第 6 章　网络设备管理与 VPN 技术

网络规模的扩大和网络设备数量的增加，使网络维护的难度越来越大，而且随着网络设备生产商数量的不断增加，各种各样的网络设备层出不穷，因此，如何更好地对网络设备进行维护是网络管理的重中之重。网络设备管理通常是指对网络设备的规划、连接、配置与维护。组建网络常用的网络设备包括交换设备、路由设备、安全设备。要想成为一名合格的网络管理员，必须熟练掌握这 3 类设备的配置、管理与维护。

在现代网络中，交换机已经取代集线器，成为网络中运用最多的设备之一。对于一个在性能、安全方面要求不高的局域网络，可以直接使用非网管交换机，此类交换机只有交换功能，无须配置，用传输介质连接后即可使用。而对于网络性能要求较高的网络来说，必须使用可网管智能型交换机。路由器是工作在 OSI 参考模型的网络层，实现网络互联的网络设备。它可以用来连接两个或多个局域网，亦可以连接局域网和广域网或广域网和广域网。路由器的主要功能是实现路由选择、访问控制和数据转发。它根据每台终端的所处子网的子网号来区分不同的网络，路由器可以隔离广播，把每个子网的广播数据包限制在网络内部。通过路由器的访问控制功能，能够实现网络间的互联与隔离，保持各个网络的独立性。

6.1　交换机的配置与管理

交换机是网络中最常见的设备之一，作为网络管理人员，必须掌握交换机的基本配置与管理。

6.1.1　交换机简介

交换机作为 OSI 参考模型中数据链路层的设备，在网络中是最基本的数据传输和通信设备，它是和通信终端直接相连的网络通信硬件设备。因此，了解、掌握交换机的通信原理对网络管理起着十分重要的作用。

1. 通信系统基本模型

通信系统由以下几个部分组成：

(1)信源和信宿。信源是指发出信息的信息源。根据信源输出信号的性质可分为模拟信源(如公共电话系统)和数字信源(如计算机)。模拟信源可通过采样和量化调制为数字信源。信宿是指信息传送的终端。

(2)调制器和解调器。调制器用于将信源发出的信号转换成适合于在信道上传输的信号。解调器完成与调制器相反的转换。

(3)信道。传输信道是指连接调制器和解调器之间的传输系统。按传输媒介类型的不同可将传输信道分为有线信道和无线信道。

(4)噪声源。噪声干扰在实际通信系统中总是客观存在的，会造成有用信号畸变，降低

通信质量。外部的干扰和系统内部设备的噪声会引起通信过程中产生杂音甚至串音。

通信系统的基本模型如图 6-1 所示。

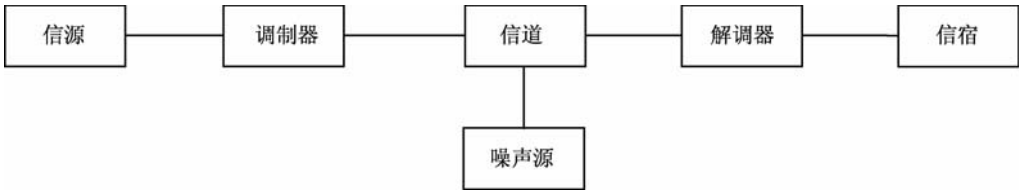

图 6-1　通信系统的基本模型

2. 交换的概念

通信作为信息产业化的基础，在信息化进程中发挥着先锋带头作用。随着通信技术的飞速发展，通信新业务不断涌现，电话通信和数据通信已成为现代社会应用最广泛的信息交流方式，是人们日常生活和工作中不可缺少的一部分。

为了实现有效的通信就需要采用交换技术。所谓交换，就是在通信网络中，交换设备根据用户的呼叫请求建立连接，相互传送话音、数据、图像、视频等信息。任何一个主叫用户的信息，都可以通过通信网络中的交换设备和传输设备发送到任何一个或多个被叫用户。

广义的交换机(switch)就是一种在通信系统中完成信息交换功能的设备。

在计算机网络中，对共享工作模式进行改进提出了交换的概念。集线器(hub)是一种共享式网络设备，集线器本身不能识别目的 MAC 地址，当位于同一个局域网内的主机 A 给主机 B 传输数据时，数据包在以集线器为架构的网络上是以广播方式传输的，由每个终端通过检查数据包头的地址信息来确定是否接收该数据包。也就是说，在这种工作方式下，同一时刻网络上只能传输一组数据帧，如果发生冲突必须随机重传。这种方式就是共享网络带宽。

而交换机则不同，交换机拥有一条很高带宽的背部总线和内部交换矩阵。交换机的所有端口都挂接在这条背部总线上，控制电路收到数据包以后，处理端口会查找内存中的 MAC 地址表，确定目的 MAC(网卡的硬件地址)所对应的端口，通过内部交换矩阵迅速将数据包传送到目的端口。若目的 MAC 不存在，则采取广播方式将数据包广播到所有的端口，接收端口回应后交换机会“学习”新的地址，并把它添加入内部 MAC 地址表中。

使用交换机也可以把网络“分段”，通过对照 MAC 地址表，交换机只允许必要的网络流量通过。通过交换机的过滤和转发，可以有效地隔离广播风暴，减少错误的数据包出现，避免共享冲突。

交换机在同一时刻可进行多个端口对之间的数据传输。每一端口都可视为独立的网段，连接在其上的网络设备独自享有全部的带宽，无须同其他设备竞争使用。当主机 A 向主机 D 发送数据时，主机 B 可同时向主机 C 发送数据，而且这两个传输都享有网络的全部带宽，都有着自己的虚拟连接。假设这里使用的是 100 Mbps 的以太网交换机，那么该交换机这时的总流通量就等于 2×100 Mbps＝200 Mbps；而使用 10 Mbps 的共享式集线器时，一个集线器的总流通量也不会超出 10 Mbps。

总之，交换机是一种基于 MAC 地址识别，能完成封装转发数据包功能的网络设备。交换机可以通过“学习”MAC 地址，将其存放在内部 MAC 地址表中，以便在数据帧的始发者和目标接收者之间建立临时的交换路径，使数据帧直接由源地址到达目的地址。

3. 交换的方式

交换技术从传统的电话交换技术发展到现代交换技术，数据的交换方式主要有电路交换、报文交换和分组交换。

1)电路交换

电路交换的概念源于电话系统交换。传统电话网由传输线路，程控交换机和电话机组成，处于网络结点的程控交换机用来完成主、被叫用户之间传输链路的选择、建立，形成一条主叫至被叫的物理电路，通话结束时拆除该物理电路，这种交换方式称为电路交换方式。电路交换的基本过程包括呼叫建立、通话和释放链路 3 个阶段。

电路交换具有实时、信道独占、延时小等优点，但是电路交换技术的缺点也很明显，如网络资源利用率低、通信效率不高等。

2)报文交换

报文交换技术是一种存储转发技术，它没有在两端通信设备间建立一条物理线路。发送设备将发送的信息作为一个整体(又被称为报文)，并附加上目的地址，交给交换设备。交换设备接收该报文，并存储在缓存中，等到有合适的输出线路时再把该报文转发给下一个交换设备。当路由器接收到报文以后会对报文进行处理，查看其目的路由器地址，然后用路由算法算出到达目的地的最佳路径后将报文送往下一路由器，经过若干个交换设备的存储、转发后，该报文到达目的地。报文交换技术适用于非实时的通信系统，如公共电报收发系统。

报文交换具有线路利用率高、能够建立报文优先级等优点，但是也存在着延迟大的缺点。

3)分组交换

分组交换源于数据通信，它解决了数据通信的通信线路资源共享问题。数据通信的特点是业务突发性高、可靠性要求高，而对实时性要求不严格。分组交换方式的工作过程是分组终端将用户要发送的数据分割为长度固定的数据分组，每个分组都有一个分组头，包含了控制信息和路由信息。采用分组交换时，同一个报文的多个分组可以同时传输，多个用户的信息也可以共享同一物理链路，因此分组交换可以实现资源共享，并为用户提供可靠、有效的数据服务。它克服了电路交换中独占线路、线路利用率低的缺点。

4. 二层交换和三层交换

前面介绍了交换的概念，下面介绍二层交换和三层交换的概念。

二层交换是利用专用集成电路(ASIC)来完成局域网内数据通信的交换。在网络系统中，具有二层交换功能的设备称为交换机，它工作在 OSI 模型中的数据链路层。交换机通过其内存中的 MAC 地址表和庞大的交换矩阵完成数据在局域网内的转发。

三层交换也是利用 ASIC 芯片，但它是用来完成计算机网络中的数据路由。三层交换其实是在二层交换的基础上加入了路由功能。因为在 OSI 模型中，路由功能由其第三层网络层来实现，故称为三层交换机或路由交换机。三层交换机技术通过“一次路由，多次交换”的工作机制和线速转发的优势，逐步代替了传统路由器，提高了数据包的转发效率，消除了网络瓶颈。

6.1.2 交换机的基本配置

交换机的基本配置包括对交换机标识、IP 地址、默认网关的配置。本章以 Cisco 交换机

为例，介绍交换机的基本配置。具体的命令及格式在此不作详细介绍，读者可以参考相关资料。

1. 交换机的配置方式

交换机常见的配置方式主要有 3 种：通过 Console 端口配置、Telnet 远程登录配置和 Web 浏览器方式配置。下面以 Cisco 交换机为例，简单介绍这 3 种配置方式。

1）通过 Console 端口进行配置

Cisco 交换机上有一个 Console 端口，它是专门用于对交换机进行配置和管理的。可以通过 Console 端口连接和配置交换机。使用串口线将 Cisco 交换机的配置线和计算机的串口相连接（注意：必须记清接入的是哪个串口）。连接示意图如图 6-2 所示。

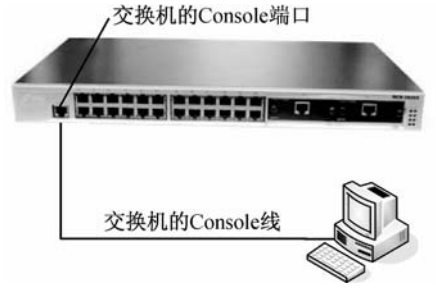

图 6-2　交换机的连接示意图

连接好后，执行以下操作：

（1）打开超级终端。执行“开始”→“程序”→“附件”→“通讯”→“超级终端”命令，打开超级终端，如图 6-3 所示。

图 6-3　超级终端

（2）执行“文件”→“新建”命令，新建一个超级终端连接，输入新建连接的名称，如图 6-4 所示。

（3）单击“确定”按钮，打开“连接到”对话框，在“连接时使用”下拉列表中选择与交换机的 Console 端口相连接的串口，这里选择 COM1，如图 6-5 所示。

图 6-4 新建超级终端连接

图 6-5 “连接到”对话框

(4)单击“确定”按钮,打开 COM1 属性对话框。在“端口设置”选项卡中根据交换机使用手册的说明分别设置每秒位数、数据位、奇偶校验、停止位、数据流控制,如图 6-6 所示。对于大部分交换机来说,只需单击“还原为默认值”按钮即可。

图 6-6 “COM1 属性”对话框

(5)单击“确定”按钮后开启交换机。此时交换机开始载入 IOS(网际操作系统),可以从载入的 IOS 界面上看到 IOS 版本号、交换机型号、内存大小等数据。当屏幕显示“Press RETURN to get started!”时按 Enter 键就能直接进入交换机。

2)通过 Telnet 对交换机进行远程配置

Telnet 是一种远程访问协议,可以用它登录远程计算机、网络设备或专用 TCP/IP 网络。目前常用的 Windows、UNIX、Linux 等系统中都内置有 Telnet 客户端程序,可以用它来实现与远程交换机的通信。

在使用 Telnet 连接至交换机前,应当确认已经做好了以下准备工作:

- 在用于管理交换机的计算机中安装有 TCP/IP,并配置好了 IP 地址信息。
- 在被管理的交换机上已经配置好 IP 地址信息。如果尚未配置 IP 地址信息,则必须通过 Console 端口进行设置。

• 必须针对 Telnet 功能配置一个登录密码，这样 Telnet 功能才会自动打开。

在计算机上运行 Telnet 客户端程序，并登录至远程交换机。这里假设已经设置交换机的 IP 地址为 192.168.1.1，下面只介绍进入交换机配置界面的方法，其他的配置则和前面介绍的一样，在此不作具体介绍。进入配置界面的步骤如下：

(1)执行“开始”→“运行”命令，在打开的“运行”对话框中输入“telnet 192.168.1.1”，如图 6-7 所示。如果为交换机配置了名称，则也可以直接在“telnet”命令后面空一个空格后输入交换机的名称。

图 6-7　Telnet 使用实例

Telnet 命令的一般格式如下：

```
telnet hostname/port
```

需要注意的是，hostname 可以是交换机的名称，更多的是指交换机的 IP 地址。格式后面的 port 一般是不需要输入的，它是用来设定 Telnet 通信所用的端口的。一般来说，Telnet 的通信端口，在 TCP/IP 中默认为 23 号端口。

(2)输入完成后，单击“确定”按钮或按 Enter 键，即建立与远程交换机的连接。

3)通过 Web 浏览器对交换机进行配置

当利用 Console 端口为交换机设置好 IP 地址并启用 HTTP 服务后，即可通过支持 Java 的 Web 浏览器访问交换机、修改交换机的各种参数对交换机进行管理，并可实时查看交换机的运行状态。不过在利用 Web 浏览器访问交换机之前，应当确认已经做好了以下准备工作：

- 在用于管理的计算机中安装了 TCP/IP 协议，且在计算机和被管理的交换机上都已经配置好 IP 地址信息。
- 用于管理的计算机中安装有支持 Java 的 Web 浏览器，如 Internet Explorer 4.0 及以上版本、Netscape 4.0 及以上版本，以及 Oprea with JAVA。
- 在被管理的交换机上建立了拥有管理权限的用户名和密码。
- 被管理交换机的 Cisco IOS 支持 HTTP 服务，并且已经启用了该服务。否则，应通过 Console 端口升级 Cisco IOS 或启用 HTTP 服务。

对于运行 IOS 的交换机，启用 HTTP 服务后，即可利用 Web 界面来管理交换机。在浏览器中输入“http://交换机管理 IP 地址”，弹出用户认证对话框，用户名可不指定，然后在密码文本框中输入进入特权模式的密码，之后就可进入交换机的管理界面。

交换机的 Web 配置界面功能较弱且安全性较差，在实际应用中，主要还是采用命令行方式来配置。交换机默认启用 HTTP 服务，因此在配置时，应禁用该服务。

启用 HTTP 服务，配置命令如下：

```
ip http server
```

禁用 HTTP 服务，配置命令如下：

```
no ip http server
```

2. 交换机的配置模式

Cisco IOS 提供了 6 种配置模式：用户 EXEC 模式、特权 EXEC 模式、全局配置模式、接口配置模式、Line 配置模式和 VLAN 数据库配置模式。

在实际配置的过程中，用户可以根据实际需要使用不同配置模式的相应命令来进行模式转换。例如：

- 由用户 EXEC 模式进入特权 EXEC 模式，使用 enable 命令。
- 由特权 EXEC 模式进入全局配置模式，使用 configure terminal 命令。
- 由全局配置模式进入接口配置模式，使用“interface ＋端口类型＋端口号”命令。
- 由特权 EXEC 模式进入 VLAN 数据库配置模式，使用 vlan database 命令。
- 由全局配置模式进入 Line 配置模式，使用“line＋接口类型＋接口号”命令。

下面具体介绍各种模式。

1）用户 EXEC 模式

当用户通过交换机的 Console 端口或 Telnet 会话连接并登录交换机时，此时所处的命令执行模式就是用户 EXEC 模式。在该模式下，只执行有限的一组命令，这些命令通常用于查看系统信息、改变终端设置和执行一些最基本的测试命令，如 ping、traceroute 等。

用户 EXEC 模式的命令行提示符为：

```
cisco2900>
```

其中，cisco2900 是交换机的名字，对于未配置的交换机的默认主机名是 Switch。在用户 EXEC 模式下，直接输入“?”并按 Enter 键，可获得在该模式下允许执行的命令的帮助信息。

2）特权 EXEC 模式

在用户 EXEC 模式下，执行 enable 命令，可进入特权 EXEC 模式。在该模式下，用户能够执行 IOS 提供的所有命令。

特权 EXEC 模式的命令行提示符为：

```
cisco2900#
```

例如：

```
cisco2900>enable
password:
cisco2900#
```

在前面的启动配置中，因为设置了登录特权 EXEC 模式的密码，所以系统提示输入用户密码，密码输入时不回显，输入完毕按 Enter 键，密码校验通过后，即进入特权 EXEC 模式。

如果要修改或设置进入特权 EXEC 模式的密码，可在全局配置模式下，利用 enable secret 或者 enable password 命令进行设置。

在该模式下输入“?”，可获得在该模式下允许执行的全部命令的提示信息。要离开特权模式，返回用户模式，可执行 exit 或 end 命令。

配置好后，重新启动交换机，则执行 reload 命令。

3）全局配置模式

在特权 EXEC 模式下，执行 configure terminal 命令，即可进入全局配置模式。在该模

式下，只要输入一条有效的配置命令并按 Enter 键，内存中正在运行的配置就会立即生效。该模式下的配置命令的作用域是全局性的，对整个交换机起作用。

全局配置模式的命令行提示符为：

```
cisco2900(config)#
```

命令格式如下：

```
cisco2900#configure terminal
cisco2900(config)#
```

在全局配置模式下，还可进入接口配置、Line 配置等子模式。从子模式返回全局配置模式，执行 exit 命令，再从全局配置模式返回特权 EXEC 模式，执行 exit 命令。若要直接返回特权 EXEC 模式，则执行 end 命令或按 Ctrl＋Z 组合键。

4)接口配置模式

在全局配置模式下，执行“interface＋端口类型＋端口号”命令，即进入接口配置模式。在该模式下，可对选定的接口(端口)进行配置，并且只能执行配置交换机端口的命令。

接口配置模式的命令行提示符为：

```
cisco2900(config-if)#
```

5)Line 配置模式

在全局配置模式下，执行“line＋接口类型＋接口号”命令，将进入 Line 配置模式。比如，执行 line vty 或 line console 命令，主要用于对虚拟终端(vty)和 Console 端口进行配置，其配置主要是设置虚拟终端和控制台的用户级登录密码。

Line 配置模式的命令行提示符为：

```
cisco2900(config-line)#
```

交换机有一个控制端口，其编号为 0，通常利用该端口进行本地登录，以实现对交换机的配置和管理。为安全起见，应为该端口的登录设置密码。具体设置方法参考对登录密码设置的介绍。

6)VLAN 数据库配置模式

在特权 EXEC 模式下执行 vlan database 配置命令，即可进入 VLAN 数据库配置模式。VLAN 数据库配置模式的命令行提示符为：

```
cisco2900(vlan)#
```

在该模式下，可实现对 VLAN(虚拟局域网)的创建、修改和删除等操作。退出 VLAN 配置模式，返回特权 EXEC 模式，可执行 exit 命令。

3. 配置主机名与 IP 地址

1)配置主机名

```
switch>enable
switch#configure terminal
switch(config)#hostname cisco2900
```

2)配置 IP 地址

```
cisco2900(config)#interface vlan 1                          /* 进入 VLAN 配置模式 */
cisco2900(config-if)#ip address 192.168.1.1 255.255.255.0 /* 配置交换机 IP */
cisco2900(config-if)#no shutdown                            /* 启用 VLAN */
cisco2900(config-if)#exit
```

```
cisco2900(config)#ip default-gateway 192.168.1.254   /* 配置交换机的默认网关 */
```

4.配置登录密码

1)控制台登录口令

```
cisco2900#config terminal
cisco2900(config)#line console 0                    /* 进入 Line 配置模式 */
cisco2900(config-line)#password cisco2900           /* 配置密码为 cisco2900 */
cisco2900(config-line)#login                        /* 启用密码 */
cisco2900(config-line)#end
```

上面的配置是将控制台登录密码设为 cisco2900,并启用该密码。配置该密码后,以后利用控制台端口登录交换机时,会首先要求输入该登录密码,密码校验成功后,才能进入交换机的用户 EXEC 模式。

2)配置远程登录密码

交换机支持多个虚拟终端,一般为 16(0～15)个。配置了密码的虚拟终端,允许登录,没有配置密码的,禁止登录。如果对 0～4 条虚拟终端线路配置了登录密码,则交换机允许同时有 5 个 Telnet 登录连接,配置远程登录密码的命令为:

```
cisco2900(config)#line vty 0 4
cisco2900(config-line)#password csico2900
cisco2900(config-line)#login
cisco2900(config-line)#end
cisco2900#write memory
```

若要配置不允许 Telnet 登录,则取消对终端密码的配置即可,为此可执行 no password 和 no login 命令来实现。

在 Cisco IOS 命令中,若要实现某条命令的相反功能,只需在该条命令前面加 no,并执行前缀有 no 的命令即可。

为了防止空闲的连接长时间存在,通常还应给通过 Console 端口和 vty 线路的 Telnet 登录连接,设置空闲超时时间,默认空闲超时时间是 10 分钟。

设置空闲超时时间的命令为:

```
exec-timeout 分钟数 秒数
```

例如,要将 vty 04 线路和 Console 的空闲超时时间设置为 3 分钟 0 秒,则配置命令为:

```
cisco2900#config t
cisco2900(config)#line vty 0 4
cisco2900(config-line)#exec-timeout 3 0
cisco2900(config-line)#line console 0
cisco2900(config-line)#exec-timeout 3 0
cisco2900(config-line)#end
```

3)配置特权 EXEC 模式密码

若要配置或修改进入特权 EXEC 模式的密码为 123456,则配置命令为:

```
cisco2900(config)#enable secret 123456
```

或

```
cisco2900(config)#enable password 123456
```

其中，enable secret 命令配置的密码在配置文件中是以密文的形式保存的，推荐采用该方式；enable password 命令所配置的密码在配置文件中是采用明文保存的。

5. 保存配置信息

对交换机的配置进行修改后，为了使配置在交换机下次断电重启后仍生效，需要将新的配置信息保存到 NVRAM 中，其配置命令为：

```
cisco2900(config)#exit
cisco#write memory
```

6. 查看交换机信息

对交换机信息的查看，使用 show 命令来实现。

1）查看 IOS 版本

查看命令：

```
show version
```

2）查看配置信息

要查看交换机的配置信息，需要在特权 EXEC 模式执行以下命令：

```
show running-config
```

显示当前正在生效的配置。

```
show startup-config
```

要查看保存在 NVRAM 中的启动配置信息。例如，若要查看当前交换机正在生效的配置信息，则执行命令：

```
cisco2900#show run
```

7. 配置交换机接口

1）配置接口模式

Cisco 交换机的接口类型有 access、trunk、dynamic。其中，access 接口主要用来接入终端设备，如 PC、服务器、打印服务器等；trunk 接口主要用于连接其他交换机，以便在线路上承载多个 VLAN；dynamic 接口中的 dynamic auto 指自动协商是否成为 trunk，属于主动方式，dynamic desirable 指把端口设置为 trunk，如果对方端口是 trunk 或 desirable，属于被动方式。

配置接口模式的命令如下：

```
cisco2900(config)#interface fa0/1
cisco2900(config-if)#switchport mode access   /* 将交换机端口接口模式配置为
                                                 access 模式 */
cisco2900(config)#no shutdown                 /* 启用端口 */
```

2）配置接口描述、速度、双工模式

配置接口描述、速度、双工模式的命令如下：

```
cisco2900(config)#interface fa0/1             /* 进入接口配置模式 */
cisco2900(config-if)#speed 100                /* 配置接口速率为 100M */
cisco2900(config-if)#description it is my port/* 配置端口描述为 it is my port */
cisco2900(config-if)#duplex full              /* 配置接口交换方式为全双工 */
cisco2900(config-if)#no shutdown
```

3)启用接口

启用某个接口的命令为：

no shutdown

注意：每次对接口进行更改过后，都必须启用一次。

6.1.3 VLAN 技术简介及配置实例

1. VLAN 技术简介

虚拟局域网(virtual local area network，VLAN)是一种将局域网设备从逻辑上划分成一个个网段，从而实现虚拟工作组的新兴数据交换技术。这一新兴技术主要应用于交换机和路由器中。IEEE 于 1999 年颁布了用以标准化 VLAN 实现方案的 802.1Q 协议标准草案。

VLAN 技术的出现，使得网络管理员能够根据实际应用需求，把同一物理局域网内的不同用户逻辑地划分成不同的广播域，每一个 VLAN 都包含一组有着相同需求的计算机工作站，与物理上形成的 LAN 有着相同的属性。由于它是从逻辑上划分，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不同物理 LAN 网段。由 VLAN 的特点可知，一个 VLAN 内部的广播和单播流量都不会转发到其他 VLAN 中，从而有助于控制流量、减少设备投资、简化网络管理、提高网络的安全性。

交换技术的发展，也加快了新的交换技术的应用速度。通过将企业网络划分为虚拟网络网段，强化了网络管理和网络安全，控制不必要的数据广播。在共享网络中，一个网段就是一个广播域。而在交换网络中，广播域可以是一组由任意选定的 MAC 地址组成的虚拟网段。这样，网络中工作组的划分可以突破共享网络中的地理位置限制，而完全根据管理功能来划分。这种基于工作流的分组模式，大大提高了网络规划和重组的管理功能。在同一个 VLAN 中的工作站，不论它们实际与哪个交换机连接，它们之间的通信就好像在独立的交换机上一样。同一个 VLAN 中的广播只有该 VLAN 中的成员才能收到，而不会传输到其他的 VLAN 中，这样可以很好地控制广播风暴的产生。同时，若没有路由，则不同的 VLAN 之间不能相互通信，这样增强了企业网络中不同部门之间的安全性。网络管理员可以通过配置 VLAN 之间的路由来全面管理企业内部不同管理单元之间的信息互访。交换机是根据用户工作站的 MAC 地址来划分 VLAN 的。所以，用户可以自由地在企业网络中移动办公，不论在何处接入交换网络，都可以与 VLAN 内其他用户自由通信。

虚拟局域网除了能将网络划分为多个广播域，从而有效地控制广播风暴的发生，以及使网络的拓扑结构变得非常灵活外，还可以用于控制网络中不同部门、不同站点之间的互相访问。VLAN 是为解决以太网的广播问题和安全性而提出的一种协议，它在以太网帧的基础上增加了 VLAN 头，用 VLAN ID 把用户划分为更小的工作组，限制不同工作组间的用户互访，每个工作组就是一个虚拟局域网。虚拟局域网的好处是可以限制广播范围，并能够形成虚拟工作组，动态管理网络。

2. VLAN 的划分

VLAN 的划分主要有 3 种方法。

1)基于端口的 VLAN

基于端口的 VLAN 是指将选定的端口划分在同一个广播域中。例如,一个交换机的 1～10 号端口组成 VLAN 10,11～20 端口组成 VLAN 20,从而减小了广播域,抑制了广播风暴的产生。随着交换机技术的发展,出现了允许跨交换机的基于端口的 VLAN 划分技术,使 VLAN 的划分更为灵活。

以交换机端口来划分网络成员,其配置过程简单明了。因此,从目前来看,这种根据端口来划分 VLAN 的方式仍然是最常用的。

2)基于 MAC 地址的 VLAN

基于 MAC 地址的 VLAN 是根据每个主机的 MAC 地址来划分的。这种划分方法的最大优点就是当用户物理位置移动时,例如,从一个交换机移动到其他的交换机时,VLAN 不需要重新配置。所以可以认为,基于 MAC 地址的划分方法是基于用户的 VLAN,这种方法的缺点是初始化时,导致交换机执行效率降低,因为在每一个交换机的端口都可能存在很多个 VLAN 组的成员,这样就无法限制广播包了。另外,对于使用笔记本电脑的用户都必须进行配置,如果有几百个甚至上千个用户,配置是非常麻烦的。而且对这种划分来说,如果网卡经常更换,VLAN 就必须不停地配置。

3)基于 IP 的 VLAN

基于 IP 的 VLAN 是根据每个主机的 IP 地址来划分的。需要明确的是,虽然这种划分方法依据 IP 地址,但其与网络层的路由功能没有任何关系。

基于 IP 的划分方法的优点是如果用户的物理位置改变了,不需要重新配置所属 VLAN,并且可以根据协议类型来划分 VLAN。另外,这种方法不需要附加的帧标签来识别 VLAN,从而减少了网络的通信量。

这种方法的缺点是效率低,因为检查每一个数据包的 IP 地址是需要消耗处理时间的(相对于前面两种方法),一般的交换机芯片都可以自动检查网络上数据包的以太网帧头,但要让芯片能检查 IP 帧头,需要更高的技术,同时也更费时。当然,这与各个厂商的实现方法有关。

以上划分 VLAN 的方式中,基于端口的 VLAN 划分方式建立在物理层;基于 MAC 地址的 VLAN 划分方式建立在数据链路层;基于 IP 的 VLAN 划分方式建立在网络层。

3. VLAN 的配置实例

下面以 Cisco 3560 交换机为例介绍 VLAN 的配置。

1)交换机 VLAN 的划分

```
Switch>en
Switch#configure terminal                    /* 进入交换机的配置模式 */
Enter configuration commands,one per line. End with CNTL/Z.
Switch(config)#vlan 10                       /* 划分一个 VLAN,ID 为 10 */
Switch(config-vlan)#name testvlan10          /* 将新建的 VLAN 命名为 testvlan10 */
Switch(config-vlan)#exit
Switch(config)#exit
Switch#show vlan                             /* 查看 VLAN 信息 */
```

```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1,Fa0/2,Fa0/3,Fa0/4
                                                 Fa0/5,Fa0/6,Fa0/7,Fa0/8
                                                 Fa0/9,Fa0/10,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,Fa0/24
                                                 Gig0/1,Gig0/2
10   testvlan10                        active
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup

VLAN  Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
----- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1     enet  100001     1500  -      -      -        -    -        0      0
10    enet  100010     1500  -      -      -        -    -        0      0
1002  fddi  101002     1500  -      -      -        -    -        0      0
1003  tr    101003     1500  -      -      -        -    -        0      0
1004  fdnet 101004     1500  -      -      -        ieee -        0      0
1005  trnet 101005     1500  -      -      -        ibm  -        0      0

Remote SPAN VLANs
------------------------------------------------------------------------------

Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
```

2)将端口 1,3～10 加入 testvlan10 中

```
Switch(config)#interface fa0/1                    /* 进入交换机端口的配置模式 */
Switch(config-if)#switchport access vlan 10       /* 将端口 1 划入 VLAN 中 */
Switch(config-if)#switchport mode access          /* 将端口配置为 access 模式 */
Switch(config-if)#no shutdown                     /* 开启端口 */
Switch(config)#interface range fastEthernet 0/3-10 /* 进入端口 3～10 */
Switch(config-if-range)#switchport access vlan 10  /* 将端口划入 VLAN 中 */
Switch(config-if-range)#switchport mode access    /* 将端口配置为 access 模式 */
Switch(config-if-range)#no shutdown               /* 开启端口 */
Switch#show vlan id 10
Switch#show vlan id 10
```

```
VLAN  Name                              Status      Ports
----  --------------------------------  ----------  -------------------------------
10    testvlan10                        active      Fa0/1,Fa0/3,Fa0/4,Fa0/5
                                                    Fa0/6,Fa0/7,Fa0/8,Fa0/9
                                                    Fa0/10

VLAN  Type  SAID   MTU   Parent  RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
----  ----  -----  ----  ------  ------ -------- ---- -------- ------ ------
10    enet  100010 1500  -       -      -        -    -        0      0
```

从上面可以看出已经将端口 Fa0/1、Fa0/3～Fa0/10 划入了 testvlan10 中。

3)给 VLAN 配置 IP 地址

```
Switch(config)#interface vlan 10     /* 进入交换机 VLAN 的接口配置模式 */
Switch(config-if)#ip address 192.168.1.1 255.255.255.0  /* 为 VLAN 指定接口
                                                          IP 地址 */
Switch(config-if)#exit               /* 退出交换机 VLAN 的接口配置模式 */
Switch(config)#exit                  /* 退出交换机的特权模式 */
Switch#show interfaces vlan 10       /* 显示 VLAN 10 的配置信息 */
Vlan10 is up,line protocol is down
Hardware is CPU Interface,address is 0002.4a80.98ca (bia 0002.4a80.98ca)
Internet address is 192.168.1.1/24
MTU 1500 bytes, BW 100000 Kbit, DLY 1000000 usec, reliability 255/255, txload
1/255,rxload 1/255
Encapsulation ARPA,loopback not set
ARP type: ARPA,ARP Timeout 04:00:00
Last input 21:40:21,output never,output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 0 bits/sec,0 packets/sec
5 minute output rate 0 bits/sec,0 packets/sec
1682 packets input,530955 bytes,0 no buffer
Received 0 broadcasts (0 IP multicast)
0 runts,0 giants,0 throttles
0 input errors,0 CRC,0 frame,0 overrun,0 ignored
563859 packets output,0 bytes,0 underruns
0 output errors,23 interface resets
0 output buffer failures,0 output buffers swapped out
```

6.1.4 链路聚合技术简介及配置实例

随着数据业务量的增长和对服务质量要求的提高，高可用性(high availability)日益成为高性能网络最重要的特征之一。网络的高可用性是指系统以有限的代价换取最大运行时间，将故障引起的服务中断损失降到最低。具有高可用性的网络系统一方面需要尽量减少硬件或软件故障，另一方面必须对重要资源进行相应备份。一旦检测到故障即将出现，系统能迅速将受影响的任务转移到备份资源上以继续提供服务。

网络的高可用性一般在系统、组件和链路 3 个级别上体现。系统级的高可用性要求网络拓扑必须有冗余结点和备份设计。组件级的高可用性着眼于网络设备自身，要求网络设备具有冗余部件和热备份机制。链路级的高可用性则要求传输链路备份，如果主要数据通路中断，备用线路将迅速启用。

1. 链路聚合的定义

传输链路的备份是提高网络系统高可用性的重要方法。目前的技术中，以生成树协议(STP)和链路聚合(link aggregation)技术应用最为广泛。生成树协议提供了链路间的冗余方案，允许交换机间存在多条链路作为主链路的备份。而链路聚合技术则提供了传输线路内部的冗余机制，链路聚合成员彼此互为冗余和动态备份。

IEEE 802.3ad 协议中规定了链路聚合技术的标准。链路聚合是可将多物理连接当做一个单一的逻辑连接，允许两个交换设备之间通过多个端口并行连接，同时传输数据以提供更高的带宽、更大的吞吐量和可恢复性的技术。聚合内部的物理链路共同完成数据收发任务并相互备份。只要还存在能正常工作的成员，整个传输链路就不会失效。

简单地说，在网络中使用链路聚合技术，可以为计算机网络提供成倍的带宽和链路备份。在使用链路聚合时，要求聚合的端口或者链路的数据传输速率一样，必须是全双工的工作模式。例如，要汇聚的链路的数据传输速率都是 100 Mbps，并且都是全双工模式。如果试图将线路传输速率不同或不同工作模式的适配器聚集在一起，也可以成功创建链路聚合，但交换设备可能不会将这些适配器聚集在一起，此时网络性能可能有所下降。

2. 链路聚合的优点

链路聚合具有如下一些显著的优点：

(1)提高链路可用性。链路聚合中，成员互相动态备份。当某一链路中断时，其他成员能够迅速接替其工作。与生成树协议不同，链路聚合启用备份的过程对聚合之外是不可见的，而且启用备份过程只在聚合链路内，与其他链路无关，切换可在数毫秒内完成。

(2)增加链路容量。聚合技术为用户提供一种经济的提高链路数据传输率的方法。通过捆绑多条物理链路，用户不必升级现有设备就能获得更大带宽的数据链路，其容量等于各物理链路容量之和。聚合模块按照一定算法将业务流量分配给不同的成员，实现链路级的负载分担功能。

某些情况下，链路聚合甚至是提高链路容量的唯一方法。例如，当市场上的设备都不能提供高于 10 G 的链路时，用户可以将两条 10 G 链路聚合，获得带宽大于 10 G 的传输线路。

(3)价格便宜，性能接近千兆以太网。

(4)不需重新布线，也无须考虑千兆网令人头疼的传输距离极限。

(5)Trunking 可以捆绑任何相关的端口，也可以随时取消设置，这样就提供了很好的灵

活性。

(6)Trunking 可以提供负载均衡能力以及系统容错。由于 Trunking 实时平衡各个交换机端口和服务器接口的流量，一旦某个端口出现故障，它会自动把故障端口从 Trunking 组中撤销，进而重新分配各个 Trunking 端口的流量，从而实现系统容错。

此外，特定组网环境下需要限制传输线路的容量，既不能太低以至影响传输速度，也不能太高超过网络的处理能力。但现有技术都只支持链路带宽以 10 为数量级增长，如 10 M、100 M、1 000 M 等。而通过聚合将 n 条物理链路捆绑起来，就能得到更适宜的、n 倍带宽的链路。

下面通过一个例子，来看一下有关链路聚合技术的配置实例。实例的拓扑图如图 6-8 所示。

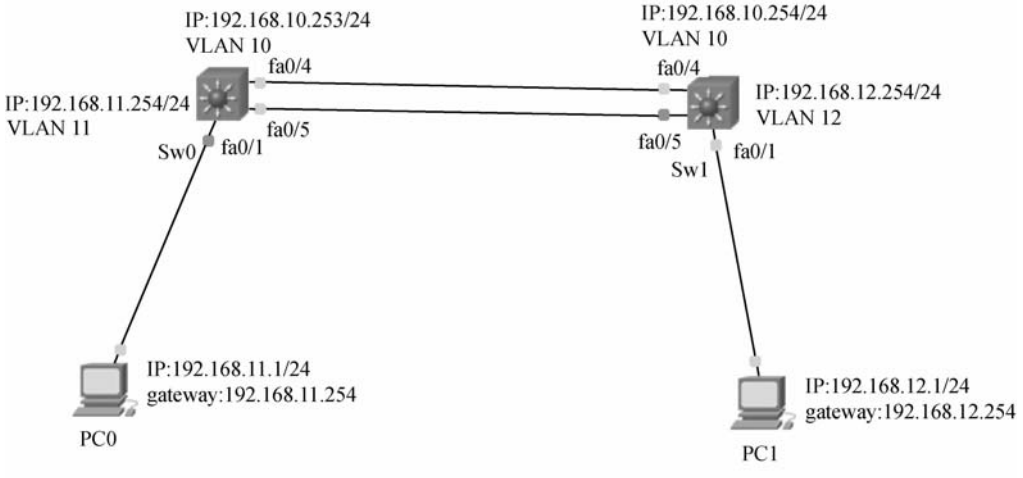

图 6-8　交换机链路聚合配置实例拓扑图

链路聚合配置代码如下：

```
Sw0# configuration terminal
Sw0(configure)#vlan 10
Sw0(configure-vlan)#exit
Sw0(configure)#vlan 11
Sw0(configure-vlan)#exit          /* 在交换机 Sw0 上创建 VLAN 10 和 VLAN 11 */

Sw1#configuration terminal
Sw1(configure)#vlan 10
Sw1(configure-vlan)#exit
Sw1(configure)#vlan 12
Sw1(configure-vlan)#exit          /* 在交换机 Sw1 上创建 VLAN 10 和 VLAN 12 */

Sw0(configure)#int range fa0/4-5
Sw0(configure-if-range)#switchport access vlan 10
Sw0(configure-if-range)#exit
```

```
Sw0(configure)#int fa0/1
Sw0(configure-if)# switchport access vlan 11
Sw0(configure)#exit                /* 在 Sw0 交换机上将端口 fa0/4-5 加入到 VLAN
                                   10 中,端口 fa0/1 加入到 VLAN 11 中 */

Sw1(configure)#int range fa0/4-5
Sw1(configure-if-range)#switchport access vlan 10
Sw1(configure-if-range)#exit
Sw1(configure)#int fa0/1
Sw1(configure-if)#switchport access vlan 12
Sw1(configure-if)#exit             /* 在 Sw1 交换机上将端口 fa0/4-5 加入到 VLAN
                                   10 中,端口 fa0/1 加入到 VLAN 12 中 */

Sw0#configuration terminal
Sw0(configure)#interface vlan 10
Sw0(configure-if-vlan)#ip address 192.168.10.253 255.255.255.0
Sw0(configure-if-vlan)#no shutdown
Sw0(configure-if-vlan)#exit        /* 在 Sw0 交换机上为 VLAN 10 设置接口地址 */
Sw0(configure)#interface vlan 11
Sw0(configure-if-vlan)#ip addresss 192.168.11.254 255.255.255.0
Sw0(configure-if-vlan)#no shutdown
Sw0(configure-if-vlan)#exit        /* 在 Sw0 交换机上为 VLAN 11 设置接口地址 */

Sw1# configuration terminal
Sw1(configure)#interface vlan 10
Sw1(configure-if-vlan)#ip address 192.168.10.254 255.255.255.0
Sw1(configure-if-vlan)#no shutdown
Sw1(configure-if-vlan)#exit        /* 在 Sw1 交换机上为 VLAN 10 设置接口地址 */
Sw1(configure)#interface vlan 12
Sw1(configure-if-vlan)#ip address 192.168.12.254 255.255.255.0
Sw1(configure-if-vlan)#no shutdown
Sw1(configure-if-vlan)#exit        /* 在 Sw1 交换机上为 VLAN 12 设置接口地址 */

Sw0# configuration terminal
Sw0(configure)#int range fa0/4-5
Sw0(configure-if-range)#channel-group 1 mode desirable
Sw0(configure-if-range)#exit       /* 在 Sw0 交换机上将 fa0/4-5 聚合 */

Sw1# configuration terminal
Sw1(configure)#int range fa0/4-5
```

```
Sw1(configure-if-range)#channel-group 1 mode desirable
Sw1(configure-if-range)#exit      /* 在 Sw1 交换机上将 fa0/4-5 聚合 */

Sw0# configuration terminal
Sw0(configure)#interface port-channel 1
Sw0(configure-if)#switchport mode trunk
Sw0(configure-if)#switchport trunk native vlan 10
Sw0(configure-if)#exit
Sw1# configuration terminal
Sw1(configure)#interface port-channel 1
Sw1(configure-if)#switchport mode trunk
Sw1(configure-if)#switchport trunk native vlan 10
Sw1(configure-if)#exit            /* 将聚合端口设置为 trunk 模式 */

Sw0# configuration terminal
Sw0(configure)#ip route 0.0.0.0 0.0.0.0 192.168.10.254
Sw0(configure)#exit
Sw1# configuration terminal
Sw1(configure)#ip route 0.0.0.0 0.0.0.0 192.168.10.253
Sw1(configure)#exit               /* 在两台交换机上分别设置默认路由 */
```

在 PC0 客户端设置其 IP 地址为 192.168.11.1，子网掩码为 255.255.255.0，网关地址为 192.168.11.254。

在 PC1 客户端设置其 IP 地址为 192.168.12.1，子网掩码为 255.255.255.0，网关地址为 192.168.12.254。

在 PC0 客户端 ping PC1 客户端的 IP 地址，检查是否能够 ping 通。

此时需要注意的是，在 Sw0 和 Sw1 交换机上进行端口聚合后，如果没有设置聚合端口为 trunk 时，交换机两边是不能够被 ping 通的。即使设置了 trunk 口，如果没有设置三层交换机的路由功能，也只能实现交换机两端设置了 trunk 口的端口 IP 能够 ping 通。所以在设置了 trunk 口后，还要开启三层交换机的路由功能，即默认路由、静态路由或动态路由。

6.2　路由器的配置与管理

路由器是重要的网络互联设备之一，网络管理人员需要掌握基本的路由器的配置与管理知识。

6.2.1　路由器简介

路由器通常用于结点众多的大型网络环境，它处于 OSI 参考模型的网络层。与交换机和网桥相比，在实现骨干网的互联方面，路由器特别是高端路由器有着明显的优势。路由器高度的智能化，对各种路由协议、网络协议和网络接口的广泛支持，安全性和访问控制等特

点是网桥和交换机等其他互联设备所不具备的。路由器的中低端产品可以用于连接骨干网设备和小规模端点的接入，高端产品可以用于骨干网之间的互联以及骨干网与互联网的连接。骨干网的互联和骨干网与互联网的互联互通，不但技术复杂，涉及的通信协议、路由协议和接口众多，信息传输速度要求高，而且对网络安全性的要求也比其他场合高得多。因此，采用高端路由器作为互联设备，有着其他互联设备不可比拟的优势。

路由器的一个作用是连通不同的网络，另一个作用是选择信息传送的线路。选择通畅快捷的线路，能大大提高通信速度，减轻网络系统通信负荷，节约网络系统资源，提高网络系统畅通率，从而让网络系统发挥出更大的效益。

1. 路由器的工作原理

当 IP 子网中的一台主机发送 IP 分组给同一 IP 子网的另一台主机时，它直接把 IP 分组送到网络上，对方就能收到。而要送给不同 IP 子网上的主机时，它要选择一个能到达目的子网上的路由器，把 IP 分组送给该路由器，由路由器负责把 IP 分组送到目的地。如果没有找到这样的路由器，主机就把 IP 分组送给一个称为“默认网关(default gateway)”的路由器。默认网关是每台主机上的一个配置参数，它是接在同一个网络上的某个路由器接口的 IP 地址。

在路由器转发 IP 分组时，根据 IP 分组的目的 IP 地址的网络号，选择合适的接口，把 IP 分组送出去。同主机一样，路由器也要判定接口所连接的是否属于目的子网，如果是，就直接把分组通过接口送到网络上，否则，就要选择下一个路由器来传送分组。路由器也有它的默认网关，用来传送未知目的地的 IP 分组。这样，通过路由器把知道如何传送的 IP 分组正确转发出去，不知道的 IP 分组送给默认网关的路由器。这样一级级地传送，IP 分组最终将送到目的地，“尽力而为”但无法传递到目的地的 IP 分组则被网络丢弃了。

路由器的工作原理可以用图 6-9 表示。

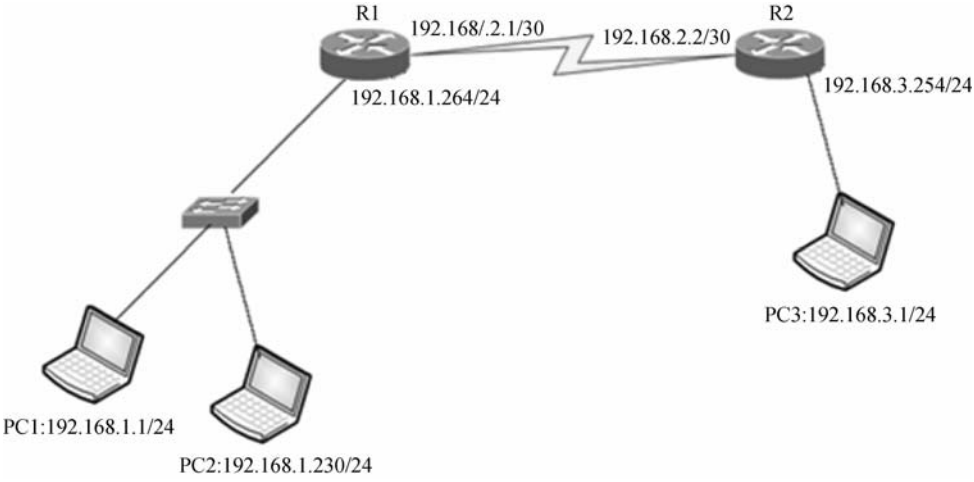

图 6-9 路由器工作原理

图 6-9 中，主机 PC1、PC2 在同一个局域网 192.168.1.0/24 中，默认网关为 192.168.1.254，主机 PC3 在局域网 192.168.3.0/24 中，默认网关为 192.168.3.254，路由器 R1 和 R2 的互联地址为 192.168.2.1/30 和 192.168.2.2/30。

当主机 PC1 向主机 PC2 发送数据包时，根据两台主机的 IP 地址和子网掩码计算可知，两台主机位于同一个子网内，此时，路由器 R1 不需要转发该数据包。而当主机 PC1 向主机

PC3 发送数据包时，根据两台主机的 IP 地址和子网掩码计算可知，主机 PC1 位于 192.168.1.0 这个网络，而主机 PC3 位于 192.168.3.0 这个网络，此时路由器 R1 根据自身的路由表，会将该数据包发送到路由器 R2 的外网接口即 192.168.2.2 这个地址。当路由器 R2 收到数据包后，根据自身路由表，会发现数据包的目的地址是自己的一个直连网络 192.168.3.0，那么此时路由器 R2 则会将该数据包直接发送到 192.168.3.0 这个网络。

目前，TCP/IP 网络全部是通过路由器互联起来的，Internet 就是成千上万个 IP 子网通过路由器互联起来的国际性网络。在以路由器为基础的网络中，路由器不仅负责对 IP 分组的转发，还要负责与别的路由器进行联络，共同确定整个网络的路由选择以及维护路由表。路由动作包括两项基本内容：寻址和转发。寻址即判定到达目的地的最佳路径，由路由选择算法来实现。由于涉及不同的路由选择协议和路由选择算法，因此寻址过程比较复杂。为了判定最佳路径，路由选择算法必须启动并维护包含路由信息的路由表，其中路由信息依赖于所用的路由选择算法。转发即沿寻找好的最佳路径传送信息分组。路由器首先在路由表中查找，判断是否知道如何将分组发送到下一个站点（路由器或主机），如果路由器不知道如何发送分组，通常将该分组丢弃；否则就根据路由表的相应表项将分组发送到下一个站点，如果目的网络直接与路由器相连，路由器就把分组直接送到相应的端口上。

在数据转发过程中，决定路由转发速度的关键技术是路由选择协议和路由选择算法。

(1)路由选择协议：用于建立和维护路由表和按照到达数据包的目的地的最佳路径转发数据包的协议，如 RIPv1、IGRP、OSPF 等。

(2)路由选择算法：就是路由选择协议用于决定到达目的网络的最佳路径的计算方法。路由选择算法越简单，则路由器将使用的处理能力就越小。这将减少路由器的日常费用。

路由选择算法和路由选择协议是相互配合又相互独立的概念，前者使用后者维护的路由表，同时后者要利用前者提供的功能来发布路由协议数据分组。

2. 路由选择协议

路由选择协议是用来确定到达路径的，它包括 RIP、IGRP、EIGRP、OSPF，在网络中起到地图导航和负责寻找路径的作用。它工作在传输层或应用层。

路由选择协议主要是运行在路由器上的协议，用来进行路径选择。路由选择协议作为 TCP/IP 协议集中的重要成员，其选择路由过程实现的好坏会影响整个 Internet 网络的效率。按应用范围的不同，路由选择协议可分为两类：在一个自治系统（autonomous system，AS，指一个互联网络，就是把整个 Internet 划分为许多较小的网络单位，这些小的网络有权自主地决定在本系统中应采用何种路由选择协议）内的路由选择协议称为内部网关协议，AS 之间的路由选择协议称为外部网关协议。这里网关是路由器的旧称。现在广泛使用的内部网关路由选择协议有 RIP-1、RIP-2、IGRP，EIGRP、IS-IS 和 OSPF。其中，前 4 种路由选择协议采用的是距离向量算法，IS-IS 和 OSPF 采用的是链路状态算法。对于小型网络，采用基于距离向量算法的路由协议易于配置和管理，且应用较为广泛，但在面对大型网络时，不但其固有的环路问题变得更难解决，所占用的带宽也迅速增长，以至于网络无法承受。因此，对于大型网络，采用链路状态算法的 IS-IS 和 OSPF 较为有效，并且得到了广泛的应用。IS-IS 与 OSPF 在质量和性能上的差别并不大，但 OSPF 更适用于 IP，较 IS-IS 更具有活力。互联网工程任务组始终在致力于 OSPF 的改进工作，其修改节奏要比 IS-IS 快得多。这使得 OSPF 正在成为应用广泛的一种路由选择协议。现在，不论是传统的路由器设计，还是即将成为标准的 MPLS（多协议标记交换），均将 OSPF 视为必不可少的路由选择协议。

外部网关协议最初采用的是 EGP。EGP 是为一个简单的树形拓扑结构设计的，随着越来越多的用户和网络加入 Internet，给 EGP 带来了很多的局限性。为了摆脱 EGP 的局限性，IETF 边界网关协议工作组制定了标准的边界网关协议——BGP。

3. 路由选择算法

路由选择算法通常指路由选择的方法或策略。

按照路由选择算法能否随网络的拓扑结构或者通信量自适应地进行调整变化进行分类，路由选择算法可以分为静态路由选择算法和动态路由选择算法。

静态路由选择算法属于非自适应路由选择算法，这是一种不测量、不利用网络状态信息，仅仅按照某种固定规律进行决策的简单的路由选择算法。静态路由选择算法的特点是简单、时间开销较小，但是不能适应网络状态的变化。静态路由选择算法主要包括扩散法和固定路由表法。

动态路由选择算法属于自适应路由选择算法，是依靠当前网络的状态信息进行决策的，从而使路由选择结果在一定程度上适应网络拓扑结构和通信量的变化。动态路由选择算法的特点是能较好地适应网络状态的变化，但是实现起来较为复杂，开销也比较大。动态路由选择算法一般采用路由表法，主要包括分布式路由选择算法和集中式路由选择算法。分布式路由选择算法是每一个结点通过定期与相邻结点交换路由选择的状态信息来修改各自的路由表，这样使整个网络的路由选择经常处于一种动态变化的状况。集中式路由选择算法是网络中设置一个结点，专门收集各个结点定期发送的状态信息，然后由该结点根据网络状态信息，动态地计算出每一个结点的路由表，再将新的路由表发送给各个结点。

6.2.2 路由器的基本配置

路由器的基本配置包括配置路由器的主机名及相关密码、配置相关接口、配置终端会话等。

1. 路由器的配置模式

路由器的配置模式分为用户模式、特权模式、全局配置模式、接口配置模式、子接口配置模式、控制台接口配置模式和路由器协议配置模式几类。

(1)用户模式：形式为 Router>，启动机器后直接进入用户模式，在该模式下只能查询路由器的一些基础信息，使用一些基本的监测命令，如 ping，traceroute 等。

(2)特权模式：形式为 Router#，在用户模式下输入 enable 命令即可进入特权模式，在该模式下可以查看路由器的配置信息和调试信息等。

(3)全局配置模式：形式为 Router(config)#，在特权用户模式下输入 configure terminal 命令即可进入全局配置模式，在该模式下主要完成全局参数的配置。

(4)接口配置模式：形式为 Router(config-if)#，在全局配置模式下输入 interface interface-list 即可进入接口配置模式，在该模式下主要完成接口参数的配置。

(5)子接口配置模式：形式为 Router(config-subif)#，该模式用于配置在路由器中创建的逻辑接口。

(6)控制台接口配置模式：形式为 Router(config-line)#，该模式通常用于配置用户口令。

(7)路由器协议配置模式：形式为 Router(config-router)#，该模式用于配置路由器协议，如 OSPF、RIP 等。

2. 配置主机名和相关密码

1)配置主机名

在网络上,路由器必须有一个唯一的主机名,所以在配置路由器时首先要为路由器配置主机名。其命令格式为:

```
Router(config)#hostname 主机名
```

如果要实现主机名和 IP 地址的对应关系,可以执行以下命令:

```
Router(config)#ip host 主机名 ip 地址
```

2)配置相关密码

为了增强网络设备的安全性,通常需要在网管员登录时设定相关的密码。这些相关的密码包括 Console 控制台登录密码、vty 通道登录密码、进入特权模式的密码等。

常用的命令格式为:

```
enable password
```

或

```
enable secret
```

前面已介绍过这两条命令的区别,在此不再赘述。

3. 配置相关接口

路由器作为连接广域网与局域网、广域网与广域网的设备,其接口类型十分丰富,其中包括局域网接口(AUI、RJ-45、FDDI、ATM、千兆以太网口等)、广域网接口(AUI、RJ-45、高速同步串口、异步串口、ISDN BRI 端口等);另外比较特殊的是,路由器上有两个配置接口,分别是 Console 和 AUX,Console 通常在进行路由器基本配置时用于通过专用连线与计算机连接, AUX 用于路由器的远程配置连接。

4. 配置终端会话

终端会话的配置主要包括 Console 控制台的配置、Telnet 远程登录会话的配置,以及其他远程登录会话的配置。这些配置主要包括为终端会话配置登录权限、离线时间等。

5. 其他

做完以上配置工作后,就需要对路由器进行路由选择协议方面的配置,这需要根据实际情况来操作。

6.2.3　路由器的配置实例

下面以 Cisco 2600 路由器为例来介绍路由器的接口、静态路由的基本配置。

1. 配置路由器的接口地址

配置路由器的接口地址的步骤如下:

(1)配置 fastEthernet 0/0 的接口地址。

```
Router>en
Router#configure terminal
Enter configuration commands,one per line. End with CNTL/Z.
Router(config)#interface fastEthernet 0/0   /* 进入 Fa0/0 配置模式 */
Router(config-if)#ip address 192.168.1.1 255.255.255.252
```

```
                                                    /* 配置 Fa0/0 的接口地址 */
Router(config-if)#exit
Router(config)#exit
Router#configuration terminal
Enter configuration commands,one per line. End with CNTL/Z.
Router(config)#interface ethernet 1/0          /* 进入 Ethernet 0/0 配置模式 */
Router(config-if)#ip address 192.168.0.254 255.255.255.0
                                                    /* 配置 Ethernet 0/0 的接口地址 */
Router(config-if)#no shutdown                  /* 启用端口 */
```

(2)查看接口配置信息。

```
Router#show interface ethernet 1/0             /* 显示接口配置信息 */
Ethernet1/0 is up,line protocol is down (disabled)
Hardware is Lance,address is 000b.bee6.ec4b (bia 000b.bee6.ec4b)
Internet address is 192.168.0.254/24
MTU 1500 bytes,BW 10000 Kbit,DLY 1000 usec,reliability 255/255,txload 1/255,
rxload 1/255
Encapsulation ARPA,loopback not set
ARP type: ARPA,ARP Timeout 04:00:00,
Last input 00:00:08,output 00:00:05,output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0 (size/max/drops); Total output drops: 0
Queueing strategy: fifo
Output queue :0/40 (size/max)
5 minute input rate 0 bits/sec,0 packets/sec
5 minute output rate 0 bits/sec,0 packets/sec
0 packets input,0 bytes,0 no buffer
Received 0 broadcasts,0 runts,0 giants,0 throttles
0 input errors,0 CRC,0 frame,0 overrun,0 ignored,0 abort
0 input packets with dribble condition detected
0 packets output,0 bytes,0 underruns
0 output errors,0 collisions,1 interface resets
0 babbles,0 late collision,0 deferred
0 lost carrier,0 no carrier
0 output buffer failures,0 output buffers swapped out
```

(3)保存配置。

```
Router#write memory                            /* 将配置信息写入内存 */
Building configuration...
[OK]
```

2.配置静态路由

在路由器上配置静态路由的方法如下：

```
Router#configure terminal
Enter configuration commands,one per line. End with CNTL/Z.
Router(config)#ip route 172.16.30.0 255.255.255.0 192.168.1.1
  /* 指定所有到达 172.16.30.0/24 子网的数据包的下一跳的网关为 192.168.1.1 */
Router(config)#exit
Router#show ip route          /* 查看路由器的路由表 */
```

在上面的两个基本配置中，需要注意的是，每做完一个完整的配置后，都必须使用 write memory 命令来保存新修改的配置。另外，在做静态路由指定的时候，格式是：

ip route ＜目的网络＞ ＜下一跳接口地址＞

其中，下一跳接口地址是指下一个相邻路由器上最近的一个端口的接口地址。

6.3　常见网络设备的安全管理和维护

网络设备的安全对整个网络的安全非常重要，作为网络管理员必须十分清楚自己所管理的网络设备的安全程度并及时作出调整，确保设备安全，以避免受到攻击而造成不必要的损失。

网络安全可以分为网络设备的安全和网络信息的安全。通常情况下，网络管理员都能够对网络信息安全给予足够的重视，但往往忽略网络设备的安全管理。几乎所有的网络设备都有一些安全上的漏洞，通过这些漏洞，其他人可以完全控制该设备，而产生的后果很可能是毁灭性的。因此，网络设备的安全管理对于整个网络的安全策略具有重大的意义。

网络设备的安全分为物理安全和访问控制安全两方面。

6.3.1　网络设备的物理安全

网络设备的物理安全是指网络设备周围环境的安全及网络设备硬件的安全，是网络安全体系中最为重要的部分。保证网络设备的安全要做到以下两点：

(1)提供良好的室内环境。良好的室内环境应该对场地的封闭、防火、防盗、防雷、防静电、室内温度和湿度的控制以及电源的安全等提供符合网络设备正常工作要求的安全保证。

(2)控制对设备的直接访问。在可能的情况下为机架上锁，并且在控制台和辅助端口设置口令。

6.3.2　网络设备的访问控制安全

网络设备的访问控制主要是防止非法用户进入网络设备并对其配置进行修改，避免网络瘫痪。

1. 路由器的访问控制安全

路由器作为网络中重要的路由设备，在其 Flash 中存放了所连接的网络的重要的路由信息和访问控制列表(access control list，ACL)等信息，所以路由器的安全对整个网络的安全稳定起着重要的作用。

以下命令都以 Cisco 2600 路由器为例。

(1)为路由器间的协议交换增加认证功能。路由器的一个重要功能是路由的管理和维护,目前具有一定规模的网络都采用动态的路由协议。当一台设置了相同路由协议和相同区域标识符的路由器加入网络后,会学习网络上的路由信息表。但此种方法可能导致网络拓扑信息泄露,也可能由于向网络发送自己的路由信息表,扰乱网络上正常工作的路由信息表,严重时可以使整个网络瘫痪。这个问题的解决办法是,对网络内的路由器之间相互交流的路由信息进行认证。当路由器配置了认证方式,就会鉴别路由信息的收发方,提高网络安全性。

(2)路由器的物理安全防范。路由器的控制端口具有特殊权限,如果攻击者物理接触路由器后,断电重启,实施"密码修复流程",进而登录路由器,就可以完全控制路由器。因此在路由器的日常管理中,要做到路由器的存放地专人专管,做好防盗报警监控等。

(3)保护路由器口令。在备份的路由器配置文件中,密码即使是用加密的形式存放的,仍存在被破解的可能。一旦密码泄露,网络也就毫无安全可言。因此为了防止密码被破解,网络管理人员应尽可能设置较为复杂的密码,并且在配置时尽量采用加密的方式。

(4)阻止查看路由器诊断信息的命令如下:

```
no service tcp-small-servers
no service udp-small-servers
```

(5)阻止查看到路由器当前的用户列表的命令为:

```
no service finger
```

(6)关闭 CDP 服务。在 OSI 二层协议即数据链路层的基础上可发现对端路由器的设备平台、操作系统版本、端口、IP 地址等重要信息。可以用命令 no cdp running 或 no cdp enable 关闭这个服务。

(7)阻止路由器接收带源路由标记的包,将带有源路由选项的数据流丢弃。IP source-route 是一个全局配置命令,允许路由器处理带源路由选项标记的数据流。启用源路由选项后,源路由信息指定的路由使数据流能够越过默认的路由,这种包就可能绕过防火墙。阻止路由器接收带源路由标记的包的命令如下:

```
no ip source-route
```

(8)关闭路由器广播包的转发。Sumrf DoS 攻击以有广播转发配置的路由器作为反射板,占用网络资源,甚至造成网络的瘫痪。应在每个端口使用 no ip directed-broadcast 命令关闭路由器广播包。

(9)管理 HTTP 服务。HTTP 服务提供 Web 管理接口。使用 no ip http server 命令可以停止 HTTP 服务。如果必须使用 HTTP,一定要使用访问列表 ip http access-class 命令,严格过滤允许的 IP 地址,同时用 ip http authentication 命令设定授权限制。

(10)抵御 spoofing(欺骗) 类攻击。使用访问控制列表,过滤掉所有目标地址为网络广播地址和宣称来自内部网络实际却来自外部的包。在路由器端口配置:

```
ip access-group list in number
```

访问控制列表如下:

```
access-list number deny icmp any any redirect
access-list number deny ip 127.0.0.0 0.255.255.255 any
access-list number deny ip 224.0.0.0 31.255.255.255 any
access-list number deny ip host 0.0.0.0 any
```

注意:上述 4 行命令将过滤 BOOTP/DHCP 应用中的部分数据包。

(11)防止包嗅探。黑客经常将嗅探软件安装在已经侵入的网络上的计算机内,监视网络数据流,从而盗窃密码,如 SNMP 通信、路由器的登录和特权密码,这样网络管理员难以保证网络的安全。因此,在不可信任的网络上不要用非加密协议登录路由器。如果路由器支持加密协议,则使用 SSH 或 Kerberized Telnet,或使用 IPSec 加密路由器所有的管理流。

(12)校验数据流路径的合法性。使用反相路径转发(reverse path forwarding,RPF)时,由于攻击者的地址是不合法的,所以攻击包被丢弃,从而达到抵御 spoofing 攻击的目的。RPF 反相路径转发的配置命令为:

```
ip verify unicast rpf
```

注意:首先要支持 CEF(Cisco express forwarding,Cisco 特快交换),才能使用该命令。

2. 交换机的访问控制安全

下面以 Cisco 交换机为例,介绍如何实施对网络设备的访问控制。

1)通过设置加密口令实现访问控制

网络设备提供的最基本的安全是在设备访问和配置过程中设置登录口令。如果对设备的访问和配置不加以审查,往往会引发安全问题。

例如,有些设备出厂时往往没有设置登录口令或设置一些缺省口令,而有些管理员就利用这些缺省的口令进行管理,这使攻击者很容易就找到一个入口,从而引发安全问题。

(1)控制台端口登录口令设置。

```
Switch(config)#line console 0        /* 从全局配置模式进入控制台线路配置模式 */
Switch(config-line)#login            /* 设置当用户使用超级终端进入控制台端口时,
                                        交换机提示输入密码 */
Switch(config-line)#password abcd123 /* 设置 abcd123 为控制台端口登录口令 */
```

这样,当下一次使用超级终端进入控制台端口时,必须输入正确的密码,以避免非授权用户进入控制台。

(2)虚拟终端远程登录口令设置。

```
Switch(config)#line vty 0 4          /* 从全局配置模式进入虚拟终端线路配置模
                                        式,其中 0 4 表示可以同时进行 5 个(即 0、1、2、3、4)虚拟终端会话 */
Switch(config-line)#password 123456  /* 设置 123456 为控制台端口登录口令 */
Switch(config-line)#login            /* 设置当用户对交换机进行远程 Telnet 时,
                                        交换机提示输入密码 */
```

(3)使能密码的设置。使能密码是由用户模式(switch>)进入特权模式(switch#)时的密码,分为两种:enable password 密码和 enable secret 密码。

enable secret 经过 MD5 加密,在交换机配置文件中无法看到 enable secret 密码;而 enable password 密码则以明文形式显示,但可通过 service password-encryption 对其进行加密,其健壮性不如 enable secret 密码。

使能密码设置格式如下:

```
Switch(config)#enable password level 15 123456    /* 表示为特权级别 15 设置
                                                     使能密码 123456,由于默认的特权级别为 15,所以在此 level 15 可以省略 */
```

或者

```
Switch(config)#enable secret level 15 abcdef
```

此时，enable secret 会覆盖 enable password 所定义的密码。上例中若同时使用了两个命令，则使能密码为 abcdef，而非 123456。

2)对虚拟终端的访问控制

虚拟端口相对于实际端口而言，一般根据需要在交换机(或路由器)上虚拟出一些端口，这些端口被称为虚拟终端或虚拟端口。每台 Cisco 设备一般有 5 个缺省虚拟终端，在虚拟终端线路上实施访问控制列表，可以控制哪些用户可以远程登录到该设备。

其设置格式如下：

```
Switch(config)#access-list 1 permit host 192.168.1.1      /* access-list 命令
                                    说明哪些源地址被允许或者拒绝访问的标准访问控制列表 */
Switch(config)#line vty 0 4      /* 从全局配置模式进入虚拟终端线路配置模式，
                                    0 4 表示可以同时进行 5 个(即 0、1、2、3、4)虚拟终端会话 */
Switch(config-line)#access-class 1 in    /* 此命令格式为 access-class in|out，
其功能是将访问列表应用到虚拟终端线路上，其中 in 表示谁可以远程登录到这台设备，
                                    out 表示当用户已登录到网络设备内部时还可以远程登录到哪里 */
```

此时表示只有 IP 地址为 192.168.1.1 的计算机可以远程登录到这台交换机。

3)对 Web 控制台的访问控制

使用 Web Console 软件配置网络设备是另一种常用的方法，该软件具有友好的操作界面，使配置网络设备变得更加容易，但同时也引出了一些安全问题。要想做到防患于未然，可以用下面几种方法来保证安全性：

(1)修改网络设备的 Web 服务的端口号，命令格式如下：

```
ip http port 端口号
```

此命令在全局配置模式下执行。修改端口号在一定程度上增加了 Web 控制的安全，但其安全性能不是很高。

(2)通过实施访问控制列表控制哪些地址可以访问网络设备的 Web 服务。设置过程如下：

```
Switch(config)#access-list 1 permit host 192.168.1.1
Switch(config)#ip http server          /* 启用 Web 控制台对交换机进行 Web 管理，
                                    在 Cisco IOS 11.3 版本后 ip http server 为默认启用 */
Switch(config)#ip http access-class 1  /* 允许 IP 地址为 192.168.1.1 的计算机
                                    通过 Web 控制台对交换机进行访问 */
```

(3)关闭网络设备的 Web 服务。Web 服务为管理人员带来方便的同时也带来了安全上的问题。必要时通过命令 no ip http server 关闭 Web 服务，以减少安全隐患。

4)对设备的访问设置不同的权限

在 Cisco 产品中可以设置 0～15 即 16 个不同的权限级别。需要说明的是，级别 15 为缺省的特权 EXEC 级别，拥有最高级别的访问权限。级别 1 为缺省的用户 EXEC 级别，仅能执行有限的命令，不能对交换机进行配置。

一般可以通过 privilege 命令设置不同级别并赋予这些级别一定的权限。其命令格式如下：

```
privilege mode {level level | reset} command-string
```

其中，mode 为配置模式；level level 为设置的特权级别；command-string 为可执行的命令。

例如，创建一个级别 3，在全局配置模式下能执行 ping 和 show run 命令，并设定级别 3 的使能密码为 123456，命令如下：

```
Switch(config)# privilege configure level 3 ping
Switch(config)# privilege configure level 3 show run
Switch(config)# enable secret level 3 123456
```

以级别 2 登录命令如下：

```
switch>enable 2
```

5)控制会话超时及设置警示登录标语消息

如果控制台在特权模式下没有人看管，那么任何用户都可以乘机修改网络设备的配置。而对空闲会话的超时设置可以获得额外的安全保障，默认空闲会话超时时间为 10 分钟，可以通过 exec-timeout 命令改变会话超时时间。其设置格式如下：

```
Switch(config)#line console 0
Switch(config-line)#exec-timeout 5 10          /* 在控制台端口设置空闲会话超时 5 分 10 秒 */
Switch(config)#line vty 0 4
Switch(config-line)#exec-timeout 5 10          /* 在虚拟终端设置空闲会话超时 5 分 10 秒 */
```

登录标语消息是当用户登录网络设备时在界面上显示的内容。这里可以显示一些对非授权访问者的警告，如“非授权访问将被依法起诉”等，从心理上吓退攻击者。

设置登录标语消息的命令格式如下：

```
Switch(config)#banner motd # message #
```

其中，# 为分界符。

例如：

```
Router(config)#banner motd #This is the Cisco2600 Router.#
```

6.4　虚拟专用网技术

近年来，虚拟专用网(virtual private network，VPN)已成为 IT 界的一个新热点。VPN 已经成为当今网络的必要组成部分，它为确保内联网(Intranet)和外联网(Extranet)在共享的 Internet 结构上的通信专用性提供了有效的手段。

6.4.1　VPN 概述

1. VPN 的定义

VPN 是指依靠 ISP(Internet 服务提供者)和其他 NSP(网络服务提供者)在公用网络(如 Internet、FrameRelay、ATM)中建立专用的数据通信网络的技术。在虚拟网中，任意两个结点之间的连接并没有传统专网所需的端到端的物理链路。VPN 适用于大中型企业的总公司和各地分公司或分支机构的网络互联和企业同商业合作伙伴之间的网络互联。

它可以通过特殊的加密的通信协议在连接在 Internet 上的位于不同地方的两个或多个

企业内部网之间建立一条专有的通信线路，但是它并不需要真正地去铺设光缆之类的物理线路。这就好比去电信局申请专线，但是不用给铺设线路的费用，也不用购买路由器等硬件设备。VPN 技术原是路由器具有的重要技术之一，目前交换机、防火墙等软件也都支持 VPN 功能，简单来讲，VPN 的核心就是利用公共网络建立虚拟私有网。

所以，VPN 被定义为通过一个公用网络（通常是 Internet）建立一个临时的、安全的连接，是一条穿过混乱的公用网络的安全、稳定的隧道。虚拟专用网是对企业内部网的扩展。虚拟专用网可以帮助远程用户、公司分支机构、商业伙伴及供应商同公司的内部网建立可信的安全连接，并保证数据的安全传输。虚拟专用网可用于不断增长的移动用户的全球因特网接入，以实现安全连接；可用于实现企业网站之间安全通信的虚拟专用线路，用于经济有效地连接到商业伙伴和用户的安全外联网、虚拟专用网。

2. VPN 的特点

1）安全保障

虽然实现 VPN 的技术和方式很多，但所有的 VPN 均应保证通过公用网络平台传输数据的专用性和安全性。在非面向连接的公用 IP 网络上建立一个逻辑的、点对点的连接，称之为建立一个隧道，可以利用加密技术对经过隧道传输的数据进行加密，以保证数据仅被指定的发送者和接收者了解，从而保证了数据的私有性和安全性。在安全性方面，由于 VPN 直接构建在公用网上，实现简单、方便、灵活，但同时其安全问题也更为突出。企业必须确保其 VPN 上传送的数据不被攻击者窥视和篡改，并且要防止非法用户对网络资源或私有信息的访问。Extranet VPN 将企业网扩展到合作伙伴和客户，对安全性提出了更高的要求。

2）服务质量保证

VPN 应当为企业数据提供不同等级的服务质量保证（QoS）。不同的用户和业务对服务质量保证的要求差别较大。如移动办公用户，提供广泛的连接和覆盖性是保证 VPN 服务的一个主要因素；而对于拥有众多分支机构的专线 VPN 网络，交互式的内部企业网应用则要求网络能提供良好的稳定性；对于其他应用（如视频等）则对网络提出了更明确的要求，如网络时延及误码率等。所有以上网络应用均要求网络根据需要提供不同等级的服务质量。在网络优化方面，构建 VPN 的另一重要需求是充分有效地利用有限的广域网资源，为重要数据提供可靠的带宽。广域网流量的不确定性使其带宽的利用率很低，在流量高峰时引起网络阻塞，产生网络瓶颈，使实时性要求高的数据得不到及时发送；而在流量低谷时又造成大量的网络带宽空闲。QoS 通过流量预测与流量控制策略，可以按照优先级分配带宽资源，实现带宽管理，使得各类数据能够被合理地先后发送，并预防阻塞的发生。

3）可扩充性和灵活性

VPN 能够支持通过 Intranet 和 Extranet 的任何类型的数据流，方便增加新的结点，支持多种类型的传输媒介，可以满足同时传输语音、图像和数据等新应用对高质量传输以及带宽增加的需求。

4）可管理性

可方便地从用户角度和运营商角度进行管理、维护。在 VPN 管理方面，VPN 要求企业将其网络管理功能从局域网无缝地延伸到公用网，甚至是客户和合作伙伴。虽然可以将一些次要的网络管理任务交给服务提供商去完成，企业自己仍需要完成许多网络管理任务。所以，一个完善的 VPN 管理系统是必不可少的。VPN 管理的目标为：减小网络风险，具有高扩展性、经济性、高可靠性等优点。事实上，VPN 管理主要包括安全管理、设备管理、配置

管理、访问控制列表管理、QoS 管理等内容。

3. VPN 的应用

目前，VPN 的应用很广泛，例如：

(1)企业员工及授权商业伙伴共享企业的商业信息。

(2)在网上进行信息及文件安全快速的交换。

(3)通过网络安全地发送电子邮件。

(4)通过网络实现无纸办公和无纸贸易。

VPN 的访问方式多种多样，包括拨号模拟方式、ISDN、DSL、专线、IP 路由器或线缆调制解调器。现在所说的 VPN 更多指的是构建在公用 IP 网络上的专用网，也可称之为 IP VPN(以 IP 为主要通信协议)。

6.4.2　VPN 中的常用技术

由于安全问题，人们总是拒绝用 Internet 进行企业网的访问。而 VPN 技术正是从保密性、完整性及可靠性 3 方面解决这个问题的。保密性确保数据传输时外人无法看到或获得数据，完整性确保数据不被修改、能够原样到达目的地，可靠性确保通信双方的身份正确无误。

目前 VPN 主要采用 4 项技术：隧道技术、加解密技术、密钥管理技术、使用者与设备身份认证技术。

1. 隧道技术

隧道技术是一种通过使用互联网络的基础设施在网络之间传递数据的技术。使用隧道传递的数据(或负载)可以是不同协议的数据帧或包。隧道协议将这些其他协议的数据帧或包重新封装在新的包头中发送。

新的包头提供了路由信息，从而使封装的负载数据能够通过互联网络传递。

被封装的数据包在隧道的两个端点之间通过公共互联网络进行路由。被封装的数据包在公共互联网络上传递时所经过的逻辑路径称为隧道。一旦到达网络终点，数据将被解包并转发到最终目的地。注意隧道技术是指包括数据封装、传输和解包在内的全过程。

隧道所使用的传输网络可以是任何类型的公共互联网络，下面主要以目前普遍使用的 Internet 为例进行说明。此外，在企业网络中同样可以创建隧道。在经过一段时间的发展和完善之后，目前较为成熟的隧道技术包括以下几种。

1)IP 网络上的 SNA 隧道技术

当系统网络结构的数据流通过企业 IP 网络传送时，SNA 数据帧将被封装在 UDP 和 IP 协议包头中。

2)IP 网络上的 Novell NetWare IPX 隧道技术

当一个 IPX 数据包被发送到 NetWare 服务器或 IPX 路由器时，服务器或路由器用 UDP 和 IP 包头封装 IPX 数据包后通过 IP 网络发送。另一端的 IP-TO-IPX 路由器在去除 UDP 和 IP 包头之后，把数据包转发到 IPX 目的地。

近几年出现了一些新的隧道技术，具体包括：

(1)点对点隧道协议(PPTP)。PPTP 允许对 IP、IPX 或 NetBEUI 数据流进行加密，然后封装在 IP 包头中通过企业 IP 网络或公共互联网络发送。

(2)第二层隧道协议(L2TP)。L2TP 允许对 IP、IPX 或 NetBEUI 数据流进行加密，然

后通过支持点对点数据报传递的任意网络发送，如 IP、X.25、帧中继或 ATM。

(3)安全 IP(IPSec)隧道模式。IPSec 隧道模式允许对 IP 负载数据进行加密，然后封装在 IP 包头中通过企业 IP 网络或公共 IP 互联网络(如 Internet)发送。

2.加解密技术

数据通信的加解密技术是一项已较成熟的技术，VPN 可直接利用现有技术，如 DES、Triple-DES 等。加密后的数据包即使在传输中被窃取，非法获取者也只能看到一堆乱码，必须拥有相应的密钥才能破译。而要破译密钥，其所需的设备与时间则需视加密技术及密钥长度而定。例如，56 位的 DES 以现今的普通 PC 需要几十年才能破译；112 位的 Triple-DES 目前则被视为不可破译。

加解密技术依密钥来区分可分为两大类：对称式密码学(有时又称密钥式密码学)和非对称式密码学(又称公用钥匙密码学)。由于对称式密码算法的运算速度较非对称式密码算法快(约 100～1 000 倍)，所以现行的 VPN 设备都采用 DES 或 Triple-DES 作为加解密所用的算法，而以对称式加上非对称式的混合密钥管理功能进行网络上密钥的交换与管理，不但可提供较快的传输速度，也有更好的保密功能，也更难破解。关于数据的加解密技术将在第 7 章介绍。

3.密钥管理技术

密钥管理的主要任务是如何在公用数据网上安全地传递密钥而不被窃取。现行常用密钥管理的技术又可分为 SKIP(simple key management for IP)与 ISAKMP(Internet security association and key management protocol)/Oakley 两种。SKIP 是由 Sun 公司开发的技术，主要是指利用 Diffie-Hellmail 的演算法则在网络上传输密钥的一种技术。在 ISAKMP 中，双方都有两把密钥，分别是公钥和私钥。将来 ISAKMP/Oakley 会整合于 IPv6 中，成为 IPv6 的标准之一。IPSec 的一个优点是，它的查验和安全性功能与它的密钥管理系统松散耦合。因此，如果未来的密钥管理系统发生变化时，IPSec 的安全机制不需要进行修改。

4.使用者与设备身份认证技术

公共网络上有众多的使用者与设备，如何正确地辨认合法的使用者与设备，使属于本单位的人员与设备能互通，构成一个 VPN，并让未授权者无法进入系统，这就是使用者与设备身份认证技术要解决的问题。辨认合法使用者的方法有很多，最常使用的是使用者的名称与密码或卡片式两段认证等方式。设备认证必须依赖由电子证书核发单位所颁发的 X.509 电子证书。通信双方将此证书进行对比，如果对比正确，才开始交换数据。

本章小结

本章介绍了网络设备中路由器和交换机的基本原理和作用，并举例说明了路由器和交换机的基本配置，同时，对网络设备的安全管理作了重点描述；对常用的网络技术虚拟专网(VPN)技术进行了介绍。本章的重点在于理解掌握交换机及路由器的原理和基本配置，掌握路由器等网络设备的安全管理，掌握 VPN 技术的原理及实际应用。需要注意在路由器的 ACL 配置及访问级别和权限设置时的问题。

习　题　6

1. 简述网络设备管理的概念。
2. 请叙述通信模型的组成及各自的作用和地位。
3. 数据交换有几种交换方式？请分别叙述。
4. 简述路由选择算法的分类。
5. 什么是 VPN？
6. 网络设备的安全包括哪些内容？以路由器为例试说明。
7. 试举例说明路由器中不同的用户级别权限的配置方法。