第3章

企业交换网络设计

在现今的网络建设中，企业网的建设是非常重要的，企业网内部各种不同业务的开展是企业网发展迅速的最主要原因。早期的企业网主要是简单的数据共享，现在的企业网要求内部全方位的数据共享，同时，网络部署也从过去单一的企业内部网到现在多个分支公司的网络互联。因此，企业网络的建设目标是建立分层的交换式以太网络，既对已建成的企业网络进行优化使其得到充分的利用，又实现了对现有网络进行升级扩建。

在建立企业交换网之前，首先要了解企业的具体需求，根据企业办公室 PC 的多少来决定网络信息点数目；其次，根据企业办公大楼和工厂车间的具体位置，考虑需要敷设的主干光纤，在合理的位置放置硬件设备，并通过网络敷设将企业中的每一个信息点连接到局域网中；最后通过路由器、防火墙等设备连接到外网。一般情况下，外网地址采用各电信运营商提供的网络地址，企业内部采用私有 IP 地址。

另外，在一个企业交换网中，子网划分是必不可少的。例如，一个企业共有 15 个分公司，每个分公司有 8 个部门，上级只给一个 172.16.0.0/16 的网段，让你给每家子公司以及子公司的每个部门分配网段。我们不可能为每一个工作站申请一个公有 IP 地址，这时就必须做子网划分，这样不仅可以缓解 IP 地址的不足，也可以为企业节省不少开支。

随着企业的发展，在企业局域网中划分 VLAN 也成为必需，VLAN 可以保证内网信息更加安全。例如，公司其他部门需要限制访问公司内部网的财务服务器资源，这时就可以通过划分 VLAN 解决。随着无线网络的部署，管理更加困难，如何保证不把无线网络的安全问题带到整个企业网，也可以通过在不同部门之间划分不同的网段解决。VLAN 技术既能保证内网更加安全，也便于管理。

企业网络建成之后，如何保证网络的传输质量，从而避免由于网络设计带来的各种问题呢？网络设计中经常会采用冗余拓扑的方法解决。冗余是保证企业网络可靠性的关键设计之一。如果设备之间的多条物理链路能够提供冗余路径，那么当某个链路或端口发生故障时，网络仍可以继续运行。同时，冗余链路可以增加网络容量，提供流量负载分担。对于二层交换环路问题，可以通过 STP(Spanning Tree Protocol，生成树协议)来管理二层冗余，STP 可以让具

有冗余拓扑的网络在发生故障时自动调整网络的数据转发路径。此外,企业网络中还会通过链路聚合的方式,来均衡各端口中的出/入流量。

3.1 实验拓扑

随着企业规模的不断扩大,企业数据量的飞速增长,企业希望内部数据能够高速共享,对外公布的信息能够及时发布,因此,企业对内部网络以及网络外部出口等有了更高的要求。在网络设计与实现中,子网划分、VLAN、MSTP、链路聚合等技术是不可或缺的。

一般企业网络的拓扑结构如图 3-1 所示。

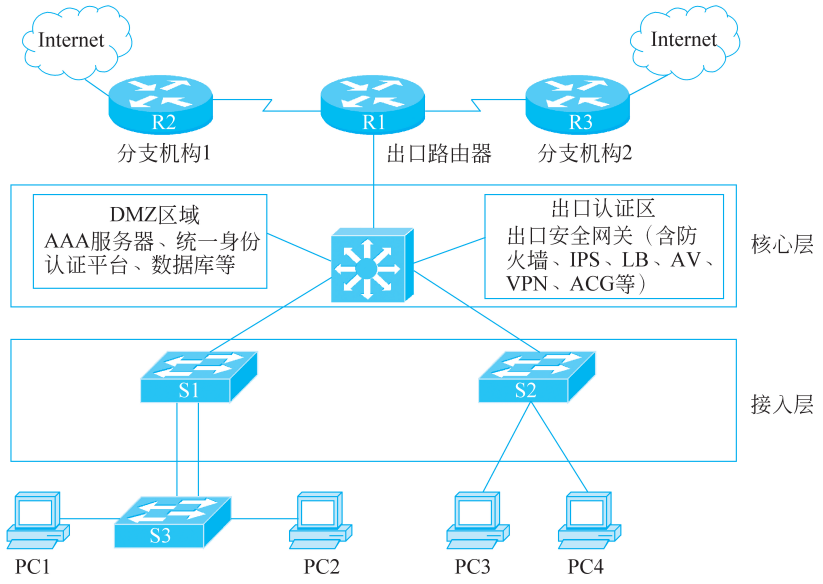

图 3-1 企业网络拓扑

3.2 子网划分

网络中,主机可采用的通信方式包括单播(Unicast)、组播(Multicast)和广播(Broadcast)三种。广播又分为定向广播和有限广播两类。

(1) 单播:指从一台主机向另一台主机发送数据包的过程。

(2) 组播:指从一台主机向选定的一组主机发送数据包的过程(注意:这些主机可以位于不同网络)。组播可以发送单个数据包到组播组中的所有主机,因此可以在一定程度上节省带宽。常见的组播应用有视频和音频组播、路由协议交换路由信息、软件分发、远程游戏等。

(3) 广播:指从一台主机向该网络中的所有主机发送数据包的过程。因为收到广播数据包的所有主机都会处理该数据包,所以广播一般受限制,以免造成网络或设备的负

担。广播分为定向广播和有限广播两类。

① 定向广播。定向广播是将数据包发送给特定网络中的所有主机。一般应用于向非本地网络中的所有主机发送广播。

② 有限广播。有限广播是将数据包发送给本地网络中的所有主机，数据包的目的 IP 地址设为 255.255.255.255(注意：路由器不会转发有限广播)。通常将网络的有限广播范围称为广播域，而路由器是广播域的边界。有限广播的应用包括 DHCP 发现数据包、ARP 请求数据包等。

在网络 IP 地址划分中，有一些地址具有特殊含义，下面是比较常见的特殊 IP 地址。

(1) 环回地址。

以“127”开头的网段，都称为环回地址，在 Windows 系统下，环回地址也称为“localhost”，环回地址一般用来测试网络协议是否正常工作。例如，可以使用“ping 127.1.1.1”来测试本地 TCP/IP 是否安装正确；可以在本地浏览器里输入“http://127.1.2.3”来测试 Web 服务是否正常启动。

注：使用该地址发送的数据不进行网络传输。

(2) 0.0.0.0 和 255.255.255.255。

0.0.0.0 表示任意网络、任意主机。例如，当在网络中设置默认网关时，Windows 系统会自动生成一个目的地址为 0.0.0.0 的默认路由。

255.255.255.255 是受限广播地址，表示本网段内所有主机。该地址一般用于主机配置过程中 IP 数据包的目的地址。

注：路由器禁止转发目的地址为 255.255.255.255 的数据包。

(3) 169.254.*.*。

如果网络中使用 DHCP(Dynamic Host Configuration Protcol，动态主机配置协议)自动获取 IP 地址，那么当 DHCP 服务发生故障或响应时间超时时，Windows 系统会自动为主机分配这样一个地址。因此，当网络中的主机 IP 地址是此类地址时，网络很可能出现了故障。

(4) 主机号全为 0 的地址。

这个地址指本地网络。路由表中经常会出现这样的地址。

在互联网发展的早期，许多 A 类地址被分配给大型网络服务提供商，B 类地址被分配给大型公司或其他组织，因此消耗掉了许多 A 类和 B 类地址。在美国国家骨干网转为全球公有互联网后，有限的 IP 地址个数远远不能满足越来越多的主机需要。此外，如果一个网络内包含的主机数量过多(如一个 B 类网络可分配 65 534 个有效 IP 地址)，采用以太网的组网方式，那么网络内会有大量的广播信息，从而导致网络拥塞。为了解决这些矛盾，子网技术应运而生。

子网是指从有类网络中，利用主机地址位，把整个大网络划分成若干较小的网络，形成若干独立的子网的过程。这样可以使 IP 地址更加有效，将原来处于同一个网段上的主机，分隔到不同网段或子网中，因此原来的一个广播域被划分成若干较小的广播域，大大地减少了广播干扰问题。划分子网可以使一个大型网络拥有多个小的局域网。

子网的划分通过子网掩码技术来实现。传统的子网划分方法是使用固定长度的子网掩码，每个子网包含的有效 IP 地址数量相同。这种划分方法在每个子网对主机数量的

要求差别比较大时,同样会造成 IP 地址的浪费。于是,可以使用可变长度子网掩码(Variable Length Subnet Mask,VLSM)技术,它可以根据网络的实际需求,使用适当的子网掩码长度,也就是对子网再划分子网的技术。使用 VLSM 进行子网划分与传统子网划分方法类似,也是从主机部分借若干位来创建子网,计算子网的个数和每个子网的主机个数的公式类似。

子网划分的公式如下。

(1) 划分子网个数:2^n。n 是网络位向主机位所借的位数。

(2) 每个子网的主机数:2^m-2。m 是借位后所剩的主机位数。

(3) 划分后的子网掩码:在原有子网掩码的基础上借了几个主机位,就添加几个 1。


实验 3-1
视频

实验 3-1:子 网 划 分

1. 实验目的

(1) 掌握 IP 地址和子网掩码的含义。

(2) 掌握计算机 IP 地址的分配。

(3) 掌握 IP 子网划分的概念和划分方法。

2. 实验拓扑

实验拓扑如图 3-2 所示。

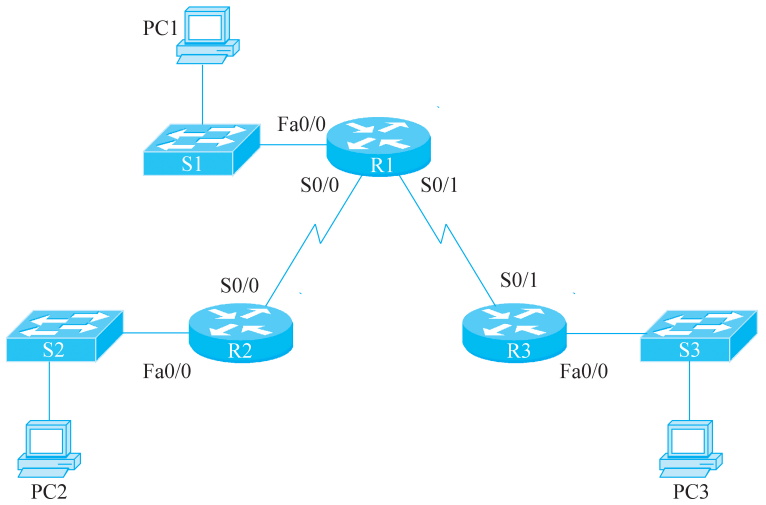

图 3-2 划分子网拓扑图

3. 实验要求

指定了一个网络地址 172.16.0.0/16。将利用它对拓扑图中显示的网络划分子网以及分配 IP 地址。该网络的编址要求如下。

(1) R1 的 LAN 子网需要 400 个主机 IP 地址。

(2) R2 的 LAN 子网需要 200 个主机 IP 地址。

(3) R3 的 LAN 子网需要 50 个主机 IP 地址。

(4) 从 R1 到 R2 的链路的两端各需要一个 IP 地址。

(5) 从 R1 到 R3 的链路的两端各需要一个 IP 地址。

4. 实验步骤

(1) 在表 3-1 中填写相应的子网信息。

表 3-1　使用 VLSM 划分子网

子网编号	子网地址	第一个可用主机地址	最后一个可用主机地址	广播地址
0	172.16.__.__	172.16.__.__	172.16.__.__	172.16.__.__
1	172.16.__.__	172.16.__.__	172.16.__.__	172.16.__.__
2	172.16.__.__	172.16.__.__	172.16.__.__	172.16.__.__

(2) 为拓扑图中显示的网络分配子网。

(3) 为网络设备分配 IP 地址。

① 将 R1 的 LAN 子网的第一个有效主机地址分配给 LAN 接口。

② 将从 R1 到 R2 的子网链路的第一个有效主机地址分配给 R1 的 S0/0 接口。

③ 将从 R1 到 R3 的子网链路的第一个有效主机地址分配给 R1 的 S0/1 接口。

④ 将 R2 的 LAN 子网的第一个有效主机地址分配给 LAN 接口。

⑤ 将从 R1 到 R2 的子网链路的最后一个有效主机地址分配给 R2 的 S0/0 接口。

⑥ 将 R3 的 LAN 子网的第一个有效主机地址分配给 LAN 接口。

⑦ 将从 R1 到 R3 的子网链路的最后一个有效主机地址分配给 R3 的 S0/1 接口。

⑧ 将 R1 的 LAN 子网的最后一个有效主机地址分配给 PC1。

⑨ 将 R2 的 LAN 子网的最后一个有效主机地址分配给 PC2。

⑩ 将 R3 的 LAN 子网的最后一个有效主机地址分配给 PC3。

5. 实验调试

(1) 查看地址分配结果。

(2) 检查在直连网络中，所有设备之间的连通性。

3.3　VLAN 划分

虚拟局域网(Virtual Local Area Network，VLAN)是通过软件功能将交换机物理端口划分成一组逻辑上的设备或用户，这些设备和用户不受物理网段的限制，可以根据功能、部门及应用等因素将其组织起来，从而实现虚拟工作组的技术。交换机不能隔离广播域，例如，通过多台交换机连接在一起的计算机都处于一个广播域中，这时任何一台计算机发送广播包，其他所有计算机都会收到，这时广播信息就会消耗大量的网络带宽，同时，收到广播信息的计算机还要消耗一部分 CPU 来处理广播信息。

利用 VLAN，可以不局限于网络设备的物理位置建立不同的工作组。VLAN 可以通过设备的位置、工作组所具备的功能或者不同的部门进行划分，甚至也可以根据应用程序或者使用的协议来划分。每一个 VLAN 都包含一组有着相同需求的计算机工作站，由于是从逻辑上划分，而不是从物理上划分，所以同一个 VLAN 内的各个工作站没有限制在同一个物理范围中，即这些工作站可以在一个交换机内，也可以跨越交换机，甚至可以跨

越路由器。

VLAN 工作在 OSI 模型的第二层,它可以对交换机端口进行逻辑分组,一个个分组即一个个 VLAN。一个分组可以由同一个交换机的端口组成,也可以由不同交换机的端口组成。一个分组就是一个 VLAN,也是一个广播域,而 VLAN 之间的通信必须通过第三层路由功能来实现。VLAN 技术相对灵活、高效,具有减小广播域大小、降低成本、提高网络性能、增强网络安全、提高管理效率等优点。一般来说,建议一个 VLAN 不要超过 255 个终端,在无线环境下,情况更为复杂,但也建议一个 VLAN 不要超过 255 个终端,如果单个 VLAN 中终端较多,往往会采用用户隔离技术来管理同一个 VLAN 下的用户之间的通信。

VLAN 分为基于端口划分和基于 MAC 地址划分两种。

(1) 基于端口划分 VLAN。基于端口划分的 VLAN 比较常用,使用起来比较简单。网络管理员可以通过手动配置把交换机的某一端口分配给某一个 VLAN。它的不足之处是当用户从一个端口移动到另一个端口时,网络管理员必须重新对交换机端口进行分配配置。

(2) 基于 MAC 地址划分 VLAN。基于 MAC 地址划分 VLAN 使用到了 VLAN 成员策略服务器(VLAN Membership Policy Server,VMPS)。一般是根据连接到交换机端口的设备的源 MAC 地址,动态地将其分配给某个 VLAN。当设备移动时,交换机能够自动识别其 MAC 地址并将其所连接的端口配置到相应的 VLAN,因此也称为动态 VLAN。


实验 3-2
视频

实验 3-2:单交换机 VLAN 划分

1. 实验目的

(1) 熟悉 VLAN 的创建。

(2) 把交换机接口划分到特定的 VLAN。

(3) 配置交换机的端口安全特性。

(4) 配置管理 VLAN。

2. 实验拓扑

实验拓扑如图 3-3 所示。

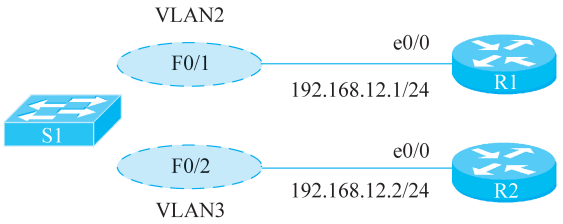

图 3-3 划分 VLAN 拓扑图

3. 实验步骤

要配置 VLAN,首先要创建 VLAN,然后再把交换机的端口划分到特定的端口上,具体步骤如下。

（1）在划分 VLAN 前，配置路由器 R1 和 R2 的 e0/0 接口，从 R1 上 ping 192.168.12.2 进行测试。默认时，交换机的全部接口都在 VLAN1 上，从 R1 和 R2 应该能够通信。

（2）在 S1 上创建 VLAN。

```
S1(config)#vlan 2
S1(Config-Vlan2)#name VLAN2
//在 S1 上创建 vlan 2,并修改名称为 VLAN2。
S1(Config-Vlan2)#exit
S1(config)#vlan 3
S1(Config-Vlan3)#name VLAN3
//在 S1 上创建 vlan 3,并修改名称为 VLAN3。
```

（3）把端口划分到相应的 VLAN 中。

```
S1(config)#vlan 2
S1(Config-Vlan2)#switchport interface f0/1
//把端口 f0/1 分配到 vlan 2 中。
S1(Config-Vlan2)#exit
S1(config)#vlan 3
S1(Config-Vlan3)#switchport interface f0/2
//把端口 f0/2 分配到 vlan 3 中。
```

（4）配置交换机端口安全。

```
S1(config)#int f0/10
S1(config-if-fastEthernet0/10)#switchport port-security
//打开交换机的端口安全功能。
S1(config-if-fastEthernet0/10)#switchport port-security maximum 1
//只允许该端口下的 MAC 条目最大数量为 1。
S1(config-if-fastEthernet0/10)#switchport port-security violation shutdown
//如果该接口的 MAC 条目超过最大数量,则该接口将会被关闭。
S1(config-if-fastEthernet0/10)#switchport port-security mac-address 00-01-
23-45-67-89
//允许 PC 从 f0/10 接口接入。
```

（5）配置管理 VLAN。

```
S1(config)#vlan 99
S1(Config-Vlan99)#name management
//一般设置 vlan 99 为管理 VLAN。
S1(Config-Vlan99)#exit
S1(config)#int vlan 99
S1(Config-if-Vlan99)#ip address 172.16.1.1 255.255.0.0
//为其分配 IP 地址。
S1(Config-if-Vlan99)#no shutdown
```

4. 实验调试

(1) 使用“show vlan”查看 VLAN 信息。

(2) 测试 VLAN 之间的连通性。

(3) 使用“show mac-address-table”检查 MAC 地址表。

(4) 模拟非法接入(修改 MAC 地址),查看端口状态。

(5) 从 PC Telnet 到交换机 S1。

实验 3-3 视频

实验 3-3：多交换机 VLAN 划分

当一个 VLAN 跨过不同的交换机时,连接在不同交换机端口的同一 VLAN 的计算机如何实现通信呢? 这时,可以在交换机之间为每一个 VLAN 都增加连线,然而这样在有多个 VLAN 时会占用交换机太多的端口,而且扩展性很差。可以采用 Trunk 技术来实现跨交换机的 VLAN 内主机通信。Trunk 技术使得在一条物理线路上可以传送多个 VLAN 的信息,交换机从属于某一 VLAN 的端口接收到数据,在 Trunk 链路上进行传输前,会加上一个标记,标识该数据所属的 VLAN,数据到了对方交换机,交换机会把该标记去掉,只发送到属于对应 VLAN 端口的主机。

1. 实验目的

配置交换机接口的 Trunk。

2. 实验拓扑

实验拓扑如图 3-4 所示。

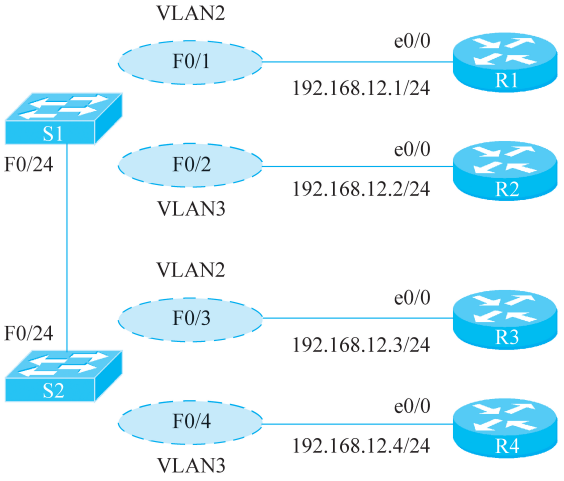

图 3-4 Trunk 配置拓扑图

3. 实验步骤

(1) 在 S1 上创建 VLAN。

```
S1(config)#vlan 2
S1(Config-Vlan2)#name VLAN2
S1(Config-Vlan2)#exit
```

```
S1(config)#vlan 3
S1(Config-Vlan3)#name VLAN3
S1(Config-Vlan3)#exit
S1(config)#vlan 98
S1(Config-Vlan98)#name native vlan
```

(2) 把端口划分在 VLAN 中。

```
S1(config)#vlan 2
S1(Config-Vlan2)#switchport interface fastEthernet 0/1
S1(Config-Vlan2)#exit
S1(config)#vlan 3
S1(Config-Vlan3)#switchport interface fastEthernet 0/2
```

(3) 在 S2 上创建 VLAN。

```
S2(config)#vlan 2
S2(Config-Vlan2)#name VLAN2
S2(Config-Vlan2)#exit
S2(config)#vlan 3
S2(Config-Vlan3)#name VLAN3
S2(Config-Vlan3)#exit
S2(config)#vlan 98
S2(Config-Vlan98)#name native vlan
```

(4) 把端口划分在 VLAN 中。

```
S2(config)#vlan 2
S2(Config-Vlan2)#switchport interface fastEthernet 0/3
S2(Config-Vlan2)#exit
S2(config)#vlan 3
S2(Config-Vlan3)#switchport interface fastEthernet 0/4
```

(5) 配置 Trunk。

```
S1(config)#interface f0/24
//注:配置实验中实际连接的接口。
S1(config-if-fastEthernet0/24)#switchport mode trunk
S1(config-if-fastEthernet0/24)#switchport trunk native vlan 98
S2(config)#interface f0/24
S2(config-if-fastEthernet0/24)#switchport mode trunk
S2(config-if-fastEthernet0/24)#switchport trunk native vlan 98
```

4. 实验调试

(1) 使用“show vlan”查看 VLAN 信息。

(2) 测试同一 VLAN 主机间的通信。


实验 3-4
视频

实验 3-4：VLAN 间路由

传统 VLAN 间路由的实现方法是通过将不同的物理路由器接口连接至不同的物理交换机端口来执行 VLAN 间路由。如果两台 PC 虽然在同一台交换机上，但是处于不同 VLAN 中，那么它们之间的通信也必须使用路由器。可以在每个 VLAN 上选择一个以太网接口和路由器连接，在路由器的以太网接口上配置 IP 地址，PC 上的默认网关指向同一 VLAN 中的路由器以太网接口地址。如果要实现 N 个 VLAN 间通信，那么路由器需要 N 个以太网接口，同时也会占用交换机的 N 个端口，因此该方法只适用于少量 VLAN 之间需要通信的情况。

而单臂路由可以通过单个物理接口实现网络中多个 VLAN 之间数据流的传递。路由器只需要一个以太网口和交换机连接，交换机的这个端口被设置为 Trunk 端口。在路由器上创建多个子接口作为不同 VLAN 主机的默认网关，根据各自 VLAN 的分配，子接口被配置到不同的子网中，从而使用路由器物理接口和子接口实现 VLAN 间路由。

1. 实验目的

(1) 路由器以太网接口上的子接口配置。

(2) 单臂路由实现 VLAN 间路由配置。

2. 实验拓扑

实验拓扑如图 3-5 所示。

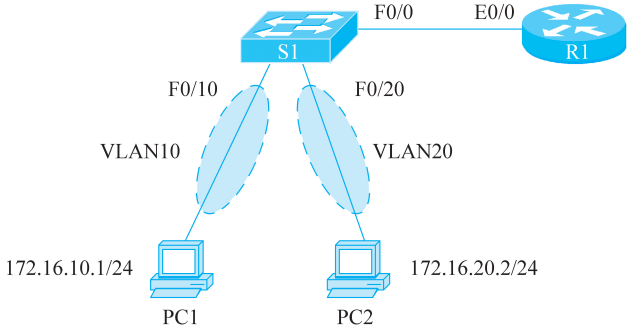

图 3-5 VLAN 间路由拓扑图

3. 实验步骤

(1) 在 S1 上创建 VLAN。

```
S1(config)#vlan 10
S1(Config-Vlan10)#name VLAN10
S1(Config-Vlan10)#exit
S1(config)#vlan 20
S1(Config-Vlan20)#name VLAN20
```

(2) 把端口划分在 VLAN 中。

```
S1(config)#vlan 10
S1(Config-Vlan10)#switchport interface fastEthernet 0/10
```

```
S1(Config-Vlan10)#exit
S1(config)#vlan 20
S1(Config-Vlan20)#switchport interface fastEthernet 0/20
```

(3) 在交换机上配置 Trunk。

```
S1(config)#int f0/0
S1(config-if-fastEthernet0/0)#switchport mode trunk
```

(4) 在路由器的物理以太网接口下创建子接口,并定义封装类型。

```
R1_config#int e0/0
R1_config_e0/0#no shutdown
R1_config#int e0/0.10
R1_config_e0/0.10#encapsulation dot1q 10
R1_config_e0/0.10#ip address 172.16.10.254 255.255.255.0
R1_config#int e0/0.20
R1_config_e0/0.20#encapsulation dot1q 20
R1_config_e0/0.20#ip address 172.16.20.254 255.255.255.0
```

4. 实验调试

(1) 使用“show vlan”查看 VLAN 信息。

(2) 测试 VLAN 之间的连通性。

3.4　MSTP

MSTP(Multiple Spanning Tree Protocol,多生成树协议)主要应用于在网络中建立树状拓扑,消除网络中的环路。一般网络设计中,为了增加局域网的冗余性,常常会引入冗余链路,然而这样却会引起交换环路。交换环路会带来广播风暴、同一帧的多个副本、交换机 CAM 表不稳定等问题,对网络性能有着极为严重的影响。STP(Spanning Tree Protocol,生成树协议)可以解决这些问题。STP 会阻塞可能导致环路的冗余路径,以确保网络中所有目的地之间只有一条逻辑路径。当一个端口阻止流量进入或离开时,称该端口处于阻塞(Block)状态。阻塞冗余路径对于防止交换环路非常关键。为了提供冗余功能,这些阻塞的物理路径实际上依然存在,只是被禁用以免产生环路。一旦网络发生故障,需要启用处于阻塞状态的端口,使 STP 重新计算路径,将需要的端口解除阻塞,使阻塞端口进入转发状态。

STP(IEEE 802.1d)的基本工作原理是阻断一些交换机接口,构建一棵没有环路的转发树。它利用 BPDU(Bridge Protocol Data Unit)和其他交换机进行通信,从而确定哪个交换机应该阻断哪个接口。为了在网络中形成一个没有环路的拓扑,网络中的交换机要进行以下三个步骤。

(1) 选举一个根桥。

(2) 在非根桥上选举根端口。

(3) 在每个网段中选择指定端口。

STP 有多个版本,是在早期的 IEEE 802.1d 上引入了一些新技术形成的。IEEE 802.1d 具有重新收敛时间较长的缺点,通常需要 30～50s 才能收敛,为了减少这个时间,在此基础上增加了一些新技术,例如 uplinkfast、backbonefast 和 postfast 等。RSTP(快速生成树协议)对 STP 做出了很大的改进,大大地减少了收敛时间,形成了新的协议。MSTP 首先通过设置 VLAN 映射表(即 VLAN 和生成树的对应关系表),把 VLAN 和生成树联系了起来。然后通过"实例"将多个 VLAN 整合到一个集合中,最后将集合中的多个 VLAN 捆绑到一个实例中,从而节省带宽和资源占用率。

实验 3-5：MSTP

1. 实验目的

生成树协议是为了防止路由环路。

(1) 理解 STP 的工作原理。

(2) 理解 MSTP 的工作原理。

(3) 利用 MSTP 进行负载平衡。

2. 实验拓扑

实验拓扑如图 3-6 所示。

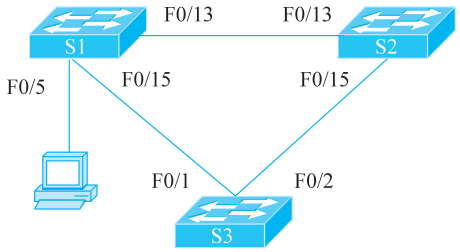

图 3-6 STP 基本配置拓扑图

3. 实验步骤

(1) 在交换机上创建 VLAN2,在 S1 和 S2 之间的链路上配置 Trunk,S3 配置 Trunk(S3 配置省略)。

```
S1(config)#vlan 2
S1(config)#int f0/13
S1(config-if-fastEthernet0/13)#switchport mode trunk
S2(config)#vlan 2
S2(config)#int f0/13
S2(config-if-fastEthernet0/13)#switchport mode trunk
```

(2) 建立 MSTP 实例,控制 S1 为 VLAN1 的根桥,S2 为 VLAN2 的根桥。

```
S1(config)#spanning-tree mst configuration
S1(config-mstp-region)#name mstp
S1(config-mstp-region)#instance 1 vlan 1
```

```
S1(config-mstp-region)#instance 2 vlan 2
S1(config-mstp-region)#exit
S1(config)#spanning-tree
S1(config)#interface f0/13
S1(config-if-fastEthernet0/13)#spanning-tree mst 1 priority 4096
S2(config-if-fastEthernet0/13)#spanning-tree mst 2 priority 4096
```

（3）控制指定端口。

从步骤(2)中可以看到，对于 VLAN1，S1 成为根桥，S1 的 f0/13 和 f0/15 处于转发状态；S2 的 f0/13 是根端口，也处于转发状态；假设 S3 的 f0/1 是根端口，也处于转发状态，那么在 S2 和 S3 之间的链路上，却是交换机 S3 的 f0/2 在转发数据，这是不合理的。

要控制指定端口，可以通过改变优先级实现。

```
S1(config-if-fastEthernet0/15)#spanning-tree mst 1 priority 8192
S2(config-if-fastEthernet0/15)#spanning-tree mst 2 priority 8192
```

4. 实验调试

使用“show spanning-tree”检查 MSTP 树。

实验 3-6：边缘端口配置

不直接与任何交换机连接，也不通过端口所连接的网络间接与任何交换机相连。简单来说，就是不需要参与到生成树协议的端口，一般指交换机接入 PC 等终端的端口。

1. 实验目的

理解 portfast 的工作场合和配置。

2. 实验拓扑

实验拓扑如图 3-7 所示。

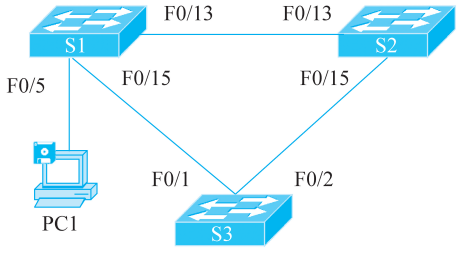

图 3-7　portfast 拓扑图

3. 实验步骤

（1）配置生成树协议，参看实验 3-5。

（2）配置 portfast。

```
S1(config)#interface fastEthernet 1/0/5
S1(Config-If-fastEthernet1/0/5)#spanning-tree portfast bpduguard recovery 60
//配置边缘端口模式为 BPDU guard，恢复时间为 60s。
```

4. 实验调试

S1 交换机 F0/5 与交换机 S3 相连后,检测 S1 交换机 F0/5 状态。

3.5 链路聚合

链路聚合(Link Aggregation)是指将多个物理端口捆绑在一起,成为一个逻辑端口,以实现出/入流量在各成员端口中的负荷分担,交换机根据用户配置的端口负荷分担策略决定报文从哪一个成员端口发送到对端的交换机。

链路聚合的使用场景一般是,当交换机多条链路相连,但是不需要 MSTP 的时候。


实验 3-7 视频

实验 3-7:链路聚合

1. 实验目的

熟悉链路聚合的配置。

2. 实验拓扑

实验拓扑如图 3-8 所示。

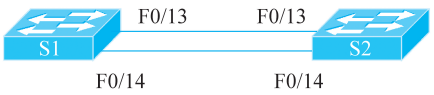

图 3-8 链路聚合配置拓扑图

3. 实验步骤

(1) 创建 S1 和 S2 之间的链路聚合端口。

```
S1(Config)#port-group 1
S2(Config)#port-group 1
```

(2) 配置 S1 和 S2 的链路聚合。

```
S1(config)#interface fastEthernet 0/13-14
S1(config-if-port-range) #port-group 1 mode on
S2(config)#interface fastEthernet 0/13-14
S2(config-if-port-range) #port-group 1 mode on
```

启动 LACP(链路聚合控制协议)的端口可以有两种工作模式,分别是 passive 和 active。

(1) passive:被动模式,该模式下端口不会主动发送 LACPDU 报文,在接收到对端发送的 LACP 报文后,该端口进入协议计算状态。

(2) active:主动模式,该模式下端口会主动向对端发送 LACPDU 报文,进行 LACP 的计算。

4. 实验调试

(1) 使用“show port-group brief”检查其 mode 是否为 on。

(2) 使用“show int port-channel 1”(group 号)检查其协议是否为 up。