1、 无边界交换网络的层次结构

无边界交换网络的创建要求使用喝咯的网络设计原理来确保可用性、灵活性、安全性和可管理性的最大化。

根据以下 4 个原理建立的：

1.分层（有助于理解各层中每个设备的作用，简化部署、运营和管理，并减少各层的故障域） 2.模块化（根据需要实现无缝网络的扩展和集成服务的启动）3.弹性（满足用户对始终保持网络运行的期望）4.灵活性（是用所有的网络资源来支持智能流量负载共享）

2、 分层网络模型

为什么要分层：分层网络设计需要将网络分成互相分离的层。每层提供特定的功能，这些功能界定了该层在整个网络中扮演的角色。

分层模型中包括 3 个层次：接入层、分布层、核心层。

1. 接入层的主要目的是提供一种将设备连接到网络并控制允许网络上的哪些设备进行通信的方法。
2. 分布层先汇聚接入层交换机发送的数据，再将其传输到核心层，最后发送到最终目的地。分布层上做路由及安全策略。
3. 分层设计的核心层是网际网络的高速主干。核心层也可连接到 Internet 资源。核心层作用快速转发数据包。

分层网络优点：

1.可扩展性：可以方便的扩展分层网络。

2.冗余性：核心层和分布层的冗余性确保网络的可用性。

3.性能：通过在各层间采用链路聚合技术并采用高性能的核心层和分布层交换机可以让整个网络接近线速运行。

4.安全性：接入层的端口安全功能和分布层的安全策略让网络更加安全。

5.易管理性：同层交换机之间的一致性，简化网络管理。

6.易维护性：分层设计的模块化让网络轻松实现扩展，不至于变得复杂。

3、 企业选择交换机设备要考虑的商业问题：

表 1-1 选择交换机设备时通常会考虑的商业问题

交换机特征	商业考虑
成本	交换机的成本取决于接口的数量和速度、支持的功能和扩展功能
端口密度	网络交换机必须支持网络中适当数量的设备
电源	通过以太网供电（PoE）为接入点、IP 电话，甚至紧凑型交换机供电现在都很常见。除了考虑使用 PoE 外，一些机箱式交换机支持冗余电源
可靠性	交换机应提供对网络的持续访问
端口速度	网络连接的速度是最终用户关注的主要问题
帧缓冲区	交换机存储帧的能力非常重要，因为网络中可能存在通往服务器或网络其他区域的拥塞端口
可扩展性	网络中的用户数量通常随时间增长；因此，交换机应具备可扩展性

4、 帧转发

交换的两个标准决策：入口端口和目的地址

动态填充交换机的 mac 地址：从源学习基于目的转发。当交换机接收到一个帧时，交换机从接受到的帧那里学习到了源 mac 地址并将这个地址计入 mac 地址表。转发帧的时候首先检查 mac 地址表有没有相对应的 mac 地址，如果有就按照 mac 地址表中的与该 mac 地址对应的端口发出，如果没有则发送到除了该帧入口端口以外的所有端口泛洪，目的设备会发出单播帧响应，并记录进 mac 地址完成转发。

存储转发交换：有 2 个区别与直通交换：错误检查和自动缓冲。

错误检查：在入口端收到整个帧后对帧的最后一个字段的帧校验序列（FCS）与其自身的 FCS 计算进行比较。没错就转发，有错就舍弃。

自动缓冲：如果入口端口和出口端口的速度不匹配，交换机会将整个帧存储到缓冲区，计算 FCS 检查，将其转发到出口端口缓冲区，然后再将其转发出去。

直通交换：优点是交换机开始转发帧的时间比存储转发交换早。有 2 个区别与存储转发交换的特点是：快速帧转发和无效帧处理。

快速帧转发：一旦从 mac 地址表中查出目的 mac 地址就会作出转发决策，交换机不必等待帧的其余部分全部进入入口端口。

无效帧处理：直通交换方法不会丢弃大多数的无效帧，有错的帧会继续发往网络的其他网段，如果网络中的错误率很高，则直通交换对网络宽带造成负面影响，阻塞带宽。

5、 交换域

冲突域：共享网络的设备都是冲突域，每个交换机端口都是一个冲突域。

广播域：路由器用来划分广播域跟冲突域。

6、 怎么解决网络拥塞：

首先可以将 lan 细分为多个单独的冲突域，交换机每个端口都是一个冲突域，为该端口连接的设备提供完全的带宽。其次他们提供设备之前的全双工通信显著提高了 lan 的性能。

7、 有助于解决拥塞的交换机特征

表 1-2 有助于解决拥塞的交换机特征

特征	解释
高端口密度	交换机具有较高的端口密度：24 和 48 端口交换机的高度通常只有 1 个机架单元（1.75 英寸），而且运行速度为 100Mbit/s、1Gbit/s 和 10Gbit/s。大型企业的交换机可以支持数百个端口
大型帧缓冲区	在必须开始丢弃收到的帧之前能够存储更多的帧是非常有用的，尤其是在服务器或网络其他部分可能存在拥塞端口时
端口速度	根据交换机的成本，交换机可能会支持速度组合。速度为 100Mbit/s 和 1Gbit/s 或 10Gbit/s 的端口很常见（100Gbit/s 也有可能）
快速内部交换	具备快速内部转发功能能够提高性能。使用的方法可能是快速内部总线或共享内存，这会影响交换机的整体性能
较低的每端口成本	交换机以较低的成本提供高端口密度。因此，LAN 交换机可以适应每个网段用户较少的网络设计，从而增加每名用户的平均可用带宽

第二章

8、是用 ipv4 配置基本交换机管理访问：

步骤 1：配置管理接口

表 2-2 配置交换机管理接口

进入全局配置模式	S1# configure terminal
进入 SVI 的接口配置模式	S1(config)# interface vlan 99
配置管理接口 IP 地址	S1(config-if)# ip address 172.17.99.11 255.255.0.0
启用管理接口	S1(config-if)# no shutdown
返回特权 EXEC 模式	S1(config-if)# end
将运行配置保存到启动配置	S1# copy running-config startup-config

步骤 2：配置默认网关

表 2-3 配置交换机默认网关的命令

进入全局配置模式	S1# configure terminal
配置交换机的默认网关	S1(config)# ip default-gateway 172.17.99.1
返回特权 EXEC 模式	S1(config)# end
将运行配置保存到启动配置	S1# copy running-config startup-config

步骤 3：检验配置

可以用 show ip interface brief 命令查看

8、 检验交换机端口配置：以下是常见的检验交换机端口的命令

表 2-6 交换机检验命令

显示接口状态和配置	S1# show interfaces [interface-id]
显示当前启动配置	S1# show startup-config
显示当前运行配置	S1# show running-config
显示有关闪存文件系统的信息	S1# show flash:
显示系统硬件和软件状态	S1# show version
显示输入命令的历史记录	S1# show history
显示接口的 IP 信息	S1# show ip [interface-id]
显示 MAC 地址表	S1# show mac-address-table 或 S1# show mac address-table

9、 lan 中的安全问题

常见的 4 种攻击方式：

1. mac 地址泛洪：虚假主机利用随机生成源 mac 地址和目的地址的虚假的帧使交换机 mac 地址表不断进行更新操作导致 mac 地址表占满。交换机会将所有收到的帧全部广播出去这样虚假主机就能收到帧了。预防的方法是配置端口安全。
2. DHCP 攻击：

   DHCP 是用于从 DHCP 池中为主机自动分配有效的 ip 地址的协议。

   DHCP 攻击包括 2 种类型：DHCP 耗竭攻击和 DHCP 欺骗。

   1. DHCP 耗竭攻击：攻击者将使用 DHCP 请求泛洪 DHCP 服务器，以耗竭 DHCP 可以发出的所有的可用的 ip 地址。导致新的客户端不能获得 ip 地址从而实现拒绝服务（Dos）攻击。

   2. DHCP 欺骗攻击：攻击者在网络中配置虚假的 DHCP 服务器像客户端发送虚假的 DHCP 地址，强迫客户端使用错误的域名或者服务器。通常在 DHCP 欺骗之前要进行 DHCP 耗竭攻击以便对合法的 DHCP 服务器拒绝服务。预防的方法是 DHCP 侦听和端口安全功能。

3.利用 CDP 攻击：

Cdp 是思科专有的思科发现协议。可以发现直接相连的其他思科设备允许这些设备自动连接。Cdp 不进行身份验证攻击者可以伪造 cdp 包并将其发送到直连的思科设备上。

4、 Telnet 攻击

这个协议是不安全的攻击者可以利用工具来对交换机的 vty 线路进行暴力密码破解。

10、端口安全：

配置端口安全以允许一个或多个 mac 地址可以连接到端口。

***安全 mac 地址的类型*:**

1. 静态安全 mac 地址： switchport port-security mac-address mac 地址 手动配置存储

在地址表里并添加到交换机的运行配置中。

2. 动态安全 mac 地址：动态获得并存在地址表但不在运行配置中交换机重启将被移除。
3. 粘滞安全 mac 地址：switchport port-security mac-address sticky 启用，可通过手动或者动态获取存在地址表里并添加到交换机的运行配置中。

端口安全违规模式：

当出现以下 2 种情况时将会发生违规：

1. 当地址表已满，mac 地址不在地址表的工作站试图访问接口。
2. 同一地址在同一 vlan 中出现在不同的安全端口中。

安全违规的 3 个模式：

1. 保护：不会发出通知
2. 限制：会发出通知
3. 关闭：关闭安全端口

安全端口的配置命令：

1.指定端口	Interface fastethernet 0/19
2.将接口模式设置为 access	Switchport mode access
3.在接口上启用端口安全	switchport port-security
4.设置最大安全地址数量	switchport port-security maximum 50
5.启用粘滞获取	switchport port-security address sticky

端口安全检验：

1.检验端口安全设置： show port-security interface 端口号

2.检验安全 mac 地址： show port-security address

第三章

11.vlan 的类型：

1.数据 vlan 用于传送用户生成的流量，也称用户 vlan，用于将网络分为用户组或设备组。

2.默认 vlan 所有的端口都分配给默认 vlan 模式 vlan 是 vlan1。

3.本征 vlan 分配给 trunk 端口，其作用是维护无标记流量的向下兼容性，充当 trunk 链路两端的公共标识符。

4.管理 vlan 创建的前提是虚拟端口（svi）分配 ip 地址和子网掩码使交换机可以通过 http、telent、ssh 或者 snmp 进行管理。

12.vlan trunk

Trunk 是两台网络设备之间的点对点链路，负责传输多个 vlan 的流量，是多个 vlan 在交换机与交换机或者交换机与路由器之间的管道，

交换机配置 trunk

表 3-6 交换机端口 Trunk 命令

进入全局配置模式	S1# configure terminal
通过一个特定的端口号进入接口配置模式	S1(config)# interface *interface_id*
如果交换机支持多种模式，为 Trunk 选择合适的 Trunk 模式	S1(config-if)# switchport trunk encapsulation [dot1q | isl]
强制链路变为 Trunk 链路	S1(config-if)# switchport mode trunk
指定无标记 802.1Q 帧的本征 VLAN	S1(config-if)# switchport trunk native vlan *vlan_id*
指定在 Trunk 链路上允许的 VLAN 列表	S1(config-if)# switchport trunk allowed vlan *vlan-list*
返回特权 EXEC 模式	S1(config-if)# end

重置 trunk 线路的配置值

表 3-7 重置 Trunk 线路的配置值

进入全局配置模式	S1# configure terminal
通过一个特定的端口号进入接口配置模式	S1(config)# interface *interface_id*
将 Trunk 设置为允许所有的 VLAN	S1(config-if)# no switchport trunk allowed vlan
将本征 VLAN 重置为默认值	S1(config-if)# no switchport trunk native vlan
配置接入模式下的端口	S1(config-if)# switchport mode access
如果进入 Trunk 模式，则将其删除	S1(config-if)# no switchport trunk encapsulation [dot1q | isl]
返回特权 EXEC 模式	S1(config-if)# end

检验 trunk 配置

使用 show interface 端口号 switchpord

13、vlan 和 trunk 故障排除

***vlan 故障排除*:**

1. 使用 vlan 的 ip 寻址问题：每个 vlan 必须对应一个 ip 子网，如果同一个 vlan 中的 2 台设备具有不同的子网地址，那么这就不能通信。
2. 缺失 vlan：使用 show vlan 命令检查端口是否属于期望的 vlan。如果成员被分配到错误的 vlan 中使用 switchport access vlan 命令纠正特定端口的 vlan 成员关系。使用 show mac address-table interface 端口号 命令检查交换机的特定端口上获知了哪些地址以及该端口分配到了哪个 vlan。

***Trunk 故障排除*:**

常见问题有三个：

1. 本征 vlan 不匹配：一个端口是本征 vlan99 一个是本征 vlan100
2. Trunk 模式不匹配：一个端口开了 trunk 模式一个端口没开
3. Trunk 上允许的 vlan：允许的 vlan 列表中不支持当前的 vlan trunk 要求

使用 show interfaces trunk 命令检查本地和对等本征 vlan 是否匹配。如果本征 vlan 在 2 端不匹配则会发生 vlan 泄漏。

使用 show interfaces trunk 命令检查是否已在交换机之间建立 trunk，尽可能静态配置 trunk 链路

第四章

14、大多数支持网络的设备如计算机要求具有：中央处理器 cpu、操作系统 os、内存和存储。路由器实际上是一种特殊的计算机，它需要 cpu 和内存来永久或者临时的存储数据以便执行操作系统指令。

15、以下总结了路由器内存的类型、易失性以及每种内存所存储的内容

内存	易失性/非易失性	存储内容示例
RAM	易失性	■ 运行的 IOS ■ 运行的配置文件 ■ IP 路由和 ARP 表 ■ 数据包缓存
ROM	非易失性	■ 启动指令 ■ 基本诊断软件 ■ 受限的 IOS
NVRAM	非易失性	■ 启动配置文件
闪存	非易失性	■ IOS ■ 其他系统文件

16、路由器的功能：

1.确定发送数据包的最佳路径

2.将数据包转发到目的地

17、拓扑图与寻址表

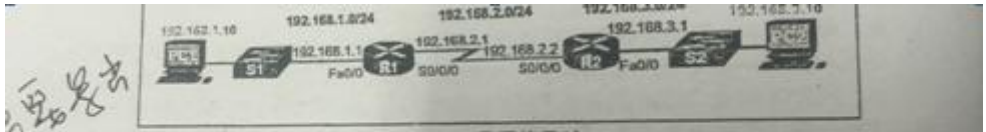

图 4-10 记录网络寻址

网络地址表

设备	接口	IP 地址	子网掩码	默认网关
R1	Fa0/0	192.168.1.1	255.255.255.0	N/A
	S0/0/0	192.168.2.1	255.255.255.0	N/A
R2	Fa0/0	192.168.3.1	255.255.255.0	N/A
	S0/0/0	192.168.2.2	255.255.255.0	N/A
PC1	N/A	192.168.1.10	255.255.255.0	192.168.1.1
PC2	N/A	192.168.3.10	255.255.255.0	192.168.3.1

18、路由器的基本设置:

配置路由器的基本设置：当配置路由器的基本设置时应首先执行以下基本任务:

1.为设备命名：将其与其他路由器区分开。命令如下：

```
Router# configure terminal
Router（config）#  hostname R1
R1（config）#。。。。。
```

2.保护管理访问：保护特权 EXEC、用户 EXEC 和 telent 访问，并对密码实施最高级加密。

3. 配置标语：提供对未授权访问的法律通知。

4. 保存配置：确保您的设置不会丢失。

2 3 4 的具体命令如下图：

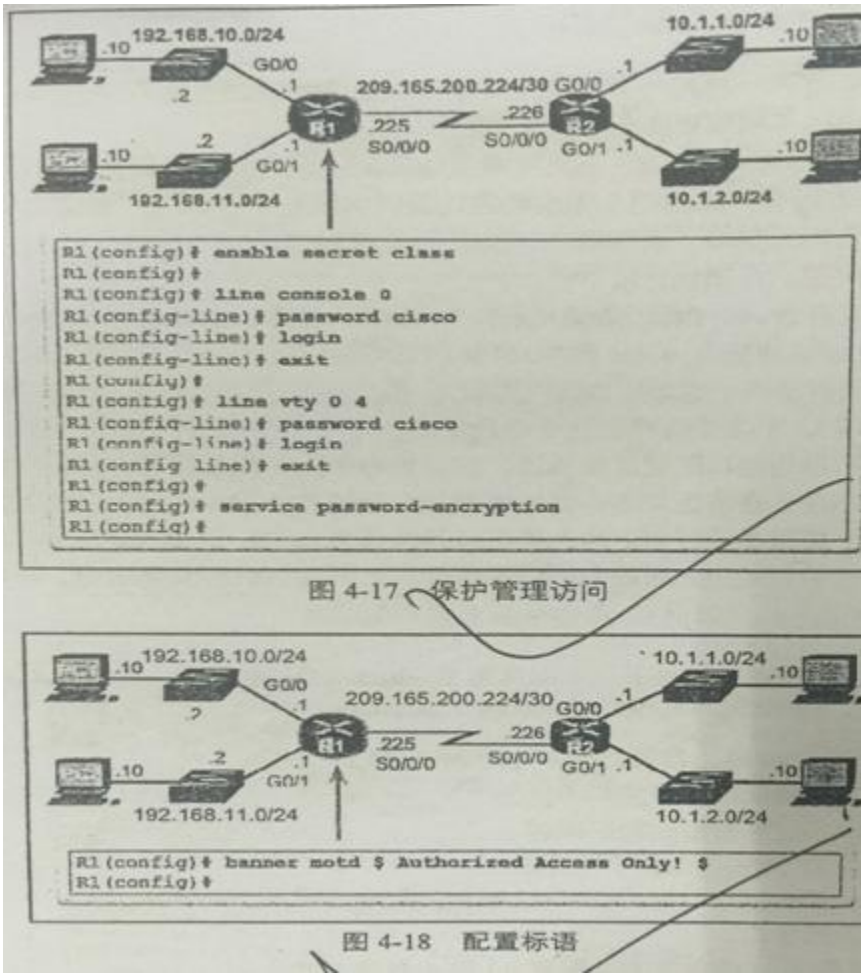

图 4-17 保护管理访问

图 4-18 配置标语

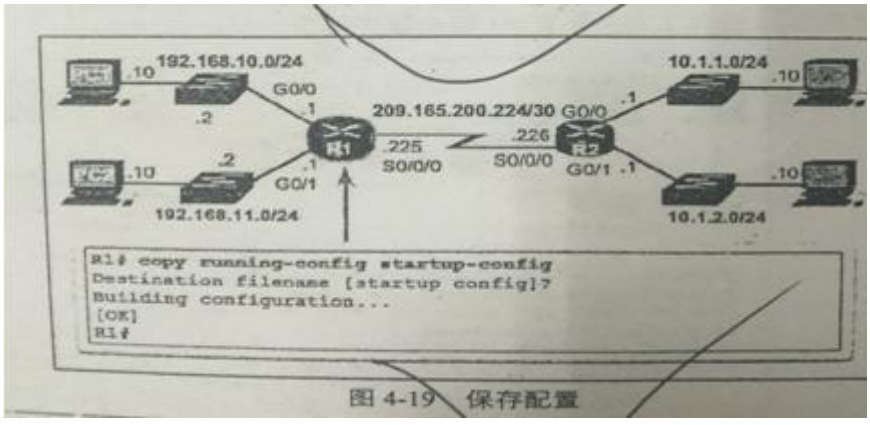

图 4-19 保存配置

19、配置 ipv4 路由器接口：

要配置 ip 以及子网掩码，常用命令有：interface g0/0 ip address 192.168.1.1 255.255.255.0 noshutdown 串行接口有 DCE 电缆插入则要加时钟频率，命令为：clockrate 128000

20、验证直连网络的连接：以下三种命令可以快速的验证接口状态：

1. show ip interface brief 显示所有接口的摘要，包括接口的 ipv4 地址和的当前的运行状态
2. Show ip route 显示存储在 RAM 中的 ipv4 路由表的内容。
3. show running-config interface 端口号 显示指定接口上的配置命令。

以下 2 种用于收集接口的更多详细信息：

1. show interface 显示设备上所有接口的接口信息和数据包流量计数。
2. show ip interface 显示路由器所有接口的 ipv4 相关信息。

21、路由器的交换功能：

路由器的交换功能的重要责任是将数据包封装成适用于传出数据链路的正确数据帧类型。 主要有以下三个步骤：

1. 通过删除第 2 层帧头和帧尾来解封装第 3 层数据包。
2. 检查 ip 数据包的目的 ip 地址以便从路由表中选择最佳路径。
3. 如果路由器找到通往目的地的最佳路径就将第 3 层数据包封装成新的第 2 层帧并将此帧从出口接口转发出去。

   看课本 4.5.2 到 4.5.5

22、路由决策

路由决策就是从路由表中确定一条发送数据包的最佳路径。路由表搜索将产生以下***三个路径***决定之一：

1. 直连网络：目的 ip 是路由器的接口的直连网络中的设备，将直接转发至目的设备。
2. 远程网络：转发至另一台路由器到达远程网络。
3. 无法决定路由：目的 ip 既不属于直连网络也不属于远程网络如果路由器有默认网关就转发至默认网关没有就直接舍弃。

最佳路径：一般把度量值最低的路径看作最佳路径。以下列出了几种动态协议使用的度量：路由信息协议（rip）：跳数；开放最短路径优先（ospf）：根据源到目的地之间的累计带宽计算出思科开销；增强型内部网关路由协议（eigrp）：带宽、延时、负载、可靠性。

负载均衡：当路由器中有 2 条或者多条路径通往目的地的开销度量相等时成为等开销负载均衡。负载均衡配置正确能够有效的提高网络的效率和性能。等开销负载均衡可配置为使用动态路由协议和静态路由。只有 EIGRP 支持非等开销负载均衡。

23、根据 R1 的路由表确定一些信息：

路由表如下：D 10.1.1.0/24 [90/2170112] via 209.1.1.1 00:00:05 s0/0

可以确定 1.路由来源：D 2.目的网络：10.1.1.0/24 3.管理距离：90 4.度量 2170112

5.下以跳 ：209.1.1.1 6.时间戳：00：00：06 7：发送接口：s0/0

第五章

24.vlan 间路由配置

1.传统的 vlan 间路由：传统的 vlan 是依靠路由器上的很多物理接口，让每个物理接口连接到一个独立的网络中，并配置不同的子网。

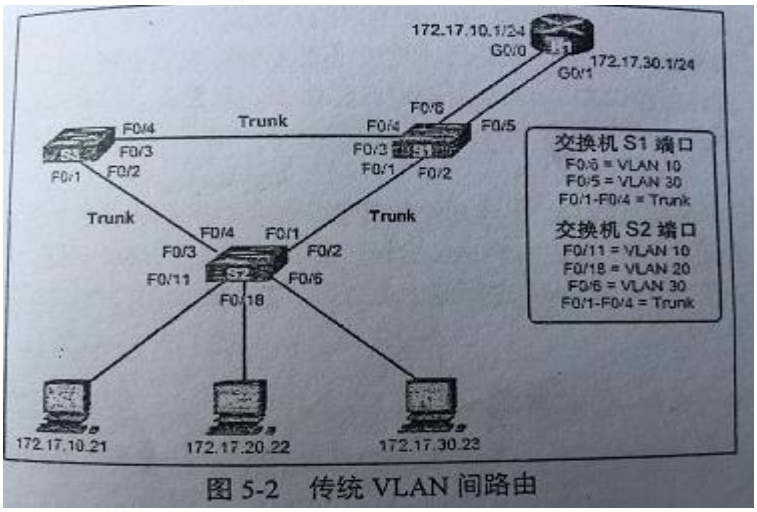

图 5-2 传统 VLAN 间路由

通信的步骤如下：

1. vlan10 中的 pc1 与 vlan30 中的 pc3 正通过路由器 r1 进行通信。
2. pc1 和 pc3 位于不同的 vlan 和子网中。
3. 对于每个 vlan 路由器 R1 都配置有不同的物理接口。
4. Pc1 将单播流量发送到 vlan10 中的交换机 s2，随后通过 trunk 链路发送到 s1。
5. S1 将其转发到 R1 的 G0/0 接口。
6. R1 又通过 vlan30 的接口 G0/1 发送到到 S1
7. S1 通过 trunk 发送到 S2. S2 在转发给 pc3

2. 单臂路由器的 vlan 间路由：就是将路由器的接口配置为 trunk 链路，与交换机上的 trunk 接口相连只需要通过单个物理接口就可以进行不同 vlan 间的路由，这个接口有属于不同 vlan 的子接口，子接口是虚拟的。

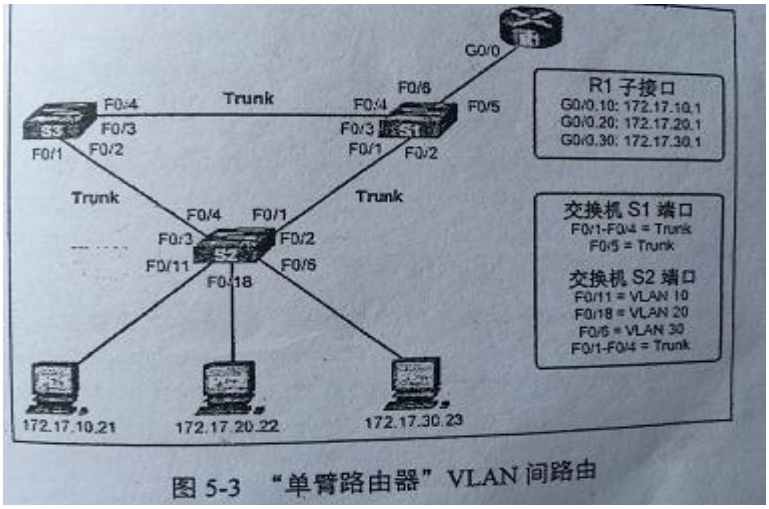

图 5-3 “单臂路由器” VLAN 间路由

通信的步骤如下：

1. 利用单个物理路由器接口，vlan10 中的 pc1 与 vlan30 的 pc3 通过 R1 进行通信。
2. Pc1 将单播流量发送到 s2. 交换机 S2 将单播流量标记为 Vlan10 然后通过 trunk 链路将流量发送到 S1.
3. S1 通过 F0/5 接口通过 trunk 链路发往 R1 的 G0/0.
4. R1 接收标记为 vlan10 的单播流量后并将其发送到 vlan30 的子接口并标记为 vlan30 然后发送到 S1
5. S1 将标记为 vlan30 的单播流量发送到 S2.
6. S2 接收到单播流量后删除了标记，最后发送给了 pc3

3. 多层交换机 vlan 间的路由：不需要用路由器作为第三层，用多层交换机来执行第 2、3 层的功能，多层交换机支持路由和 vlan 间路由。

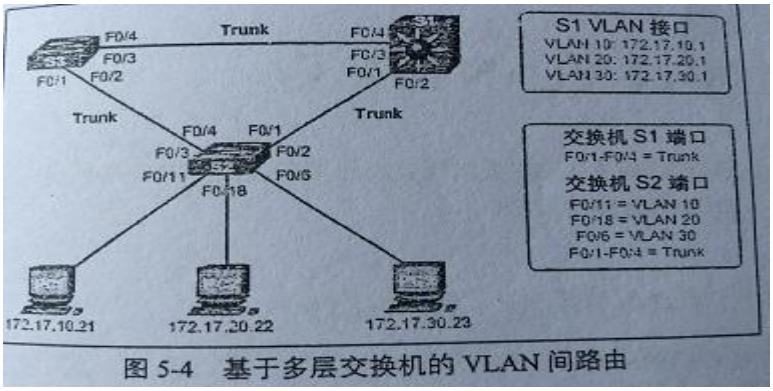

图 5-4 基于多层交换机的 VLAN 间路由

通信的步骤如下：

1. vlan10 中的 pc1 正通过交换机 S1 上为各 vlan 配置的 vlan 接口与 vlan30 中的 pc3 通信。
2. pc1 发送到 S2
3. S2 收到后从 trunk 链路发送到交换机 S1 时，将该单播流量标记为来源于 vlan10.
4. 交换机 S1 收到后将标记删除
5. 路由到它的 vlan30 接口。
6. 然后 S1 对该单播流量重新标记为 vlan30 通过 trunk 发往 S2.
7. S2 删除 vlan 标记发往 pc3

25、配置传统路由：

1. 交换机配置：

命令大体如下：

```
S1（config）#vlan 10
S1（config-vlan）#vlan 30
S1（config-vlan）#interface f0/11
S1（config-if）#switchport mode access
S1（config-if）#switchport access vlan10
```

2. 路由器接口配置：

命令大体如下：

```
R1（config）#interface g0/0
R1（config-if）#ip address 192.1.1.1 255.255.255.0
R1（config-if）#no shutdown
```

3. 使用 show ip route 检查路由表

26、配置单臂路由：

1. 交换机配置：***要将路由器临近的交换机一个端口设置为 trunk 模式***

命令大体如下：

1. S1（config）#vlan 10
   S1（config-vlan）#vlan 30
   S1（config-vlan）#interface f0/11
   S1（config-if）#switchport mode trunk

2. 路由器子接口配置：物理接口下的多个子接口

命令大体如下：

1. R1（config）#interface ***g0/0.10***
   R1(config-subif)#***encapsulation dot1q 10***
   R1(config-subif)# ip address 192.1.1.1 255.255.255.0

3. 使用 show vlans 检查子接口信息

第六章

27、动态路由与静态路由的对比：必考

表 6-1　动态和静态路由的对比

	动态路由	静态路由
配置复杂性	通常不受网络规模限制	随着网络规模的增大而愈趋复杂
拓扑结构变化	自动根据拓扑结构变化进行调整	需要管理员参与
扩展	简单拓扑结构和复杂拓扑结构均适合	适合简单的拓扑结构
安全	不够安全	更安全
资源使用率	占用 CPU、内存和链路带宽	不需要额外的资源
可预测性	根据当前拓扑结构确定路由	总是通过同一路径到达目的网路

静态路由的管理距离(AD)为 1.因此静态路由优先于所有的动态获知的路由。

28、什么情况下使用静态路由：

1.在不会显著增长的小型网络中，使用静态路由便于维护路由表。

2.通过末节网络进行路由。末节网络路由器只有一个邻居。

3.使用但已默认路由。如果某个网络在路由表中找不到更匹配的路由条目，则使用默认路由代替通往该网络的路径

29、静态路由类型：

1.标准静态路由：比如末节网络的静态路由配置

2.默认静态路由：默认静态路由是与所有的数据包都匹配的路由，在没有获取路由或者静态路由的情况下，路由器将把所有的数据包发给由默认路由标识的网关的 ip 地址。配置静态路由还可以创建最后求助网关。

当以下 2 种情况下经常用默认静态路由：

1.路由表中没有与目的 ip 地址匹配的路由

2.末节路由器可以配置默认静态路由。

3.汇总静态路由：要减少路由表条目的数量，多条静态路由可以汇总成一条静态路由条件如下：1.目的网络是连续的，并且可以汇总成一个网络地址。

2.多条静态路由都使用相同的出口接口或者下一跳 ip 地址。

4.浮动静态路由:如果链路发生故障，浮动静态路由提供备份的路径。

30、配置 ipv4 静态路由：

1.ip route 命令：常见的命令语法如下所示：

Ip route network-address subnet-mask {ip-address|exit-info}

其中 network-address 是目的网络地址

Subnet-mask 是目的网络的子网掩码

Ip-address 指下一跳的 ip 地址 exit 不常用

2. 下一跳路由：包括了以下三种：下一跳静态路由；直连静态路由；完全指定静态路由。

1.下一跳静态路由：ip route 192.1.1.1 255.255.255.0 192.2.2.2

仅仅指定了下一跳的 ip 地址没有指定发送接口，输出接口是下一条地址派生出来的。

要进行 2 次路由查表：

1.查表获得了下一跳的 ip 为 192.1.1.1 但是不知道发送端口是哪一个。

2.再次查表搜索 192.1.1.1 的匹配项的到出口接口为 S0/0（假设）然后才能转发数据包。

因为在转发数据包之前要进行多次查表查找过程就是一种递归查找，占用了路由器资源。

*2.直连静态路由：*使用出口的接口指定下一跳地址没有指明 ip

ip route 192.1.1.1 255.255.255.0 s0/0/0

比较直连静态路由（指定出口接口）跟下一跳静态路由（递归查询）的区别:

前者只需搜索一次路由表即可转发出去，后者要搜索 2 次，前者管理距离可以为 0，后者为 1；

3.配置完全指定静态路由：同时指定 ip 跟出口接口

ip route 192.1.1.1 255.255.255.0 s0/0/0 192.2.2.2

31.CIDR 和 VLSM 太繁琐不整理了但是会考

第 7 章

32、动态路由的分类：

分为内部网关协议（IGP）跟外部网关协议（本书没介绍）；内部网关协议包括距离矢量路由协议和链路状态路由协议；其中距离矢量路由协议包括 RIPv2 跟 EIGRP，链路状态路由协议包括 ospfv2 和 is-is。

33、动态路由协议的运行过程如下：

1.路由器通过其接口发送和接收路由信息

2.路由器和使用统一路由协议的其他路由器共享路由信息和路有消息。

3.路由器通过交换路由信息来了解远程网络

4.如果网络拓扑发生变化路由协议可以将变化告诉其他路由

34、距离矢量路由协议：RIPv2　EIGRP

距离：根据度量（如跳数、开销、带宽、延迟等）确定与目的网络的距离。

矢量：指定下一跳路由器或出口接口的方向以达到目的。

使用距离矢量路由协议的路由器并不了解到达目的网络的整条路径,距离矢量协议将路由器作为通往最终目的地的路径上的路标。路由器唯一了了解的是远程网络的距离。

路由信息协议（RIP）v1 跟 v2 的对比：

两者相同的是都是用跳数作为度量最大跳数为 15；

不同的是 1. v2 支持 vlsm 跟 cidr 并支持路由汇总、身份验证等，v1 不支持

2. v2 效率更高将更新转发至组播地址 224.0.0.9，而 v1 广播到 55.255.255.255

检查默认 RIP 设置：

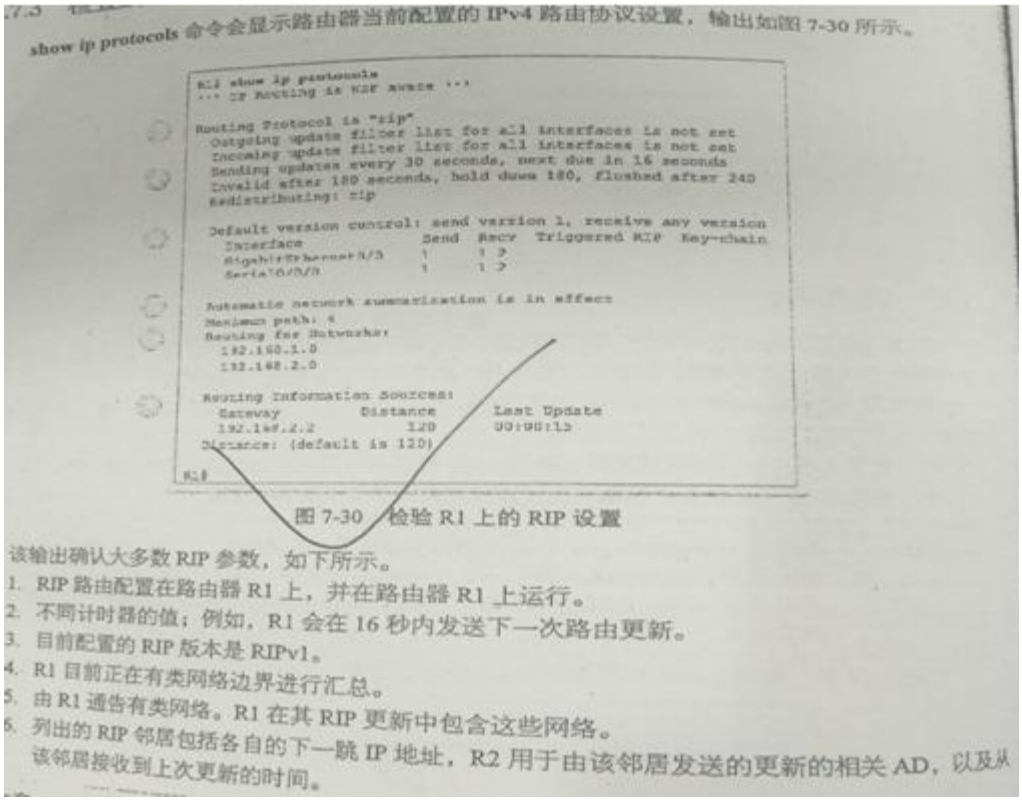

图 7-30　检验 R1 上的 RIP 设置

用 router rip 命令启用 ripv1。

用 version 2 命令启用 ripv2。

使用 no auto-summary 禁用自动汇总

使用 passive-interface 端口号 配置被动端口

35、**链路状态路由协议：**OSPFv2　IS-IS

配置了链路状态路由协议的路由器可以获取所有其他的路由器信息来创建网络的完整视图即拓扑结构。

链路状态路由协议的路由过程:

1. 每台路由器了解其自身的链路和与其直连的网络。这通过检测哪些接口处于工作状态来完成
2. 每台路由器负责联系直连网络中的相连的路由器，通过发送并互换 hello 数据包完成。
3. 每台路由器创建一个链路数据包（LSP）,其中包含与该路由器直接相连的每条链路的的状态，这通过记录每个邻居的所有相关信息来完成。
4. 每台路由器将 LSP 泛洪到所有邻居，这些邻居将受到的所有的 Lsp 存入数据库接着他们将 LSP 泛洪给自己的邻居直到区域中所有的路由器均收到了这些 LSP 为止。
5. 每台路由器根据数据库中的 LSP 构建一个网络拓扑图在通过 SPF 算法确定最佳路径

链路状态信息如下图:

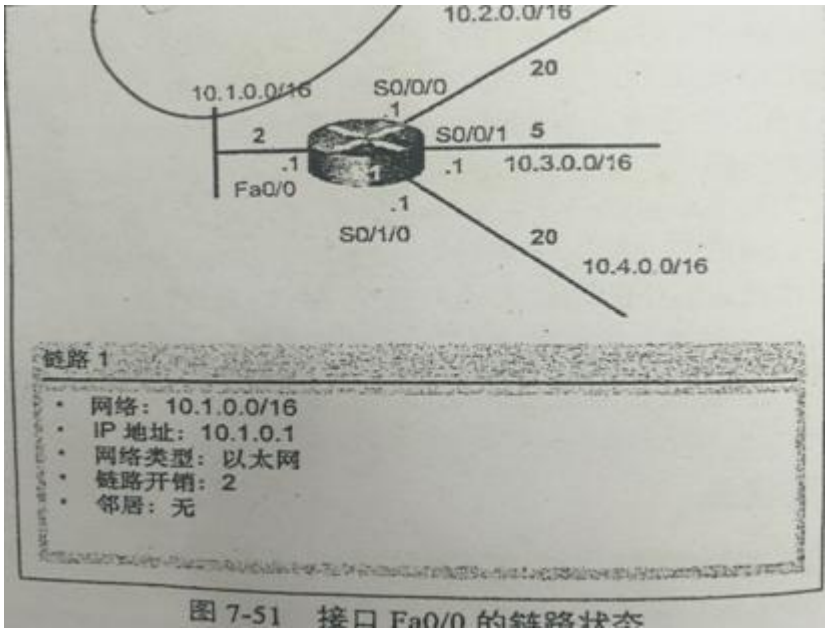

图 7-51 接口 Fa0/0 的链路状态

36、几种路由协议的相关比较:

	距离矢量				链路状态	
	RIPv1	RIPv2	IGRP	EIGRP	OSPF	IS-IS
收敛速度	慢	慢	慢	速度快	速度快	速度快
可扩展性——网络规模	小型	小型	小型	大型	大型	大型
使用 VLSM	否	是	否	是	是	是
资源利用率	低	低	低	中等	高	高
实施和维护	简单	简单	简单	复杂	复杂	复杂

第 8 章

37、OSPF 的三个主要组件：

1. 数据结构：

邻接数据库：创建邻居表

链路状态数据库（LSDB）：创建拓扑表

转发数据库：创建路由表。

2.路由协议消息：

Hello 数据包

数据库状态描述包 DBD

链路状态请求数据包 LSR

链路状态更新数据包 LSU

链路状态确认数据包 LSAcK

3.算法：

SPF 算法

38、OSPF 工作原理：

1.OSPF 运行状态:当 OSPF 第一次加入网络中他会进行以下几步:

1.与邻居建立邻接关系

2.交换路由信息

3.计算最佳路由

4.实现收敛

2.多状态：

Down 状态（不可用状态）；Init（初始化状态）；Two-Way（双向状态）；ExStart（预启动状态）；Exchange（交换状态）；Loading（加载状态）；Full（完全邻接状态）

39、配置单区域的 OSPFv2

使用 router ospf process-id 命令 （process-id 是一个介于 1 到 65535 的数字）启用 ospfv2；

使用 router-id 1.1.1.1 将 id 1.1.1.1 分配给路由器；

使用 show ip protocols 命令检验路由器 id

修改路由器 id 先清除 ofps 进程使用 chear ip ospf process 在特权 EXEC 模式下

使用环回接口作为路由器 id：

R1（config）#interface loopback 0

R1（config-if）#ip address 1.1.1.1 255.255.255.255

40、开销：

开销=参考带宽/接口带宽 默认参考带宽为一亿 bit ；

第 9 章 重点 acl