一、网络基础

1.1 基础

网络性能指标：带宽（每秒链路能传输的数据位数）、延迟；

电路交换：建立一条数据通道，可以是物理线路也可以是多路复用得到的逻辑电路；

分组交换：存储转发“包”（分组）；

1.2 OSI

应用层

表示层（处理数据格式、加密）

会话层（建立、维护、管理会话）

传输层

网路层

链路层

物理层

1.3 一般网络设备

路由器：隔离广播域

交换机：隔离冲突域

二、局域网技术

2.1 数据链路层

IEEE将数据链路层划分为LLC和MAC子层

LLC：封装和标识上层数据；

MAC：适应各种传输介质并且处理信道占用、站点标识和寻址问题；

2.2 以太网

CSMA/CD（载波监听多路访问/碰撞检测）；

以太网帧长度：64~1518B；

以太网运行模式分为半双工模式和全双工模式，半双工采用CSMA/CD，全双工没有冲突；

标准以太网（10Mbps）、快速以太网（100Mbps）、千兆以太网（1000Mbps）、万兆以太网（10000Mbps）

2.3 WLAN

WLAN：以无线信道作为传输媒介的计算机局域网（WiFi）

CSMA/CA：先侦听线路是否空闲，空闲时会继续侦听一个分布式帧间间隔（DIFS），随后发送数据帧，主机接收到数据帧后等待一个短帧间间隔（SIFS）返回ACK确认，如果没有收到ACK即重传。

三、广域网技术

3.1 概述

广域网（WAN）：连接相距遥远的局域网；

连接方式：专线方式、电路交换（PSTN、ISDN）、分组交换（X.25、帧中继、ATM）；

3.2 HDLC

异步协议：以字符为独立的信息传输单位，在每个字符的起始处开始同步，但字符与字符之间的间隔不固定；因为每个字符需要添加起始位、校验位、停止位等，所以信道利用率很低，一般用于数据速率较低场合；

同步协议：许多字符组成的数据块（帧）为传输单位；能更好的利用信道；

HDLC：一种面向比特的链路层协议，对于任意一种比特流均可以实现透明传输；

零比特填充法：发现有连续5个1出现时，在其后添插一个0；

HDLC通过周期性发送Keepalive消息探测链路对端状态；

HDLC协议只支持点到点链路、且只能用于同步链路、不支持验证；

3.3 PPP

PPP：一种点到点链路传输、封装网络层数据包的数据链路层协议；支持全双工的同步/异步链路；

特点：

1.既支持同步链路，也支持异步链路；

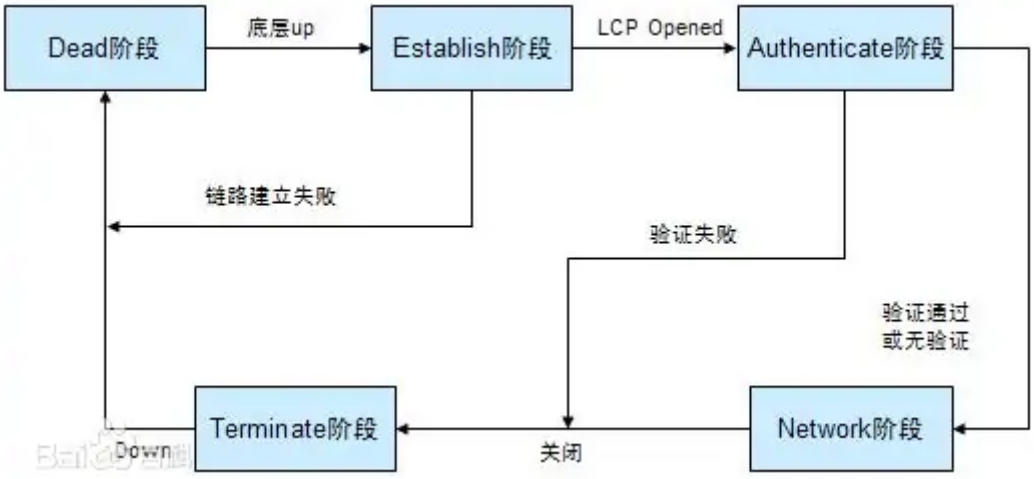
2.支持安全验证；

3.支持多种网络层协议；

4.支持IP地址的远程分配，满足拨号需求；

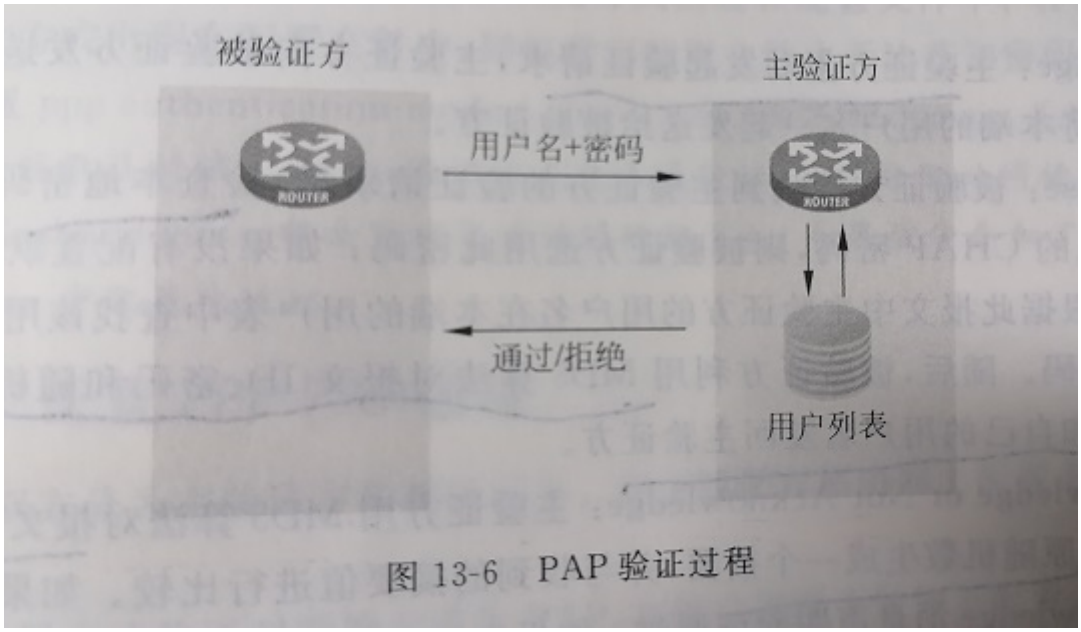
5.无重传机制，网络开销较小；

会话建立：



PAP验证：

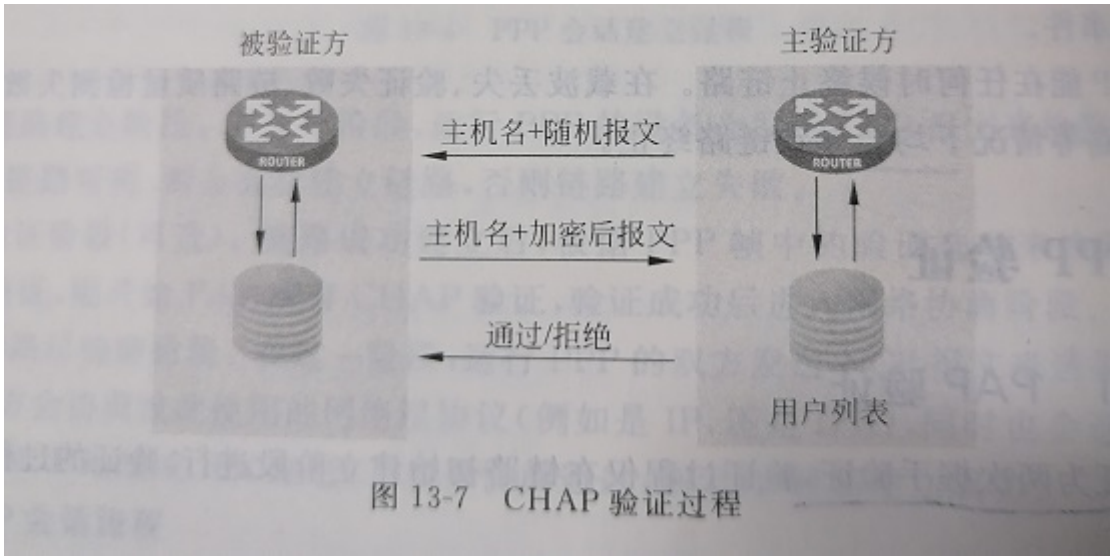
两次握手验证、密码明文传输



CHAP验证：

被验证方：使用MD5对报文ID、密码和随机报文生成摘要；

主验证方：使用MD5对报文ID、本地保存的被验证方密码、随机报文生成摘要，并比较摘要；



PPP MP

PPP MP：为了增加带宽，将多个PPP链路捆绑使用；

3.4 帧中继

帧中继：数据链路层使用简化的方法传送和交换数据单元的一种快速分组交换方式；主要用于数据业务，将数据信息以帧的形式进行传送；

DTE：数据终端设备

DCE：数据通信设备

NNI：帧中继交换机之间通过NNI接口互相连接

VC：两个需要通信的DTE接口之间的逻辑通路

PVC：永久虚电路，通过人工预先设定产生（多数情况使用PVC）；

SVC：交换虚电路，协议自动分配的虚电路；

DLCI：位于帧中继帧头中的一个编号，标识不同的VC，也称为帧中继地址；仅本地有效，即只在本地接口和与之直接相连的对端接口之间有效；

LMI：用于建立和维护帧中继DTE和DCE接口之间的连接，维护虚电路状态等；

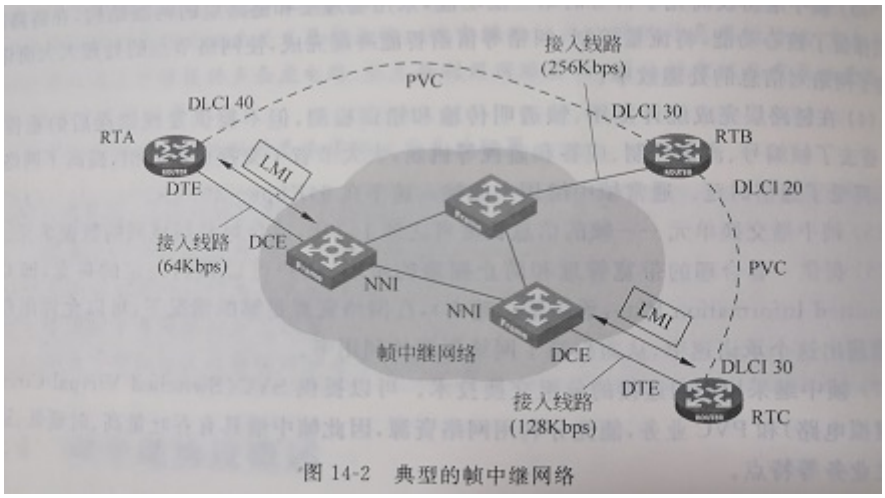


图 14-2　典型的帧中继网络

地址映射：

将对端设备的协议地址（IP）与对端设备的帧中继地址（DLCI）关联，使高层协议能够通过对端设备的协议地址寻址到对端设备；

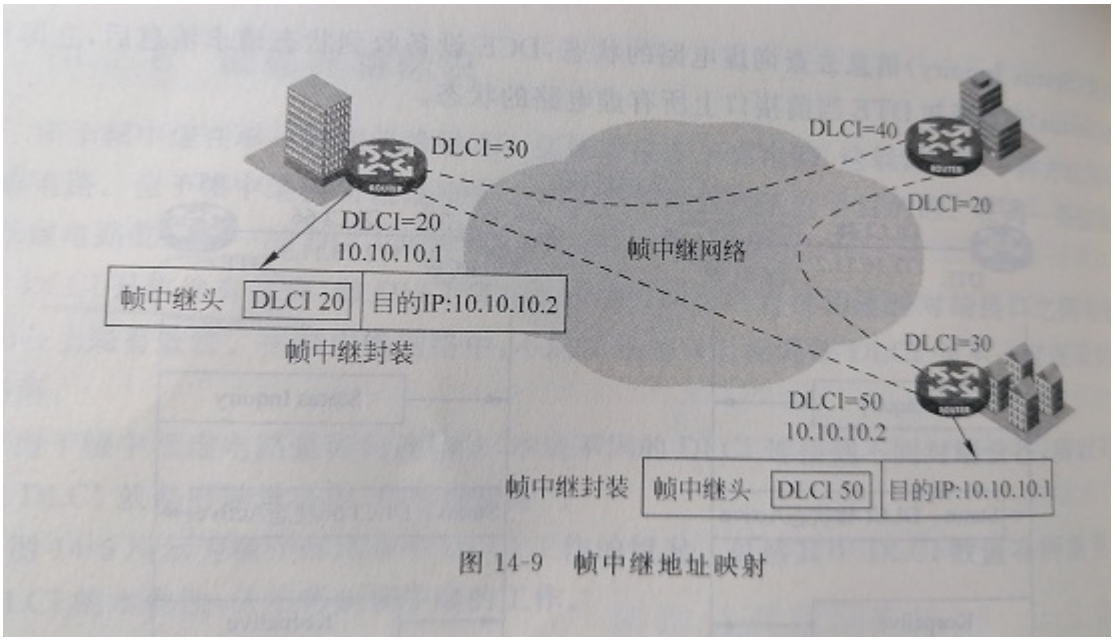


图 14-9 帧中继地址映射

Inverse ARP：

自动解析每条虚电路连接的对端设备的网络层协议地址。

发现新的虚电路时，Inverse ARP在该虚电路上发送Inverse ARP请求报文给对端，报文包含本地网络层协议地址；设备收到请求后，生成地址映射并发送Inverse ARP响应报文（发送自己的网络层地址）；

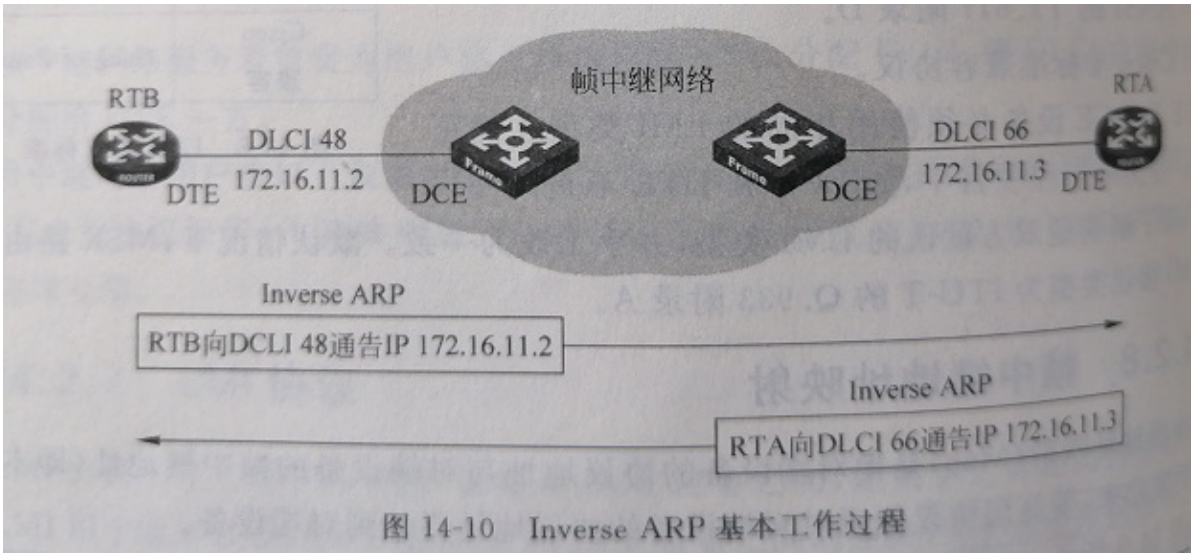


图 14-10 Inverse ARP 基本工作过程

3.5 ADSL

DSL：数字用户线路，以铜质电话线为传输介质的传输技术形成的组合；让数字信号加载到电话线路未使用频段（高频），实现在不影响语音服务的前提下在普通电话线上提供数据通信；

对称DSL：适用于大量数据传输、视频会议等，HDSL、SDSL；

非对称DSL：可以根据双绞铜线质量优劣和传输距离动态调整用户访问速度，ADSL、VDSL；

四、网络层

4.1 IP

IP地址分类：

A类：1.0.0.0~126.255.255.255

B类：128.0.0.0~191.255.255.255

C类：192.0.0.0~223.255.255.255

D类：224.0.0.0~239.255.255.255（组播地址）

IP与子网掩码计算：...

4.2 ARP&RARP

ARP：动态将IP地址解析为MAC地址

工作原理：

1.先查看自己ARP表；

2.如果表中没有相应表项，发送ARP请求报文，填上目的IP和全0的MAC地址广播出去；

3.各主机比较目的IP和自己IP，如果相同向自己ARP表中添加表项并发送ARP响应包；

4.接收到响应包，添加相应表项。

代理ARP：由路由器作为代理ARP，解析其它广播域的IP地址；

RARP：

无盘工作站广播请求报文，请求RARP服务器分配一个IP地址；

RARP服务器维护一个“MAC-IP”映射表

4.3 ICMP

...

4.4 DHCP

...

4.5 IPv6

压缩方式（了解）

五、传输层

TCP&UDP

六、应用层

6.1 FTP

FTP：采用TCP，能够用户登录

数据连接端口号：20

控制连接端口号：21

TFTP：采用UDP

6.2 DNS

...

6.3 other

SMTP：负责邮件在网络上主机之间传输

POP3/IMAP：负责把邮件从邮件服务器传输到本地邮件客户端

七、以太网交换技术

7.1 VLAN

VLAN：隔离广播域，使不同VLAN间设备不能互通，只能通过路由器等三层设备而互通；

类型：

基于端口的划分：最常用

基于MAC地址的划分：物理机移动使不用重新配置VLAN

基于协议的划分：IP、IPX

基于子网的划分：管理灵活，但耗费交换机资源较多

原理：

通过给以太网帧添加一个Tag来标记这个以太网帧能够在哪个VLAN中传播；

单交换机VLAN标签操作：

- VLAN标签由交换机端口在数据帧进入交换机时添加
- 交换机负责剥离出端口的以太网帧的VLAN标签

Access端口：只允许默认VLAN的以太网帧通过的端口

PVID：端口所属VLAN，即默认VLAN

垮交换机VLAN标签操作：

Trunk端口：不对VLAN标签进行剥离的端口；Trunk端口可以接收和发送多个VLAN的数据帧，并且不对帧中标签做任何处理；但发送帧时，Trunk端口要剥离默认VLAN帧中的标签，Trunk端口接收到不带标签帧时打上默认标签；

Hybrid端口：可以接收和发送多个VLAN数据帧，同时还能指定对任何VLAN进行剥离标签操作；当大部分主机需要隔离，但都需要与另一台主机互通时使用；

7.2 STP

STP：用于在局域网中消除数据链路层物理环路的协议；物理成环，逻辑成树；

BPDU：桥协议数据单元

根桥ID：由优先级和MAC地址组成；通过比较BPDU中根桥ID来决定谁是根桥；

根路径开销：到根桥的最小路径开销；

指定桥ID：生成或转发BPDU的桥ID；

指定端口ID：发送BPDU的端口ID；

根桥选举：

每台设备都有自己的桥ID（优先级+MAC），在比较时先比较优先级，再比较MAC（小者优先）；

网络初始化时，每台设备都认为自己是根桥，设备间交换BPDU比较桥ID，选出桥ID最小者作为根桥。

确定端口角色：

1.根桥上所有端口为指定端口（DP）；

2.为每个非根桥选择路径开销最小的端口作为根端口（RP）；

3.为每个物理段选出根路径开销最小的那个网桥作为指定桥，指定桥到物理段的端口作为DP；

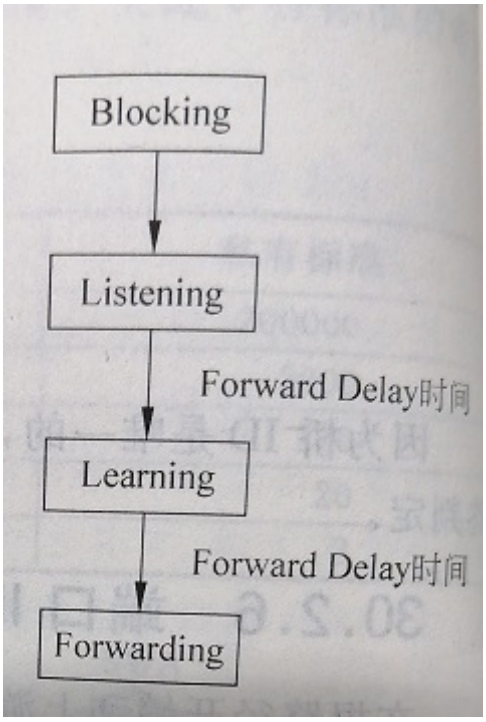
4.既不是DP也不是RP的端口作为AP，置于阻塞状态。

桥ID作用：

当一个非根桥上多个端口经过不同上游桥到达根桥，且这些路径开销相同时，比较各端口上游指定桥ID，ID小者被选举为RP；

端口状态：

从Listening迁移到Learning，或从Learning迁移到Forwarding状态都需要经过Forward Delay时间



默认Forward Delay时间为15s，所以，当一个端口被选为根端口或者指定端口后，至少需要30s后才能转发数据；

RSTP

取消了Forward Delay的非必须情况

1.端口被选为根端口；

2.指定端口是非边缘端口：向下游发送一个握手报文，询问下游网桥是否同意进入转发状态，收到报文后发现自己没有端口连接到其它网桥（即边缘网桥），返回赞同报文，此时不需要Forward Delay；但只有在点对点链路上生效；

3.指定端口是边缘端口；

MSTP

定义多个生成树实例，每个实例对应多个VLAN，每个实例维护自己的独立生成树；

7.3 链路聚合

链路聚合：多个物理以太网链路聚合在一起形成一个逻辑上的聚合端口组；

增加链路带宽、提供链路可靠性；

八、IP路由技术

8.1 概述

路由表、最长匹配原组、默认路由、优先级...

单臂路由

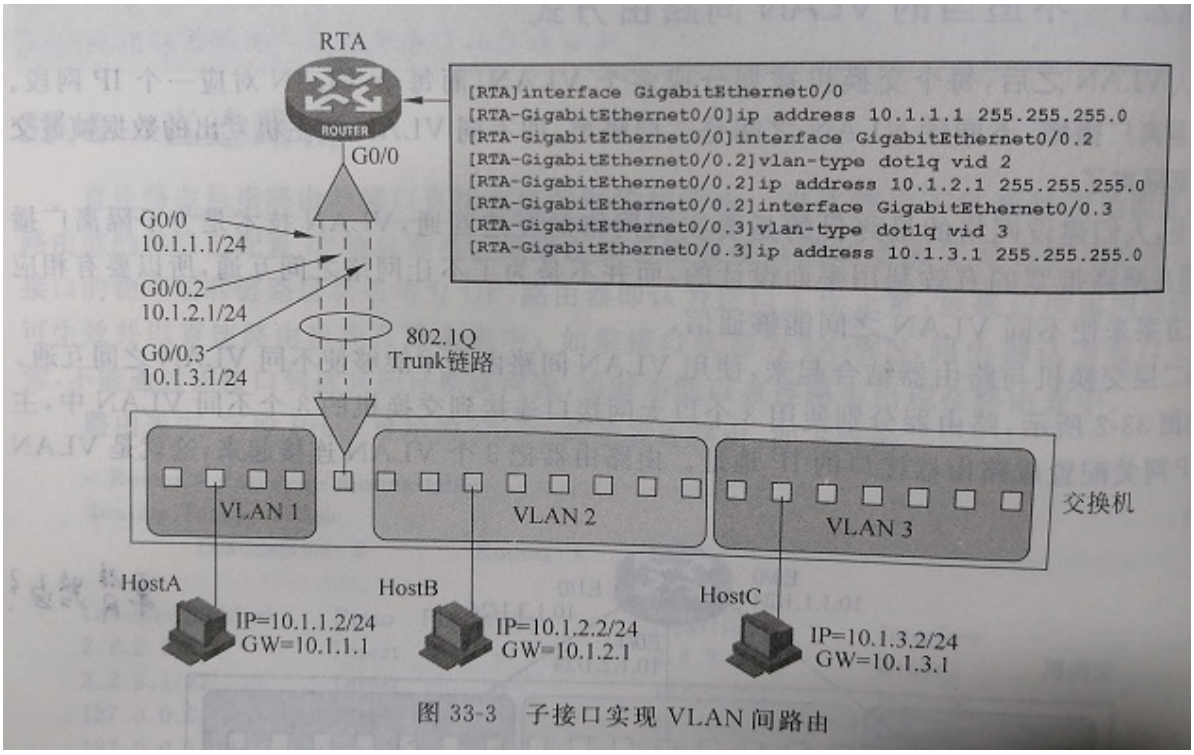


图 33-3 子接口实现 VLAN 间路由

静态黑洞路由：配置静态路由时，对应接口配置为 NULL 0；

```
ip route-static 10.0.0.0 255.255.0.0 null 0
```

8.2 RIP

路由毒化：路由器主动把路由表中发生故障的路由项以度量值无穷大（16）告诉给RIP邻居；

水平分割：RIP路由器从某个接口学到的路由，不会再从该接口发回给邻居；

毒性逆转：RIP从某个接口学到路由后，该路由度量值设置为无穷大（16），并从原接口发回给邻居；

抑制时间：当一条路由度量值变为无穷大时，该路由器将进入抑制状态；

触发更新：路由表中信息发生改变时，路由器不必等到更新周期到来，而立刻发送路由更新给相邻路由器；

RIPv2：

1.支持VLSM（可变长子网掩码）和CIDR（无类域间路由）；

2.支持组播发送更新报文；

3.支持验证；

8.3 OSPF

P116~136 几乎全是重点

九、网络安全

9.1 ACL

ACL：由一系列有顺序的规则组成；这些规则包括源地址、目的地址、端口号来定义匹配条件，并执行permit或者deny操作；

工作原理：配置在路由器接口上，且每个接口的入站方向（Inbound）和出站方向（Outbound）均可配置ACL；

工作流程：从第一条规则开始依次匹配，符合规则条件则执行相应操作，直到最后执行默认规则；

通配符掩码：反掩码

分类：

基本ACL：只根据报文源IP地址信息制定规则；

高级ACL：根据报文源IP、目的IP、协议类型等制定规则；

9.2 NAT

Basic NAT

只对数据包IP层参数进行转换；在地址池中查找公网IP，将内网IP映射到公网IP；

NAPT

对数据包的IP地址、协议类型、端口号同时进行转换；