Idle	Conn Name
1	router1	10.1.1.1	0	0	router1
2	router2	10.1.1.1	0	0	router2

```
Term_Server#disconnect 2 断开会话2
```

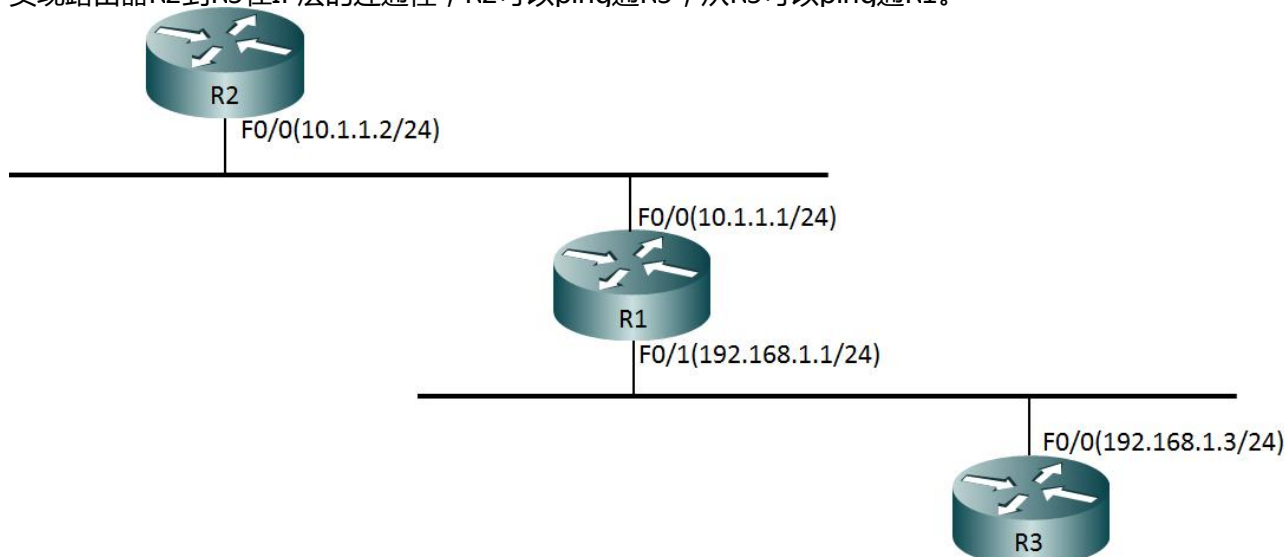
```
Term_Server#show line 1 查看线路1的状态
```

```
Term_Server#clear line 2 清除线路2
```

实验六

IPv4静态路由设置

实现路由器R2到R3在IP层的连通性，R2可以ping通R3，从R3可以ping通R1。



首先根据拓扑结构图配置各个路由器的以太网接口。

首先对R1进行基本的配置：

```
R1>en
R1#config terminal
R1(config)#interface f0/0
R1(config-if)#ip address 10.1.1.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface f0/1
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#no shutdown
```

对R2进行基本的配置：

```
R2>en
R2#config Terminal
R2(config)#interface f0/0
R2(config-if)#ip address 10.1.1.2 255.255.255.0
R2(config-if)#no shutdown
```

对R3进行基本的配置：

```
R3>en
R3#configure terminal
R3(config)#interface f0/0
R3(config-if)#ip address 192.168.1.3 255.255.255.0
R3(config-if)#no shutdown
```

查看一下配置：

R3#show ip route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP

i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area

* - candidate default, U - per-user static route, o - ODR

P - periodic downloaded static route

Gateway of last resort is not set

C 192.168.1.0/24 is directly connected, FastEthernet0/0

直连的, 网段是192.168.1.0、24, 端口是F0/0

Ping的结果:

R1可以ping通R2, R3。

R1#ping 10.1.1.2 R2的f0/0

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.1.1.2, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms

R1#ping 192.168.1.3 R3的f0/0

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.1.3, timeout is 2 seconds:

.!!!!

Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms

R2不能ping通R1的F0/0端口。

R2#ping 192.168.1.1 R1的f0/1

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:

.....

Success rate is 0 percent (0/5)

通过查看R2的路由表

R2#show ip route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP

i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area

* - candidate default, U - per-user static route, o - ODR

P - periodic downloaded static route

Gateway of last resort is not set

10.0.0.0/24 is subnetted, 1 subnets

C 10.1.1.0 is directly connected, FastEthernet0/0

只有直连的路由, 所以ping不通

对R2路由器进行相应的配置: (增加一条静态路由)

R2#config t

R2(config)#ip route 192.168.1.0 255.255.255.0 10.1.1.1

R2(config)#

目的网段

子网掩码

下一跳地址

静态路由表明出发往192.168.1.0网段, 下一跳 (Next Hop) 为10.1.1.1, 即通过R1的f0/0。通过查看R2的路由表:

R2#show ip route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP

i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area

* - candidate default, U - per-user static route, o - ODR

P - periodic downloaded static route

Gateway of last resort is not set

10.0.0.0/24 is subnetted, 1 subnets

C 10.1.1.0 is directly connected, FastEthernet0/0

S 192.168.1.0/24 [1/0] via 10.1.1.1

出现了标记为s的静态路由

添加了静态路由以后, R2再ping R1的F0/1端口的时候:

R2#ping 192.168.1.1 R1的F0/1端口

可以ping通

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms

R2#

继续用R2 ping R3的F0/0端口 (192.168.1.3)

R2#ping 192.168.1.3 R3的F0/0端口

ping不通

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.1.3, timeout is 2 seconds:

.....

Success rate is 0 percent (0/5)

为R3添加一条静态路由

R3#config t

R3(config)#ip route 10.1.1.0 255.255.255.0 192.168.1.1

目的网段

子网掩码

下一跳地址

再用R2 ping R3的F0/0端口 (192.168.1.3)

R2#ping 192.168.1.3 R3的F0/0端口

ping通

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.1.3, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms

在看路由表的时候注意记住！！！！

R2#show ip route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external

type 2

E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP

i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area

* - candidate default, U - per-user static route, o - ODR

P - periodic downloaded static route

Gateway of last resort is not set

10.0.0.0/24 is subnetted, 1 subnets

直连 C 10.1.1.0 is directly connected, FastEthernet0/0 下一跳: 只能是端口

静态路由 S 192.168.1.0/24 [1/0] via 10.1.1.1

下一跳: IP或者是端口

(笔记17 PFD 496页)

IPv6的静态路由和IPv4基本一样。

但需要特别注意以下命令：

R1(config)#ipv6 unicast-routing (开启IPv6单播路由)

R1(config-if)#ipv6 address 2005:CCCC::1/64 (设置E0口的IPv6地址)

R1(config)#interface Serial0/0

R1(config-if)#clock rate 128000 (设置S0端口的时钟频率)

R1(config)#ipv6 route 2004:CCCC::/64 Seral0/0 (设置IPv6静态路由)

目的网络/前缀

下一跳 (端口)

(笔记17 PFD 499页)

配置路由协议：

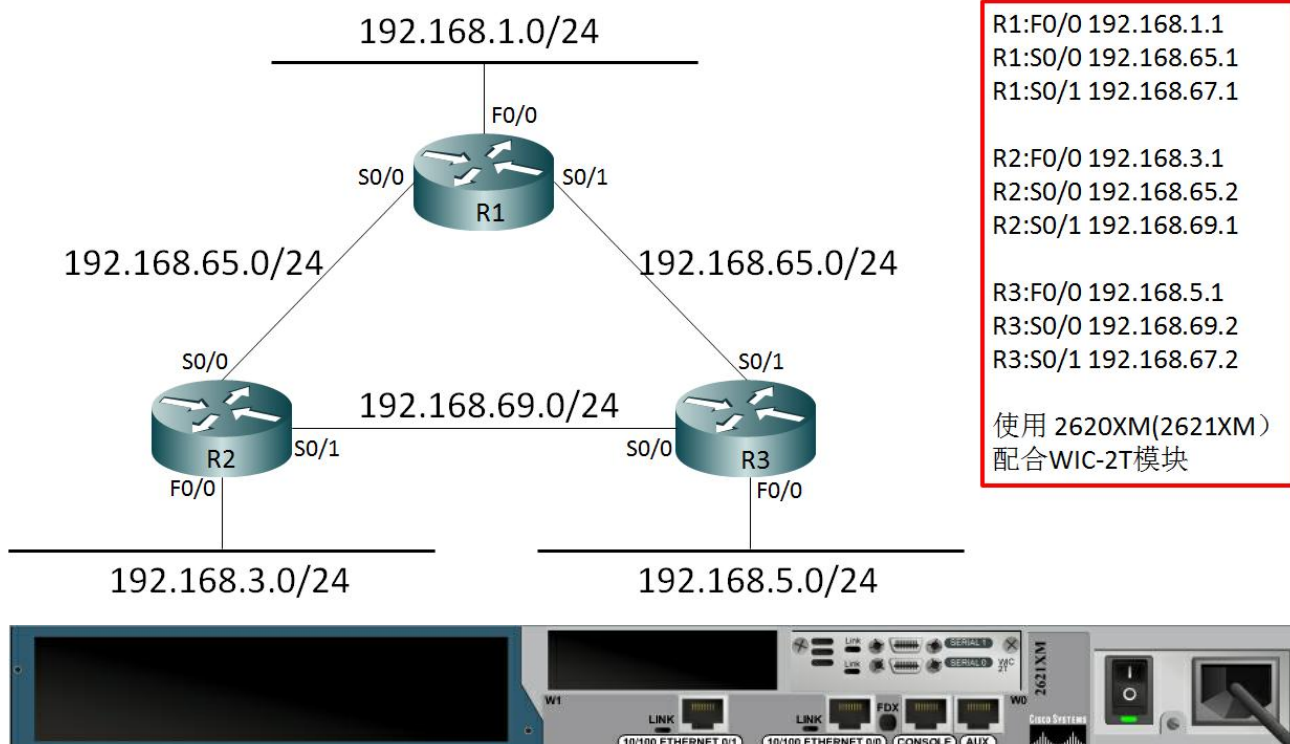
1、距离矢量 (Distance Vector) ，典型的距离矢量路由协议RIP (Routing Information Protocol ，路由选择信息协议) 和IGRP (Interior Gateway Touting Protocol ，内部网关路由协议)

2、链路状态 (Link State) 路由协议，典型路由协议OSPF (Open Shortest Path First ，开放最短路径优先) 路由协议。

3、平衡混合 (Balanced Hybrid) 代表 EIGRP ，即增强型内部网关协议。

RIPv2支持无类域间路由 (Classless Inter-Domain Routing ，CIDR) ，可变长子网掩码 (Variable Length Subnetwork Mask ，VLSM) ，及不连续的子网，组播地址发送路由信息等特性。最大跳数 15 ，RIP每隔30s广播/组播一次路由信息。

RIP协议路由实验：



对R1设备进行基本配置：

```
R1>en
R1#conf t
R1(config)#interface f0/0
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface s0/0
R1(config-if)#ip address 192.168.65.1 255.255.255.0
R1(config-if)#clock rate 128000 时钟频率
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface s0/1
R1(config-if)#ip address 192.168.67.1 255.255.255.0
R1(config-if)#clock rate 128000 时钟频率
R1(config-if)#no shutdown
R1(config-if)#
```

R2的路由表

```
C 192.168.65.0/24 is directly connected, Serial0/0
C 192.168.67.0/24 is directly connected, Serial0/1
```

对R2设备进行基本配置：


```
R2>en
R2 #conf t
R2(config)#interface f0/0
R2(config-if)#ip address 192.168.3.1 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#interface s0/0
R2(config-if)#ip address 192.168.65.2 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#interface s0/1
R2(config-if)#ip address 192.168.69.1 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#
```

R2的路由表

```
C 192.168.65.0/24 is directly connected, Serial0/0
C 192.168.69.0/24 is directly connected, Serial0/1
```

对R3设备进行基本配置：

```
R3>en
R3#conf t
R3(config)#interface f0/0
R3(config-if)#ip address 192.168.5.1 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#interface s0/0
R3(config-if)#ip address 192.168.69.2 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#interface s0/1
R3(config-if)#ip address 192.168.67.2 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#
```

R3的路由表

```
C 192.168.67.0/24 is directly connected, Serial0/1
C 192.168.69.0/24 is directly connected, Serial0/0
```

完成基本配置之后，开启R1设备的RIP路由协议：

```
R1>en
R1#conf t
R1(config)#router rip 进入RIP协议配置子模式
R1(config-router)#version 2 设置为RIPv2
R1(config-router)#network 192.168.1.0 声明网络
R1(config-router)#network 192.168.65.0
R1(config-router)#network 192.168.67.0
```

完成基本配置之后，开启R2设备的RIP路由协议：

```
R2>en
R2#conf t
R2(config)#router rip
R2(config-router)#version 2
R2(config-router)#network 192.168.3.0
R2(config-router)#network 192.168.65.0
R2(config-router)#network 192.168.69.0
```

完成基本配置之后，开启R3设备的RIP路由协议：

```
R3>en
R3#conf t
R3(config)#router rip
R3(config-router)#version 2
R3(config-router)#network 192.168.5.0
R3(config-router)#network 192.168.69.0
R3(config-router)#network 192.168.67.0
```

完成上述配置后，查看R3的路由表。

R3#show ip route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP

i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area

* - candidate default, U - per-user static route, o - ODR

P - periodic downloaded static route

Gateway of last resort is not set

R 192.168.65.0/24 [120/1] via 192.168.69.1, 00:00:19, Serial0/0

[120/1] via 192.168.67.1, 00:00:12, Serial0/1

C 192.168.67.0/24 is directly connected, Serial0/1

C 192.168.69.0/24 is directly connected, Serial0/0

新增了RIP协议的路由, 从R1上去ping R3的两个串口IP已经可以ping通, 并且ping R2路由的也同样可以, 证明RIP路由已经生效。

R1#ping 192.168.67.2

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.67.2, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

R1#ping 192.168.69.2

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.69.2, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/11/46 ms

RIP路由的几个重要标识:

Gateway of last resort is not set

C 192.168.65.0/24 is directly connected, Serial0/0

C 192.168.67.0/24 is directly connected, Serial0/1

R 192.168.69.0/24 [120/1] via 192.168.65.2, 00:00:09, Serial0/0

[120/1] via 192.168.67.2, 00:00:12,

- 1) R: 表示该路由由RIP协议获取
- 2) 192.168.69.0: 表示目标网段。
- 3)、4) [120/1], 120表示RIP协议额管理距离默认为120, 1是该路由的度量值, 即通过1跳可达目标网段。
- 5) via: 经由
- 6) 192.168.65.2, 表示当前路由到达后目标网后的下一跳地址。
- 7) 00:00:24:表示该条路由有条目已产生的时间。
- 8) Serial0/0: 表示路由使用的端口。

内部网关路由协议 (Interior Gateway Routing protocol , IGRP) , 动态距离向量路由, 包括延迟, 带宽、可靠性和负载。不支持VLSM和不连续的子网。(思科公司自己制定的协议, 复杂, 淘汰)

默认情况下,IGRP每90s发送一次路由更新广播。

router igrp autonomous-system (指定使用IGRP协议)

network network

与Rip协议配置不同的是,配置接口是需要配置各个路由链路的**带宽**。

以对DTE提供时钟同步信号,命令clockrate 500000设置S0、S1接口时钟为500kHz,即对应速率500kbps。

用bandwidth命令指明接口带宽为多少来模拟实际网路带宽。

no keepaliv保持激活,实际设备用不到。

clockrate 500000 (配置时钟 bps Hz)

bankwindth 500 (配置带宽 kbps)

router igrp 100 (100为自治系统号,3个路由器的自治系统号必须相同,否则彼此的路由信息将不被互相传递和学习)

network 192.168.1.0 (声明网路)

管理距离: RIP 120 OSPF 90 IGRP 100

R *.*.* [120/1]RIP的管理距离120,1的度量值,1跳可达目标网段。

I *.*.* [100/160250]IGRP协议管理距离100,160250度量值。

配置OSPF协议

开放最短路径优先协议,它是一种链路状态路由选择协议,链路是路由接口的另一种说法,OSPF也称为接口状态路由协议。

(1) 自治系统。OSPF是内部网关路由协议,工作与自治系统内部。

(2) 链路状态,指接口的状态,路如UP,DOWN,IP地址,网络类型、链路开销和它邻接路由的关系,通过链路状态通告(LSA)扩散。

(3) 最短路径优先算法。

(4) 路由器标识

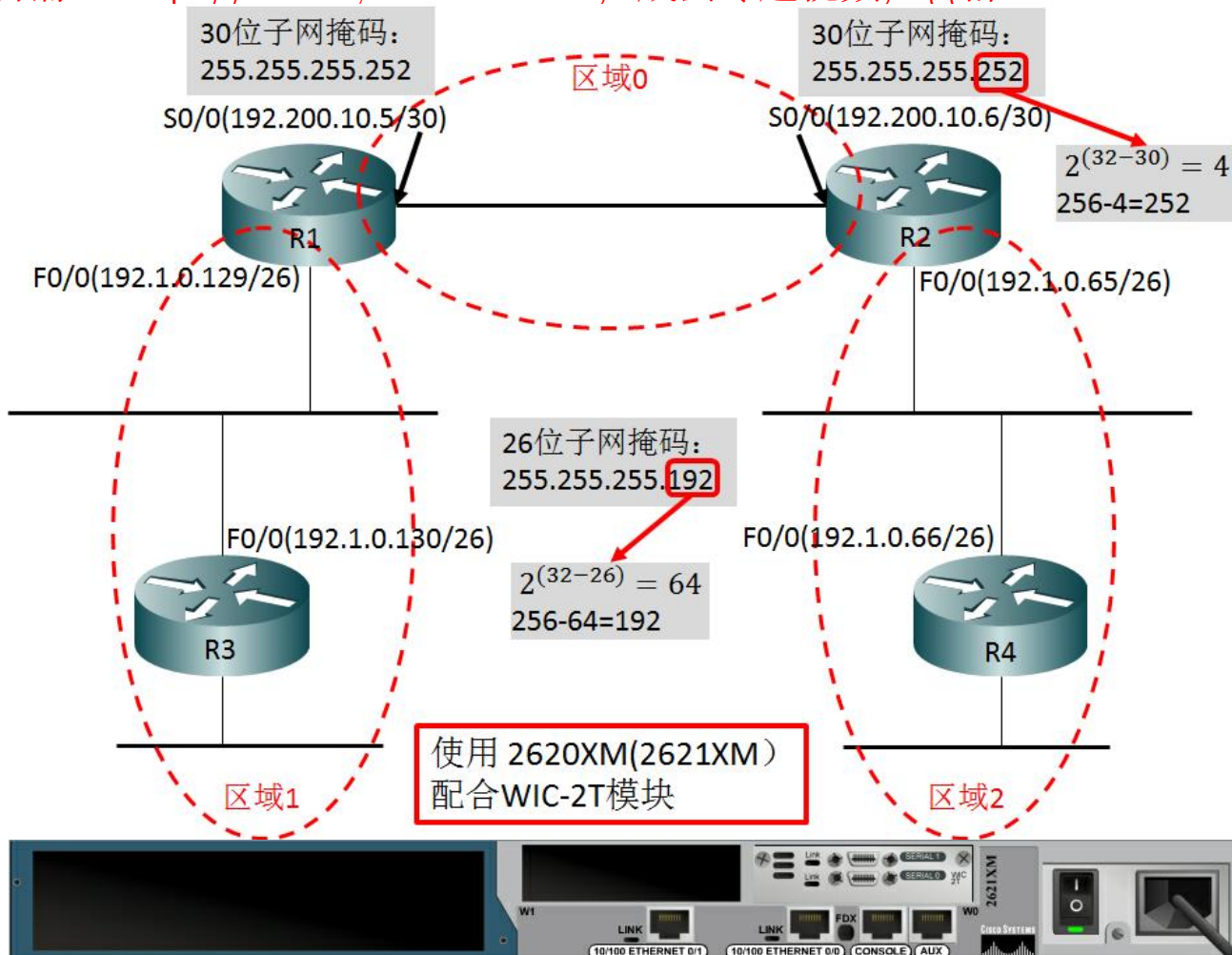
(5) 邻居和邻接,使用Hello包来建立和维护邻居路由关系

(6) 区域,区域0是OSPF网路中必须具有的区域。也叫主干区域,其他所有区域要通过Area0互连。

命 令	功 能
router ospf process-id	指定使用OSPF协议
network address wildcard-mask area area-id	指定与该路由器相连的网络
show ip route	查看路由表信息
show ip route ospf	查看OSPF协议的路由信息

实验八

通过设置完成OSPF协议的使用:



先对路由器R1进行配置：

```
R1#conf t
R1(config)#interface f0/0
R1(config-if)#ip address 192.1.0.129 255.255.255.192
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface s0/0
R1(config-if)#ip address 192.200.10.5 255.255.255.252
R1(config-if)#no shutdown
R1(config-if)#router ospf 100
R1(config-router)#network 192.200.10.4 0.0.0.3 area 0
R1(config-router)#network 192.1.0.128 0.0.0.63 area 1
```

进程号，区分不同OSPF，范围1-65535

反掩码=全掩码-子网掩码

网络号：0~3 4~7 8~11 12~15

而R1与R2的S0/0分别使用了4~7段的5、6，这段4为网络号。

网络号

$2^{(32-30)} = 4$
256-4=252

$2^{(32-26)} = 64$
256-64=192

网络号：0~63 64~127 128~191 192~254
R1与R3的F0/0分别使用了128~191段的129和130，这段的网络号为128

对路由器R2进行配置：

175/241

```
R2#conf t
R2(config)#interface f0/0
R2(config-if)#ip address 192.1.0.65 255.255.255.192
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#interface s0/0
R2(config-if)#ip address 192.200.10.6 255.255.255.252
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#router ospf 200
R2(config-router)#network 192.200.10.4 0.0.0.3 area 0
R2(config-router)#network 192.1.0.64 0.0.0.63 area 2
```

对路由器R3进行配置：

```
R3#conf t
R3(config)#interface f0/0
R3(config-if)#ip address 192.1.0.130 255.255.255.192
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#router ospf 300
R3(config-router)#network 192.1.0.128 0.0.0.63 area 1
```

对路由器R4进行配置：

```
R4#conf t
R4(config)#interface f0/0
R4(config-if)#ip address 192.1.0.66 255.255.255.192
R4(config-if)#no shutdown
R4(config-if)#exit
R4(config)#router ospf 400
R4(config-router)#network 192.1.0.128 0.0.0.63 area 2
```

从R4路由器ping R3的F0/0：

R4#ping 192.1.0.130 R3

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.1.0.130, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/10 ms

配置EIGRP协议

EIGRP是增强型的IGRP协议，是最典型的平衡混合路由选择协议，它融合了距离矢量和链路状态两种路由选择协议的优点。

（不作为重点记忆）

注意，反掩码的计算。

注意的命令：

router eigrp 200

network 192.200.10.0 0.0.0.3

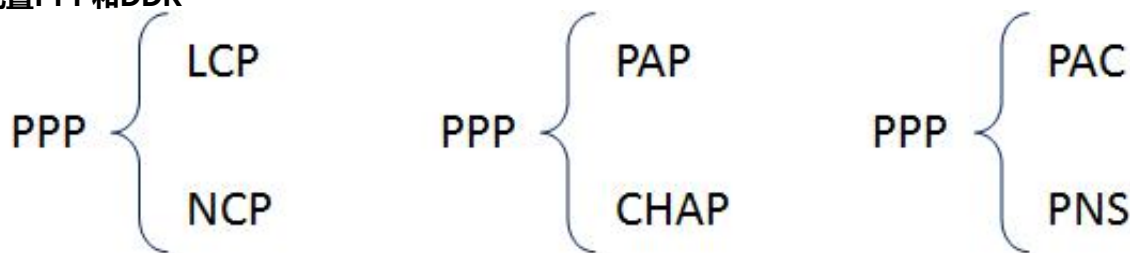
no auto-summary（不进行（取消）子网自动汇总）

配置广域网的接入

综合业务数字网（Integrated Service Digital Network，ISDN）

ISDN属于淘汰技术，做一般了解即可。

配置PPP和DDR



按需拨号路由（Dial on Demand Routing，DDR）

实际中ISDN和PPP与DDR综合使用。

配置帧中继

帧中继是一种高性能的WAN协议，运行在物理层和数据链路层，是数据包交换技术，是X.25的简化版本。省略了窗口技术和数据重发技术，依靠高层协议提供纠错功能，严格对应OSI参考模型的最低两层，而X.25还提供第三层的服务，所以帧中继比X.25具有更高的性能和更有效的传输效率。

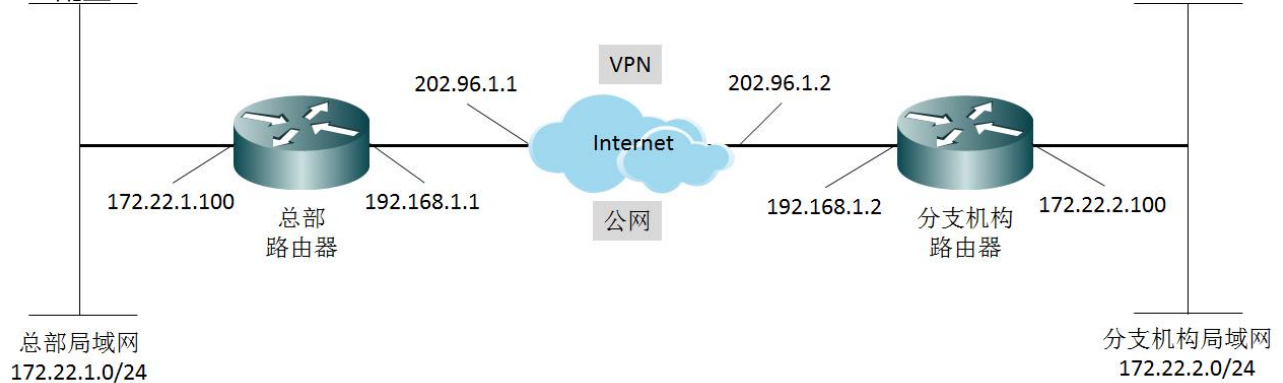
都以数据链路识别码（DLCI）（类似邮政编码或区号）标识自己，帧中继支持PVC（永久交换）也支持SVC（虚电路交换）。

注意的命令：

encapsulation frame-relay FR（封装协议FR）

clockrate 64000 配置时钟, bps Hz 带宽kbps
frame-relay lmi-type cisco (帧中继管理类型cisco)

VPN配置:



	总部	分支机构
路由器串口IP地址 (公网IP)	202.96.1.1	202.96.1.2
隧道端口IP地址	192.168.1.1	192.168.1.2

总部端路由器部分配置:

- 01 crypto isakmp policy 1 (配置IKE策略1)
- 02 authentication pre-share (将IKE策略1的验证方式设为pre-share (预共享密钥))
- 03 group 2 (1024位Diffie-Hellman, 加密算法未设置则取默认值DES) D-H算法。
- 04 crypto isakmp key test123 address 202.96.1.2 (对端公网IP) (设置Pre-share密钥为test123, 此值两端需要一致) ▲
- 05 crypto ipsec transform-set VPNtag ah-md5-hmac esp-des (设置AH散列算法为MD5) (ESP加密算法为DES)
- 06 crypto map VPNdemo 10 ipsec-isakmp (定义crypto map加密图)
- 07 set peer 202.96.1.2 (设置公网对端IP地址)
- 08 set transform-set VPNtag (设置隧道AH及ESP)
- 09 match address 101 (match 匹配)
- 10 interface Tunnel0 (定义隧道接口)
- 11 ip address 192.168.1.1 255.255.255.0 (隧道端口IP地址)
- 12 no ip directed-broadcast (禁止定向广播转发)
- 13 tunnel source 192.168.1.1 (隧道源端地址)
- 14 tunnel destination 192.168.1.2 (隧道目的端地址) ▲
- 15 crypto map VPNdemo (应用VPNdemo于此接口)
- 16 ip route 0.0.0.0 0.0.0.0 202.96.1.2 (默认路由) (目的不明确) ▲
- 17 ip route 172.22.2.0 255.255.0.0 192.168.1.2 (到内网的静态路由, 经过隧道) (目的明确) ▲
- 18 access-list 101 permit gre host 202.96.1.1 host 202.96.1.2 (定义存取列表) (扩展ACL)

三对应

1、转换集名称5、8

2、加密图名称6、15

3、ACL编号9、18

测试时常见的故障:

考试时的回答策略:

原因: 本段和对端的xxx值不同, 或策略不同
解决: 检查双方的配置信息, 使其匹配, 解决故障

rec 'd IPSEC packet from IPADDR has invalid spi

原因: 对端outbound的spi值与本端的inbound不同或配置的策略不同 (esp、ah)。

判断方法和解决方案: 检查双方的配置信息, 尤其在IPSec-manual方式下检查双方的SPI值是否按照方向 (inbound、outbound) 匹配。而在IPSec-isakmp下, 则可能是协商出错。

关键值:

spi policy padding verify packet

(笔记18, 结束)

访问控制列表 (ACL) 根据源地址、目标地址、源端口或目标端口等协议信息对数据包进行过滤, 从而达到访问控制的目的, 在路由器和三层交换机上使用, 后来扩展到二层交换机支持。

ACL对入站 (Inbound, 通过端口流入路由器) 或出站 (Outbound, 通过端口流出路由)

ACL局限性, 是不能对路由器本身发出的通讯进行过滤。

ACL是由编号或名字组合起来的一组语句。

ACL分为标准的和扩展的两种类型, 标准ACL只能根据分组中的IP源地址进行过滤。扩展ACL不仅可以根
据源地址或目标地址进行过滤, 还可以根据不同的上层协议和协议信息进行过滤。

过滤信息	标准ACL	扩展ACL
原地址	✓	✓
目标地址	x	✓
上层协议	x	✓
协议信息	x	✓

路由器自顶向下逐个处理ACL语句。

ACL处理规则的要点

- 1) 一旦发现匹配语句, 就不再处理列表中的其它语句。
- 2) 语句的排序顺序很重要。
- 3) 如果整个列表中没有匹配的语句, 则分组被丢弃。

1、先匹配原则
2、排序原则
3、默认丢弃原则

ACL的默认动作是拒绝 (Implicit Deny)

每一个ACL至少要有一条 “允许” 语句, 否则只有 “拒绝” 语句的ACL将丢弃所有分组。

ACL配置命令

1. Router(config)#**access-list** **ACL** **#****permit|deny** **conditions**

↑ 关键词
↑ 编号
↑ 动作
↑ 条件

定义ACL

ACL类型	ACL编号范围
IP标准	1~99，1300~1999
IP扩展	100~199，2000~2699

2. Router(config)#interface type [module_#]port_# 进入应用接口

3. Router(config-if)#**ip access-group** **ACL** **#****in|out** 应用ACL

↑ 关键词
↑ 编号
↑ 方向

通配符掩码就是子网掩码按位取反的结果。

通配符掩码0.0.0.0表示ACL语句中的32位地址要求全部匹配，因而叫做主机掩码。

例如：

1) 192.168.1.1 0.0.0.0实际上路由器把这个地址转换为 host 192.168.1.1。通配符掩码

255.255.255.255表示任意地址都是匹配的，通常与地址0.0.0.0一起使用。

2) 0.0.0.0 255.255.255.255

表示任意

路由器吧这个地址转换为关键字any

例 1：下面是配置 ACL 的一个例子。

1、定义ACL

2、应用到端口

3、应用到流入

```

Router#conf t
Router(config)# access-list 1 permit 192.168.1.1
Router(config)# access-list 1 deny 192.168.1.2
Router(config)# access-list 1 permit 192.168.1.0 0.0.0.255
Router(config)# access-list 1 deny any
Router(config)# interface serial 0
Router(config-if)# ip access-group 1 in
                    
```

↑ 允许
↑ 禁止
↑ 可以不写，路由默认自动加上

上边的例子在实际应用当中是有问题的，教材后面有相关修改的内容。

扩展的ACL

Router(config)# **access-list** **100-199** **2000-2699** **permit** **deny** **protocol**
 源地址 *source_address source_wildcard_mask* [protocol_information]
 目的地址 *destination_address destination_wildcard_mask* [protocol_information] [log]
 通配符掩码（反掩码）

实例：

特殊关键字，只在TCP协议下使用，建立连接

```
Router#conf t
Router(config)# access-list 100 permit tcp any 172.16.0.0 0.0.255.255 established log
Router(config)# access-list 100 permit udp any host 172.16.1.1 eq dns log
Router(config)# access-list 100 permit tcp 172.17.0.0 0.0.255.255 host 172.16.1.2 eq telnet log
Router(config)# access-list 100 permit icmp any 172.16.0.0 0.0.255.255 echo-reply log
```

回声响应
echo回声请求

表 10-17 用于 TCP 和 UDP 端口号的操作符

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		

表 10-18 常用 TCP 和 UDP 端口号

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

(笔记19 PDF544)

特殊关键字，只在TCP协议下使用，建立连接

```
Router#conf t
Router(config)#access-list 100 permit tcp any 172.16.0.0 0.0.255.255 established log
Router(config)#access-list 100 permit udp any host 172.16.1.1 eq dns log
Router(config)#access-list 100 permit tcp 172.17.0.0 0.0.255.255 host 172.16.1.2 eq telnet log
Router(config)#access-list 100 permit icmp any 172.16.0.0 0.0.255.255 echo-reply log
Router(config)#access-list 100 deny ip any any log

Router(config)#interface ethernet 0
Router(config)#ip access-group 100 in
```

1、定义ACL

2、应用到端口

3、应用到流入

echo-reply log echo回声请求
回声响应

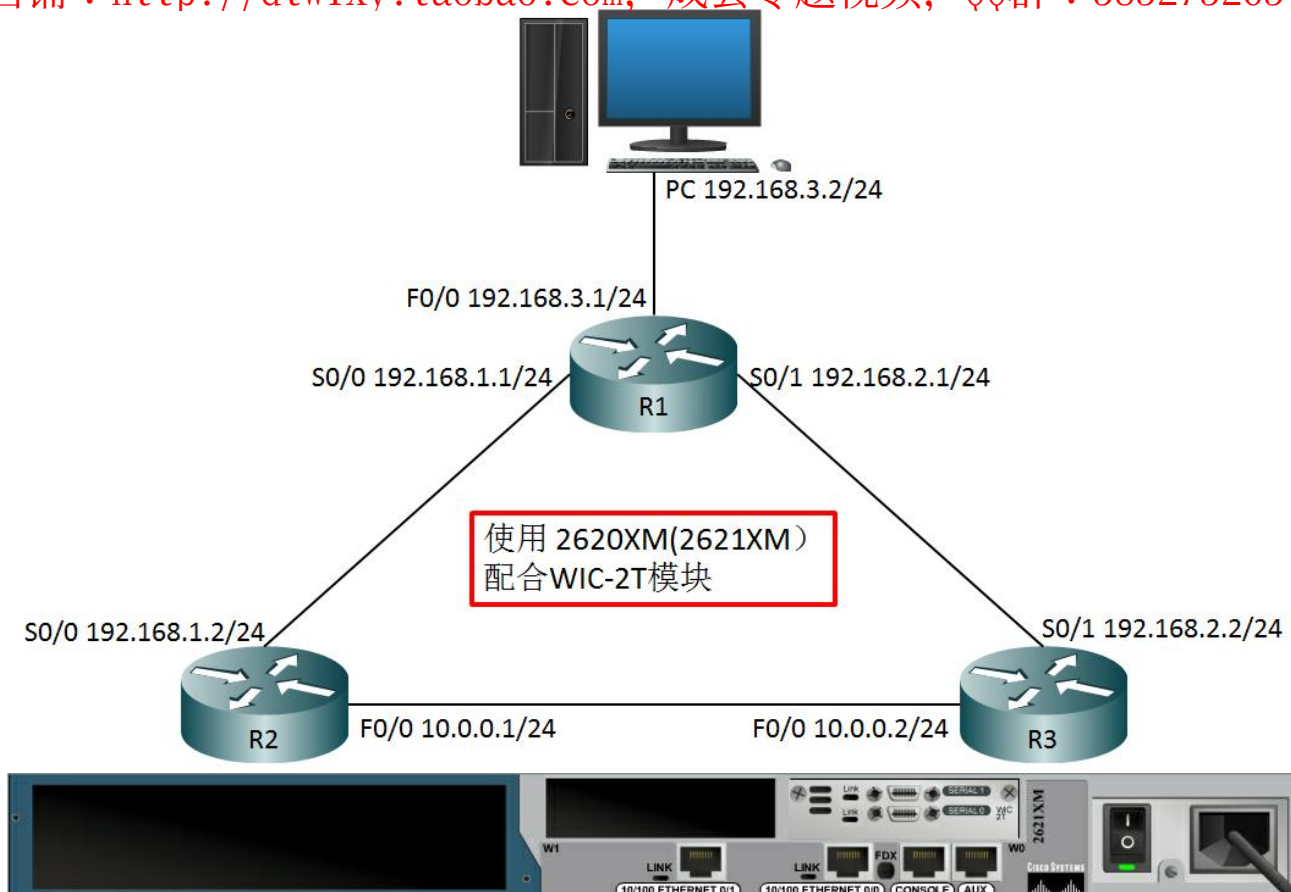
表 10-19 ICMP 报文类型

报 文 类 型	报 文 解 释
administratively-prohibited	分组被过滤，目的网络被禁止访问
echo	回声请求
echo-reply	回声响应
host-unreachable	主机不可到达
net-unreachable	网络不可到达
port-unreachable	端口不可访问
time-exceeded	分组 TTL 超时
timestamp-request	时间戳请求
timestamp-reply	时间戳响应
traceroute	Traceroute 协议 (RFC 1393)
mask-request	子网掩码请求
mask-reply	子网掩码响应
parameter-problem	分组参数出错
redirect	路由重定向
source-quench	源抑制

配置命名ACL的命令

Router(config)#ip access-list standard|extended *ACL_name*

ACL综合配置网络实验拓扑结构



1) 完成对R1的基本设置:

```
R1>en
R1#conf t
R1(config)#interface f0/0
R1(config-if)#ip address 192.168.3.2 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface s0/0
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface s0/1
R1(config-if)#ip address 192.168.2.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#
```

根据拓扑图分别对R2和R3及PC进行基本配置:

对PC进行设置的时候, 需要将网关地址设置为: 192.168.3.1

2) 配置RIP, 通过router rip命令, 配置并发布网络:

```
R1(config-if)#exit
R1(config)#router rip
R1(config-router)#network 192.168.1.0
R1(config-router)#network 192.168.2.0
```

R2要发布的网络, 192.168.1.0和10.0.0.0

R3要发布的网络, 192.168.2.0和10.0.0.0

分别设置完成后: PC可以ping通拓扑上所有端口的IP地址:

```
PC>ping 10.0.0.1
Pinging 10.0.0.1 with 32 bytes of data:
Reply from 10.0.0.1: bytes=32 time=3ms TTL=254
```

```
PC>ping 10.0.0.2
Pinging 10.0.0.2 with 32 bytes of data:
Reply from 10.0.0.2: bytes=32 time=3ms TTL=254
```

```
PC>ping 192.168.1.1
Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=1ms TTL=255
```

```
PC>ping 192.168.1.2
Pinging 192.168.1.2 with 32 bytes of data:
Reply from 192.168.1.2: bytes=32 time=2ms TTL=254
```

```
PC>ping 192.168.2.1
Pinging 192.168.2.1 with 32 bytes of data:
Reply from 192.168.2.1: bytes=32 time=0ms TTL=255
```

```
PC>ping 192.168.2.2
Pinging 192.168.2.2 with 32 bytes of data:
Reply from 192.168.2.2: bytes=32 time=1ms TTL=254
```

3) 配置ACL (通过设置ACL让PC无法ping通10.0.0.1)


```
R1(config)#access-list 50 deny 10.0.0.0 0.0.0.255
R1(config)#access-list 50 permit any
R1(config)#interface f0/0
R1(config-if)#ip access-group 50 out
```

4) 验证:

通过ACL的配置, 已经无法ping通10.0.0.1

```
PC>ping 10.0.0.1
```

Pinging 10.0.0.1 with 32 bytes of data:

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

Ping statistics for 10.0.0.1:

Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

如果需要取消这条ACL通过命令:

```
R1(config)#no access-list 50
```

PC再ping 10.0.0.1的时候, 又可以ping通了。

教材上有设置R2和R3为web服务器的命令, 但模拟器不支持:

```
R2(config)#ip http server
```

```
R3(config)#ip http server
```

包括下面几条命令:

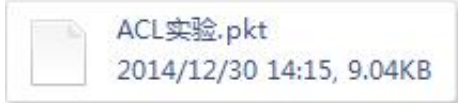
```
R1(config)#access-list 101 deny tcp 192.168.3.0 0.0.0.255 eq www
```

```
R1(config)#access-list 101 deny tcp 192.168.3.0 0.0.0.255 any eq ftp
```

```
R1(config)#access-list 101 permit ip any any
```

```
R1(config)#interface fastethernet 0/0
```

```
R1(config-if)#ip access-group 101 in (以后注意in和out的使用)
```



扩展的基于协议的, 所以多出ip和any

标准的基于源地址, 所以直接跟any

R1(config)#access-list 101 permit ip any any

扩展到ACL基于协议permit后面跟IP和多一个any

R1(config)#access-list 50 permit any

标准到ACL基于源地址permit直接跟any

IPv6的配置与部署

IPv4过渡到IPv6的技术实现方式: 双栈、隧道、翻译。(重点了解, 概念及优缺点)

1) 双栈: 同时具有IPv4和IPv6两个协议栈(4对4, 6对6)。优点, 易于理解, 网络规划相对简单, 同时在IPv6逻辑网络中可以充分发挥IPv6的协议的优点。缺点, 维护大量的协议和数据。网络升级改造将牵涉到网络中所有网元设备, 投资大, 建设周期长。

2) 隧道策略: 经常使用的机制, 隧道技术的工作机理就是在IPv6网路与IPv4网络间的隧道入口处, 路由器将IPv6的数据分组封装如IPv4中, 6to4隧道, 隧道技术充分利用了现有的网络投资, 因此过渡初期是用一种方便的选择。但是增加了隧道出入口的实现复杂度, 不利于大规模的应用。



3) 翻译技术: (迫不得已使用) IPv4与IPv6协议层翻译, 应用层翻译, 前者通过NAT-PT实现, 后者通过应用代理网关ALG来实现。缺点: IPv4节点访问IPv6的实现方法比较复杂, 玩过设备进行协议转换, 地址转换的处理开销较大, 该次略一般在其他方法无法使用情况下使用。

隧道>双栈>翻译。

在隧道的入口处, 将IPv6的数据封装到IPv4, IPv4报文的源地址和目的地址分别隧道如何和隧道出口的IPv4地址, 但是隧道技术不能实现IPv4主机与IPv6主机的直接通信。使用标准GRE技术, GRE隧道吧IPv6作为乘客协议, 将GRE作为承载协议。

s(源), d(目的)

隧道技术重要命令:

Router(config-if)#tunnel mode gre ipv6 (tunnel模式为IPv6的GRE隧道)

Router(config-if)#interface tunnel 0

Router(config-if)#ipv6 rip test enable (在路由器tunnel 0上启用RIP协议, 别名为test)

Router(config-if)#interface f0/0

Router(config-if)#ipv6 rip test enable (在F0/0上启用RIP协议, 别名为test)

IPv6的RIP协议有一个别名。

ISATAP隧道配置(属于双栈技术)

站内自动隧道寻址协议(Intra-Site Automatic Tunnel Addressing Protocol, ISATAP)过渡技术采用而来双栈和隧道技术实现了从IPv4向IPv6的过渡。

ISATAP地址: Prefix(64bit):0:5EFE:IPv4ADDR, 开头是前缀, 其中, 0:5EFE是ISATAP的规定格式, IPv4ADD是单播IPv4地址, 全球单播地址前缀(2001::, 2002::, 3ffe::开头)

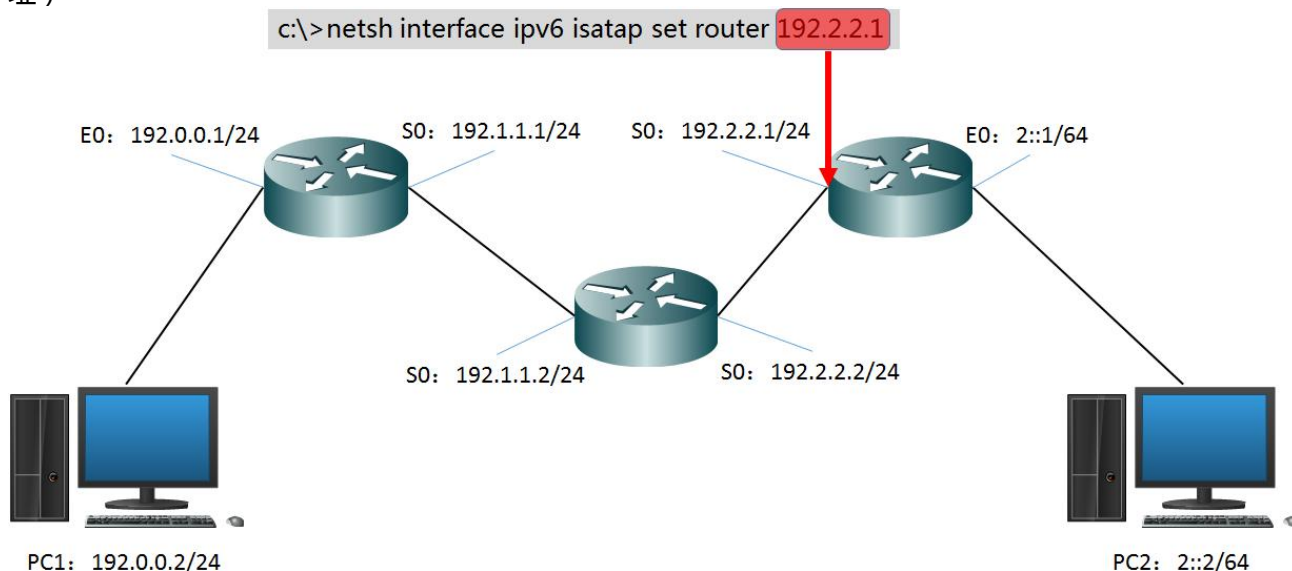
ISATAP隧道适用于IPv4网络中IPv6主机之间的通信或IPv4网络中IPv6主机接入到IPv6的网络通信。

ISATAP的重要命令：

- 1) tunnel mode ipv6 ip isatap (Tunnel模式为IPv6的隧道接口类型是ISATAP)
- 2) no ipv6 nd suppress-ra (默认是禁止隧道接口路由器广播，用改命令来启用广播)

PC上需要配置一个命令：

c:\>netsh interface ipv6 isatap set router 192.2.2.1(这个地址是IPv4网络的下一跳，v4的最后一个地址)



NAT-PT

实现方法比较复杂，处理开销大，一般在其他互通方式无法使用的情况下使用。

静态NAT-PT静态模式提供一对一的v6对v4映射。

动态NAT-PT，动态模式也提供一对一映射，但是v4地址数量决定了v6到v4的最大数目。

表 10-12 静态 NAT-PT 映射命令

命 令	功 能
Router(config)# <u>interface</u> interface-type interface-number	指定启用 NAT-PT 机制的网络接口
Router(config-if)# <u>ipv6 nat</u>	在接口上启用 NAT-PT 机制，这个命令基于接口启用
Router(config)# <u>interface</u> interface-type interface-number	指定另外一个启用 NAT-PT 的接口
Router(config-if)# <u>ipv6 nat</u>	在接口上启用 NAT-PT
Router(config)# <u>ipv6 nat prefix</u> ipv6-prefix /96	详细说明在 IPv6 域内 NAT-PT 使用的 IPv6 前缀，NAT-PT 只支持/96 的网络前缀
Router(config)# <u>ipv6 nat v6v4 source</u> <u>ipv6-address</u> <u>ipv4-address</u>	强制将源 IPv6 地址的输出 IPv6 数据包转换成 IPv4 数据包 6->4
Router(config)# <u>ipv6 nat v4v6 source</u> <u>ipv4-address</u> <u>ipv6-address</u>	强制将源 IPv4 地址的输出 IPv4 数据包转换成 IPv6 数据包 4->6

NAPT-PT (网络地址端口转换协议转换) 多对一动态映射。

表 10-13 动态 NAT-PT 映射命令

命 令	功 能
Router(config)# ipv6 access-list name permit Source-ipv6-prefix/prefix-length	规定了 IPv6 单协议网络中允许被转换的 IPv6 地址范围， ipv6 access-list 命令配置了一个标准的 IPv6 ACL
Router(config)# ipv6 nat v6v4 pool natpt-pool-name start-ipv4 end-ipv4 prefix-length prefix-length	规定转换过程中使用的源 IPv4 地址池，参数 natpt- pool-name 指定这个池的名称。像 IPv4 池的前缀一样， 必须指定地址池的第一个和最后一个 IPv4 地址，分别 用参数 start-ipv4 和 end-ipv4 表示
Router(config)# ipv6 nat v6v4 source {list route-map} {list-name map-name pool-natpt-pool-name}	配置动态 NAT-PT 映射，关键词 list 和参数 list-name 指 定一个标准的 IPv6 ACL 来规定 IPv6 地址的范围，关 键词 route-map 和参数 map-name 可以作为替换，关键词 pool 和参数 natpt-pool-name 规定了源 IPv4 地址池

IPv6的ALC可以直接命名

参看下面命令：

```
R1(config)#ipv6 access-list ipv6 permit 2001:B00:0::/48 any （定义ACL策略）
R1(config)#ipv6 nat prefix 2001:b00:0:0:0:1::/96
R1(config)#ipv6 nat v6v4 pool ipv4-pool 16.23.31.10 16.23.41.20 prefix-length （定义IPv4地址池）
R1(config)#ipv6 nat v6v4 source list ipv6 pool ipv4-pool （定义6到4转换）
```

ACL名称

地址池（pool）名称

NAPT-PT

需要增加**overload**参数。

```
R1(config)#ipv6 nat v6v4 source list ipv6 pool ipv4-pool overload
```

其它命令和NAT-PT一样。

三层交换机实现VLAN间路由（实验）

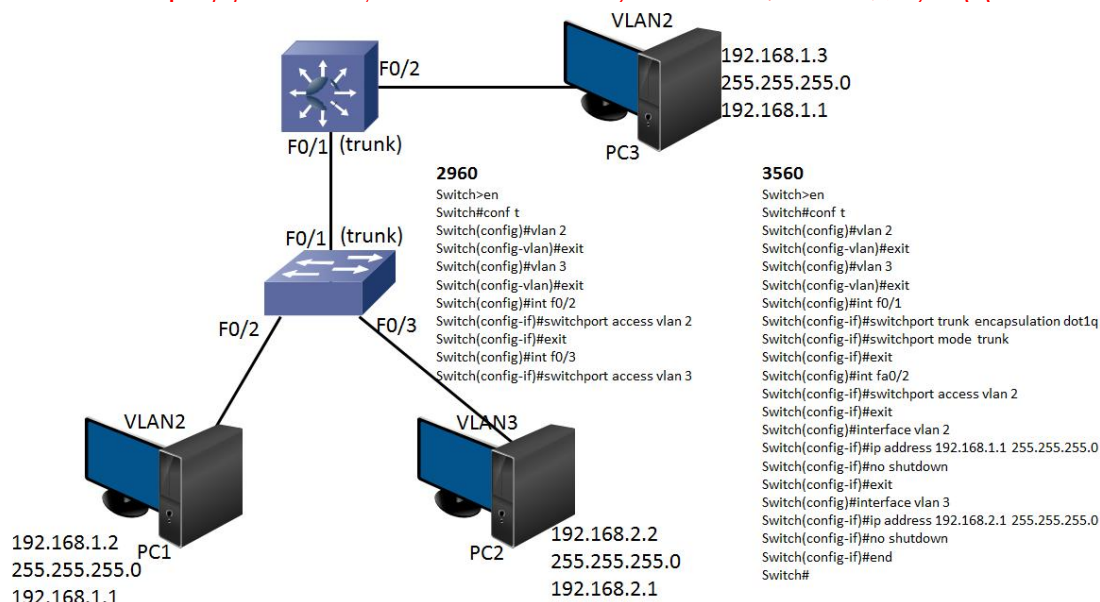
实验目标

- 掌握交换机 Tag VLAN 的配置
- 掌握三层交换机基本配置方法；
- 掌握三层交换机 VLAN 路由的配置方法；
- 通过三层交换机实现 VLAN 间相互通信；

实验设备：

Switch_2960 1台，3560 1台，PC3台，直连线。

分别配置3台PC的参数：



PC1 ping PC3 可以通

PC1 ping PC2 不通

交换机2960的配置：

```
Switch>en
Switch#conf t
Switch(config)#vlan 2
Switch(config-vlan)#exit
Switch(config)#vlan 3
Switch(config-vlan)#exit
Switch(config)#int f0/2
Switch(config-if)#switchport access vlan 2
Switch(config-if)#exit
Switch(config)#int f0/3
Switch(config-if)#switchport access vlan 3
```

交换机3560的配置：


```
Switch>en
Switch#conf t
Switch(config)#vlan 2
Switch(config-vlan)#exit
Switch(config)#vlan 3
Switch(config-vlan)#exit
Switch(config)#int f0/1
Switch(config-if)#switchport trunk encapsulation dot1q
Switch(config-if)#switchport mode trunk
Switch(config-if)#exit
Switch(config)#int fa0/2
Switch(config-if)#switchport access vlan 2
Switch(config-if)#exit
Switch(config)#interface vlan 2
Switch(config-if)#ip address 192.168.1.1 255.255.255.0
Switch(config-if)#no shutdown
Switch(config-if)#exit
Switch(config)#interface vlan 3
Switch(config-if)#ip address 192.168.2.1 255.255.255.0
Switch(config-if)#no shutdown
Switch(config-if)#end
Switch#
```

完成配置后：

PC1 ping PC3 通

PC1 ping PC2 通



策略路由（精细控制）

路由策略（粗放控制）

直连路由、静态路由、默认路由和各种动态路由协议。

策略路由（Policy Based Routing, PBR）能够对分组的转发和路由的传播进行精确控制，使分组按特定的路由按照管理员的策略实现转发和路由。

（笔记20，PDF549）

策略路由是使用路由映射表（route-map）实现的。路由映射表彪悍match和set两个命令，路由映射表也可以有两个关键字permint和deny。

映射表实现策略路由的步骤:

- 1) 分组抓取。
- 2) match命令指定需要控制的数据流。
- 3) set命令指定match匹配到的数据流进行处理。
- 4) 表应用于入站数据流
- 5) 检验 (show命令)

路由映射表命令:

- 1、route-map (定义路由图)

route-map *map-tag* [**permit** | **deny**] [*sequence-number*] 定义路由图

默认情况下, 路由映射表的处理方法是permit。在路由映射表的末尾也隐含式的包含一条deny any语句。
sequence-number 默认序列号10, 可以使用no route-map map-tag sequence-number可以删除指定的路由映射表。

- 2、match (定义匹配条件)

在路由映射表中, match用于指定分组所需要的匹配的条件。

match ip address

match ip address { access-list-number | name } [...access-list-number | name] |
prefix-list prefix-list-name [...prefix-list-name]

- 3、set (定义转发规则)

set命令指定对匹配的分组进行转发的方式和规则。

- ①set ip next-hop

指定分组目的地的下一跳路由器。

- ②set interface

指定转发分组的接口

- ③set ip default next-hop

指定默认下一跳转发地址。

- ④set default interface

指定默认分组转发接口

- 4、在几口应用策略路由命令 (应用到接口上)

ip policy route-map *map-tag*

- 5、查看路由策略命令 (验证策略路由)

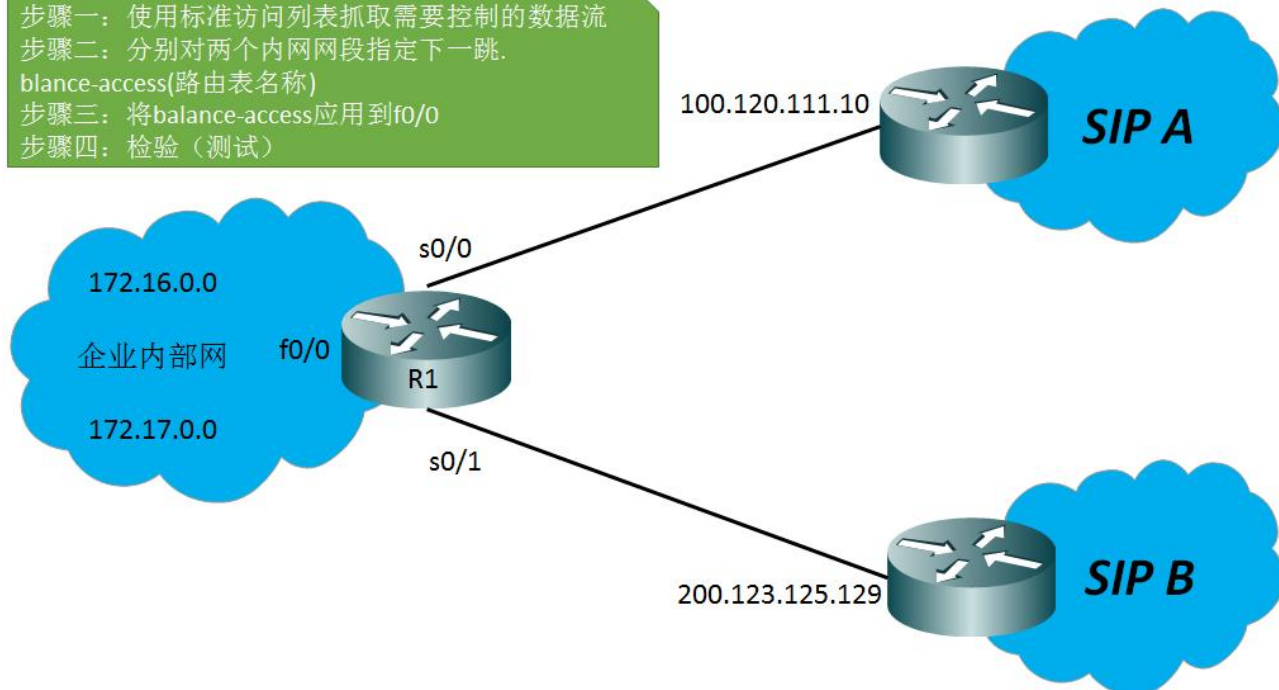
- ①show route-map

- ②show ip policy

策略路由实例

实例1园区网路连接到多个运营商时, 采用策略路由实现分流

步骤一：使用标准访问列表抓取需要控制的数据流
 步骤二：分别对两个内网网段指定下一跳。
 balance-access(路由表名称)
 步骤三：将balance-access应用到f0/0
 步骤四：检验（测试）



步骤一：R1(config)#access-list 1 permit 172.16.0.0 0.0.255.255
 R1(config)#access-list 2 permit 172.17.0.0 0.0.255.255

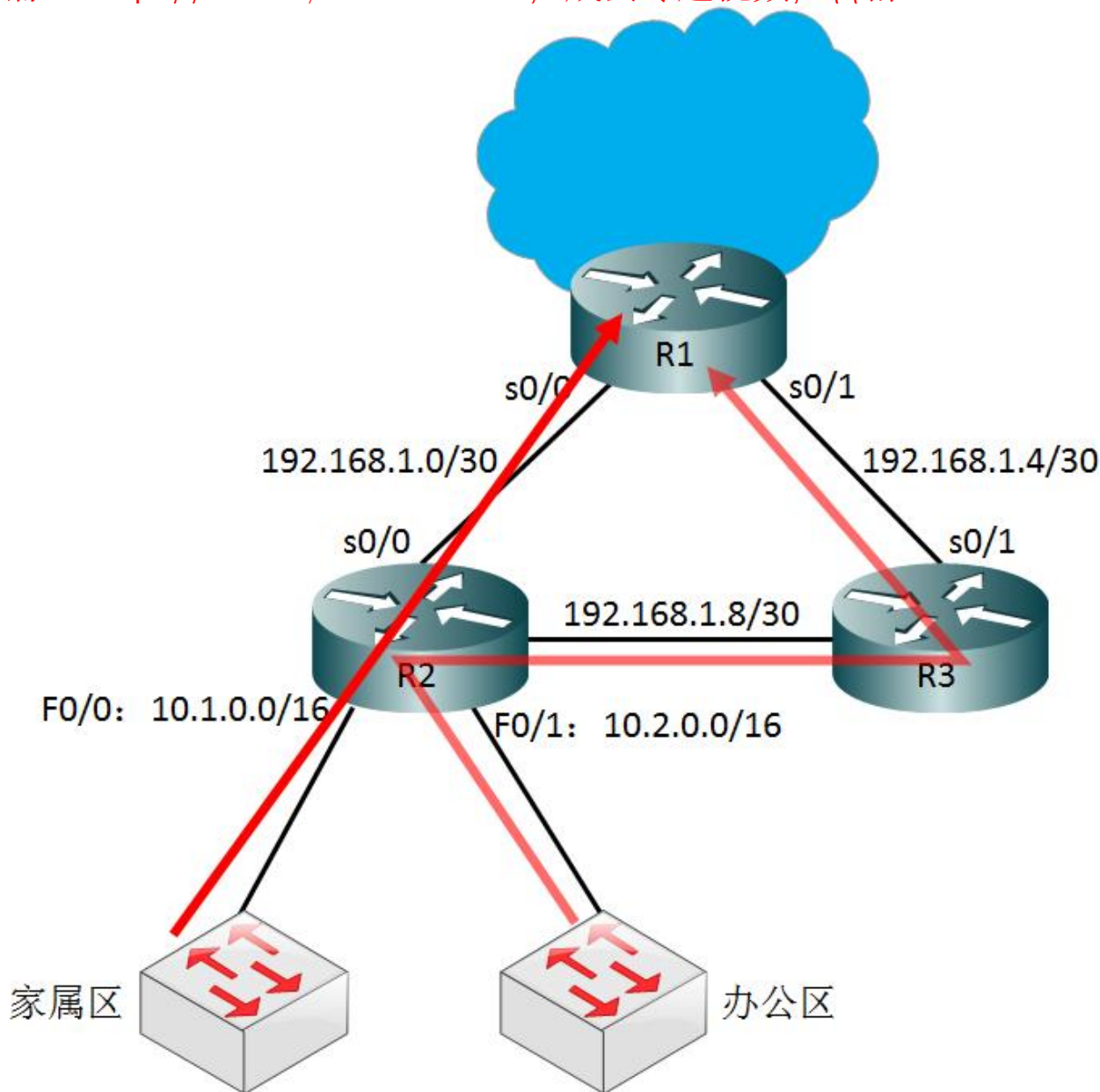
步骤二：R1(config)#route-map balance-access permit 10
 R1(config-route-map)#set ip default next-hop 100.120.111.10 SIP A
 R1(config-route-map)#route-map balance-access permit 20 路由图 20
 R1(config-route-map)#match ip address 2 ACL 2
 R1(config-route-map)#set ip default next-hop 200.123.125.129 SIP B
 R1(config-route-map)#route-map balance-access permit 30 路由图 30
 R1(config-route-map)#set default interface null0
 R1(config-route-map)#exit

步骤三：R1#conf t
 R1(config)#interface f0/0
 R1(config-if)#ip address 10.1.1.1 255.255.255.0
 R1(config-if)#ip policy route-map balance-access
 R1(config-if)#exit
 R1(config)#interface f0/0
 R1(config-if)#ip address 10.1.1.1 255.255.255.0
 R1(config-if)#ip policy route-map balance-access 入站分组有效
 R1(config-if)#exit

步骤四：R1#show ip policy
 Interfac Route map
 f0/0 balance-access

实例2：使用基于源地址的策略路由

家属区数据使用R2到R1链路转发，办公区数据使用R2到R3到R1转发。



通过在R2上设置策略路由来实现：

步骤一：在R2上创建标准访问控制列表来抓取需要分流的数据流。

```
R2(config)#access-list 1 permit 10.1.0.0 0.0.255.255
```

```
R2(config)#access-list 2 permit 10.2.0.0 0.0.255.255
```

步骤二：在R2上创建路由映射表jsq


```
R2(config)#toute-map jsq permit 10
R2(config-route-map)#match ip address 1
R2(config-route-map)#set ip next-hop 192.168.1.1
R2(config)#route-map jsq permit 20
R2(config-route-map)#match ip address 2
R2(config-route-map)#set ip next-hop 192.168.1.10
R2(config)#route-map jsq permit 30
R2(config-route-map)#set default interface null0
```

有2条语句, 序号号, 10, 20, 30

步骤三: 将jsq应用到f0/0

```
R2(config-route-map)#int f0/0
R2(config-if)#ip policy route-map jsq
```

测试四: 测试路映射表。

show ip policy查看

```
R2#show ip policy
Interfac      Route map
f0/0          jsq
```

使用show route-map命令查看:

```
R2#show route-map
route-map jsq,permit,sequence 10
  Match clauses:
    ip address(access-lists):1
  Set clauses:
    ip next-hop 192.168.1.1
  Policy routing matches:5 packets, 570 byte
```

第11章 网络管理

笔记本: 网络工程师学习

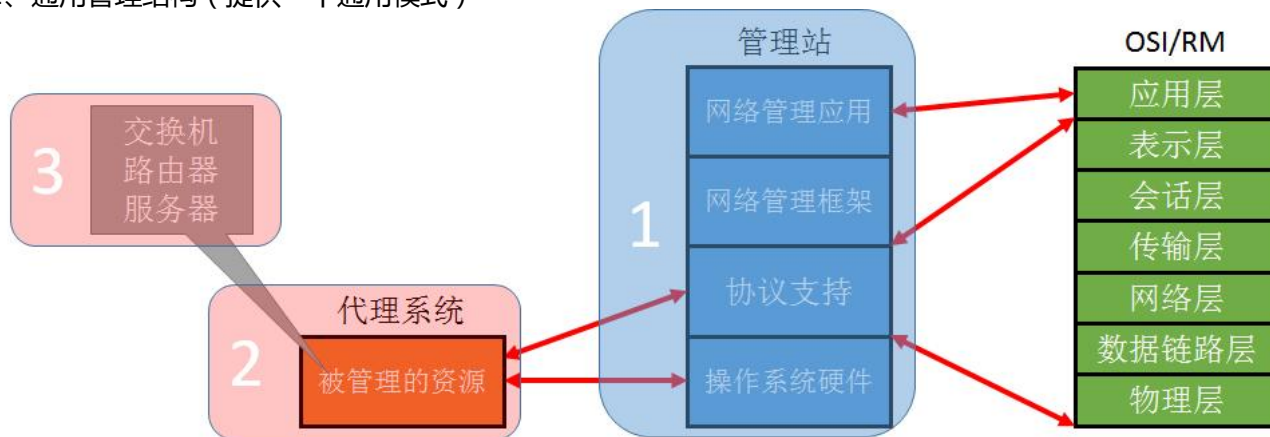
创建时间: 2015/1/21 11:50

更新时间: 2015/1/21 11:50

URL: about:blank

网络管理系统的层次结构:

1、通用管理结构 (提供一个通用模式)



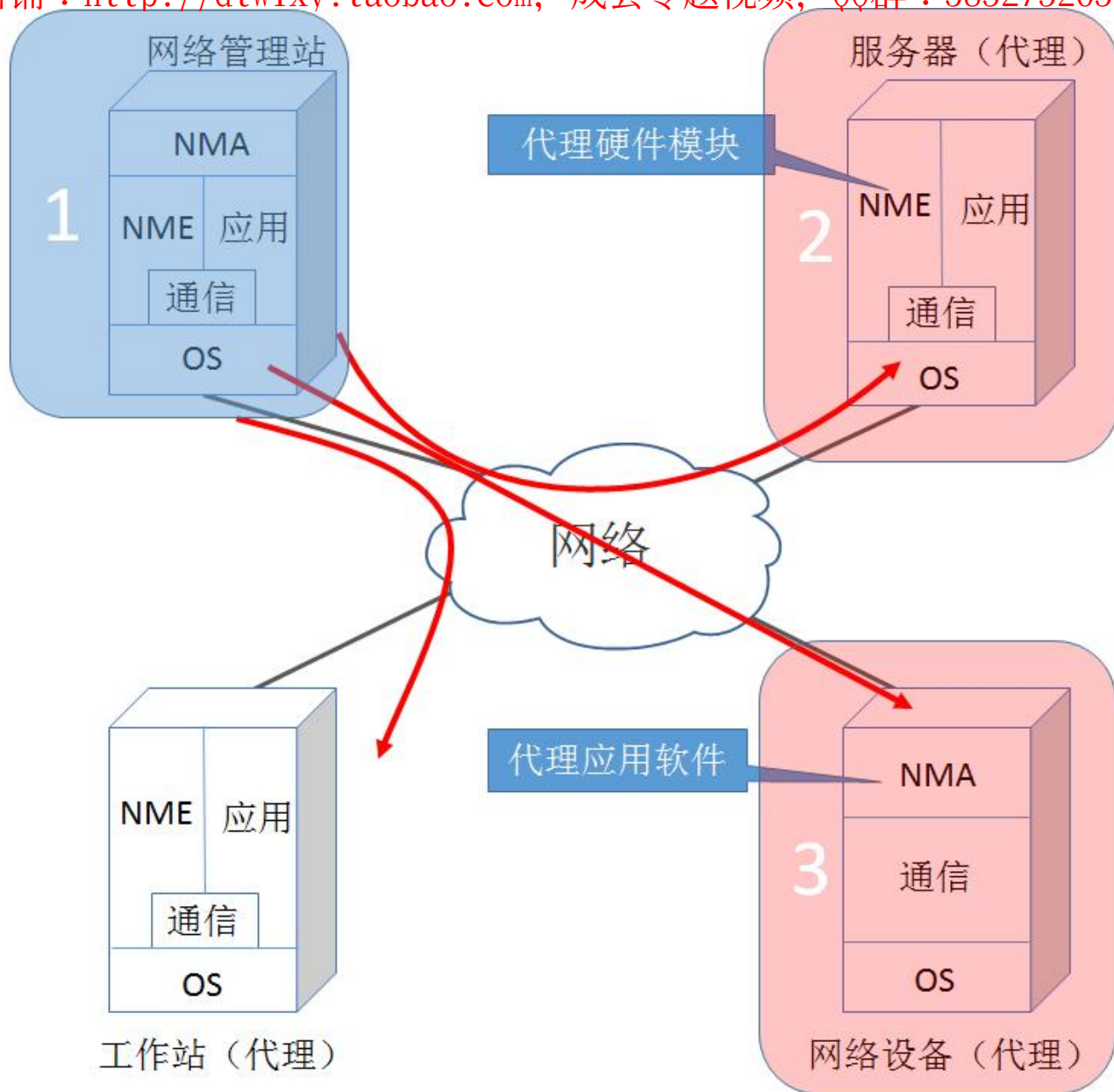
管理功能分为管理站 (Manager) 和代理 (Agent) 两部分。

代理进程通过网络管理协议与管理站对话。

二、集中式管理结构 (适用于小型网络。)

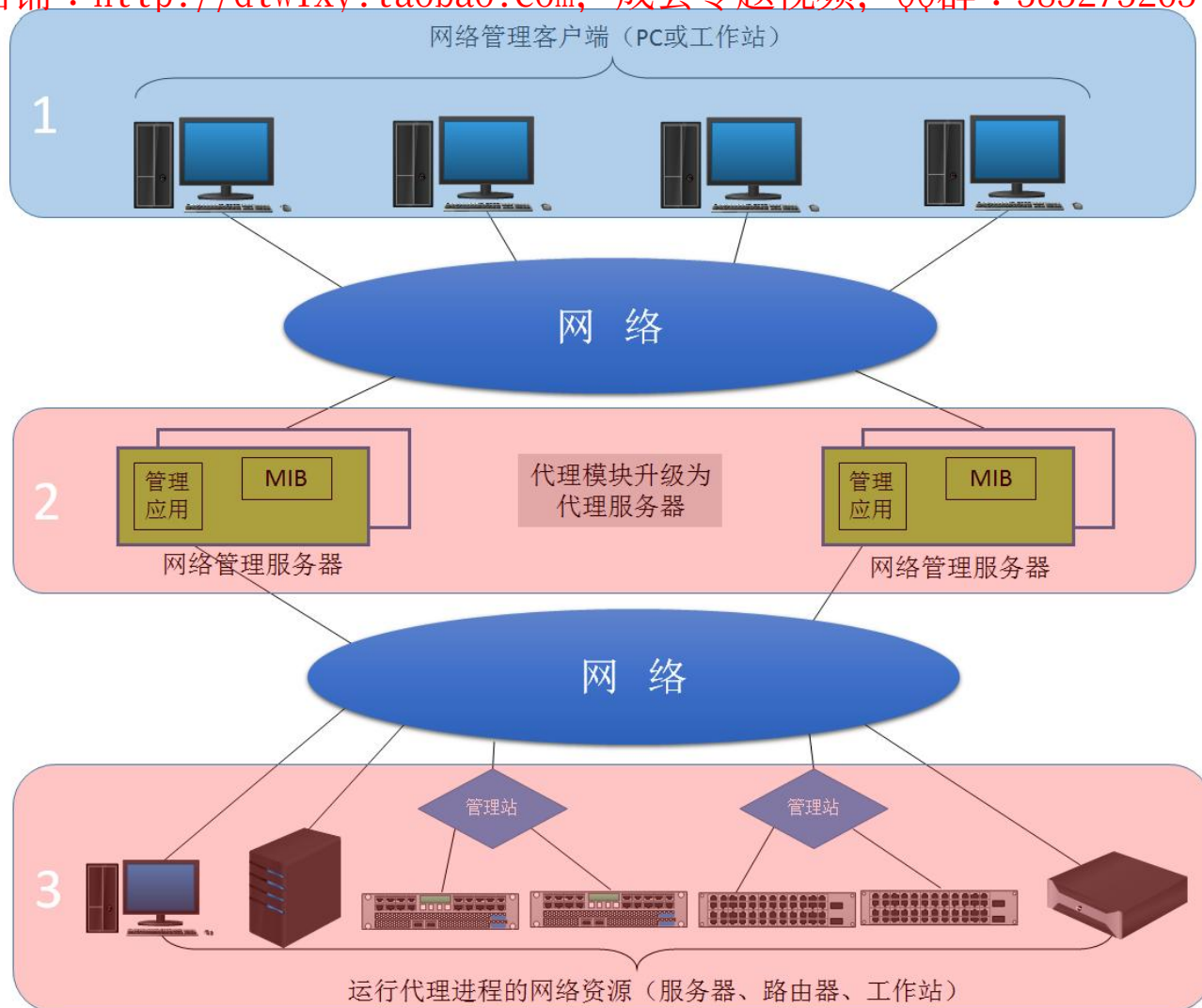
网络管理实体 (Network Management Entity, **NME**) 代理硬件模块。

网络管理应用 (Network Management Application, **NMA**) 代理应用软件。



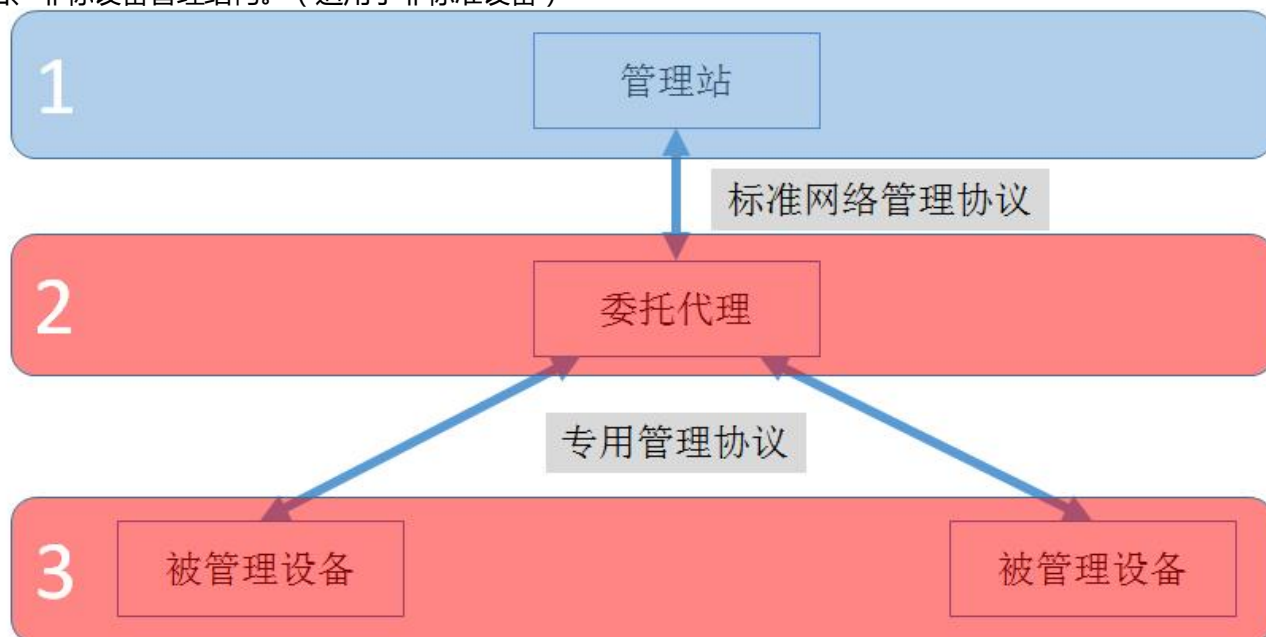
集中式网络管理策略的**好处**是管理人员可以有效地控制整个网络资源, 根据需要平衡网络负载, 优化网络性能。

三、分布式管理结构 (适用于大型网络)



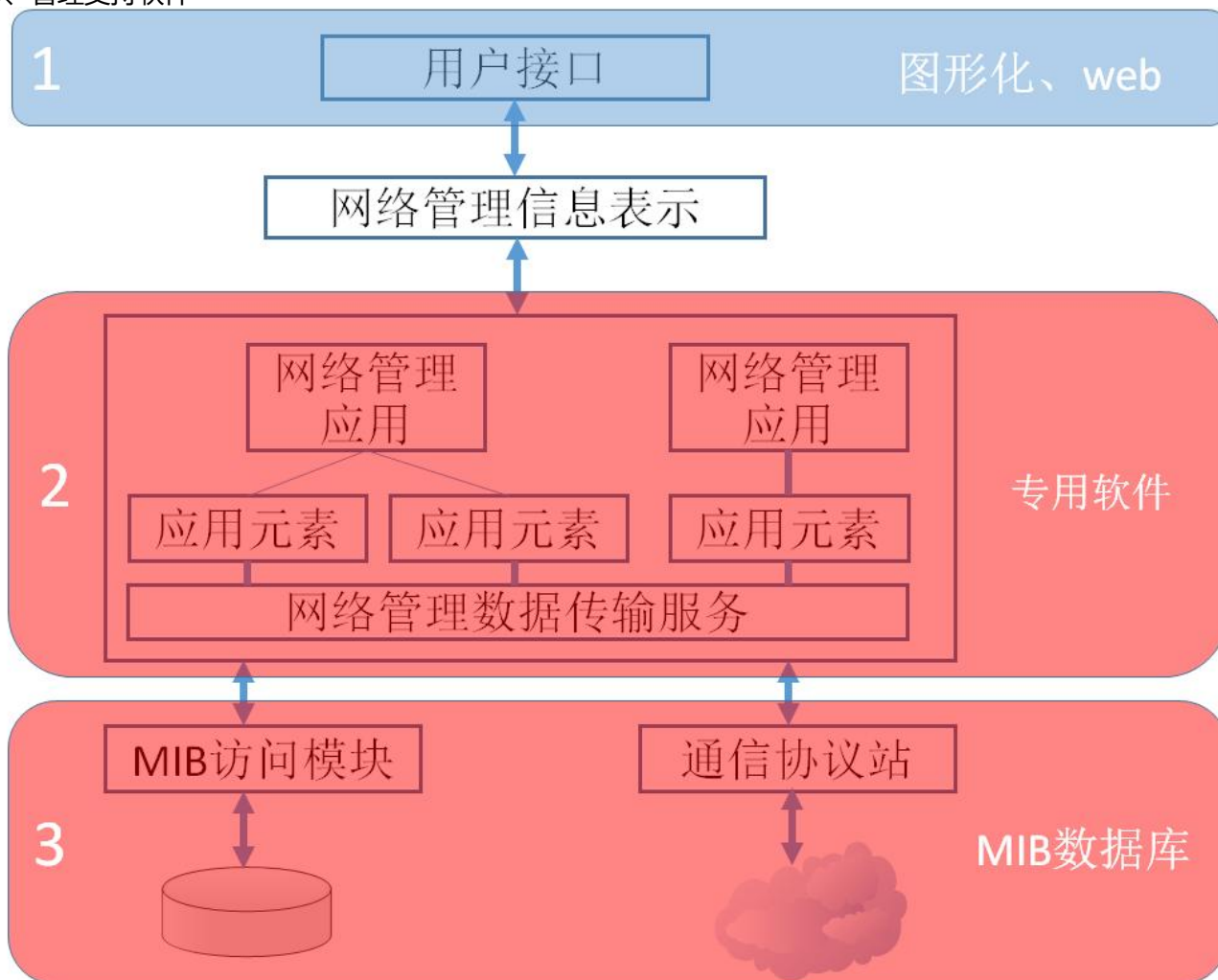
分布式网络管理的灵活性 (Flexibility) 和可伸缩性 (Scalability) 带来的好处日益为网络管理工作者所青睐, 这方面的研究和开发是目前网络管理中最活跃的领域。

四、非标设备管理结构。(适用于非标准设备)



网络管理软件的结构:

- 1、用户接口软件
- 2、管理专用软件
- 3、管理支持软件



32:51/1:19:37

(笔记21 PDF563页)

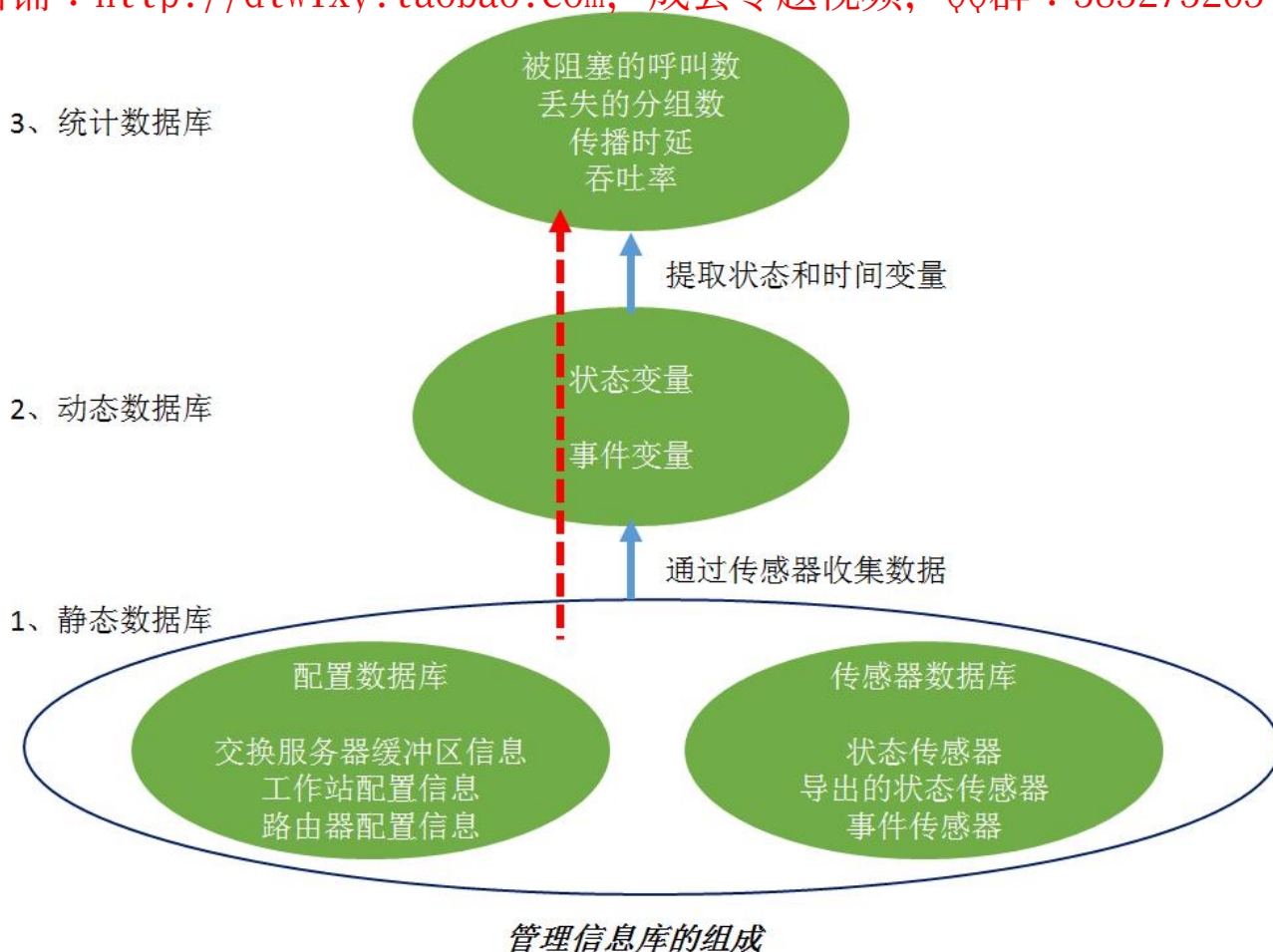
由于网路管理协议位于应用层 (SNMP)

网络管理功能分为: 网络监视和网络控制, 统称**网络监控**。

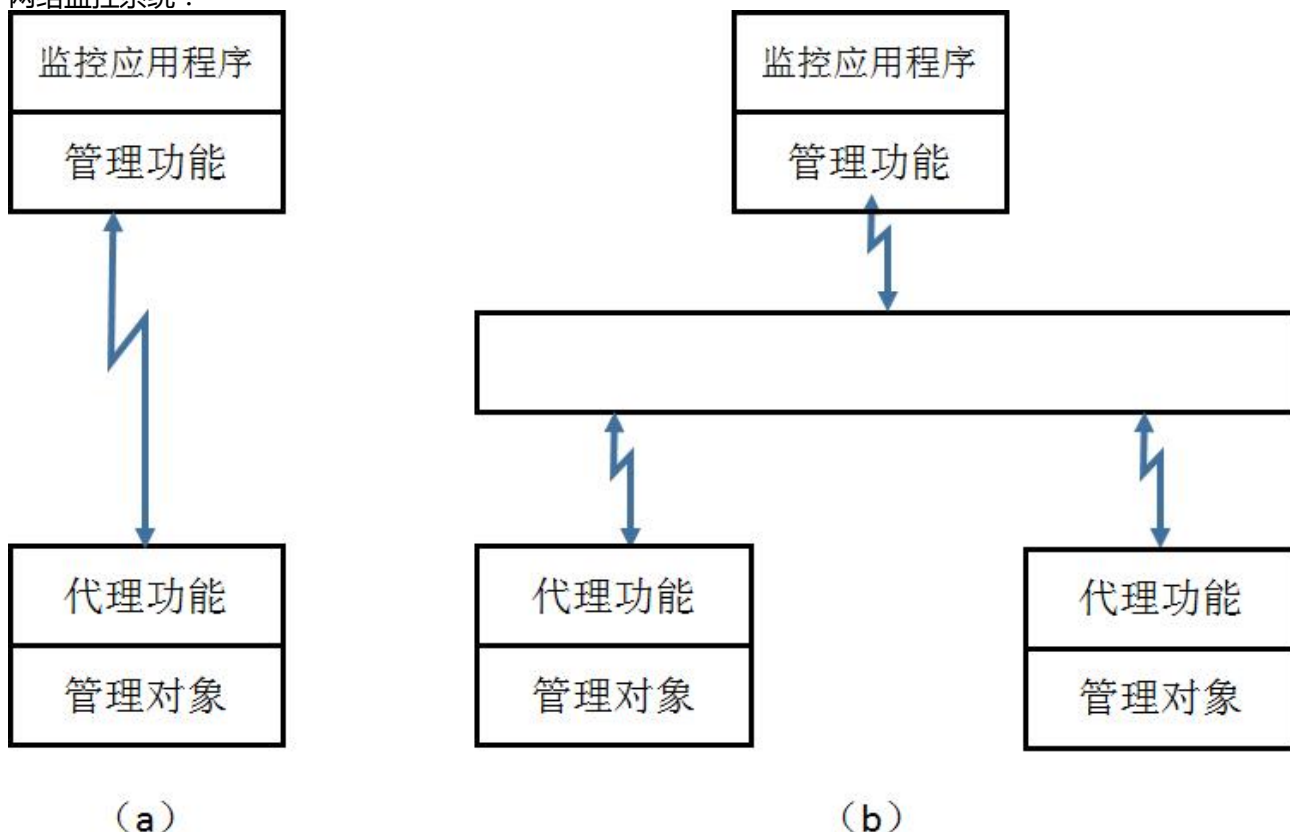
- 1、网路监视是指收集系统和子网的状态信息。
- 2、网络控制是指修改设备参数或重新配置网络资源。

MIB

- 1、静态信息, 包括系统和网络的配置信息, 例如路由器的端口数和端口编号, 标识和CPU类型, 这些信息不常变化。
- 2、动态信息, 与网络中出现的事件和设备的工作状态有关, 例如: 分组数、网络链接状态等。
- 3、统计信息。即从动态信息推导出的信息, 例如, 平均每分钟的分组数、传输失败的概率等。



网络监控系统：



网络监控系统的体系结构

网络监控系统的通信机制:

一种叫轮询 (polling), 一种叫做事件报告 (Event Reporting)

- 1、轮询是一种请求响应式的交互作用, 即有监视器向代理发出请求。
- 2、时间报告是有代理主动发送给管理站的信息。



网络管理的功能:

有5大功能域, 即故障管理 (Fault Management)、配置管理 (configuration Management)、计费管理 (Accounting Management)、性能管理 (Performance Management) 和安全管理 (Security Management)。简称为F-CAPS。

记忆口诀: 计安性配故

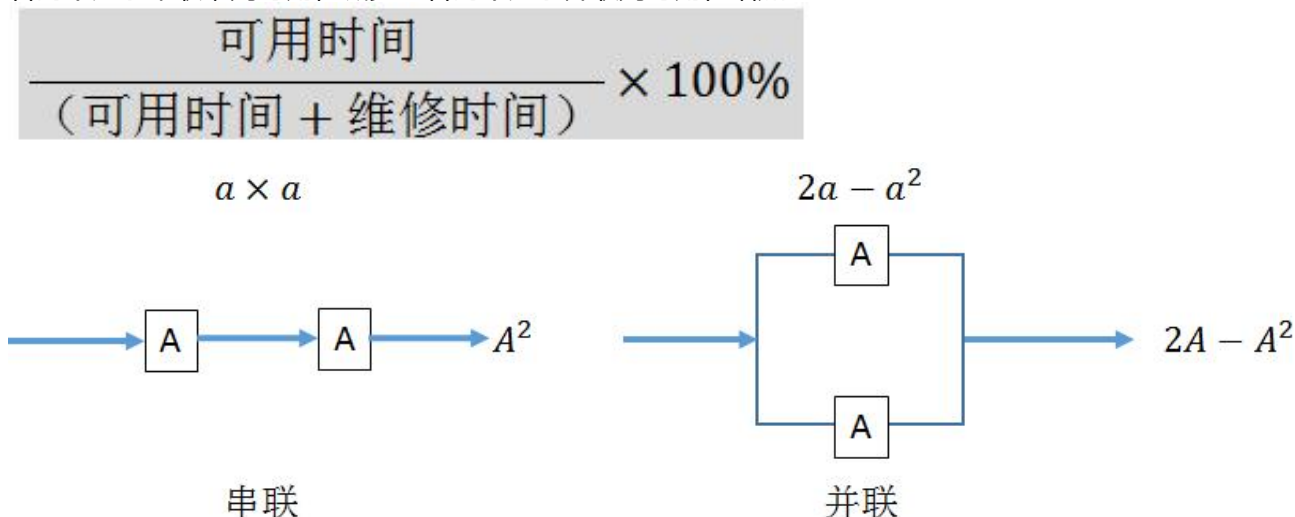
1) 性能管理

①可用性, 指网络系统, 网络元素, 或网络应用对用户可利用的时间的**百分比**。

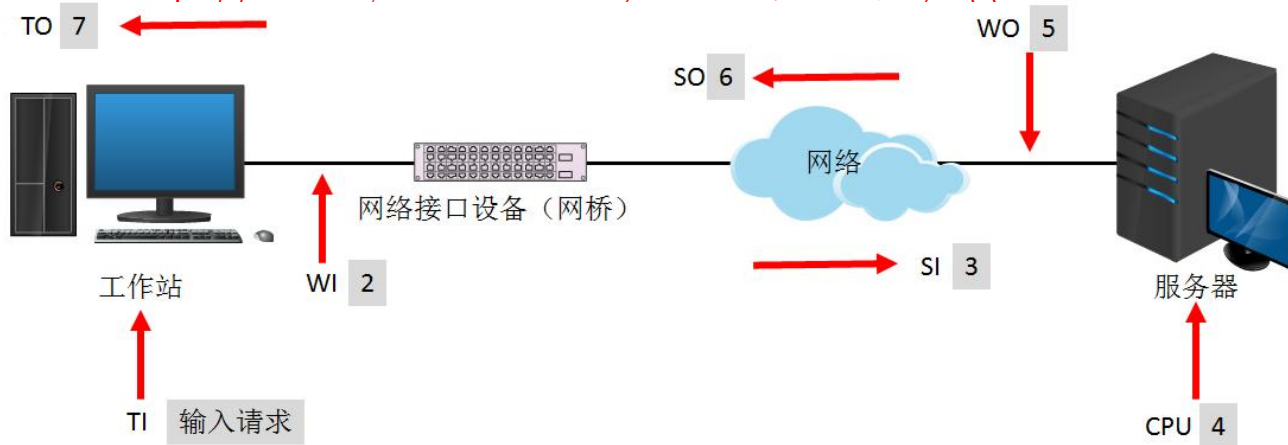
平均无故障时间MTBF。

平均维修时间MTTR。

若两个元素串联, 则可用性减少。若两个元素并联则可用性增加。



②响应时间, 是指从用户输入请求到系统在终端上返回计算结果的时间间隔。



性能测试报告：

- (1) 主机对通信矩阵。一对源主机和目标主机之间，总分组数、数据分组数、数据字节数以及它们所占百分比。
- (2) 主机组通信矩阵，一组主机之间通信量的统计。

2) 故障管理

3) 计费管理

4) 配置管理



管理站通过轮询随时访问代理保存的配置信息，或者代理通过事件报告及时向管理站通知配置参数改变的情况。

5) 安全管理

简单网络管理协议

第一种标准：即ISO 9595公共管理信息服务定义 (CMIS) 和ISO 9596公共管理协议规范 (CMIP)。

第二种标准：有关TCP/IP，简单网络管理第一版 (Simple Network Management Protocol SNMPv1) 后又产生了第二版 SNMPv2和SNMPv3。

第三种标准：监控局域网通信标准——远程网络监控 (RMON) RMON-1和RMON-2

第四种标准：IEEE局域网，管理物理层和数据链路层，叫做CMOL。

第五种标准：为了适应电信网，ITU-T定义了TMN。

SNMPv1

SNMP体系结构

由于SNMP定义了为应用层协议，所以它依赖于UDP数据服务。

其之所以选择UDP协议而不是TCP协议，是以为UDP效率高，这样实现网络管理不会太多增加网络负载。但由于UDP不是很可靠，所以SNMP报文容易丢失。

团体名作为团体的全局标识符，是一种简单的身份认证手段。一般来说，代理进程不接受没有通过团体名验证的报文，这样可以防止未经授权的管理命令。

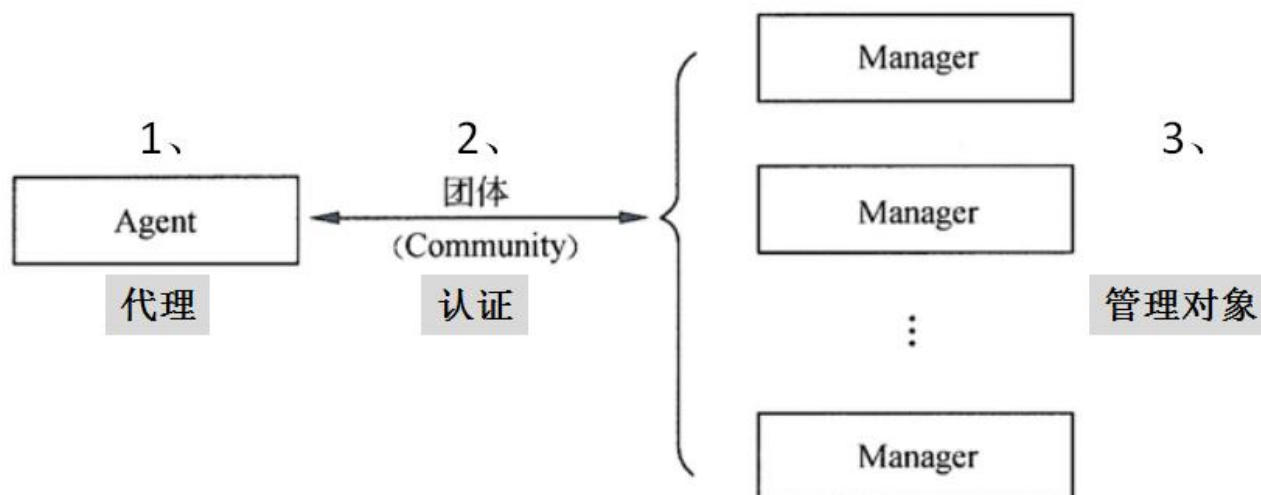


图 11-18 SNMPv1 的团体关系

SNMP 报文由3个部分组成，即版本号，团体名和协议数据单元（PDU），报文头中的版本号是指SNMP的版本，团体名用于身份认证，SNMP共有5种管理操作，但只有4种PDU格式。

SNMP 报文

版本号		团体名		SNMP PDU			
GetRequestPDU、GetNextRequestPDU 和 SetRequestPDU							
PDU 类型	请求标识	0	0	变量绑定表			
GetResponsePDU							
PDU 类型	请求标识	错误状态	错误索引	变量绑定表			
TrapPDU							
PDU 类型	制造商ID	代理地址	一般陷入	特殊陷入	时间戳	变量绑定表	
变量绑定表							
名字 1	值 1	名字 2	值 2	...	名字 n	值 n	

SNMP
V1报文

- 管理站发出
 - 1、GetRequest
 - 2、GetNextRequest
 - 3、SetRequest
- 代理响应
 - 4、GetResponse
- 陷入报文
 - 5、Trap

图 11-19 SNMP 报文格式

SNMP协议的操作。

包含GetRequest、GetNextRequest、SetRequest的报文由管理站发出，代理以GetResponse响应。

最基本的团体名验证功能。团体名以明文的形式传输，SNMP的实现只允许Get和Trap操作。管理站主要靠轮询收集信息。

$$N \leq T/\Delta$$

N——被轮询的代理数

T——轮询间隔

Δ——单个轮询需要的时间

例：每分钟轮询所有被管理设备一次，没明显的网络拥塞，Δ大约是0.202s

11.2 15

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

即管理站最多可以支持4500个设备。

例11.3网桥引入延迟，Δ大约是1.2s

$$N \leq T/\Delta = 15 \times \frac{60}{1.2} = 750$$

管理站可支持的设备最多为750个。

基于团体的SNMP, 简称SNMPv2c。

SNMPv2既可以支持完全集中的网络管理, 又可以支持分布式网络管理。

- (1) 管理信息结构的扩充
- (2) 管理站之间的通信能力。
- (3) 新的协议操作

v2引入了两种新的PDU, 分别用于大块数据的传送和管理站之间的通信。



GetBulkRequestPDU 块检索操作。

TrapPDU

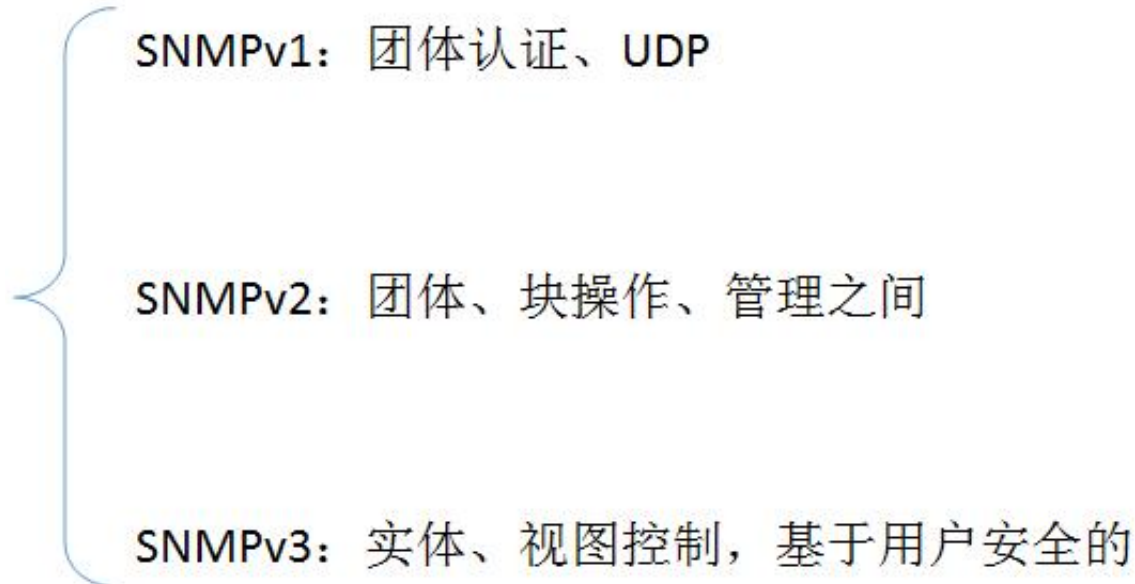
InformRequestPDU, 管理站之间的通讯机制是分布式网络管理所需的功能。

SNMPv3

前两版中叫管理站和代理的在v3中统一叫做SNMP实体 (SNMP entity)。由一个或多个SNMP引擎和一个或多个SNMP应用 (SNMP Application)

基于用户的安全模型 (USM)

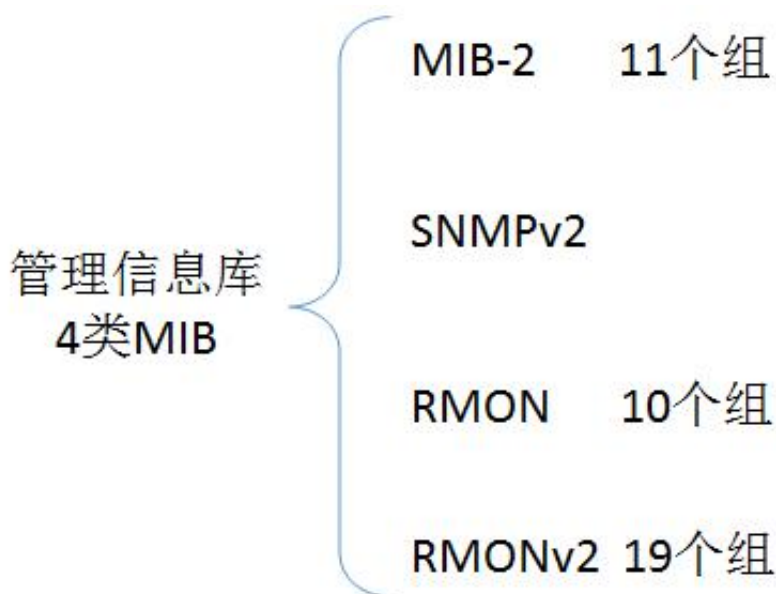
SNMPv3把对网络协议的安全威胁分为**主要的**和**次要的**两类。



基于视图访问控制 (VACM) 模型

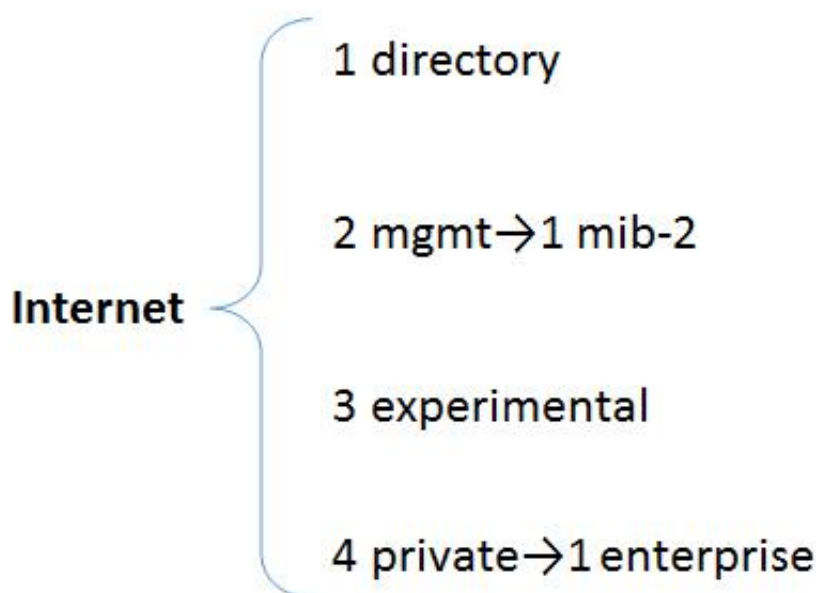
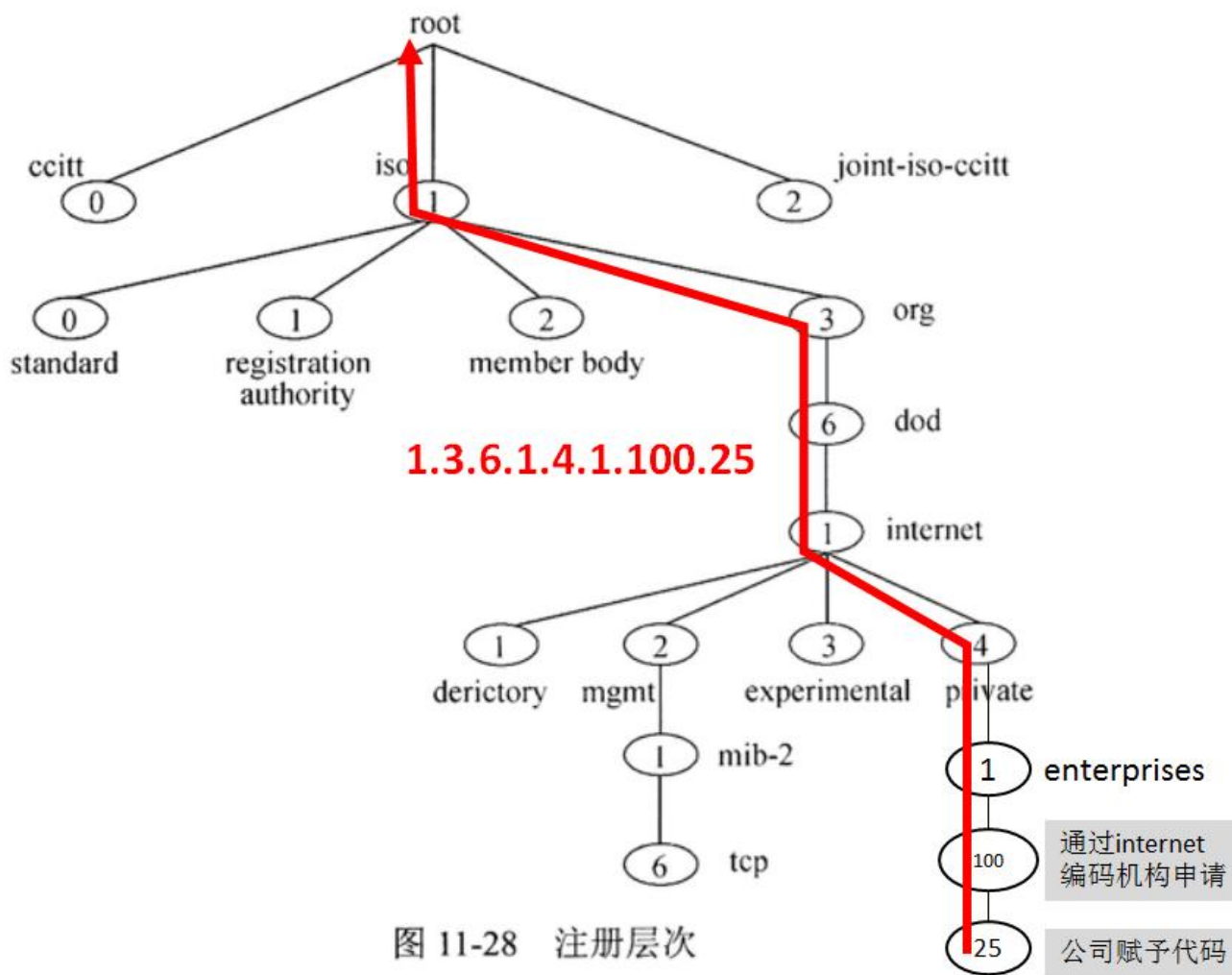
管理数据库MIB-2

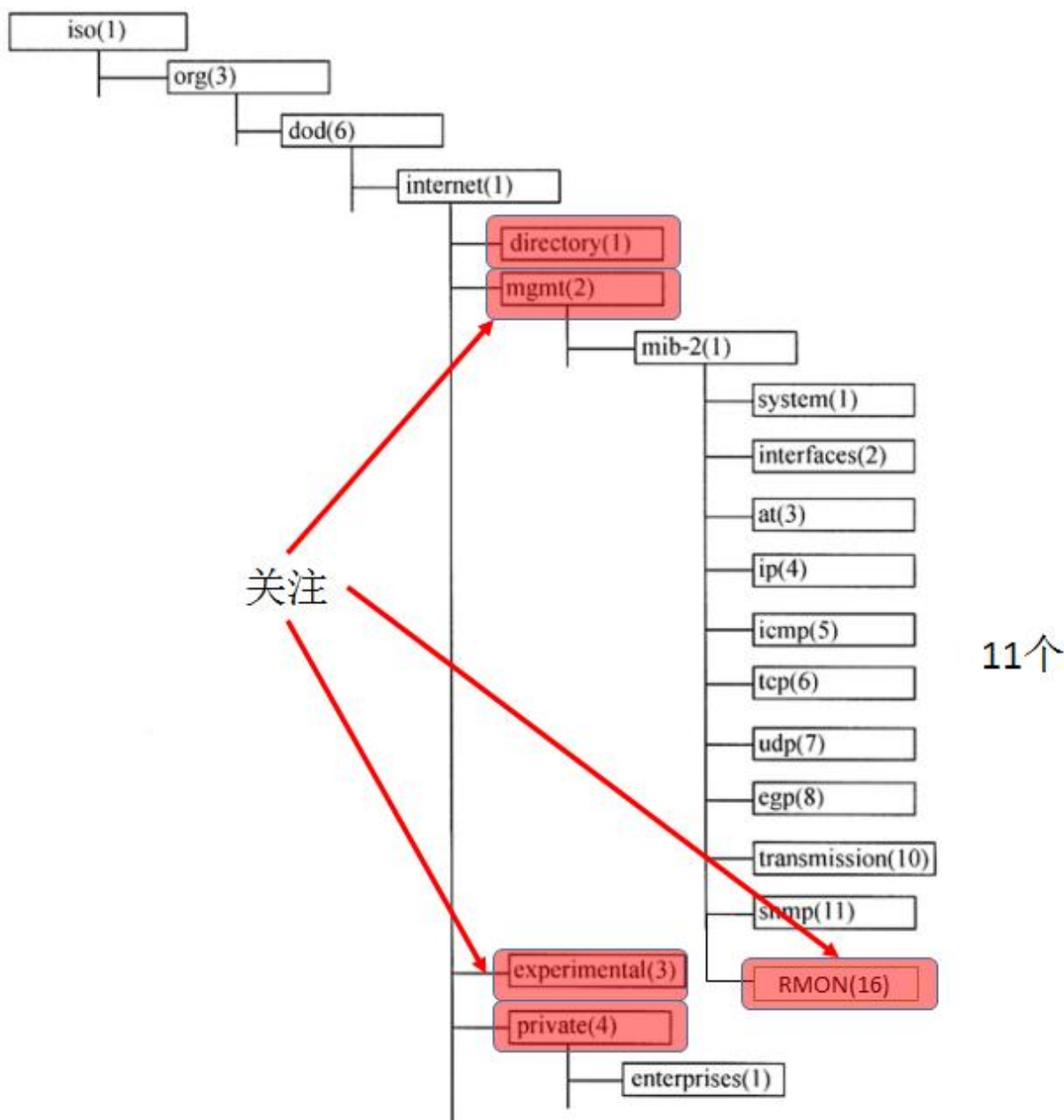
树形结构。



默认为抽象语法标识ASN.1

internet下面4个节点, directory(1)是OSI的目录服务, mgmt(2)包括管理对象, 而mib-2是mgmt(2)的第一个孩子节点。experimental(3)子树用来标识因特网上实验的所有管理对象。private(4)子树是为私有企业管理信息准备的, 只有一个enterprises(1)。注册的得到代码100, 公司为他赋予代码25, 标识符为1.3.6.1.4.1.100.25





网络管理定义了应用类型

NetworkAddress: 多种网络地址

IPAddress: 32位的IP地址

Counter: 计数器达到最大值 $2^{32}-1$ 后回零, 再从头开始增加。

Gauge: 计数器类型 (一个非负整数), 计数器达到最大值后不回零, 而是锁定在 $2^{32}-1$

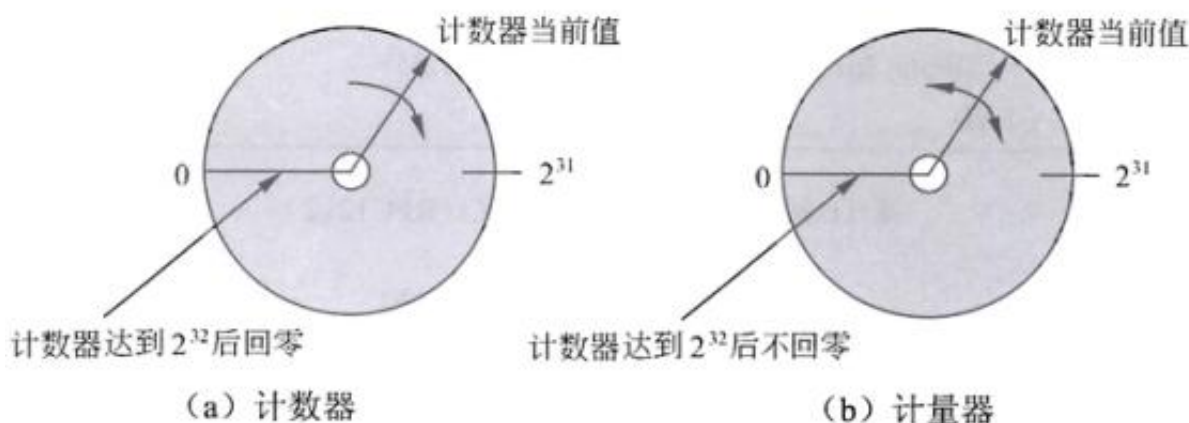


图 11-31 计数器和计量器

TimeTicks：时钟类型

Opaque：不透明类型，即未知数据类型。

SNMPv2增加了两种新的数据类型Unsigned32和Counter64。

MIB-2包含11个功能组。

(1) 系统组 (System group) 提供了系统的一般信息。

关键词：sys

表 11-3 系统组对象

对 象	语 法	访问方式	功 能 描 述
sysDescr (1)	DisplayString (SIZE (0..255))	RO	有关硬件和操作系统的描述
sysObjectID (2)	OBJECT IDENTIFIER	RO	系统制造商标识
sysUpTime (3)	Timeticks	RO	系统运行时间
sysContact (4)	DisplayString (SIZE (0..255))	RW	系统管理人员描述
sysName (5)	DisplayString (SIZE (0..255))	RW	系统名
sysLocation (6)	DisplayString (SIZE (0..255))	RW	系统的物理位置
sysServices (7)	INTEGER (0..127)	RO	系统服务

(2) Interface组，包含关于主机接口的配置信息和统计信息。

关键词：if

表 11-4 接口组对象

对 象	语 法	访问方式	功 能 描 述
ifNumber	INTEGER	RO	网络接口数
ifTable	SEQUENCE OF ifEntry	NA	接口表
ifEntry	SEQUENCE	NA	接口表项
ifIndex	INTEGER	RO	唯一的索引
ifDescr	DisplayString (SIZE (0..255))	RO	接口描述信息、制造商标名、产品名和版本等
ifType	INTEGER	RO	物理层和数据链路层协议确定的接口类型
ifMtu	INTEGER	RO	最大协议数据单元大小 (位组数)

(3) 地址转换组。表示网络地址到接口物理地址的映射关系。

(4) IP组。IP组提供了与IP协议有关的信息。

关键词: IP

表 11-5 IP 组对象

对 象	语 法	访问方式	功 能 描 述
ipForwarding (1)	INTEGER	RW	IP gateway (1), IP host (2)
ipDefaultTTL (2)	INTEGER	RW	IP 头中的 Time To Live 字段的值
ipInReceives (3)	Counter	RO	IP 层从下层接收的数据报总数
ipInHdrErrors (4)	Counter	RO	由于 IP 头出错而丢弃的数据报

(5) ICMP组。ICMP是IP的伴随协议

关键词: ICMP

表 11-6 IP 组对象

对 象	语 法	访问方式	功 能 描 述
icmpInMsgs (1)	Counter	RO	接收的 icmp 报文总数 (以下为输入报文)
icmpInErrors (2)	Counter	RO	出错的 icmp 报文数
icmpInDestUnreachs (3)	Counter	RO	目标不可送达型 icmp 报文
icmpInTimeExcds (4)	Counter	RO	超时型 icmp 报文
icmpInPramProbe (5)	Counter	RO	有参数问题型 icmp 报文
icmpInSrcQuenchs (6)	Counter	RO	源抑制型 icmp 报文
icmpInRedirects (7)	Counter	RO	重定向型 icmp 报文
icmpInEchos (8)	Counter	RO	回声请求型 icmp 报文

(6) TCP组。TCP组包含与TCP协议的实现和操作有关的信息。

关键词: TCP

表 11-7 TCP 组对象

对 象	语 法	访问方式	功 能 描 述
tcpRtoAlgorithm (1)	INTEGER	RO	重传时间算法
tcpRtoMin (2)	INTEGER	RO	重传时间最小值
tcpRtoMax (3)	INTEGER	RO	重传时间最大值
tcpMaxConn (4)	INTEGER	RO	可建立的最大连接数

(7) UDP组, 关于UDP数据报和本地接收端点的详细信息。

(8) EGP组, EGP组提供了关于EGP路由器发送和接收的EGP报文信息。

(9) 传输组, 针对各种传输介质提供详细的管理信息。

SNMPv2管理信息库

(1) 系统组, SNMPv2的系统组是MIB-2系统组的扩展。

(2) SNMP组。这个组是由MIB-2的对应组改造而成的。

(3) MIB对象组。这个新组包含的对象与管理对象的控制有关。

RMON基本概念

通常用于监视整个网络通信情况的设备叫做网络监视器 (Monitor) 或网络分析器 (Analyzer)、探测器 (Probe) 等。

MIB-2下面的第16个子树。分为10组。

实现连带关系：

- 1) 实现警报组时必须实现事件组。
- 2) 实现最高N台主机组时必须实现主机组。

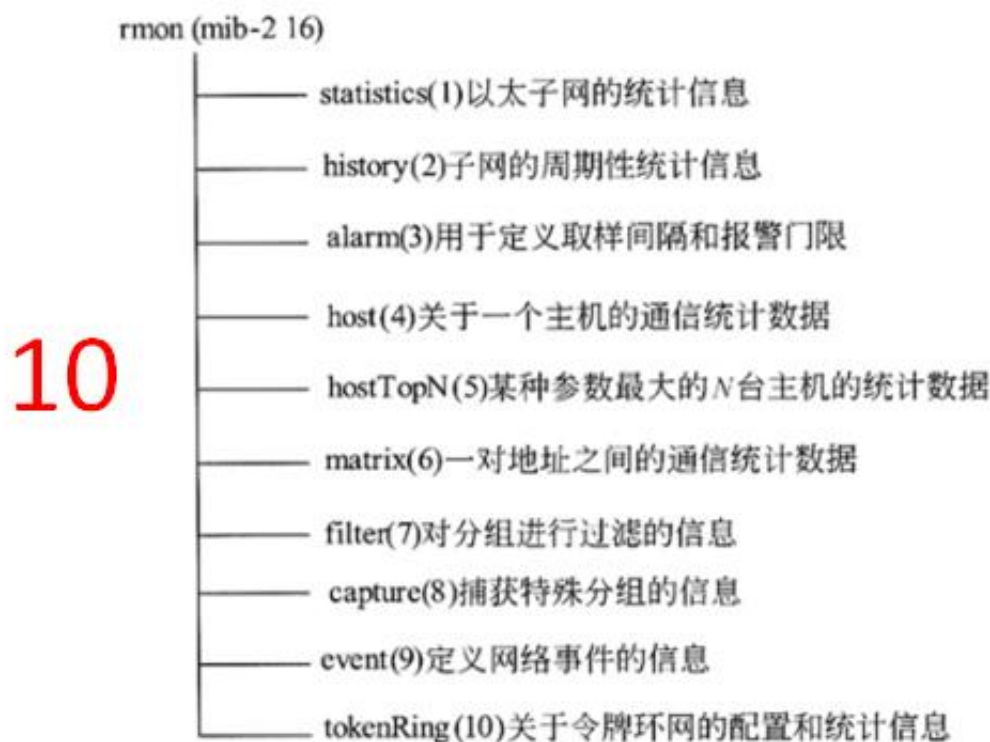


图 11-36 RMON MIB 子树

- 3) 实现捕获组时必须实现过滤组。

RMON2扩充了增加了9个新功能组 (变为19个)

网路诊断和配置命令：

windows在开始中运行CMD.exe，进入DOS命令窗口。

ipconfig命令相当于win9x下winipcfg，可以显示所有网卡的TCP/IP配置参数，可以刷新动态主机配置协议 (DHCP) 和域名系统的设置：

ipconfig的参数及解释：


```

选项：
/?          显示此帮助消息。
/all        显示完整配置信息。
/release    释放指定适配器的 IPv4 地址。
/release6   释放指定适配器的 IPv6 地址。
/renew      更新指定适配器的 IPv4 地址。
/renew6     更新指定适配器的 IPv6 地址。
/flushdns   清除 DNS 解析程序缓存。
/registerdns 刷新所有 DHCP 租约并重新注册 DNS 名称。
/displaydns 显示 DNS 解析程序缓存的内容。
/showclassid 显示适配器的所有允许的 DHCP 类 ID。
/setclassid  修改 DHCP 类 ID。
/showclassid6 显示适配器允许的所有 IPv6 DHCP 类 ID。
/setclassid6 修改 IPv6 DHCP 类 ID。
    
```

ping命令通过发送ICMP回声请求报文来检验与另一个计算机的连接，用于链接故障的测试命令。

ping的参数及设置

```

用法: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
        [-r count] [-s count] [[-j host-list] ! [-k host-list]]
        [-w timeout] [-R] [-S srcaddr] [-4] [-6] target_name

选项：
-t          Ping 指定的主机，直到停止。
            若要查看统计信息并继续操作 - 请键入 Control-Break;
            若要停止 - 请键入 Control-C。
-a          将地址解析成主机名。
-n count    要发送的回显请求数。
-l size     发送缓冲区大小。
-f          在数据包中设置“不分段”标志<仅适用于 IPv4>。
-i TTL      生存时间。
-v TOS      服务类型<仅适用于 IPv4。该设置已不赞成使用，且
            对 IP 标头中的服务字段类型没有任何影响>。
-r count    记录计数跃点的路由<仅适用于 IPv4>。
-s count    计数跃点的时间戳<仅适用于 IPv4>。
-j host-list 与主机列表一起的松散源路由<仅适用于 IPv4>。
-k host-list 与主机列表一起的严格源路由<仅适用于 IPv4>。
-w timeout  等待每次回复的超时时间<毫秒>。
-R          同样使用路由标头测试反向路由<仅适用于 IPv6>。
-S srcaddr  要使用的源地址。
-4          强制使用 IPv4。
-6          强制使用 IPv6。
    
```

-a用IP地址标识目标，进行反向名字解析。

-n设置次数，默认4次。

-l 回声请求报文字节数，默认32，最大65527。

arp命令用于显示和修改地址解析协议缓存表的内容，缓存表项是IP地址与网卡地址对。

arp命令参数说明：

C:\Users\admin>arp /?

显示和修改地址解析协议<ARP>使用的“IP 到物理”地址转换表。

ARP -s inet_addr eth_addr [if_addr]

ARP -d inet_addr [if_addr]

ARP -a [inet_addr] [-N if_addr] [-v]

-a 通过询问当前协议数据, 显示当前 ARP 项。
如果指定 inet_addr, 则只显示指定计算机的 IP 地址和物理地址。如果不止一个网络接口使用 ARP, 则显示每个 ARP 表的项。
-g 与 -a 相同。
-v 在详细模式下显示当前 ARP 项。所有无效项和环回接口上的项都将显示。
inet_addr 指定 Internet 地址。
-N if_addr 显示 if_addr 指定的网络接口的 ARP 项。
-d 删除 inet_addr 指定的主机。inet_addr 可以是通配符 *, 以删除所有主机。
-s 添加主机并且将 Internet 地址 inet_addr 与物理地址 eth_addr 相关联。物理地址是用连字符分隔的 6 个十六进制字节。该项是永久的。
eth_addr 指定物理地址。
if_addr 如果存在, 此项指定地址转换表应修改的接口的 Internet 地址。如果不存在, 则使用第一个适用的接口。

示例:

> arp -s 157.55.85.212 00-aa-00-62-c6-09.... 添加静态项。
> arp -a 显示 ARP 表。

netstat命令

netstat命令用于显示TCP连接、计算机正在监听的端口、以太网计信息、IP路由表、IPv4统计信息(包括IP、ICMP、TCP、和UDP等协议)和IPv6统计信息(包括IPv6、ICMPv6、TCP over IPv6和UDP over IPv6等协议)

```
C:\Users\admin>netstat /?
```

显示协议统计和当前 TCP/IP 网络连接。

```
NETSTAT [-a] [-b] [-e] [-f] [-n] [-o] [-p proto] [-r] [-s] [-t] [interval]
```

```
-a      显示所有连接和侦听端口。
-b      显示在创建每个连接或侦听端口时涉及的可执行程序。
        在某些情况下, 已知可执行程序承载多个独立的
        组件, 这些情况下, 显示创建连接或侦听端口时涉
        及的组件序列。此情况下, 可执行程序的名称
        位于底部[]中, 它调用的组件位于顶部, 直至达
        到 TCP/IP。注意, 此选项可能很耗时, 并且在您没有
        足够权限时可能失败。
-e      显示以太网统计。此选项可以与 -s 选项结合使用。
-f      显示外部地址的完全限定域名(FQDN)。
-n      以数字形式显示地址和端口号。
-o      显示拥有的与每个连接关联的进程 ID。
-p proto 显示 proto 指定的协议的连接; proto 可以是下列任
        何一个: TCP、UDP、TCPv6 或 UDPv6。如果与 -s 选
        项一起用来显示每个协议的统计, proto 可以是下列任
        何一个: IP、IPv6、ICMP、ICMPv6、TCP、TCPv6、UDP
        或 UDPv6。
-r      显示路由表。
-s      显示每个协议的统计。默认情况下, 显示
        IP、IPv6、ICMP、ICMPv6、TCP、TCPv6、UDP 和 UDPv6
        的统计; -p 选项可用于指定默认的子网。
-t      显示当前连接卸载状态。
interval 重新显示选定的统计, 各个显示间暂停的间隔秒数。
        按 CTRL+C 停止重新显示统计。如果省略, 则 netstat
        将打印当前的配置信息一次。
```

-r参数显示路由表内容, 等同于route print

State: 表示TCP连接的状态。

- CLOSE_WAIT: 收到对方的连接释放请求。
- CLOSED: 连接已关闭。
- ESTABLISHED: 连接已建立。
- FIN_WAIT_1: 已发出连接释放请求。
- FIN_WAIT_2: 等待对方的连接释放请求。
- LAST_ACK: 等待对方的连接释放应答。
- LISTEN: 正在监听端口。
- SYN_RECEIVED: 收到对方的连接建立请求。
- SYN_SEND: 已主动发出连接建立请求。
- TIMED_WAIT: 等待一段时间后将释放连接。

举例:

显示以太网的统计信息和所有协议的统计信息

```
netstat -e -s
```

显示TCP和UDP的协议统计信息

netstat -s -p tcp udp

显示TCP连接及其对应的进程ID, 4秒显示一次。

netstat -o 4

数字形式显示TCP连接及进程ID。

netstat -n -o

tracert命令的功能是确定达到目标的路径, 并显示通路上每一个中间路由器的IP地址。通过多次向目标发送ICMP回声 (echo) 请求报文, 每次增加IP头中TTL字段的值, 到达各个路由器的时间。

```
C:\Users\admin>tracert /?

用法: tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout]
        [-R] [-S srcaddr] [-4] [-6] target_name

选项:
    -d          不将地址解析成主机名。
    -h maximum_hops  搜索目标的最大跃点数。
    -j host-list  与主机列表一起的松散源路由<仅适用于 IPv4>。
    -w timeout    等待每个回复的超时时间<以毫秒为单位>。
    -R          跟踪往返行程路径<仅适用于 IPv6>。
    -S srcaddr    要使用的源地址<仅适用于 IPv6>。
    -4          强制使用 IPv4。
    -6          强制使用 IPv6。
```

举例: 跟踪到达主机corp7.microsoft.com的路径

tracert corp7.microsoft.com

跟踪到达主机corp7.microsoft.com的路径, 并不进行名字解析, 只显示中间节点IP地址, 则输入

tracert -d corp7.microsoft.com

pathping命令

pathping结合了ping和tracert两个命令的功能, 可以显示通信线路上每个子网的延迟和丢包率。可以根据此确定哪些路由器或者子网存在通信问题。

```
C:\Users\admin>pathping /?

用法: pathping [-g host-list] [-h maximum_hops] [-i address] [-n]
        [-p period] [-q num_queries] [-w timeout]
        [-4] [-6] target_name

选项:
    -g host-list  与主机列表一起的松散源路由。
    -h maximum_hops  搜索目标的最大跃点数。
    -i address     使用指定的源地址。
    -n            不将地址解析成主机名。
    -p period      两次 Ping 之间等待的时间<以毫秒为单位>。
    -q num_queries  每个跃点的查询数。
    -w timeout     每次回复等待的超时时间<以毫秒为单位>。
    -4            强制使用 IPv4。
    -6            强制使用 IPv6。
```

-n 不进行名字解析, 以加快显示速度。

nbstat命令

命令显示NetBT (NetBIOS over TCP/IP) 协议的统计信息，包括本地计算机和远程计算机的NetBIOS名字表，以及NetBIOS名字缓存。

```
C:\Users\admin>nbstat /?
```

显示协议统计和当前使用 NBT 的 TCP/IP 连接
(在 TCP/IP 上的 NetBIOS)。

```
NBTSTAT [ [-a RemoteName] [-A IP address] [-c] [-n]
          [-r] [-R] [-RR] [-s] [-S] [interval] ]
```

-a	<适配器状态>	列出指定名称的远程机器的名称表
-A	<适配器状态>	列出指定 IP 地址的远程机器的名称表。
-c	<缓存>	列出远程[计算机]名称及其 IP 地址的 NBT 缓存
-n	<名称>	列出本地 NetBIOS 名称。
-r	<已解析>	列出通过广播和经由 WINS 解析的名称
-R	<重新加载>	清除和重新加载远程缓存名称表
-s	<会话>	列出具有目标 IP 地址的会话表
-S	<会话>	列出将目标 IP 地址转换成计算机 NETBIOS 名称的会话表。
-RR	<释放刷新>	将名称释放包发送到 WINS，然后启动刷新

RemoteName	远程主机计算机名。
IP address	用点分隔的十进制表示的 IP 地址。
interval	重新显示选定的统计、每次显示之间暂停的间隔秒数。
	按 Ctrl+C 停止重新显示统计。

route命令

显示和修改本地的IP路由表

-f 删除路由表中的网络路由

-p与add命令联合使用，一条路由被添加到注册表中。

gateway 说明下一跃点的IP地址。

举例如下：

route print (等同netstat -r)

对网关地址192.168.12.1添加默认路由：

```
route add 0.0.0.0 mask 0.0.0.0 192.168.12.1
```

添加到10.41.0.0，子网掩码255.255.0.0的路由，下一跃点10.27.0.1

```
route add 10.41.0.0 mask 255.255.0.0 10.27.0.1
```

添加一条到10.41.0.0，子网掩码255.255.0.0的持久路由，下一跃点10.27.0.1

```
route -p add 10.41.0.0 mask 255.255.0.0 10.27.0.1
```

删除到达10.41.0.0 255.255.0.0的路由

```
route delete 10.41.0.0 mask 255.255.0.0
```

netsh命令

是一个命令行脚本实用程序，可用于修改计算机的网络配置。

nslookup命令

```
C:\Users\admin>nslookup /?
```

用法:

```
nslookup [-opt ...]           # 使用默认服务器的交互模式
nslookup [-opt ...] - server  # 使用 "server" 的交互模式
nslookup [-opt ...] host      # 仅查找使用默认服务器的 "host"
nslookup [-opt ...] host server # 仅查找使用 "server" 的 "host"
```

用于显示DNS查询信息，诊断和排除DNS故障。

举例说明：

非交互方式的用法

1) 应用程序的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
```

正向解析 A

```
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
```

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
```

反向解析 PTR

```
Name:ns1.isi.edu
Address:128.9.0.107      #查出的IP地址
```

交互式工作

(1) >set all：列出当前设置的默认选项

(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
```

(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) ls

(5) set type : 该命令的作用是设置查询的资源记录类型。

A (域名到IP地址的映射)

PTR (IP地址到域名的映射)

MX (邮件服务器及优先级)

CNAM (别名)

NS (区域的授权服务器)

用set all命令显示默认设置。

(6) set type=any 显示各种可用的信息资源记录

A、CNAME、MX、NS、PTR、SOA、SRV等。

net命令 , windows中的网络服务都使用以net开头的命令 , 在cmd提示符下输入net /?

```
C:\Users\admin>net /?
```

此命令的语法是:

NET

```
[ ACCOUNTS | COMPUTER | CONFIG | CONTINUE | FILE | GROUP | HELP |  
  HELPMMSG | LOCALGROUP | PAUSE | SESSION | SHARE | START |  
  STATISTICS | STOP | TIME | USE | USER | VIEW ]
```

net命令的例子

c:\>net user : 显示所有用户的列表。

c:\>net share : 显示共享资源。

c:\>net start : 显示已经启动的服务列表

c:\>net start telnet : 启动telnet服务。

c:\>net stop telnet : 停止telnet服务。

c:\>net use : 显示已经建立的网络连接。

网络监视和管理工具

最常见的网络监视工具有 , Sniffer、NetXray和Ethereal , Sniffer功能最强 , 使用普遍。

把网卡设置为混杂模式 (Promiscuous Mode) 它就能接收所有分组 , 无论是不是发送给自己的。

混杂模式可以被检查出来的 : 1、一种是根据时延来判断。2、另一种方法是使用错误的MAC地址和正确

进行ARP欺骗的计算机必定把网卡设为混杂模式, 所以检测那些滥用混杂模式的计算是很重要的。

嗅探器 (Sniffer) 就是采用混杂模式工作的协议分析器, 可以用纯软件实现, 运行在普通的计算机上; 也可以做成硬件, 用独立的设备实现高效率网络监控。

这里可以选择用于监控的网卡, 将其置于混杂模式

Network : 显示网络利用率等统计信息。

Detail Errors : 显示出错统计信息。

Size Distribution : 显示各种不同大小分组数的统计信息。

HP OpenView 有多个功能套件组成, 形成了一个网络管理和系统管理为一体的完整系统。

IBM Tivoli NetView是IBM公司的网络管理工具, 提供整个网路环境的完整视图, 实现网络产品的管理。

CiscoWorks for Windows是基于Web的网络管理解决方案, 主要应用于中小企业网络, 提供了一套功能强大、价格低廉且易于使用的监控和配置工具, 用于管理Cisco的交换机, 路由器、集线器、防火墙和访问服务器等设备。

廉价磁盘冗余阵列 (RAID)

RAID 0需要两个以上硬盘 驱动器, 不能用于对数据稳定性要求高的场合。如果进行图像编辑, 或其他要求传输速度比较高的场合, 使用RAID0比较合适。RAID0速度最快, 利用率100%

RAID 1具有磁盘镜像功能, 并利用并行读写特性将数据分块并同时写入主磁盘和镜像盘, 利用率50%。

RAID 1容错能力强, 并具有热替换功能。

RAID 2 和RAID 3已经淘汰。

RAID 5利用率 $(n-1)/n$

RAID 0+1 利用率50%

RAID 0+1适用于既有大量数据需要存取, 又对数据安全性有严格要求的领域, 例如: 银行, 金融, 商业超市、仓储库房和各种档案管理。

实际应用中最常见的是RAID 0 RAID1 RAID5 RAID10 RAID2~4已经退出市场, 一般认为用于开发研究。

直连式存储

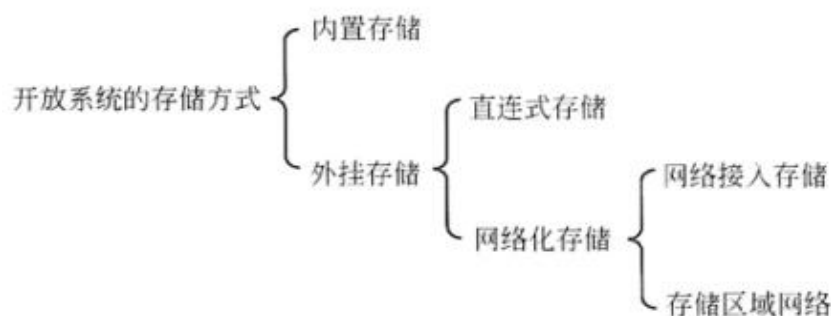


图 11-72 存储系统的分类



图 11-73 DAS

网络接入存储（NAS）是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。

存储区域网络（SAN）是一种连接存储设备和存储管理子系统的专用网络，专门提供数据存储和管理功能。

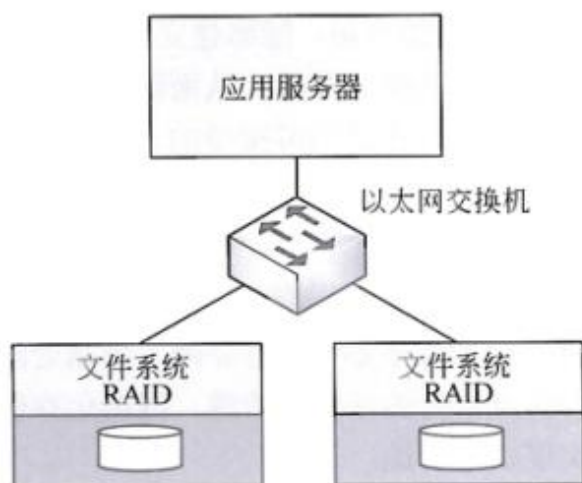


图 11-74 NAS 的体系结构

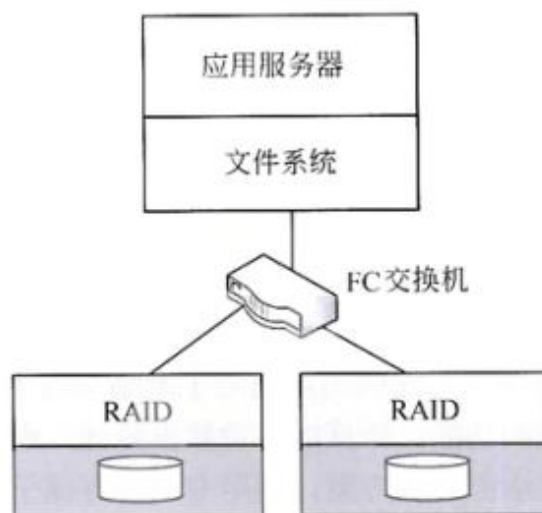


图 11-75 SAN 拓扑结构

第12章 网络规划和设计

笔记本: 网络工程师学习

创建时间: 2015/1/21 11:51

更新时间: 2015/1/21 11:54

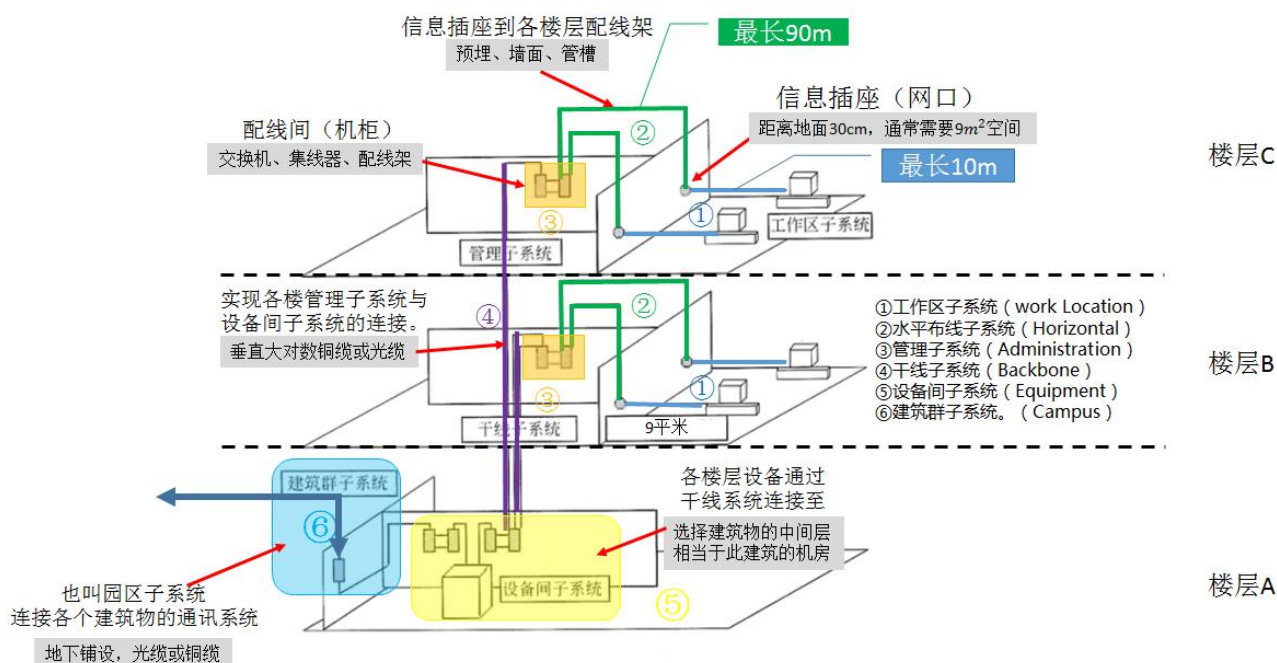
URL: about:blank

结构化布线系统

- 1、建筑物综合布线系统 (Premises Distribution System , PDS)
- 2、智能大厦布线系统 (Intelligent Building Systme , IBS)
- 3、工业布线系统 (Industry Distribution System , IDS)

注意区分:
IDS 入侵检测系统
IPS 入侵防御系统

PDS分为六个子系统:



结构化布线示意图

①工作区子系统 (work Location)

小于等于10米, 信息插座, 距离地面30cm, 通常一个信息插座负责9平米空间。

②水平布线子系统 (Horizontal)

楼层配线架到信息插座, 最大90米。

③管理子系统 (Administration)

每一楼需要一个配线间 (或机柜) 用于放置交换机、集线器、配线架。

④干线子系统 (Backbone)

使用垂直大对数铜缆或光缆, 连接管理子系统和设备间子系统。

⑤设备间子系统 (Equipment)

选择建筑物的中间层 (机房)

⑥建筑群子系统。(Campus)

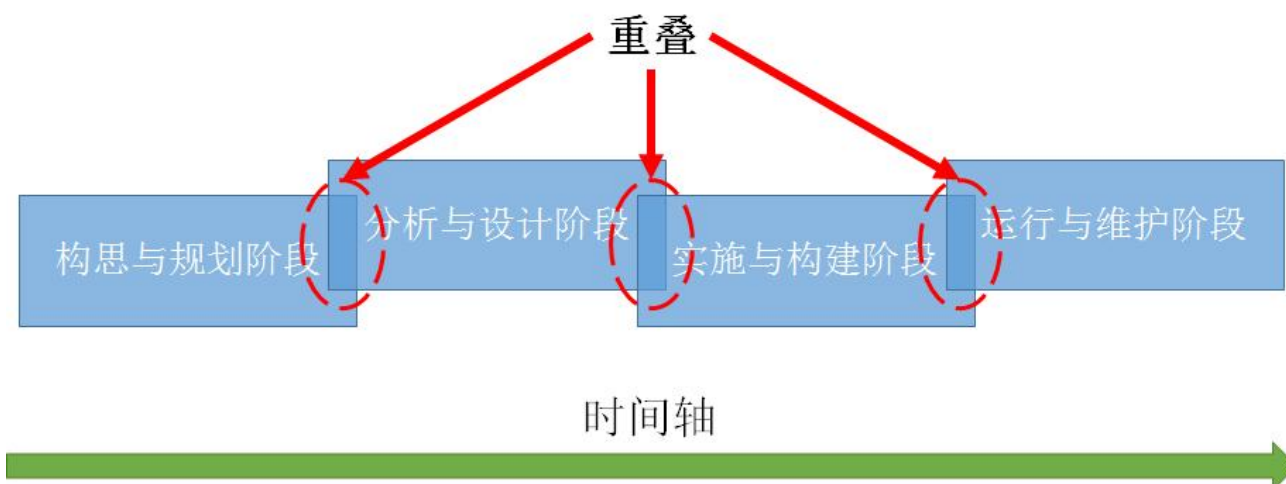
也叫园区子系统, 它是连接各个建筑物的通信系统。

网络分析与设计过程

网络系统生命周期

一个网络系统从构思开始, 到最后被淘汰的过程称为网络生命周期。

1. 四阶段周期



4个阶段分别为构思与规划阶段、分析与设计阶段、实施与构架阶段、运行与维护阶段, 4个阶段之间有一定重叠。

四阶段周期的长处在于工作成本较低、灵活性好, 适用于网络规模较小, 需求较为明确、网络结构比较简单的工程项目。

小、明、花钱少、简单、灵活

2. 五阶段周期

一次迭代划分为5个阶段。

- 1) 需求规范。
- 2) 通信规范。
- 3) 逻辑网络规范设计。
- 4) 物理网络设计。
- 5) 实施阶段。

类似软件工程中的瀑布模型。



这种方法的**优势**：所有计划在较早的阶段完成、系统负责人对系统的具体情况以及工作进度都非常清楚，更容易协调工作。

缺点：死板不灵活。用户需求发生变化，经常修改，影响工作的进程。

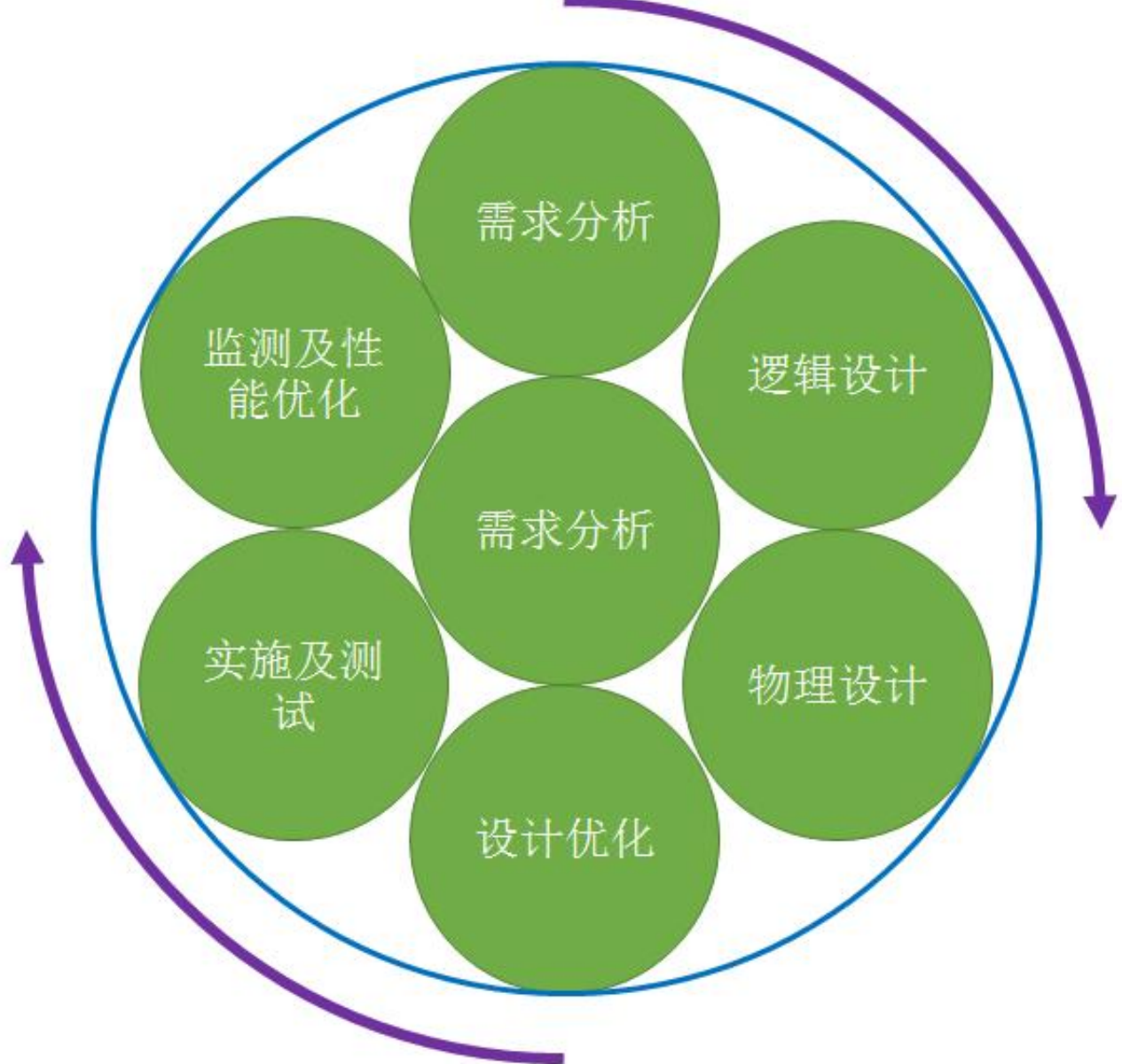
较为严谨，适用于网络规模较大、需求较为明确，需求改变较小的网路工程。

大、明、看瀑布死板、变化小。

3.六阶段周期

在五阶段周期的实施阶段后增加了**测试和优化**。

需求分析、逻辑设计、物理设计、设计优化、实施及测试、监测及性能优化。



六阶段

六阶段周期偏重于网络的测试和优化，侧重于网络需求的不断变更，由于其严格的逻辑设计和物理设计规范，使得这种模式适合于大型网络的建设工作。

网络开发过程。

例如：在网络建设初期，由于网络规模比较小，因此第一次迭代周期的开发工作应采用四阶段模式。随着应用的发展，需要基于初期建成的网络进行全面的网络升级，可以在第二次迭代周期中采用五阶段或六阶段的模式。

根据**五阶段迭代周期模型**，网络开发划分为：

需求分析。

现有网络体系分析，即通信规范分析。

确定网络逻辑结构，即逻辑网络设计。

确定网络物理结构，即物理网络设计。

安装和维护。

1) 需求分析

收集需求规范:

- ①业务需求
- ②用户需求
- ③应用需求
- ④计算机平台需求
- ⑤网络通信需求。

产生一份 **需求说明书**

2) 现有网络系统的分析。

包括:

- ①现有网络的拓扑结构
- ②现有网络的容量, 以及新网络所需的通信量和通信模式
- ③详细统计数据, 直接反映现有网络性能的测量值
- ④Internet接口和广域网提供的服务质量报告
- ⑤限制因素列表, 例如使用线缆和设备清单。

3) 确定逻辑网络结构

包括:

- ①网络逻辑设计图
- ②IP地址分配方案
- ③安全管理方案
- ④具体的软/硬件、广域网连接设备和基本的网络服务。
- ⑤照片和培训网络员工的具体说明。
- ⑥对软/硬件费用、服务提供费用及员工和培训费用的初步估计。

4) 确定网络物理结构

包括:

- ①网络物理结构图和布线方案
- ②设备和部件的详细列表清单
- ③软/硬件和安装费用的估算
- ④安装日程表, 详细说明服务时间以及期限
- ⑤安装后的测试计划
- ⑥用户的培训计划

5) 安装和维护

必须准备好人员、培训、服务和协议等资源。

网络设计的约束因素

1、来自于政策。2、预算。3、时间。4、应用目标。

需求分析的规范

- 1、业务需求
- 2、用户需求
- 1) 观察和问卷调查
- 2) 集中访谈
- 3) 采访关键人物
- 3、应用需求
- 4、计算机平台需求

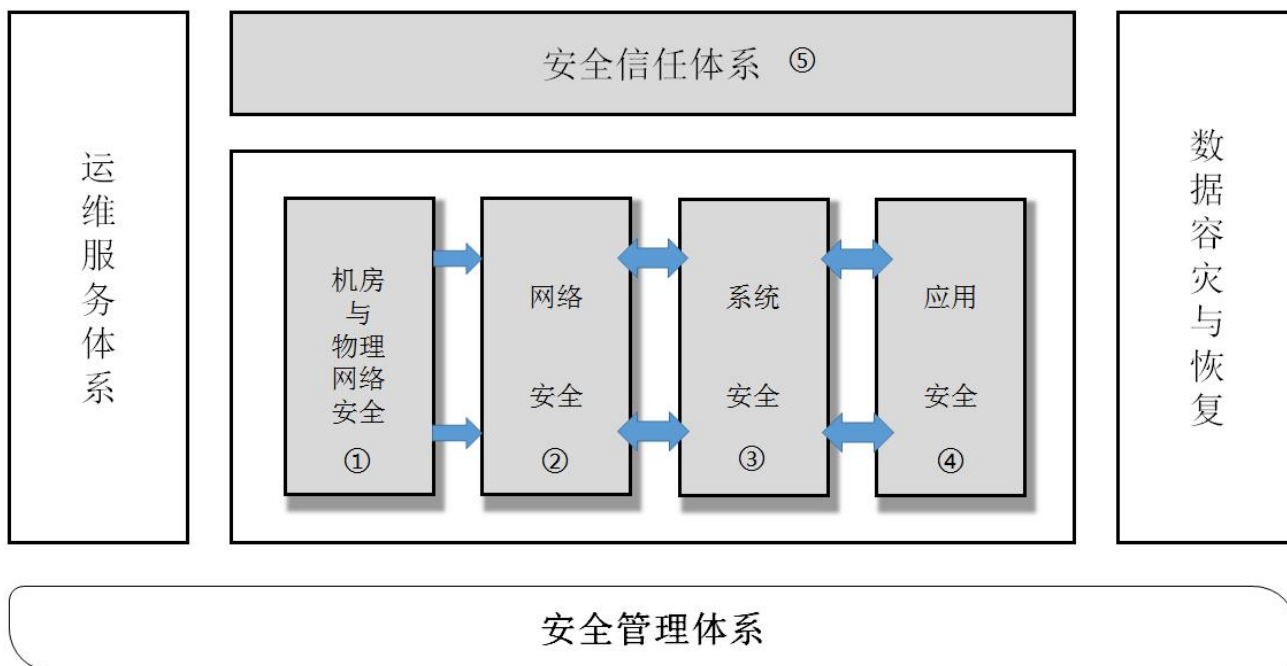
5、网络需求。

6) 网络安全需求

安全技术措施包括：

- ①机房及物理线路安全
- ②网络安全
- ③系统安全
- ④应用安全
- ⑤安全信任体系

请手抄此图熟悉内容

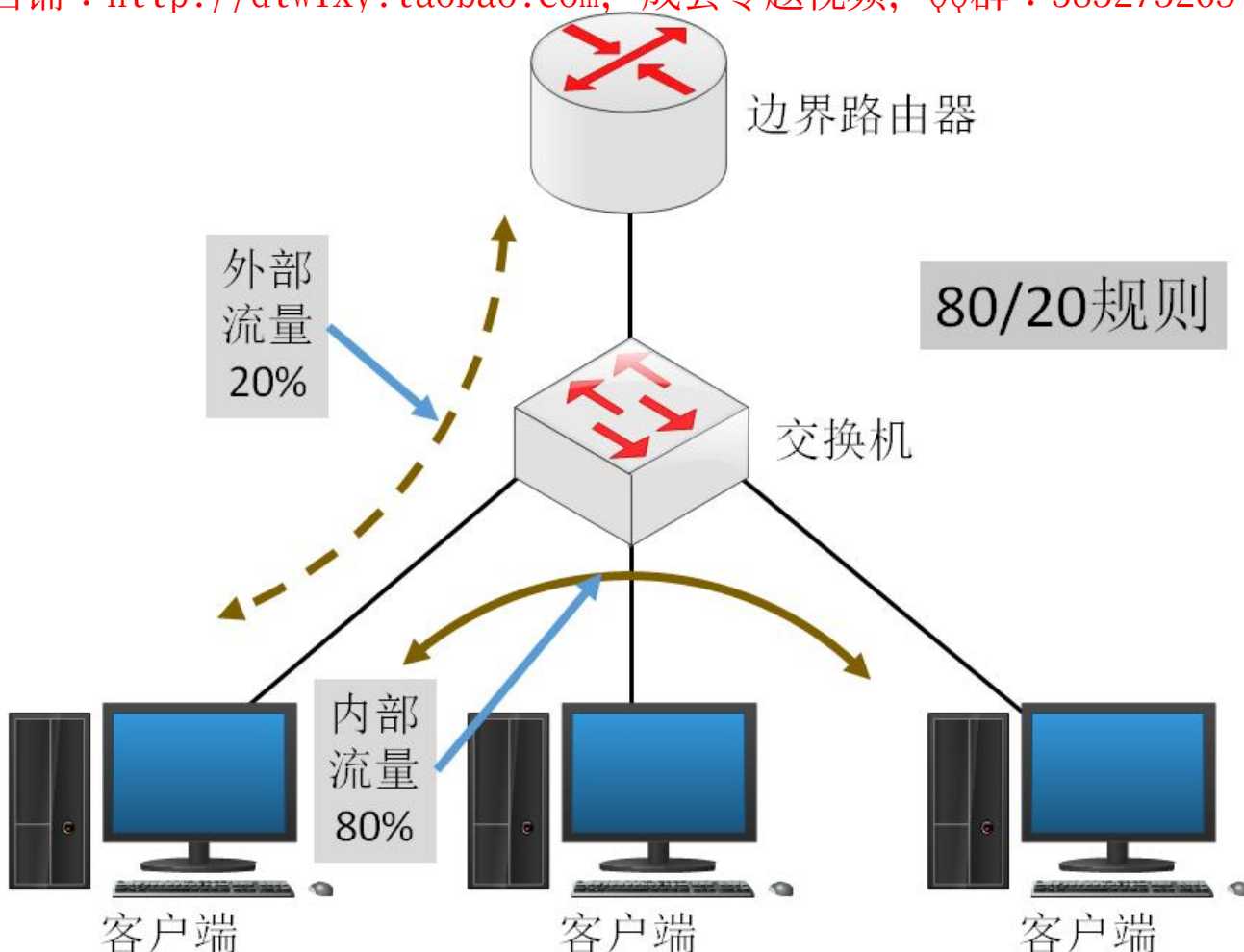


通信流量分析

例如80/20规则，或20/80规则等。

80/20规则是传统网络中广泛应用的一般规则。80/20规则适用与内部交流多，外部访问相对较少。

20/80规则，认为20%是网段内部的流量，而80%是网段外部的流量。



逻辑网络设计：

包括：

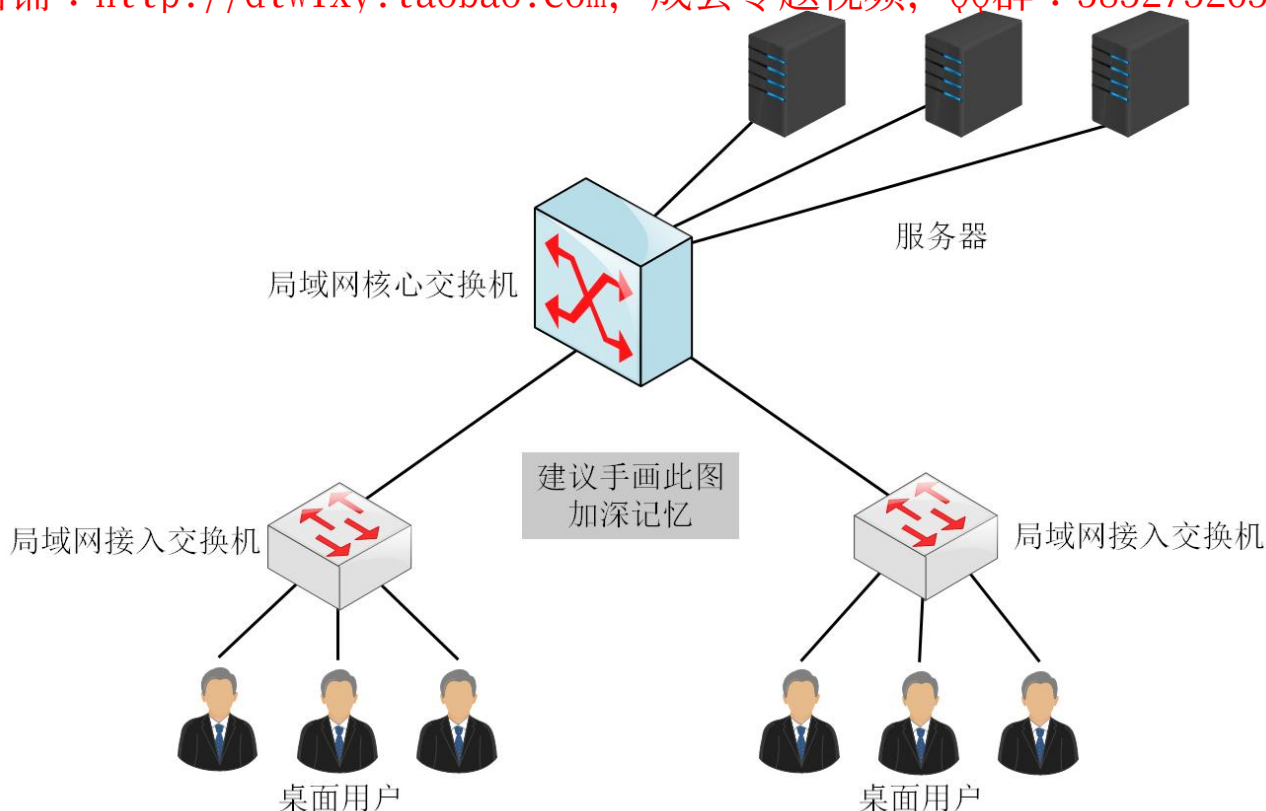
- 1) 网络结构的设计
- 2) 物理层技术的选择
- 3) 物理网技术的选择
- 4) 广域网技术的选择与应用
- 5) 地址设计和命名模型
- 6) 路由选择协议
- 7) 网络管理
- 8) 网络安全
- 9) 逻辑网络设计文档

网络结构设计：

- 1、局域网主要讨论数据链路层的设备互连方式
- 2、广域网结构主要讨论网络层的设备互联方式

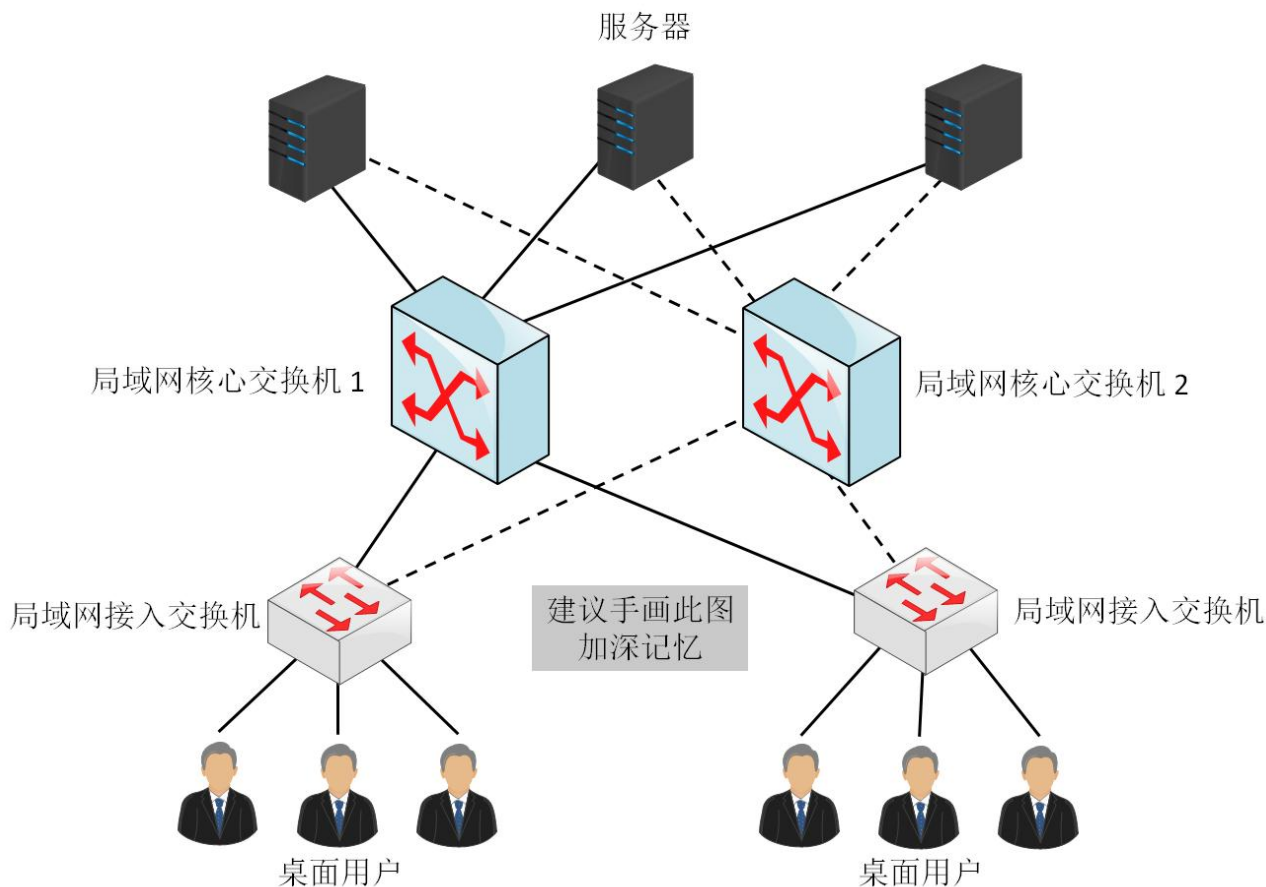
核心局域网结构

采用二层、三层交换机或多层交换机。



双核心局域网结构：

采用三层或多层交换机，核心交换机之间运行特定的网关保护或负载均衡协议，例如：HSRP、VRRP和GLBP等。

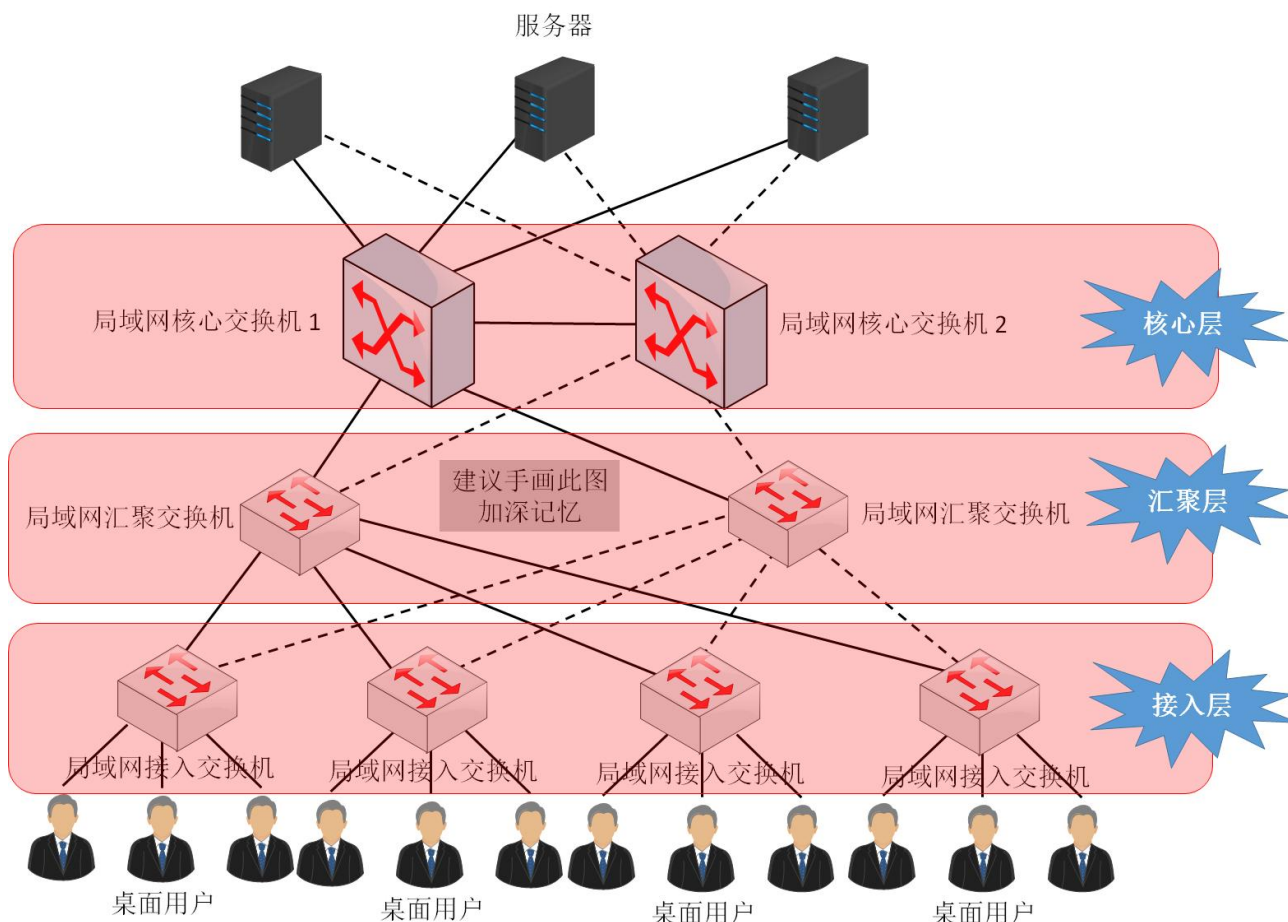


环形局域网结构

双RPR

层次局域网结构

1) 核心层 2) 汇聚层 3) 接入层



核心层实现**高速数据转发**。

汇聚层实现丰富的接口和接入层之间的互访控制 (**策略控制**)

接入层实现**用户接入**

层次化网络设计。

进过可用性和性能优化的高端路由器和交换机组成的**核心层**。

用于实现策略的路由器和交换机构成的**汇聚层**。

用于连接用户的低端交换机构成**接入层**。

层次化优点：

可以使网络成本降到最低。

设计中可以采用不同层次上的模块化

改变变得更加容易

网络冗余设计。

主要目标：一个是备用路径 (**冗余备份**)，另一个是**负载分担**。

广域网络技术

传统的PSTN接入技术

PSTN接入技术主要使用两种协议，分别为PPP和SLIP，其中SLIP（串行线路网际协议）只能为TCP/IP提供通道。

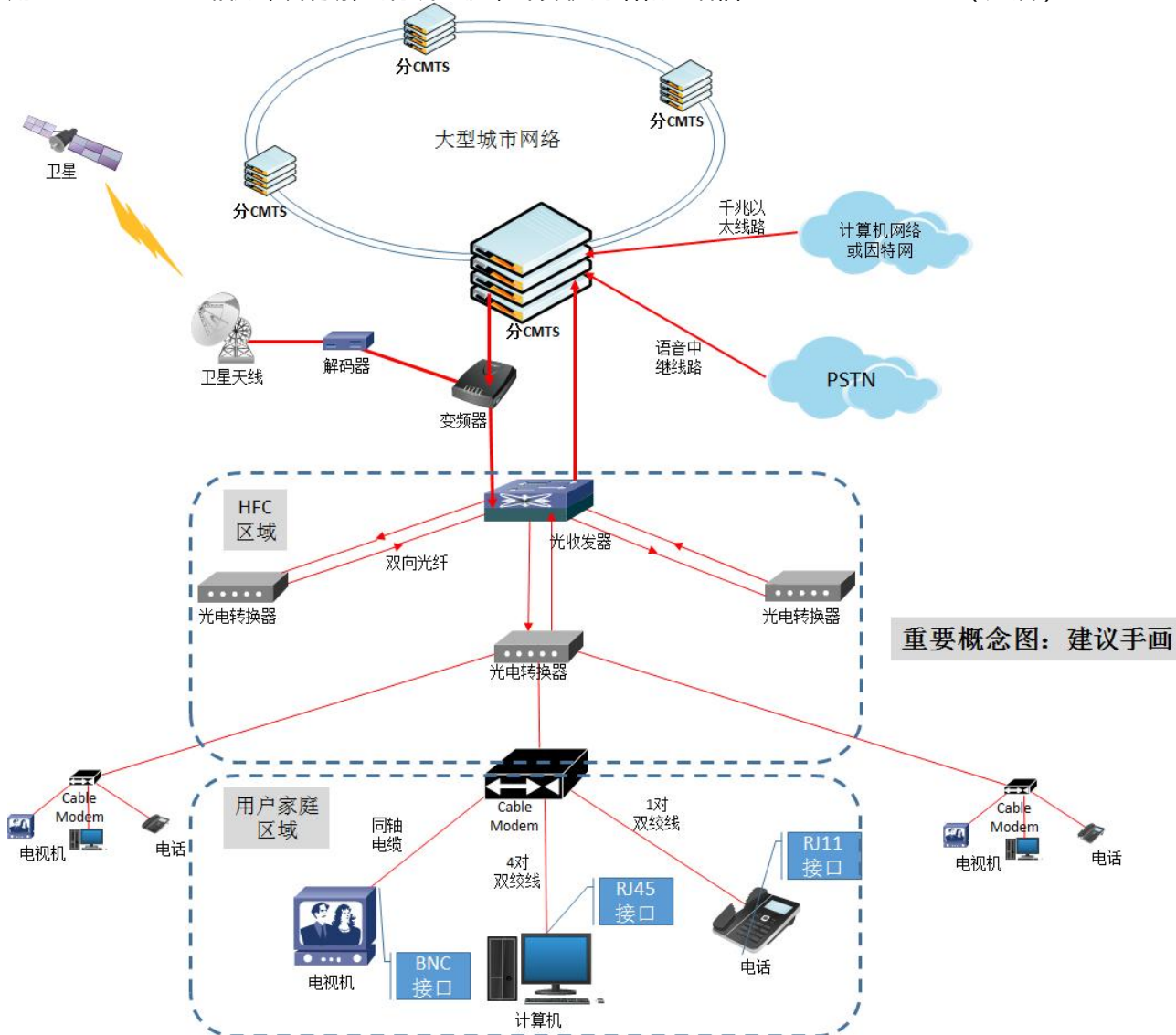
综合业务数据网 (ISDN)

- 1、基本速率接口主要用于个人用户的远程接入 (144K)
- 2、基群速率接口主要用于企业或者团体的接入 (1.984M)

线缆调制解调器接入

线缆调制解调器运行在有线电视 (CATV), 典型的CATV提供25~50Mbps的下行和2~3Mbps的上行带宽。

光纤/铜缆 (Hybrid Fiber/Coax, HFC), 依赖运营商的线缆调制解调器终结设备 (CMTS)。客户端采用 Cable Modem相连, 并分解出有线电视, 计算机网络和电话信号。Cable Modem (大猫)。



数字用户线路远程接入

数字用户线路 (Digital Subscriber Line, DSL), 通过电话线提供高速数据传输。

ADSL, 非对称DSL, 1.544~9Mbps的高速下行信道。ADSL Modem (小猫)

HDSL

VDSL, 甚高比特率DSL (下行58M)

非对称数字用户线路记忆口诀:

RCAV, 日产AV

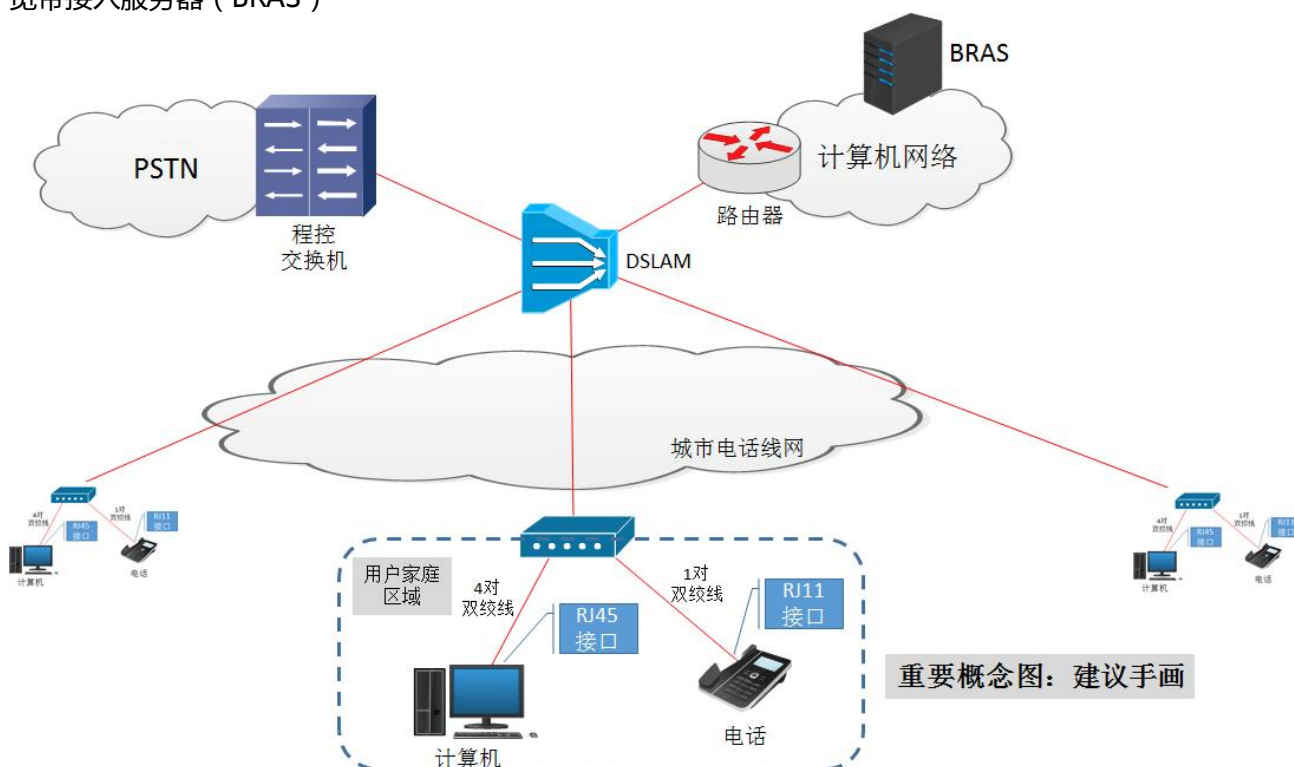
RDSL

CDSL

ADSL

VDSL

宽带接入服务器 (BRAS)



重要概念图: 建议手画

- 广域网接入
- 1、PSTN
 - 2、ISDN
 - 3、CATV
 - 4、ADSL

(笔记24 PDF 702页)

广域网互联技术

1、数字数据网 (Digital Data Network , DDN)

2、SDH (Synchronous Digital Hierarchy , 同步数字体系)

同步光网络 (SONET))

SDH网络是基于光纤的同步数字传输网络, 采用分组交换和时分复用 (TDM) 技术。

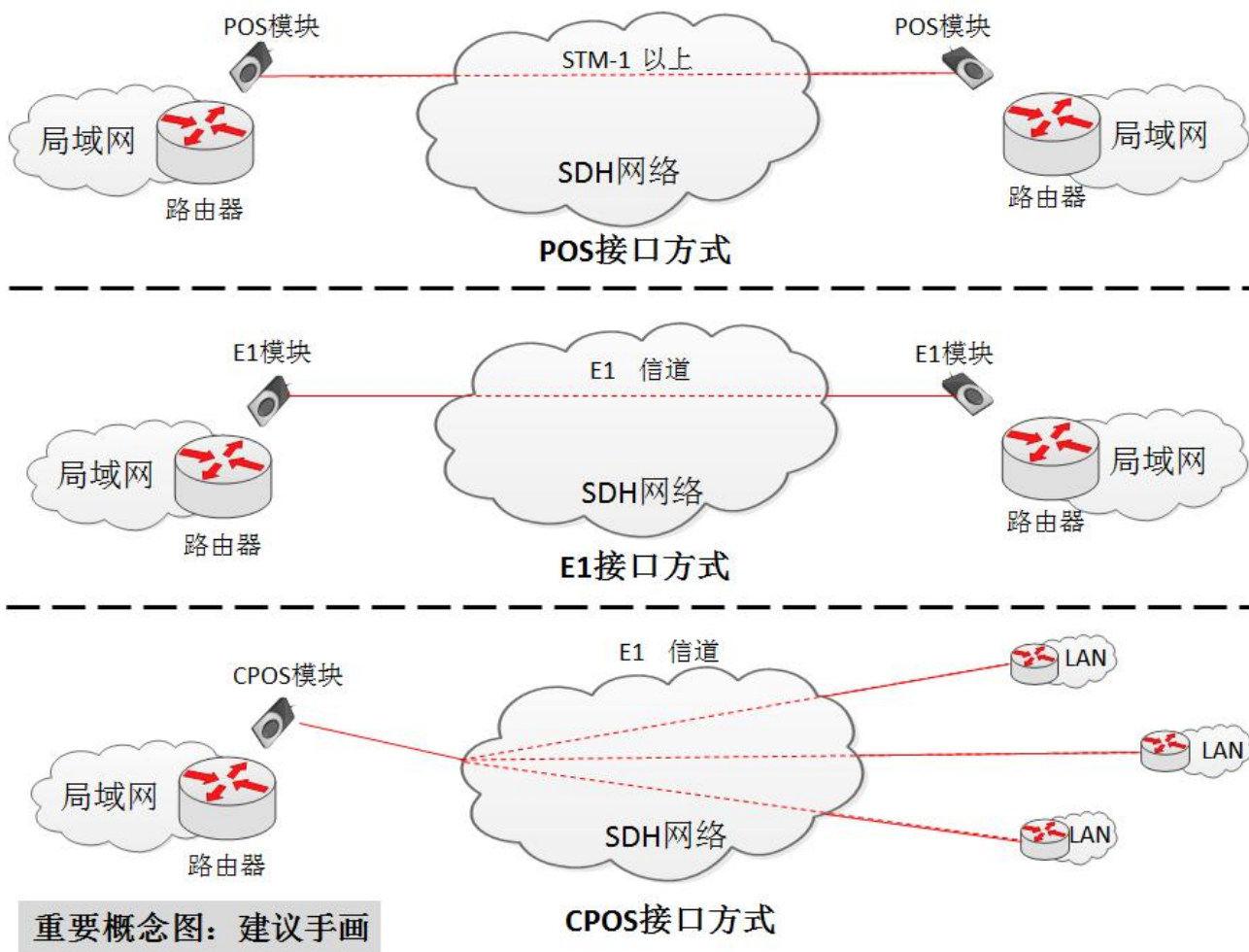
STM-1的传输速率为155.520Mbps。(相当于OC-3的速率)

SDH是主要的广域网互联技术, 利用运营商的SDH网络实现互联, 可以采用两种方式, 分别是IP VOER SDH和PDH兼容方式。

①IP over SDH, 接口主要是POS接口, 该接口可以提供STM-1及以上的速率。

②准同步数字系列 (PDH) 兼容方式, 63个E1信道, 同时向63个用户提供2Mbps接入速率。提供两种方式接口, 一是传统E1接口, 二是封装的多个E1的CPOS。

通过所SDH网络实现网络互连:



3、MSTP

SDH的多业务传送平台 (Multi-Service Transpotr Plarfom , MSTP)

4、传统VPN技术

虚拟专用网络, 二层协议主要是对传统拨号协议PPP的扩展, 典型协议为L2TP。

典型的三层协议包括IPSec和GRE, 其中, IPSec主要在IP协议上实现封装, GRE是一种规范, 可以适用于多种协议的封装。

5、MPLS VPN技术

MPLS技术主要为了提高路由器转发速度而提出的。其核心思想是利用标签交换取代复杂路由运算和路由交换。核心是在IP数据包之外封装一个32位的MPLS包头 (属于2.5层)

典型MPLS VPN平台主要设备: ①P设备。②PE设备。③CE设备。

P (Provider Router) 路由器是MPLS核心网中的路由器, 这些路由器只负责依据MPLS标签转发。

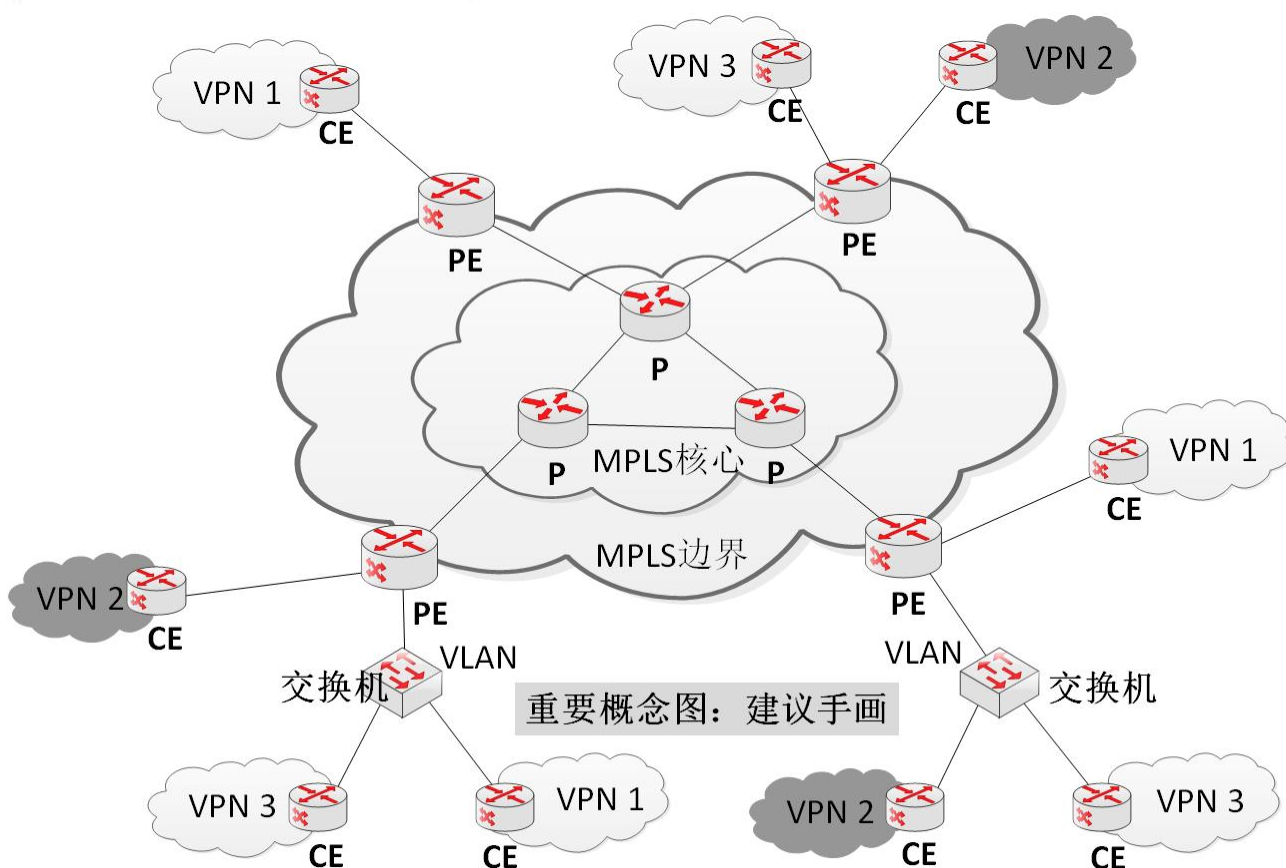
关键字: 高速转发

PE (Provider Router) 路由器是MPLS核心网上的边缘路由器与用户CE路由器互连, PE设备负责待传送数据包的MPLS标签的生成和弹出。

关键字: 标签生成

CE (Custom Edge) 路由器是直接和电信运营商相连的用户端路由器。

关键字: 连客户端



网络故障诊断与故障排除工具。

排除工具分三类: 1、设备或系统诊断命令、2、网络管理工具。3、专用故障排除工具。

诊断命令:

show、debug、ping、trace。

网络管理工具: Cisco Works、HP Open View)

故障排除工具: 欧姆表、数字万用表及电缆测试器。

时域反射计与光时域反射计。

时域反射计 (Time Oomain Reflectors , TDR) 测试电缆。

光纤测试, 使用光时域反射计 (Optical Time Domain Reflectors , OTDR)

断接盒、只能测试盘和位/数据块错误测试器。

网络监视器。

网络分析仪也称为协议分析仪 (protocol analyzer)

物理层及其诊断

show interface命令，参考 连线，指示灯。

数据链路层及其诊断

使用show命令查看

网络层及其整段

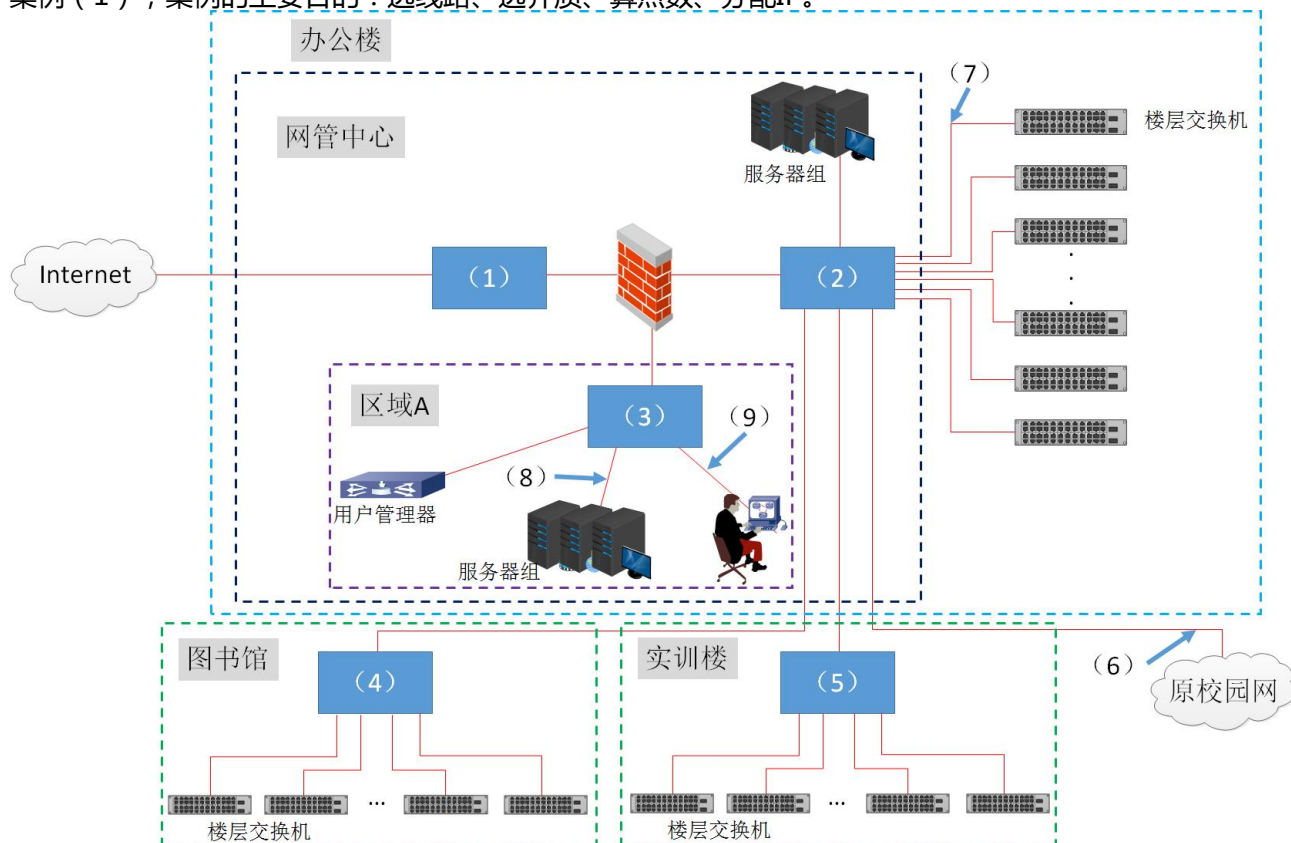
show ip route

应用层及其诊断

show run ping

网络规划案例

案例（1），案例的主要目的：选线路、选介质、算点数、分配IP。



问题1，设备选型的基本原则：

根据实际要求和市场供应情况，选择技术上先进的、可靠的、性能好的，管理性强的，灵活性高，扩展性好，安全，支持QoS的，性价比高的。

问题2，从表中为上图（1）～（5）处选择合适的设备，将设备名称写在答题纸的相应位置。

设备表

设备类型	设备名称	数量	性能描述
路由器	Router1	1	模块化接入，固定的广域网接口+可选广域网接口，固定的局域网接口 100/1000Base-T/TX
交换机	Switch1	1	交换容量：1.2T，转发性能：285Mpps，可支持接口类型：100/1000 BaseT、GE、10GE，电源冗余：1+1
	Switch2	1	交换容量：140G，转发性能：100Mpps，可支持接口类型：GE，电源冗余：无，20 百/千兆自适应电口
	Switch3	2	交换容量：100G，转发性能：66Mpps，可支持接口类型：FE、GE，电源冗余：无，24 千兆光口

(1) 使用Router1。(2) 使用Switch1。(3) 使用Switch2。(4) (5) 使用Switch3。

问题3，对(6)~(9)处选择介质。

备选介质：

千兆双绞线 百兆双绞线 双千兆光纤链路 千兆光纤

(6) 双千兆光纤链路 (7) 千兆光纤 (8) 千兆双绞线 (9) 百兆双绞线

问题4，针对不同用户进行动态和静态IP地址配置的优点，并说明下表配置方式。

	IP 地址配置方式
邮件服务器	(静态分配)
网管 PC	(静态分配)
学生 PC	(动态分配)

静态分配IP地址的优点(是指给每一台计算机都分配一个固定的IP地址)，便于管理，不需要从DHCP获取地址，节省联网时间。

动态分配IP地址的优点：减少管理员的工作量，减少输入错误，避免IP地址冲突，当网络更改设置时，不需要重新配置每台计算机的IP，当计算机在多个区域变换时，不需要重新配置IP。

问题5，采用什么策略方式静态IP被盗用？

采用IP-MAC地址绑定的策略，或在IP-MAC绑定的基础增加交换机端口的绑定。

问题6，区域A是什么区？

答：DMZ区

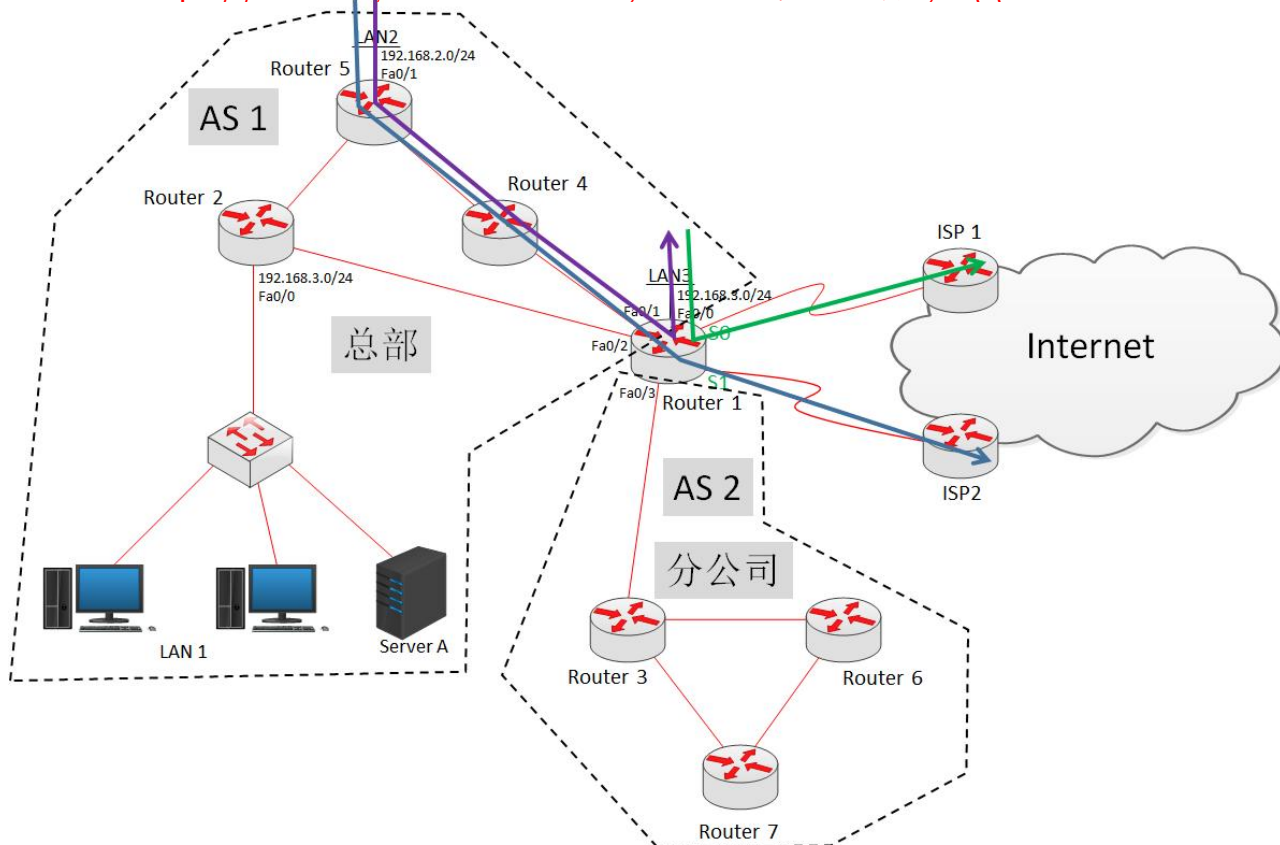
那些服务器放入DMZ中？

邮件服务器，电子商务系统和应用网关，既要外网访问，又要内网访问的要保障他们的安全性。参考答案：

(6) 区域 A 是 DMZ 区域。区域 A 中放置邮件服务器、应用网关、电子商务系统；内网中放置存储学校机密数据的服务器、存储资源代码的 PC 和存储私人信息的 PC。

DMZ (Demilitarized Zone) 可以理解为一个不同于外网或内网的特殊网络区域。DMZ 内通常放置一些不含机密信息的公用服务器，例如 Web、Mail 和 FTP 等。这样，来自外网的访问者可以访问 DMZ 中的服务，但不可能接触到存放在内网中的公司机密或私人信息等。即使 DMZ 中服务器受到破坏，也不会对内网中的机密信息造成影响。

案例2，拓扑如图：



分公司 (AS 2) 采用 OSPF, 总公司 (AS 1) 采用 RIPv2 路由协议。有两个出口 S0 连接 ISP 1, S1 连接 ISP 2。

注意各路由器标注有 IP 地址的端口。

【问题 1】

与 Router2 连接的局域网 LAN 1 是一个末节网络, 而且已接近饱和, 为了减少流量, 需要过滤进入 LAN 1 的路由更新, 可以采用什么方法实现? 请写出配置过程。

【问题 2】

LAN 2 中的计算机不需要访问 LAN 3 中的计算机, 为了进一步控制流量, 网络管理员决定通过访问控制列表阻止 192.168.2.0/24 网络中的主机访问 192.168.3.0/24 网络, 请问应将访问控制列表设置在哪个路由器上? 如何配置?

【问题 3】

如果希望采用策略路由将来自 192.168.3.0/24 网络去往 Internet 的数据流转发到 ISP1, 将来自 192.168.2.0/24 网络去往 Internet 的数据流转发到 ISP2, 应如何配置?

【问题 4】

要求自治系统 1 中的路由器 Router2 能学习到自治系统 2 (OSPF 网络) 中的路由信息, 同时 Router3 也能学习到自治系统 1 中的路由信息, 应采用什么方法? 请写出配置过程。

需要过滤进入 LAN1 的路由更新, 可以将连接 LAN1 的 Fa0/0 端口配置为被动端口, 只接收路由更新不发送路由更新。

Router(config-router)#passive-interface type number

将 Router2 的 Fa0/0 配置为被动接口。

```
Router2(config)#router rip
```

```
Router2(config-router)# passive-interface fa0/0
```

被动接口

将访问控制列表设置在Router5上。

```
Router5(config)#access list 101 deny ip 192.168.2.0 0.0.0.255 192.168.3.0 0.0.0.255
```

```
Router5(config)#access-list 101 permit ip any any
```

```
Router5(config)#int fa0/1
```

```
Router5(config-if)#ip access-group 101 in
```

标准ACL基于源地址，放置在目的端
扩展ACL基于目的地址，放置在源端

在Router1上配置策略路由：

```
Router1(config)#access list 1 permit 192.168.3.0 0.0.0.255
```

定义ACL抓取流量

```
Router1(config)#access-list 1 permit 192.168.2.0 0.0.0.255
```

```
Router1(config)#route-map ISP1 permit 10
```

路由映射图

```
Router1(config-route-map)#match ip address 1
```

匹配ACL

```
Router1(config-route-map)#set interface serial 0
```

设置转发接口

```
Router1(config-route-map)#exit
```

```
Router1(config)#route-map ISP2 permit 20
```

```
Router1(config-route-map)#match ip address 2
```

匹配ACL

```
Router1(config-route-map)#set interface serial 1
```

每个路由图应用到Router1的适当接口，指进入路由器的接口

```
Router1(config)#interface fa0/0
```

```
Router1(config-if)#ip policy route-map ISP1
```

应用策略ISP1

```
Router1(config-if)#interface fa0/1
```

```
Router1(config-if)#ip policy route-map ISP2
```

应用策略ISP2

```
Router1(config-if)#interface fa0/2
```

```
Router1(config-if)#ip policy route-map ISP2
```

应用策略ISP2

在两个自治系统的边界路由器Router1上设置路由重发布（OSPF路由重发布命令）

```
Router1(config)#router ospf 101
```

```
Router1(config-router)#redistribute rip subnets
```

路由重发布

```
Router1(config-router)#network x.x.x.x wildcard area 0
```

配置RIP协议和路由重发布。

Router1(config)#router rip

Router1(config-router)#network x.x.x.x //配置多条network命令

Router1(config-router)#passive-interface fa0/3

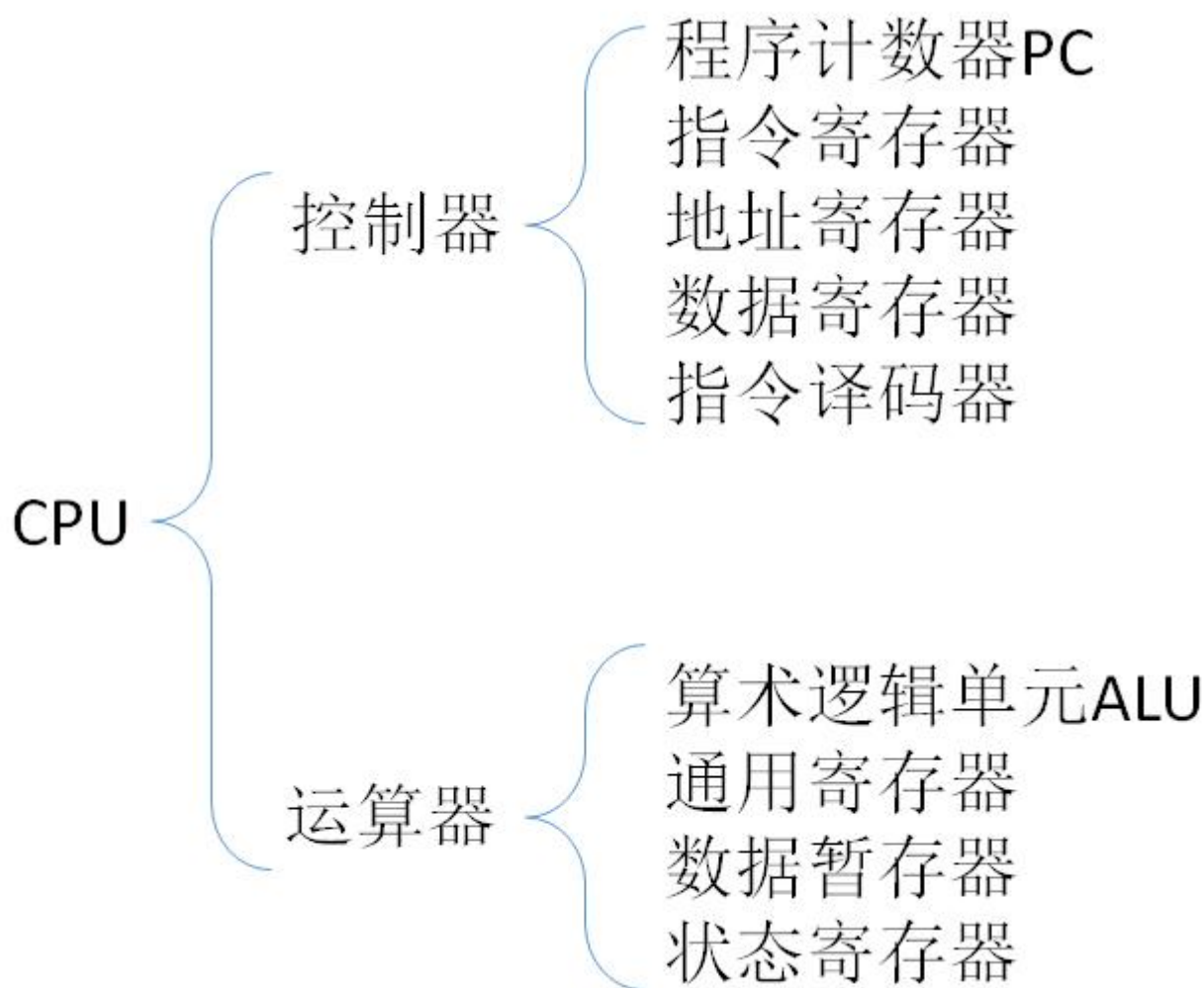
Router1(config-router)#redistribute ospf 101 match internal external 1 external 2

Router1(config-router)#default-metric 10

补充章 计算机硬件及软件

笔记本: 网络工程师学习
创建时间: 2015/1/21 11:54
URL: about:blank

更新时间: 2015/1/21 11:54



CPU是中央处理单元 (Central Processing Unit) 的缩写。

控制器由：程序计数器PC、指令寄存器IR、地址寄存器AR、数据寄存器DR、指令译码器等组成。

- (1) 程序计数器PC, 用于指出下条指令在主存中的存放地址, 也就是指向下一条指令的地址。
- (2) 指令寄存器IR
- (3) 地址寄存器AR
- (4) 数据寄存器DR
- (5) 指令译码器

运算器由算术逻辑单元ALU、通用寄存器、数据暂存器等组成, 程序状态寄存器PSW

通用寄存器: 存放操作数, 中间结果和各种地址信息。

CPU的指令系统:

- (1) 复杂指令集 (Complex Instruction Set Computer , CISC)
- (2) 精简指令集 (Reduced Instruction Set Computer , RISC)

指令的数目、 编程的便利性、 寻址方式、 指令长度、 控制器复杂性
C多R少 C灵活R不灵活 C丰富R少 C可变R等长 C复杂R简单

CISC: 复杂, 多、灵活、可变量

RISC: 简单、少、高效、等长

位: 0 和 1, 0或1是1位。

字长: CPU在单位时间内能一次处理的二进制的位数称为字长。一次处理16bit数据的CPU叫16位CPU。

缓存: 缓存位于CPU与内存之间的告诉存储器。缓存是为了解决CPU运算速度与内存读写速度之间**不匹**配的问题。

CPU→缓存→内存→硬盘

一级缓存 (L1 Cache)、二级缓存 (L2 Cache)、三级缓存 (L3 Cache)

流水线 (Pipeline) 是一种将指令分解为多个小的步骤, 如取指令、译码、执行。

若指令流水线把一条指令分为取指、分析和执行三部分, 且三部分的时间分别是 $t_{\text{取指}} = 2\text{ns}$, $t_{\text{分析}} = 2\text{ns}$, $t_{\text{执行}} = 1\text{ns}$, 则100条全部执行完毕需要多长时间?

分为两种情况:

1、顺序执行

$$(2 + 2 + 1) \times 100 = 500\text{ns}$$

2、流水线执行

$$(2 + 2 + 1) + (100 - 1) \times 2 = 5 + 198 = 203\text{ns}$$

3、其它计算方法:

最大时间 剩余两个


$$2 \times 100 + 2 + 1 = 203\text{ns}$$

加速比计算:

使用顺序执行的时间/流水执行的时间: $500/203=2.463$

内存储器的类型

- (1) 随机存取存储器 (Random Access Memory , RAM) , 断电后信息丢失。
- (2) 只读存储器 (Read Only Memory , ROM) , 信息是固定的。
- (3) 顺序存取存储器 (Sequential Access Memory , SAM) 按照某种顺序存取, 例如磁带。
- (4) 直接存取存储器 (Direct Access Memory , DAM) 直接存取, 直接指向磁盘某个磁道
- (5) 相联存储器 (Content Addressable Memory , CAM) 基于数据内容, 内容检索地址, CAM速度非常快。

若某系统内存按双字节编址 (每个字节16bit) , 地址从B5000H到DCFFFH共多少双字节? 若存储容量为16K*8bit的存储芯片构成该内存, 至少需要多少片芯片?

内存容量=最高地址-最低地址+1

若某系统内存按双字节编址(每个字节16bit), 地址从B5000H到DCFFFH共多少双字节? 若存储容量为16K*8bit的存储芯片构成该内存, 至少需要多少片芯片?

内存容量=最高地址-最低地址+1

DCFFF-B5000+1

DCFFF+1-B5000=DD000-B5000=28000(十六进制)字节B

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

将十六进制数28000转为十进制

十进制: 163840

163840/1024=160K

每字节16bit

160K*16bit, 那么容量为16K*8bit的存储芯片, 最少需要

160K*16bit/16K*8bit=20片。

数的标识与计算

原码表示法在数值前面增加了一位符号位, 通常用0表示正数, 1表示负数。8位原码的标识范围是(-127~0 0~127)共256个(2^7)。

原码:

$X_1 = +1001$ 则 $[X_1]_{\text{原}} = 01001$

$X_2 = -1001$ 则 $[X_2]_{\text{原}} = 11001$

反码:

正整数的反码就是其本身, 而负整数的反码除符号位外其余取反。

$X_1 = +1001$ 则 $[X_1]_{\text{反}} = 01001$

$X_2 = -1001$ 则 $[X_2]_{\text{反}} = 10110$

补码:

正数的补码=原码, 负数的补码是对其原码(除符号位外)按各位取反, 并在末位补加1而得到的。负数的补码就是对反码加1, 因此正数的原码、反码和补码是一样的, 网络工程师考试往往就考这些特殊的数字。(适合加减运算)

$X_1 = +1001$ 则 $[X_1]_{\text{补}} = 01001$

$X_2 = -1001$ 则 $[X_2]_{\text{补}} = 10111$

移码:

又叫增码, 是符号位取反的补码, 一般用做浮点数的阶码表示, 只用于整数。(适合浮点阶码)

$X = +1001$, 则 $[X]_{\text{补}} = 01001$, 移码 $[X]_{\text{移}} = 11001$

$X = -1001$, 则 $[X]_{\text{补}} = 10111$, 移码 $[X]_{\text{移}} = 00111$

总线分为两类: 一类是内部总线, 一类是外部总线。

内部总线包括: 数据总线、地址总线和控制总线。

外部总线包括: 并行总线、串行总线和逻辑总线。

在存储器的地址总线中, 设地址线的根数为 N , 则此地址总线可以访问的最大存储容量为 $M=2^n$ 字节, 根据需要可以进一步换算成KB和MB。

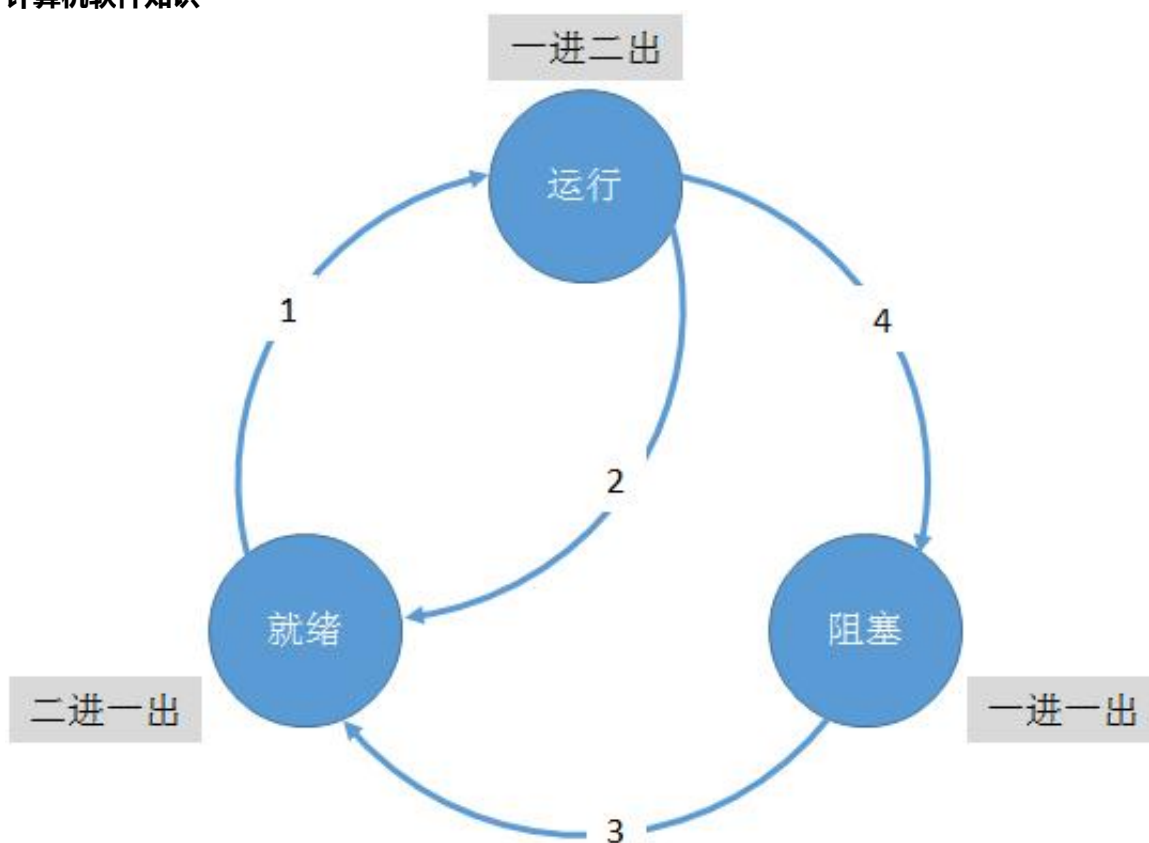
数据传输的控制方法: 程序控制方式、中断方式、DMA等。

1、程序控制方式

2、中断的控制方式, 保存现场, 简称终端

3、在DMA控制方式下, CPU初始化这个传输动作, 由DMA控制器来实行和完成, 不需要CPU参与。

计算机软件知识



进程的状态转换

在网络工程师考试中考察较多的是系统中进程资源的分配问题, 在进程的互斥资源分配过程中, 只要能在极端情况下保证各个进程都能获得其等待的资源, 而不至于死锁, 这就是系统不死锁的基本条件。

软件开发

结构化程序设计

结构化程序设计是以模块功能和详细处理过程设计为主的一种传统的程序设计思想, 通常采用由顺序、选择、循环, 三种个基本结构。

面向对象的基本概念

对象是一个程序模块, 对象提供用户希望的行为 (属性)

主要特征: (1) 继承性, (2) 多态性, (3) 封装性。

主要方法: Booch、Coad方法和OMT方法等。

德尔菲法 (Delphi Technique) 是最流行的一种专家评估技术 (头脑风暴)

UML统一建模语言

有七个描述图: 例图、类图、序列图、状态图、活动图、组件图和部署图。

开发布会、找个例子、分类、排序、画出状态和活动。
有哪些组件构成, 然后统一部署。

软件开发模型:

- 1、瀑布模型 (顺序) 像瀑布一样逐级落下。
- 2、快速原型模型, 建立一个快速原型 (样品), 迅速修改 (抛弃) 原型以反映客户需求。
- 3、增量模型, 演化模型 (样品+修改, 完工)
- 4、螺旋模型, 强调风险分析, 特别适合大型复杂的系统。
- 5、喷泉模型, 面向对象的生存期模型, 以相重叠和多次反复 (喷泉→重复)
- 6、混合模型, 几种模型混合使用。

能力成熟度模型 (Capability Maturity Model for Software CMM)

五个等级: (1) 初始级, (2) 可重复级, (3) 可定义级, (4) 可管理级 (标准衡量), (5) 优化级。

软件测试

- (1) 单元测试
- (2) 集成测试: 应用系统各个部件的联合测试。
- (3) 系统测试: 放到实际运行环境下进行测试。
- (4) 验收测试: 让系统用户决定是否接收系统。

白盒测试 (White Box Testing) 。

可以看作一个能打开, 可以看见内部结构的盒子。

黑盒测试 (Black Box Testing)

看作一个不能打开的盒子, 因此不考虑软件内部的运作原理。

项目管理基础

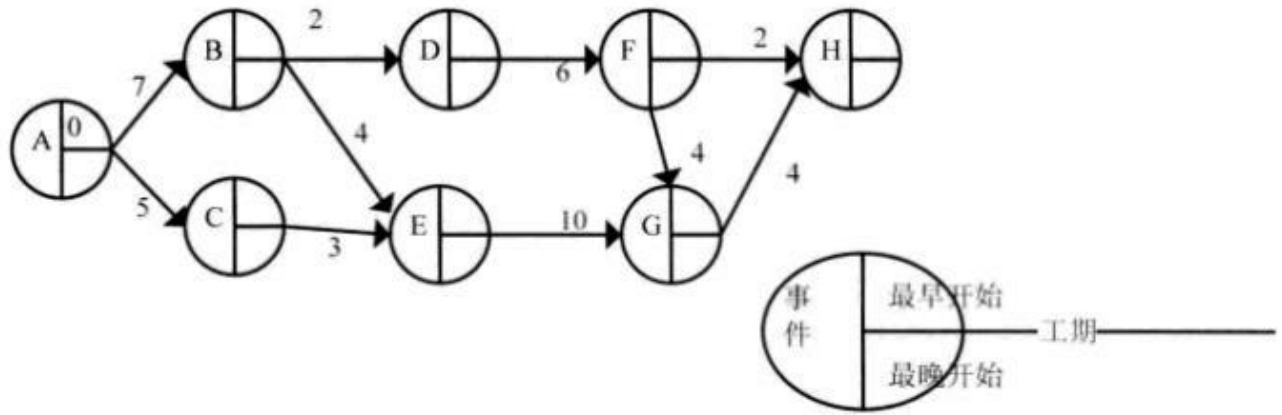
1、关键路径法 (Critical Path Method CPM) 只有项目网络中最长的或耗时最多的活动完成之后, 项目才能结束。

2、关键路径法的时间计算。

正推法.

逆推法

典型题图:



3、甘特图

基本是一条线条图，横轴表示时间，纵轴表示活动，线条表示完成情况，也可以表示子任务之间的并行和串行关系，但不能清晰描述任务之间的依赖关系，也不能清晰指出关键任务哪里。

权利保护期限：著作权中作者的署名权、修改权、保护作品完整权的保护期不受限制。作品发表后保护期为作者终生及其死后五十年，截至于作者**死亡后第五十年的12月31日**。

权利的限制：在下列情况使用作品可以不经著作权人许可，不向其支付报酬，但应当指明作者姓名和作品名称，并且不得侵犯著作权人依照本法享有的其他权利。（不盈利情况下不侵权），例如课堂教学或科学研究。