路由与交换技术

计算机工程系网络技术教研室

2006 年 9 月

目　　录

第1章　　IP 地址的分配及 IP 子网划分

随着电脑技术的普及和因特网技术的迅猛发展,因特网已作为 21 世纪人类的一种新的生活方式而深入到寻常百姓家。谈到因特网，IP 地址就不能不提，因为无论是从学习还是使用因特网的角度来看，IP 地址都是一个十分重要的概念，Internet 的许多服务和特点都是 IP 地址体现出来的，而 IP 地址和子网掩码的设置，更是每个人事网络工作的人必须具备的网络基础知识，只有理解了 IP 地址和子网掩码的真正含义，才能得心应手的管理一个网络。我们要想理解 IP 地址的真正应用，首先要理解 IP 地址与子网掩码的常识。本章将详细介绍 IP 地址的分类规则以及如何灵活的运用子网掩码技术规划网络等基础知识。

1.1　IP 地址

1.1.1 概述

在网络中，我们需要唯一地标识 Internet 上的每一个设备以确保所有设备的全球通信。这好象在电话系统中，每一个电话用户都有唯一的电话号码（如果我们把国家码和地区码都看成是这个标志系统的一部分）。

Internet 协议地址(简称 IP 地址)对网上某个节点来说是一个逻辑地址。IP 地址是唯一的。地址唯一是指每一个地址定义了一个且仅有一个到 Internet 的连接。在 Internet 上的两个设备永远不会有相同的地址。但是，如果一个设备通过两个网络与 Internet 相连，那么这个设备就有两个 IP 地址。

1.1.2 地址空间

IP 协议定义的地址具有地址空间。地址空间就是协议所使用的地址总数。如果协议使用 N 位来定义地址，那么地址空间就是 2^n，因为每一个位可以有两种不同的值（1 或 0）。

现在采用的 IP 协议版本为 IPv4，IPv4 使用 32 位地址，这表示地址空间是 2^{32}，或 4,294,967,296（超过 40 亿）。这就表明，从理论上讲，可以有超过 40 亿个设备连接到 Internet。我们将会看到，实际的数字要远小于这个数值。

1.1.3 IP 地址的表示方法

IP 地址有三种常用的表示方法：二进制表示法、点分十进制表示法和十六进制表示法。

1. 二进制表示法

在二进制表示法中，IP 地址表现为 32 位。为了使这个地址有更好的可读性，通常在每个字节（8 位）之间加上一个或更多的空格。这样，有时就会听到说：IP 地址是 32 位地址、4 个八位组地址，或者 4 字节地址。下面是二进制 IP 地址的示例：

01110101 10010101 00011101 11101010

2. 点分十进制表示法

为了使 32 位地址更加简洁和更容易阅读，Internet 的地址通常写成小数点将各字节分隔开的形式。图 1-1 表示了点分十进制的 IP 地址。应当注意到，因为每个字节仅有 8 位，因此在点分十进制表示法中的每个数目一定在 0 至 255 之间。

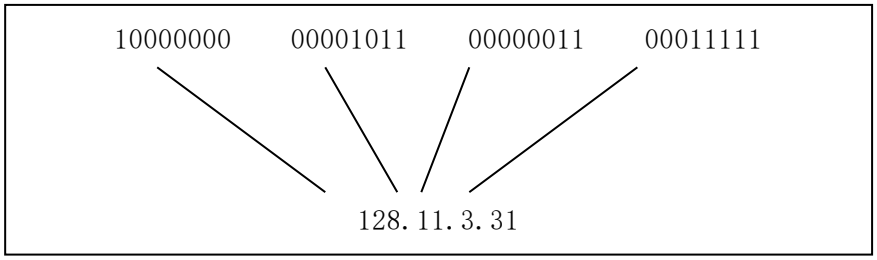


图 1-1 点分十进制的 IP 地址

3. 十六进制表示法

有时我们会见到十六进制表示法的 IP 地址。每一个十六进制数字等效于四个位。这就是说，一个 32 位的地址要用 8 个十六进制数字来表示。这种表示方法常用于网络编程中。如：

10000001 00001011 00001011 11100111

表示成十六进制：0x819B0BEF

1.1.4 地址的分类

在刚开始使用 IP 地址时，IP 地址使用分类的概念。这种体系结构叫做分类编址。在 20 世纪 90 年代中期，一种叫做无分类编址的新的体系出现了，这种体系将最终代替原来的体系。但是，绝大多数的 Internet 地址目前还是使用分类编址，而过渡还较慢。我们先来讨论“分类编址”。“分类”的概念有助于理解“无分类”的概念。

假如某个网络不想加入到公用的 Internet 中去，那么它可以用强制规定的形式来选择其 IP 地址。若采用这种方式，则对于该网络上的所有节点，IP 地址必须满足以下规定：

(1)每个 IP 地址的网络号部分相同。

(2)网络上每个节点的 IP 地址必须是唯一的。

IP 地址可分成五类，即 A 类、B 类、C 类、D 类和 E 类。见图 1-2。

图 1-2 IP 地址介绍

每一类占据整个地址空间的某一部分。图 1-3 给出了每一类地址空间的占用情况(近似的)。

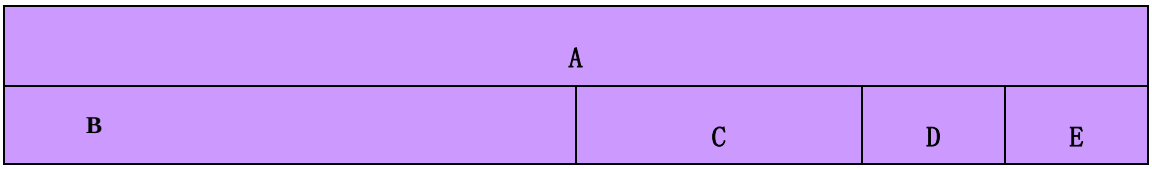


图 1-3 地址空间的占用情况

从图 1-3 中可以看出，A 类地址占据了整个地址空间的一半，这是设计中的一个缺陷。B 类地址占据了整个地址空间的 1/4，这也是一个缺陷。C 类地址占据地址空间的 1/8，而 D 类和 E 类地址各占据地址空间的 1/16。表 1-1 给出了每一类的地址数。

表 1-1

类	地址数	百分数
A	2^{31}=2,147,483,648	50%
B	2^{30}=1,073,741,824	25%
C	2^{29}=536,870,912	12.5%
D	2^{28}=268,435,456	6.25%
E	2^{28}=268,435,456	6.25%

如图 1-4 所示，A 类地址的最高位 0 和随后的 7 位是网络号部分，剩下的 24 位表示网内主

机号。这样在一个互连网络内可能会有 126 个 A 类网络(网络号 1—126，号码 0 和 127 保留)，而每一个 A 类网络中允许有 1600 万个节点。非常大的地区网，如美国的 MLNET 和某些很大的商业网，才能使用 A 类地址。

B 类地址的最高两位 10 和后随的 14 位是网络号部分，剩下的 16 位表示网内的主机号。这样，在某种互连环境下可能会有大约 16000 个 B 类网络，而每个 B 类网络中可以有 65000 多个节点。一般大单位和大公司营建的网络使用 B 类地址。

C 类地址的最高三位 110 和后随的 21 位是网络号部分，剩下的 8 位表示网内主机号。这样，一个互连网将允许包含 200 万个 C 类网络，每一个 C 类网络中最多可以有 254 个节点，较小的单位和公司都使用 C 类地址。

D 类地址的最高四位为 1110，表示多播地址。即一个多播组的组号。

如果你不喜欢使用二进制，也可以按照 IP 地址第一字节值的十进制表示划分三类网络。A 类地址以 1—126 开始，B 类地址以 128—191 开始，C 类地址以 192—223 开始，C 类地址以 224－239 开始。

图 1-4　IP 地址的分类

1.1.5 网络掩码和默认掩码

网络掩码是一个 32 位数。当用掩码和地址段中的一个地址按位相“与”（AND）时，就可得出该地址段的第一个地址（网络地址）。

网络掩码中二进制位为 1 的位代表该位为网络位，二进制位为 0 的位代表该位为主机位。

A、B、C 三类地址中的默认子网掩码见下表：

表 1-2 默认掩码

类	二进制表示的掩码	点分十进制表示的掩码
A	11111111 00000000 00000000 00000000	255.0.0.0
B	11111111 11111111 00000000 00000000	255.255.0.0
C	11111111 11111111 11111111 00000000	255.255.255.0

1.1.6 特殊地址

A 类、B 类和 C 类地址中的某部分空间可用作特殊的地址（见表 1-3）。

表 1-3 特殊地址

特殊地址	网络位	主机位	源地址或目的地址
网络地址	特写的	全 0	都不是
直接广播地址	特写的	全 1	目的地址
受限广播地址	全 1	全 1	目的地址
环回地址	127	任意	目的地址

1. 网络地址

对于 A、B、C 类地址中的第一个地址定义了该主机所在的网络地址。

如：主机 123.50.16.90 所在的网络地址为 123.0.0.0；150.48.0.1 所在的网络地址为 150.0.0.0。

2. 直接广播地址

在 A、B、C 类地址中，若主机位是全 1，则这个地址称为直接广播地址。路由器使用这种地址把一个数据包发送到一个特定网络上的所有主机。所有的主机都会收到具有这种类型目的地址的数据包。要注意，这个地址在 IP 数据包中只能用作目的地址。还要注意到，这个特殊的地址也减少了 A 类、B 类和 C 类地址中每一个网络中的可用主机数。

如：路由器发送数据报，目的地址为 221.45.71.255，而该网络内采用默认的子网掩码 255.255.255.0 分配 IP 地址，则这个网络上的所有设备都接收和处理这个数据包，即以 221.45.71 开头的所有设备。

3. 受限广播地址

在 A、B、C 类地址中，若网络位和主机位都是全 1（32 位），即 255.255.255.255，则这个地址用于定义在当前网络上的广播地址。一个主机若想把报文发送给所有其他主机，就可使用这样的地址作为数据包中的目的地址。但路由器把具有这种类型地址的数据包阻挡住，

使这样的广播只局限在本地网络。应注意，这种地址属于 E 类地址。

如：主机可以发送使用全 1 目的 IP 地址的数据包，在该网络上的所有设备都接收和处理这个数据包。

4. 环回地址

第一个字节等于 127 的 IP 地址用作环回地址，这个地址用来测试机器的 TCP/IP 协议是否安装正常。当使用这个地址时，数据包永远不离开这台机器；这个数据包就简单地返回到 TCP/IP。因此这个地址可用于测试 IP 软件。例如，像“PING”这样的应用，可以发送把环回地址作为目的地址的数据包，以便测试 IP 软件能否接收和处理数据包。另一个示例就是客户进程（运行着的程序）用环回地址发送数据包给同样机器上的服务器进程。应该注意，这种地址在数据包中只能用作目的地址。

1.1.7 专用地址

在每一类地址中都有一些段被指派作为专用。这些地址或者用在隔离的情况下，或者用在网络地址转换技术中。见表 1-4。

表 1-4

类	网络位	网络总数
A	10.0.0	1
B	172.16-172.31	16
C	192.168.0-192.168.255	256

2.2.8 单播、多播和广播地址

Internet 上的通信可用单播、多播和广播来完成。

1. 单播地址

单播通信是一对一的。单播通信就是从单个的源端将数据包发送到单个的目的端。在 Internet 上的所有系统必须至少有一个唯一的单播地址。单播地址可以是 A 类、B 类和 C 类。

2. 多播地址

多播，又称组播。多播通信是一对多的。多播通信就是从单个的源端把数据包发送到一组目的端。多播地址是 D 类地址。整个的地址定义了一个组号。在 Internet 上的系统可以有一个或多个 D 类多播地址（除了它的一个或多个单播地址外）。如果某个系统（通常是个主机）有 7 个多播地址，就表示它属于 7 个不同的组。应该注意，D 类地址只能用作目的地址，不能用作源地址。

Internet 上的多播可以是本地级的，也可以是全局级的。在本地级，局域网上的一些主机可构成一个组，并被指派一个多播地址。在全局级，不同网络上的一些主机可构成一个组，并被指派一个多播地址。

3．广播地址

广播通信是一对所有的。Internet 只允许进行本地级广播。我们已经看到在本地级使用的两个广播地址：受限广播地址（全 1）和直接广播地址（主机位全 1）。

广播不允许在全局级进行。这表示一个系统（主机或路由器）不能向 Internet 上的所有主机或路由器发送数据包。

1.2 子网划分

IP 地址被设计成两级层次结构，即网络地址和主机地址。然而在很多情况下，这两级层次结构还不够用。例如，想象有一个机构的网络地址是 141.14.0.0（B 类地址）。这个机构有两级的层次结构的编址，但是正如图 1-5 所示，这个机构拥有的物理网络数却不能大于一个。应当注意到默认子网掩码（255.255.0.0）表示所有地址都有 16 位是共同的。剩下的位定义这个网络上的不同地址。还应当注意到，网络地址是这个地址段的第一个地址；在网络地址中，主机部分是全 0。

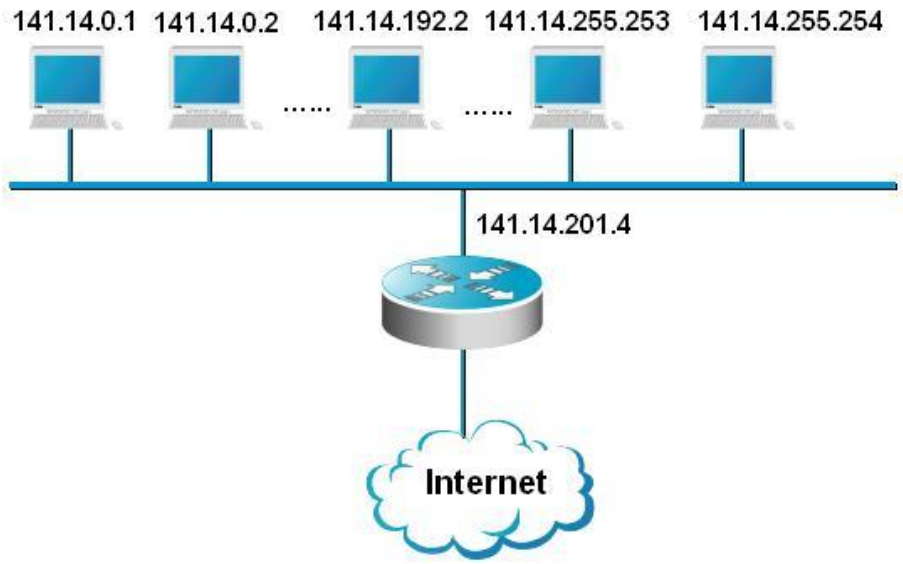


图 1-5 网络地址 141.14.0.0

按照这个方案，这个机构受到两级层次结构的限制。众多的主机不能再划分为组，而所有的主机都在同一个层次上。这个机构只有一个拥有很多主机的网络。

对这个问题的一种解决方法是划分子网，即把一个网络再为更小的一些网络，称为子网。例如，图 1-6 表示把图 1-5 中的网络再划分为四个子网。

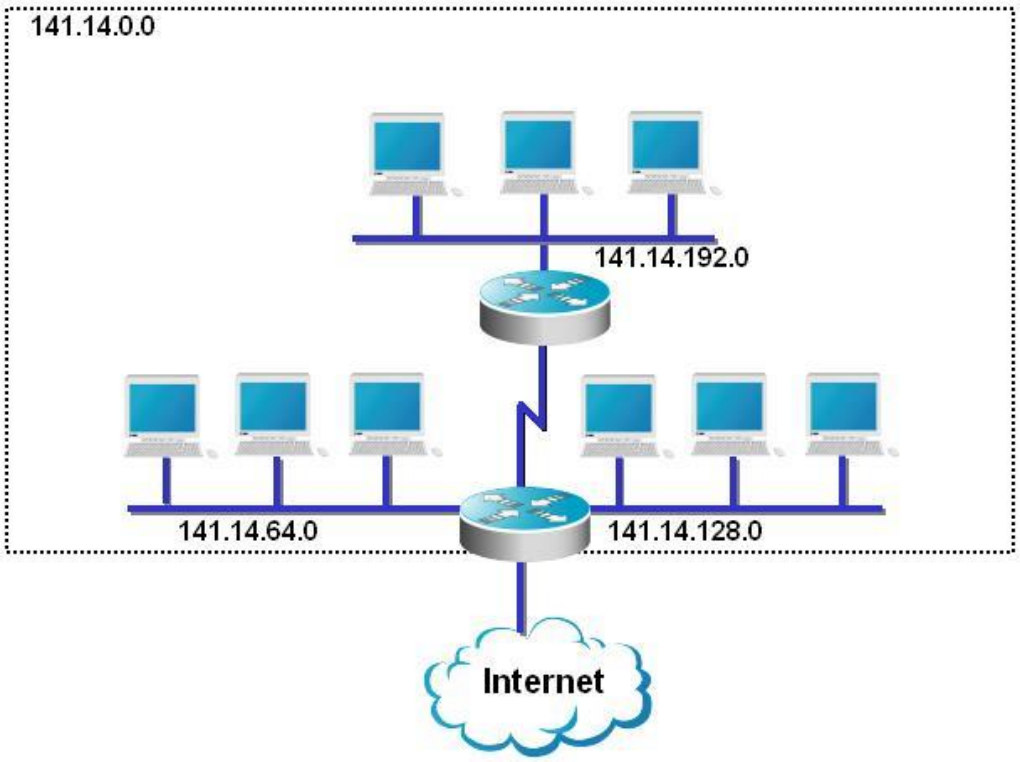


图 1-5 分成子网

在以上的示例中，Internet 的其余部分并不知道这个网络已划分为三个物理子网：这三个子网对 Internet 的其余部分来说仍然是一个网络。发送给主机 141.14.192.2 的数据仍到达路由器 R1。但是，当数据到达 R1 后，对 IP 地址的解释却改变了。路由器 R1 知道网络 141.14 在物理上已为三个子网。它知道分组必须交付给子网 141.14.192.0。

1.2.1 三级层次结构

增加子网就在 IP 编址系统中产生了一个中间级的层次。现在我们有三个级：主网、子网和主机。主网是第一级，子网是第二级，主机是第三级。见图 2-5-1-1。

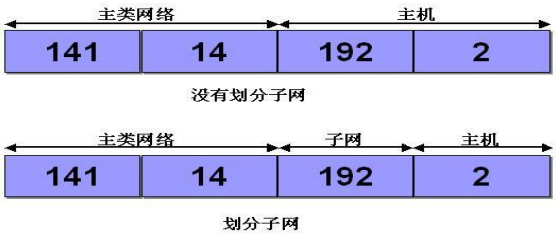


图 1-7 不划分子网和划分子网的地址

现在 IP 数据包的路由选择就包含三个步骤：主网、子网和主机。这有点像我们公司里的电话号码。如下所示，一个电话号码分为三级：地区号、总机号和分机号。如：020-66886688-6001。

1.2.2 子网掩码

当网络没有划分子网时，网络掩码就已经被使用了。网络掩码是用来找出地址段的第一个地址，也就是网络地址。但是，当划分子网时，情况就不同了。这时子网掩码有更多的 1。网络掩码产生了网络地址，子网掩码则产生子网地址。

1.2.2.1 子网掩码规则

在使用掩码的初期可以使用不连续子网掩码。所谓不连续子网掩码是指这些位并非一串 1 后面跟随一串 0，而是指将 1 和 0 混杂在一起。但是在今天，我们都使用连续的掩码（即一串 1 后面跟随一串 0）。

例如：11111111 11111111 11110000 00000000（即 255.255.240.0）是合法的子网掩码，而 11111111 11111111 11000011 00000000（即 255.255.195.0）是非法的子网掩码。

1.2.2.2 计算子网地址

只要给出了 IP 地址，我们就可以对地址进行掩码运算，从而找出子网地址。有两种方法：直接的或快捷的。

1. 直接的方法

使用直接的方法时，我们把二进制表示法的地址和掩码进行“与”操作，找出子网地址。

若主机地址是 144.45.34.56，而子网掩码是 255.255.240.0，则求子网地址的过程如下：

我们对主机地址和子网掩码进行与操作

主机地址　10001000 00101101 00100010 00111000

子网掩码　11111111 11111111 11110000 00000000

子网地址　10001000 00101101 00100000 00000000

子网地址是：144.45.32.0

2. 快捷的方法

若子网掩码是连续的，我们就可以使用快捷的方法，我们要使用的三条规则是：

（1） 若掩码中的字节是 255，就复制这个字节到地址中。

（2） 若掩码中的字节是 0，就在地址中用 0 代替这个字节。

（3） 若掩码中的字节既不是 255 也不是 0，我们就用二进制写出掩码和地址，然后使用与运算。

以上示例，我们可以采取这种方法来计算：

主机地址　144. 45.00100010.56

子网掩码　144.255.11110000. 0

子网地址　144. 45.00100000. 0

子网地址是：144.45.32.0

1.2.2.3 子网数和每一个子网内的地址数

计算在使用子网掩码时给默认掩码增加的 1 的个数，就可以找出子网数。例如，在上例中，额外的 1 的个数为 4，因此，子网数是 $2^3=8$。

计算子网掩码中 0 的个数就可找出每一个子网的地址数。例如，在上例中，0 的个数是 12，因此在每一个子网中可能的地址数是 $2^{12}=4096$。

但是，每一个子网中的第一个地址（即主机位全 0）是子网地址。每一个子网中的最后一个地址（即主机位全 1）保留在子网内进行受限广播地址之用。故在每一个子网内有效的主机地址数是 2^N-2。

1.2.3 设计子网

为了更好地理解子网划分，我们给出网络管理员是怎样设计他的公司的子网。这需要几个步骤。

1. 决定子网数

设计的第一步是确定这个机构需要的子网数。作出决定所根据的几个因素是：场所的物理位置（建筑物和楼层的数目）、部门数、每一个子网需要的主机数，等等。子网数必须为 2 的若干次方（0,2,4,8,16,32 等等）。应当注意到，选择 0 表示不划分子网。

2. 找出子网掩码

第二步就是要找出连续的子网掩码。下面的一些规则可帮助我们很容易地找出子网掩码：

（1） 找出默认掩码中的 1 的个数。

（2） 找出定义子网的 1 的个数。

（3） 把步骤 1 和 2 中的 1 的个数相加。

（4） 找出 0 的个数，它等于从 32 减去步骤 3 得出的 1 的个数。

3. 找出每一个子网的地址范围

在确定好子网掩码后，网络管理员就能找出每一个子网的地址范围。有两种方法可用来寻找每一个子网的第一个和第二个地址。

第一种方法是从第一个子网开始。第一个子网的第一个地址是这个地址段的第一个地址。然后我们加上每一个子网的地址数就可得出最后一个地址。然后我们把这个地址加 1 找出下一个子网的第一个地址。对这个子网重复以上过程。

第二种方法是从最后一个子网开始。最后一个子网的最后一个地址是这个地址段的最后一个地址。接着我们进行掩码运算来获得这个子网的第一个地址。然后我们把这个地址减 1 找出倒数，第二个子网的最后一个地址。对这个子网重复以上过程。

我们可以看个例子：

某个公司分到的地址是 201.70.64.0（C 类）。该公司需要 6 个子网。试设计这个子网。

分析过程：

（1） 默认掩码中的个数是 24（C 类）。

（2） 公司需要 6 个子网。数目 6 不是 2 的整数次方。下一个 2 的整数次方是 8（2 的 3 次方）。子网掩码中需要有 3 个 1。

（3） 子网掩码中 1 的个数是 27（24+3）。

（4） 子网掩码中 0 的个数是 5（32-27）。

（5） 掩码是 11111111 11111111 11111111 11100000，即 255.255.255.224。

（6） 子网数是 8。

（7） 每个子网中的地址数是 2^5（5 是 0 的个数）或 32。

（8） 我们现在使用第一种方法找出地址的范围。我们从第一个子网开始：

a. 这个子网第一个地址是 201.70.64.0（地址段中的第一个地址）。

b. 计算这个子网的最后一个地址可在这个地址上加 31（每一个子网的地址数是 32，但我们只能加 31）。最后一个地址是 201.70.64.31。

（9） 现在我们找出第二个子网的地址范围：

a. 这个子网第一个地址是 201.70.64.32（在第一个子网最后一个地址的后面）。

b. 计算这个子网最后一个地址可在第一个地址上加 31。得出 201.70.64.63。

（10） 在剩下的子网中地址的范围可用类似的方法求出。

习　题

1．简述几种网络分类方法，以及主要的网络拓扑结构。

2．简述 IP 地址的作用及其分类方法

3．简述子网划分的方法

4．若主机地址是 19.30.80.5，而网络掩码是 255.255.192.0，试求子网地址和广播地址。

5．某个公司分到的地址是 201.70.64.0（C 类）。这个公司需要 6 个子网。试设计这个子网。

第2章　　园区网中的广播流量控制

2.1 VLAN 概述

2.1.1 什么是 VLAN?

VLAN（Virtual LAN），翻译成中文是“虚拟局域网”。LAN 可以是由少数几台家用计算机构成的网络，也可以是数以百计的计算机构成的企业网络。VLAN 所指的 LAN 特指使用路由器分割的网络--也就是广播域。

在此让我们先复习一下广播域的概念。广播域，指的是广播帧（目标 MAC 地址全部为 1）所能传递到的范围,亦即能够直接通信的范围。严格地说,并不仅仅是广播帧,多播帧(Multicast Frame）和目标不明的单播帧（Unknown Unicast Frame）也能在同一个广播域中畅行无阻。

本来，二层交换机只能构建单一的广播域，不过使用 VLAN 功能后，它能够将网络分割成多个广播域。

那么，为什么需要分割广播域呢？那是因为，如果仅有一个广播域，有可能会影响到网络整体的传输性能。具体原因，以图 1-1 为例来加深理解。

图 2-1 中，是一个由 5 台二层交换机（交换机 1～5）连接了大量客户机构成的网络。假设，计算机 A 需要与计算机 B 通信。在基于以太网的通信中，必须在数据帧中指定目标 MAC 地址才能正常通信，因此计算机 A 必须先广播“ARP 请求（ARP Request）信息”，来尝试获取计算机 B 的 MAC 地址。

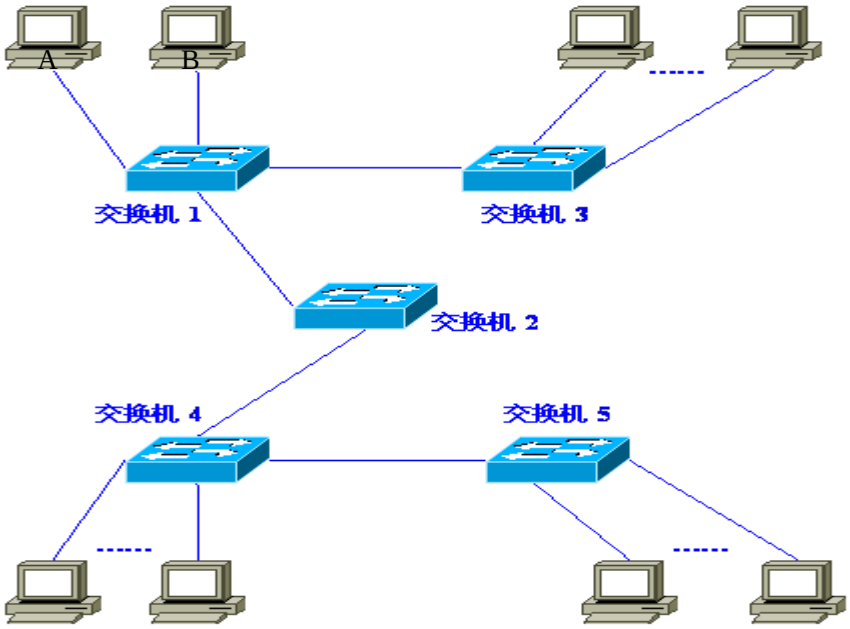


图 2-1　广播域

如图 2-2 所示，交换机 1 收到广播帧（ARP 请求）后，会将它转发给除接收端口外的其他所有端口，也就是 Flooding 了。接着，交换机 2 收到广播帧后也会 Flooding。交换机 3、4、5 也还会 Flooding。最终 ARP 请求会被转发到同一网络中的所有客户机上。

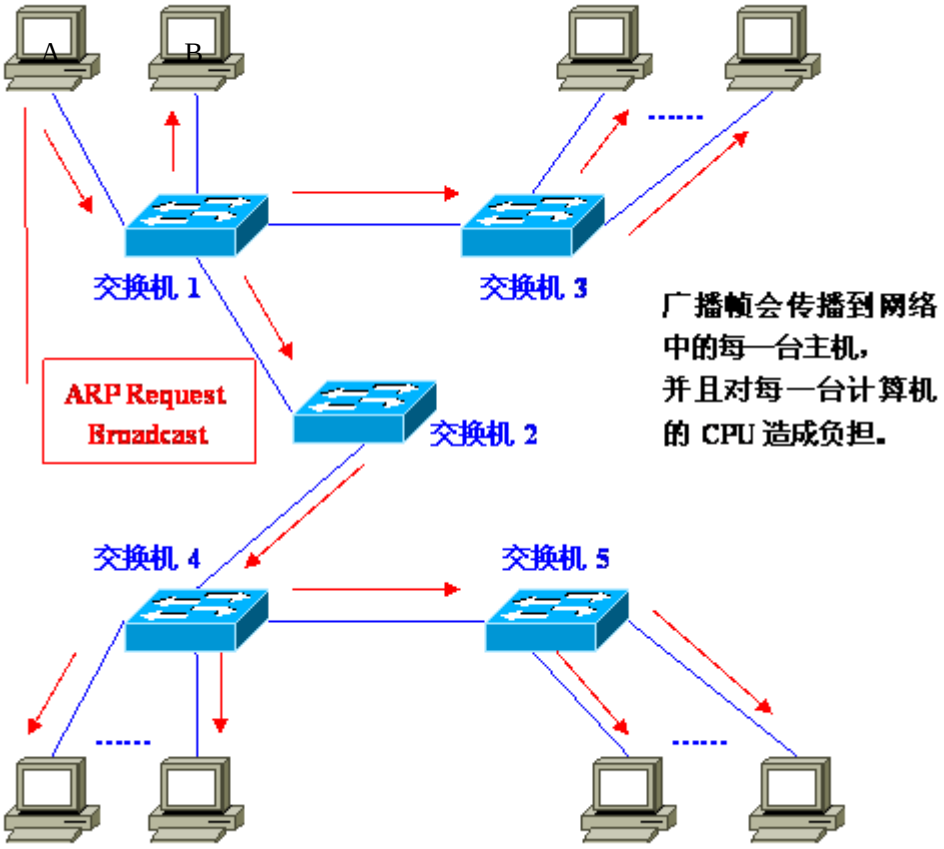


图 2-2　ARP 请求

在这里要注意，这个 ARP 请求原本是为了获得计算机 B 的 MAC 地址而发出的。也就是说：只要计算机 B 能收到就可以了。但是事实上，数据帧却传遍整个网络，导致所有的计算机都收到了它。如此一来，一方面广播信息消耗了网络整体的带宽，另一方面，收到广播信息的计算机还要消耗一部分 CPU 时间来对它进行处理。造成了网络带宽和 CPU 运算能力的大量无谓消耗。

也许人们会有这样的问题：广播信息是这样经常发出的吗？广播信息真是那么频繁出现的吗？

答案是：是的！实际上，广播帧会非常频繁地出现。利用 TCP/IP 协议栈通信时，除了前面出现的 ARP 外，还有可能需要发出 DHCP、RIP 等很多其他类型的广播信息。

ARP 广播，是在需要与其他主机通信时发出的。当客户机请求 DHCP 服务器分配 IP 地址时，就必须发出 DHCP 的广播。而使用 RIP 作为路由协议时，每隔 30 秒路由器都会对邻近的其他路由器广播一次路由信息。RIP 以外的其他路由协议使用多播传输路由信息，这也会被交换机转发（Flooding）。除了 TCP/IP 以外，NetBEUI、IPX 和 Apple Talk 等协议也经常需要用到广播。例如在 Windows 下双击打开“网络计算机”时就会发出广播（多播）信息。（Windows XP 除外）

总之，广播就在我们身边。下面列出的就是一些常见的广播通信：

- ARP 请求：建立 IP 地址和 MAC 地址的映射关系。
- RIP：一种路由协议。
- DHCP：用于自动设定 IP 地址的协议。
- NetBEUI：Windows 下使用的网络协议。
- IPX：Novell Netware 使用的网络协议。
- Apple Talk：苹果公司的 Macintosh 计算机使用的网络协议。

如果整个网络只有一个广播域，那么一旦发出广播信息，就会传遍整个网络，并且对网络中的主机带来额外的负担。因此，在设计 LAN 时，需要注意如何才能有效地分割广播域。

2.1.2　广播域的分割与 VLAN 的必要性

分割广播域时，一般都必须使用到路由器。使用路由器后，可以以路由器上的网络接口（LAN Interface）为单位分割广播域。

但是，通常情况下路由器上不会有太多的网络接口，其数目多在 1～4 个左右。随着宽带连接的普及，宽带路由器（或者叫 IP 共享器）变得较为常见，但是需要注意的是，它们上面虽然带着多个（一般为 4 个左右）连接 LAN 一侧的网络接口，但那实际上是路由器内置的交换机，并不能分割广播域。

况且使用路由器分割广播域的话，所能分割的个数完全取决于路由器的网络接口个数，使得用户无法自由地根据实际需要分割广播域。

与路由器相比，二层交换机一般带有多个网络接口。因此如果能使用它分割广播域，那么无疑运用上的灵活性会大大提高。

用于在二层交换机上分割广播域的技术，就是 VLAN。通过利用 VLAN，我们可以自由设计广播域的构成，提高网络设计的自由度。

2.2 交换机的端口

交换机的端口，可以分为以下两种：

1）访问链接（Access Link）

2）汇聚链接（Trunk Link）

接下来就让我们来依次学习这两种不同端口的特征。

2.2.1 访问链接

访问链接，指的是“只属于一个 VLAN，且仅向该 VLAN 转发数据帧”的端口。在大多数情况下，访问链接所连的是客户机。

通常设置 VLAN 的顺序是：

1）生成 VLAN；

2）设定访问链接（决定各端口属于哪一个 VLAN）。

设定访问链接的方法，可以是事先固定的、也可以是根据所连的计算机而动态改变设定。前者被称为“静态 VLAN”、后者自然就是“动态 VLAN”了。

1、静态 VLAN

静态 VLAN 又被称为基于端口的 VLAN（Port Based VLAN）。顾名思义，就是明确指定各端口属于哪个 VLAN 的设定方法，如图 2-3 所示。

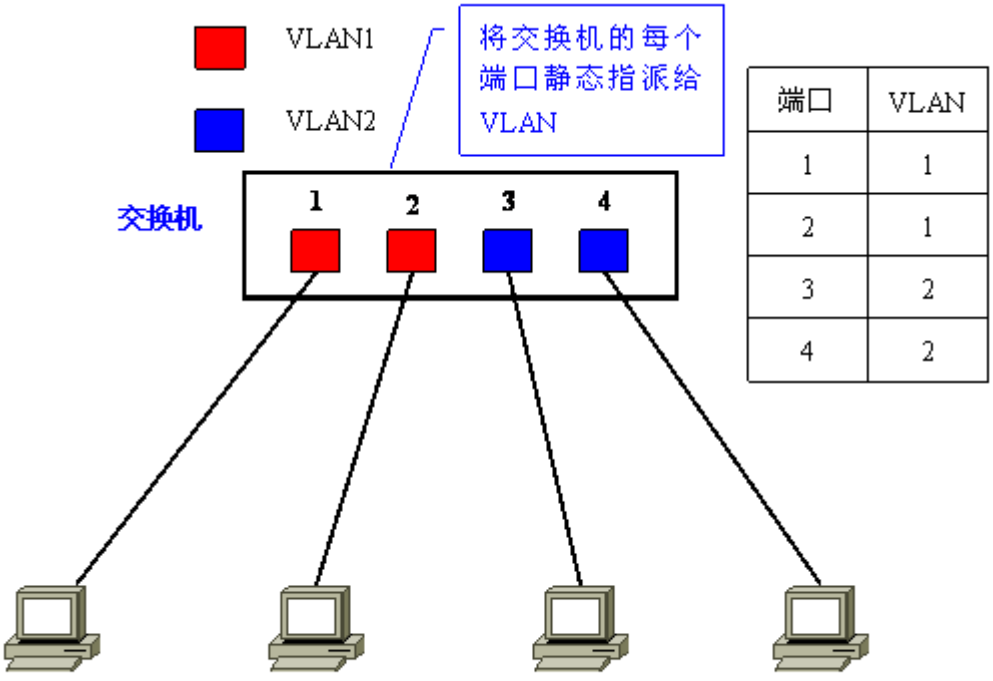


图 2-3　基于端口的静态 VLAN

由于需要一个个端口地指定，因此当网络中的计算机数目超过一定数字（比如数百台）后，设定操作就会变得非常烦杂。并且，客户机每次变更所连端口，都必须同时更改该端口所属 VLAN

的设定，这显然不适合那些需要频繁改变拓扑结构的网络。

2、动态 VLAN

另一方面，动态 VLAN 则是根据每个端口所连的计算机，随时改变端口所属的 VLAN。这就可以避免上述的更改设定之类的操作。动态 VLAN 可以大致分为 3 类：

1）基于 MAC 地址的 VLAN（MAC Based VLAN）

2）基于子网的 VLAN（Subnet Based VLAN）

3）基于用户的 VLAN（User Based VLAN）

其间的差异，主要在于根据 OSI 参照模型哪一层的信息决定端口所属的 VLAN。

基于 MAC 地址的 VLAN，就是通过查询并记录端口所连计算机上网卡的 MAC 地址来决定端口的所属。假定有一个 MAC 地址“A”被交换机设定为属于 VLAN“10”，那么不论 MAC 地址为“A”的这台计算机连在交换机哪个端口，该端口都会被划分到 VLAN10 中去。计算机连在端口 1 时，端口 1 属于 VLAN10；而计算机连在端口 2 时，则是端口 2 属于 VLAN10。 如图 2-4 所示。

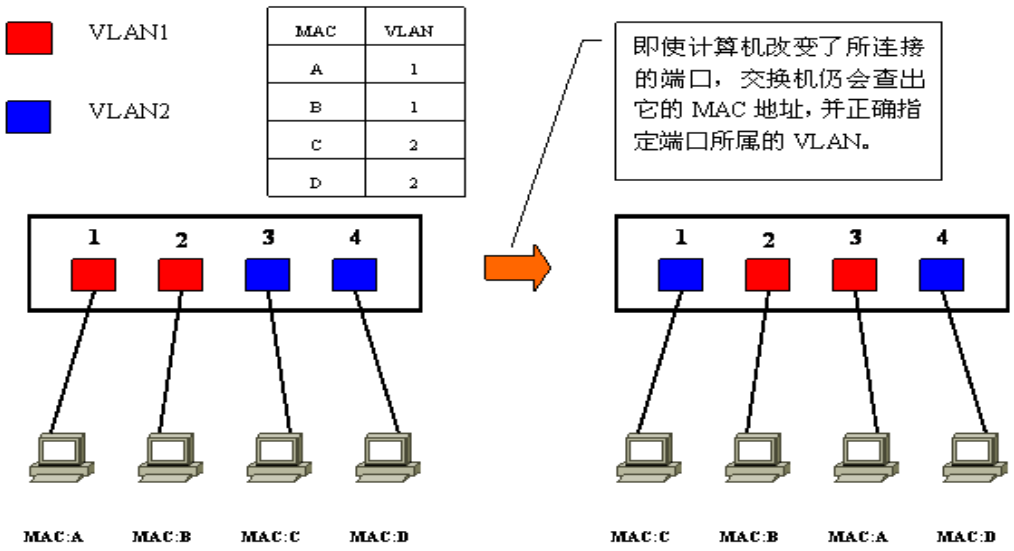


图 2-4　基于 MAC 地址的动态 VLAN

由于是基于 MAC 地址决定所属 VLAN 的，因此可以理解为这是一种在 OSI 的第二层设定访问链接的方法。

但是，基于 MAC 地址的 VLAN，在设定时必须调查所连接的所有计算机的 MAC 地址并加以登录。而且如果计算机更换了网卡，还是需要更改设定。

基于子网的 VLAN，则是通过所连计算机的 IP 地址，来决定端口所属 VLAN 的。不像基于 MAC 地址的 VLAN，即使计算机因为交换了网卡或是其他原因导致 MAC 地址改变，只要它的 IP 地址不变，就仍可以加入原先设定的 VLAN。如图 2-5 所示。

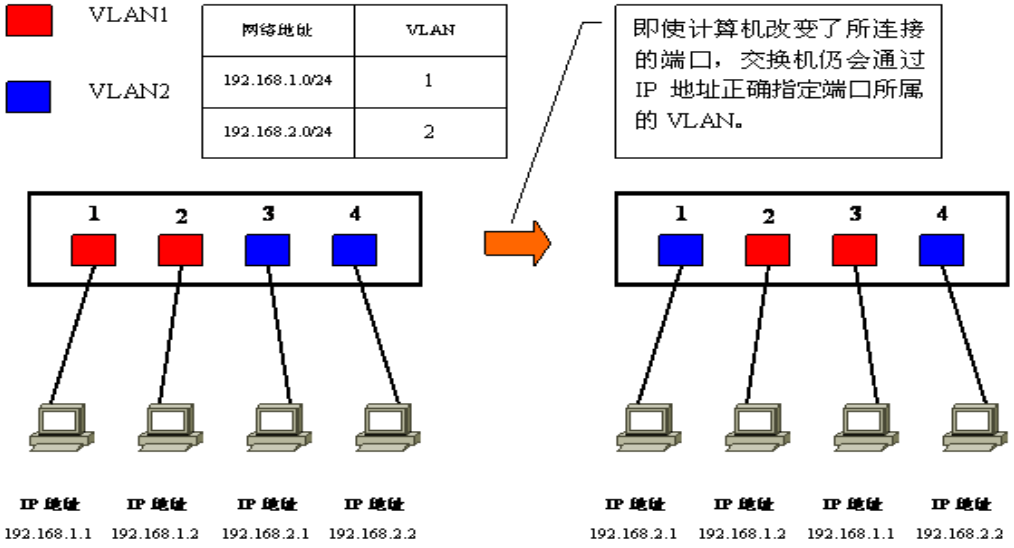


图 2-5　基于 IP 地址的动态 VLAN

因此，与基于 MAC 地址的 VLAN 相比，能够更为简便地改变网络结构。IP 地址是 OSI 参照模型中第三层的信息,所以我们可以理解为基于子网的 VLAN 是一种在 OSI 的第三层设定访问链接的方法。

基于用户的 VLAN，则是根据交换机各端口所连的计算机上当前登录的用户，来决定该端口属于哪个 VLAN。这里的用户识别信息，一般是计算机操作系统登录的用户，比如可以是 Windows 域中使用的用户名。这些用户名信息，属于 OSI 第四层以上的信息。

总的来说，决定端口所属 VLAN 时利用的信息在 OSI 中的层面越高，就越适于构建灵活多变的网络。

2.2.2 访问链接的总结

综上所述，设定访问链接的方法有静态 VLAN 和动态 VLAN 两种，其中动态 VLAN 又可以继续细分成几个小类。

基于子网的 VLAN 和基于用户的 VLAN 有可能是网络设备厂商使用独有的协议实现的，不同厂商的设备之间互联有可能出现兼容性问题，因此在选择交换机时，一定要注意事先确认。

下面总结了静态 VLAN 和动态 VLAN 的相关信息。

种类	说明
静态 VLAN（基于端口的 VLAN）	将交换机的各端口固定指派给 VLAN
基于 MAC 地址的动态 VLAN	根据各端口所连计算机的 MAC 地址设定
基于子网的动态 VLAN	根据各端口所连计算机的 IP 地址设定
基于用户的动态 VLAN	根据端口所连计算机上登录用户设定

2.3 实现 VLAN 的机制

在理解了“为什么需要 VLAN”之后，接下来让我们来了解一下交换机是如何使用 VLAN 分割广播域的。

首先，在一台未设置任何 VLAN 的二层交换机上，任何广播帧都会被转发给除接收端口外的所有其他端口（Flooding）。例如，计算机 A 发送广播信息后，会被转发给端口 2、3、4。

这时，如果在交换机上生成红、蓝两个 VLAN，同时设置端口 1、2 属于红色 VLAN、端口 3、4 属于蓝色 VLAN。再从 A 发出广播帧的话，交换机就只会把它转发给同属于一个 VLAN 的其他端口，也就是同属于红色 VLAN 的端口 2，而不会再转发给属于蓝色 VLAN 的端口。

同样，C 发送广播信息时，只会被转发给其他属于蓝色 VLAN 的端口 4，而不会被转发给属于红色 VLAN 的端口。如图 2-6 所示。

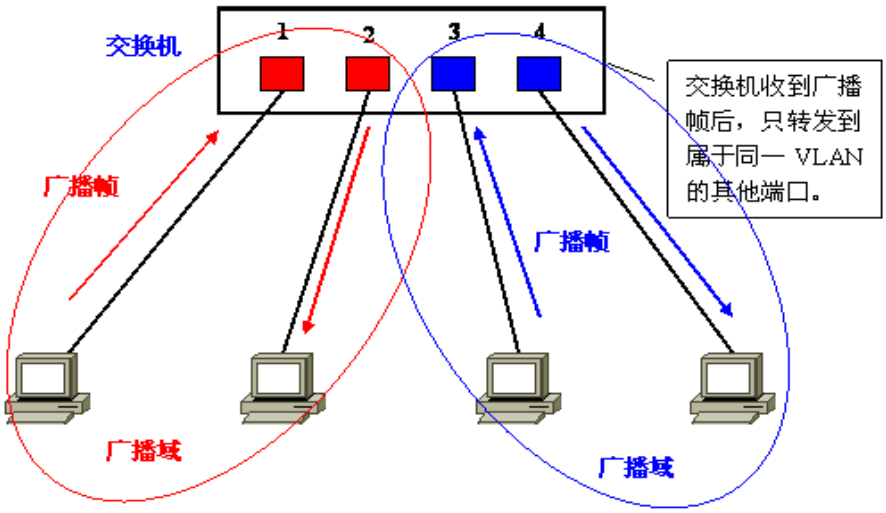


图 2-6　设置 VLAN

就这样，VLAN 通过限制广播帧转发的范围分割了广播域。上图中为了便于说明，以红、蓝两色识别不同的 VLAN，在实际使用中则是用“VLAN ID”来区分的，这里的 ID 用于标识不同的 VLAN，其范围是 1 至 4094。

2.3.1 直观地描述 VLAN

如果要更为直观地描述 VLAN 的话，我们可以把它理解为将一台交换机在逻辑上分割成了数台交换机。在一台交换机上生成红、蓝两个 VLAN，也可以看作是将一台交换机换做一红一蓝两台虚拟的交换机。如图 2-7 所示。

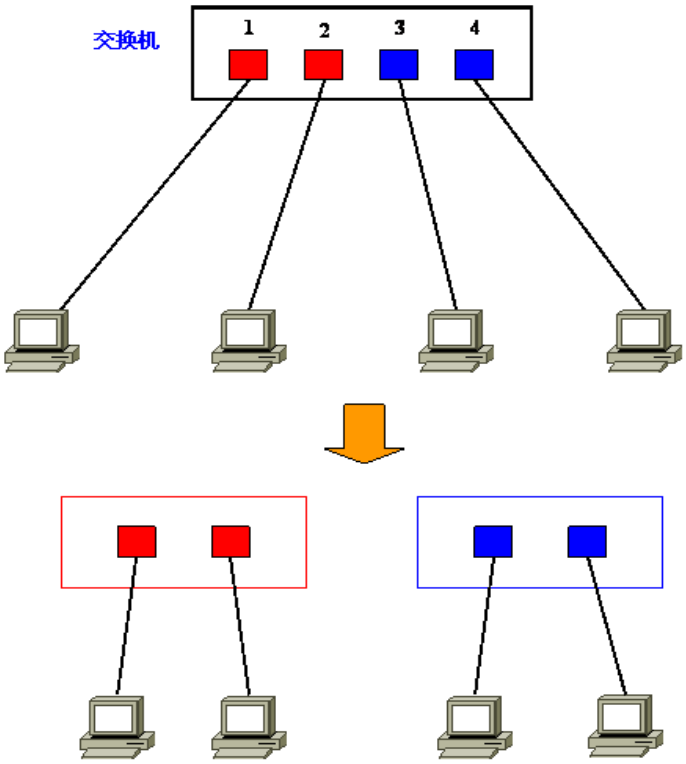


图 2-7　将一个交换机分成两个虚拟的交换机

在红、蓝两个 VLAN 之外生成新的 VLAN 时，可以想象成又添加了新的交换机。

但是，VLAN 生成的逻辑上的交换机是互不相通的。因此，在交换机上设置 VLAN 后，如果未做其他处理，VLAN 间是无法通信的。

明明接在同一台交换机上，但却偏偏无法通信，这个事实也许让人难以接受。但它既是 VLAN 方便易用的特征，又是使 VLAN 令人难以理解的原因。

2.3.2　需要 VLAN 间通信时怎么办

那么，当我们需要在不同的 VLAN 间通信时又该如何处理呢？

请读者再次回忆一下：VLAN 是广播域，而通常两个广播域之间由路由器连接，广播域之间来往的数据包都是由路由器中继的。因此，VLAN 间的通信也需要路由器提供中继服务，这被称作“VLAN 间路由”。

VLAN 间路由，可以使用普通的路由器，也可以使用三层交换机。

在这里首先记住，不同 VLAN 间互相通信时需要用到路由功能。

2.4　VLAN 的汇聚链接

需要设置跨越多台交换机的 VLAN 时，交换机将如何联接呢？

到此为止，我们学习的都是使用单台交换机设置 VLAN 时的情况。那么，如果需要设置跨越多台交换机的 VLAN 时又如何呢？

在规划企业级网络时，很有可能会遇到隶属于同一部门的用户分散在同一座建筑物中的不同楼层的情况，这时可能就需要考虑到如何跨越多台交换机设置 VLAN 的问题了。假设有如下图

2-8 所示的网络，且需要将不同楼层的 A、C 和 B、D 设置为同一个 VLAN。

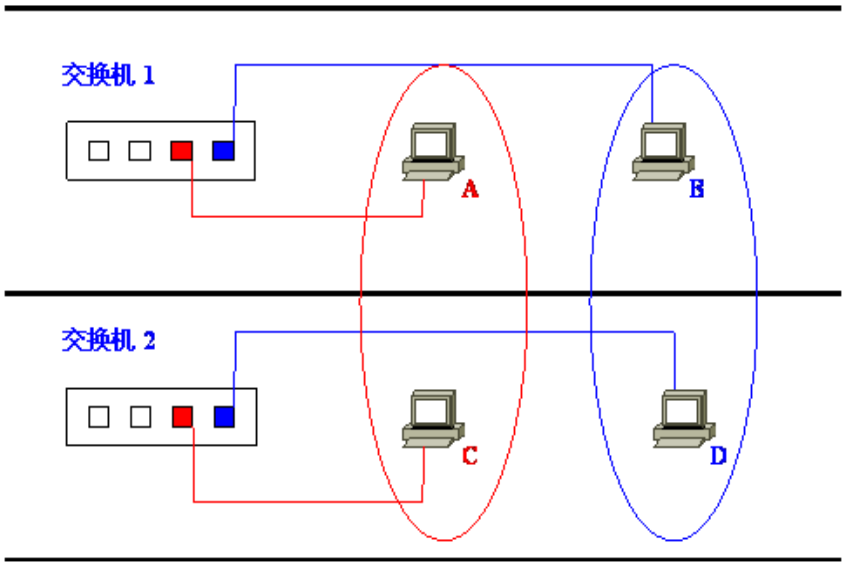


图 2-8　跨越多台交换机的 VLAN

这时最关键的就是“交换机 1 和交换机 2 如何进行连接”

最简单的方法，自然是在交换机 1 和交换机 2 上各设一个红、蓝 VLAN 专用的接口并互联了。如图 2-9 所示。

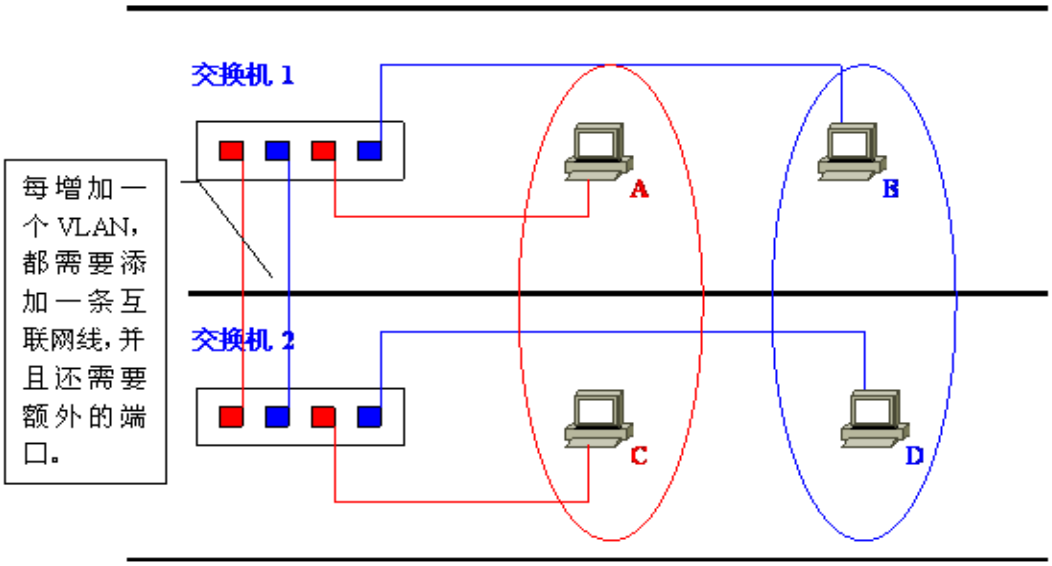


图 2-9　两个交换机的简单连接

但是，这个办法从扩展性和管理效率来看都不好。例如，在现有网络基础上再新建 VLAN 时，为了让这个 VLAN 能够互通，就需要在交换机间连接新的网线。建筑物楼层间的纵向布线是比较麻烦的，一般不能由基层管理人员随意进行。并且，VLAN 越多，楼层间（严格地说是交换机间）互联所需的端口也越来越多，交换机端口的利用效率低是对资源的一种浪费、也限制了网络的扩展。

为了避免这种低效率的连接方式，人们想办法让交换机间互联的网线集中到一根上，这时使用的就是汇聚链接（Trunk Link）的方法。

2.4.1 何谓汇聚链接？

汇聚链接（Trunk Link）指的是能够转发多个不同 VLAN 的通信的端口。

汇聚链路上流通的数据帧，都被附加了用于识别分属于哪个 VLAN 的特殊信息。

现在再让我们回过头来考虑一下图 1-9 的网络如果采用汇聚链路？用户只需要简单地将交换机间互联的端口设定为汇聚链接就可以了。这时使用的网线还是普通的 UTP 线，而不是什么其他的特殊布线。

2.4.2 汇聚链接方法

下面让我们具体看看汇聚链接是如何实现跨越交换机间的 VLAN 的。

A 发送的数据帧从交换机 1 经过汇聚链路到达交换机 2 时，在数据帧上附加了表示属于红色 VLAN 的标记。

交换机 2 收到数据帧后，经过检查 VLAN 标识发现这个数据帧是属于红色 VLAN 的，因此去除标记后根据需要将复原的数据帧只转发给其他属于红色 VLAN 的端口。这时的转发，是指经过确认目标 MAC 地址并与 MAC 地址列表比对后只转发给目标 MAC 地址所连的端口。只有当数据帧是一个广播帧、多播帧或是目标不明的帧时，它才会被转发到所有属于红色 VLAN 的端口。如图 2-10 所示。

蓝色 VLAN 发送数据帧时的情形也与此相同。

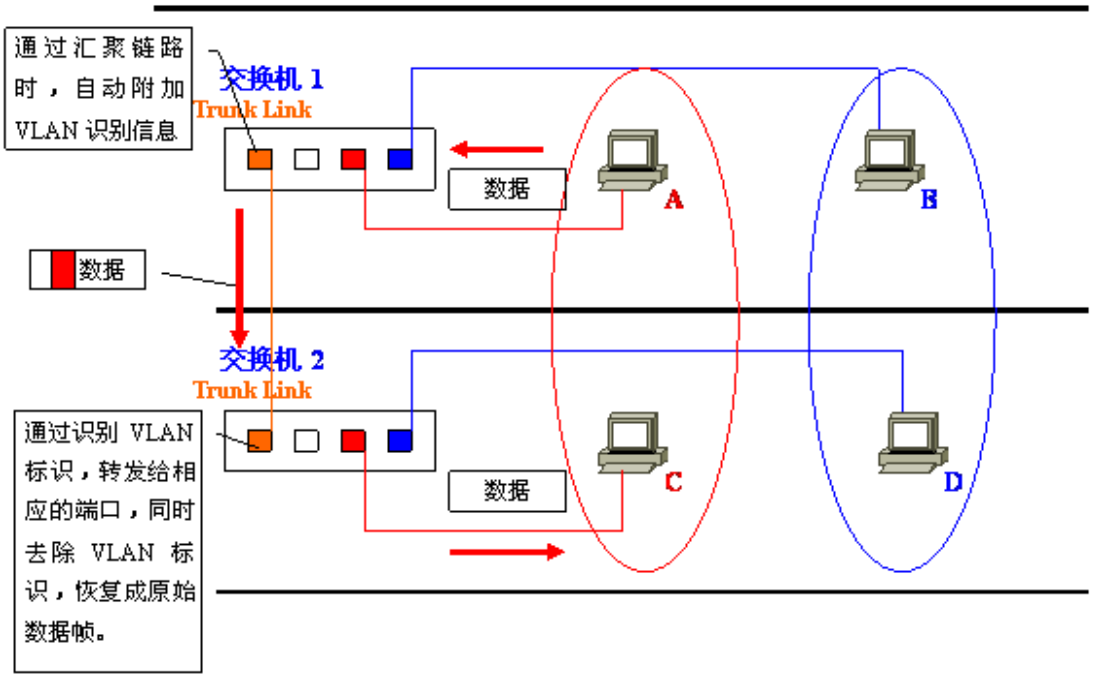


图 2-10　交换机之间的汇聚链接

通过汇聚链路时附加的 VLAN 识别信息，有可能支持标准的“IEEE 802.1Q”协议，也可能是 Cisco 产品独有的“ISL（Inter Switch Link）”。如果交换机支持这些规格，那么用户就能够高效率地构筑横跨多台交换机的 VLAN。

另外，汇聚链路上流通着多个 VLAN 的数据，自然负载较重。因此，在设定汇聚链接时，有一个前提就是必须支持 100Mbps 以上的传输速度。

在默认条件下，汇聚链接会转发交换机上存在的所有 VLAN 的数据。换一个角度看，可以认

为汇聚链接（端口）同时属于交换机上所有的 VLAN。由于实际应用中很可能并不需要转发所有 VLAN 的数据，因此为了减轻交换机的负载、也为了减少对带宽的浪费，我们可以通过用户设定限制能够经由汇聚链路互联的 VLAN。

关于 IEEE802.1Q 和 ISL 的具体内容，将在下一讲中提到。

2.5 IEEE802.1Q 与 ISL

在交换机的汇聚链接上，可以通过对数据帧附加 VLAN 信息，构建跨越多台交换机的 VLAN。

附加 VLAN 信息的方法，最具有代表性的有：

1）IEEE802.1Q

2）ISL

现在就让我们看看这两种协议分别如何对数据帧附加 VLAN 信息。

2.5.1 IEEE802.1Q

IEEE802.1Q，俗称“Dot One Q”，是经过 IEEE 认证的对数据帧附加 VLAN 识别信息的协议。

在此，我们先来回忆一下以太网数据帧的标准格式。

IEEE802.1Q 所附加的 VLAN 识别信息，位于数据帧中“发送源 MAC 地址”与“类别域（Type Field)”之间。具体内容为 2 字节的 TPID 和 2 字节的 TCI，共计 4 字节。 如图 2-11 所示。

在数据帧中添加了 4 字节的内容，那么 CRC 值自然也会有所变化。这时数据帧上的 CRC 是插入 TPID、TCI 后，对包括它们在内的整个数据帧重新计算后所得的值。

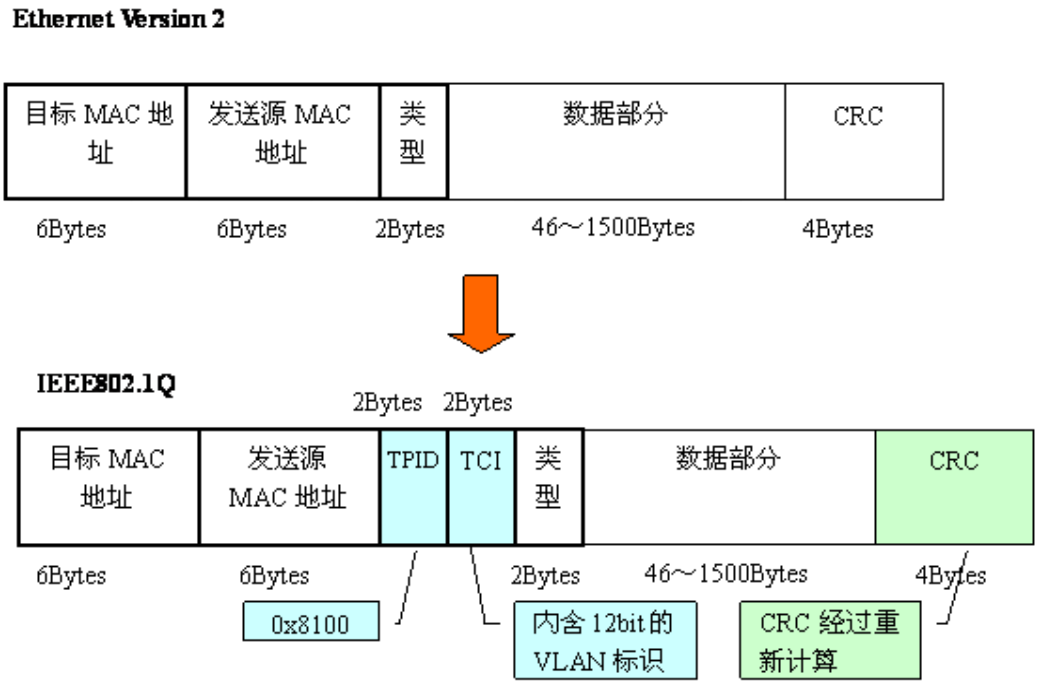


图 2-11　数据帧中加入 VLAN 识别信息（基于 IEEE802.1Q）

而当数据帧离开汇聚链路时，TPID 和 TCI 会被去除，这时还会进行一次 CRC 的重新计算。

TPID 的值，固定为 0x8100。交换机通过 TPID，来确定数据帧内附加了基于 IEEE802.1Q 的 VLAN 信息。而实质上的 VLAN ID，是 TCI 中的 12 位元。由于总共有 12 位，因此最多可供识别 4096 个 VLAN。

基于 IEEE802.1Q 附加的 VLAN 信息，就像在传递物品时附加的标签。因此，它也被称作“标签型 VLAN（Tagging VLAN）”。

2.5.2 ISL（Inter Switch Link）

ISL，是 Cisco 产品支持的一种与 IEEE802.1Q 类似的、用于在汇聚链路上附加 VLAN 信息的协议。

使用 ISL 后，每个数据帧头部都会被附加上 26 字节的“ISL 包头（ISL Header）”，并且在帧尾带上通过对包括 ISL 包头在内的整个数据帧进行计算后得到的 4 字节 CRC 值。换而言之，就是总共增加了 30 字节的信息。如图 2-12 所示。

在使用 ISL 的环境下，当数据帧离开汇聚链路时，只要简单地去除 ISL 包头和新 CRC 就可以了。由于原先的数据帧及其 CRC 都被完整保留，因此无需重新计算 CRC。

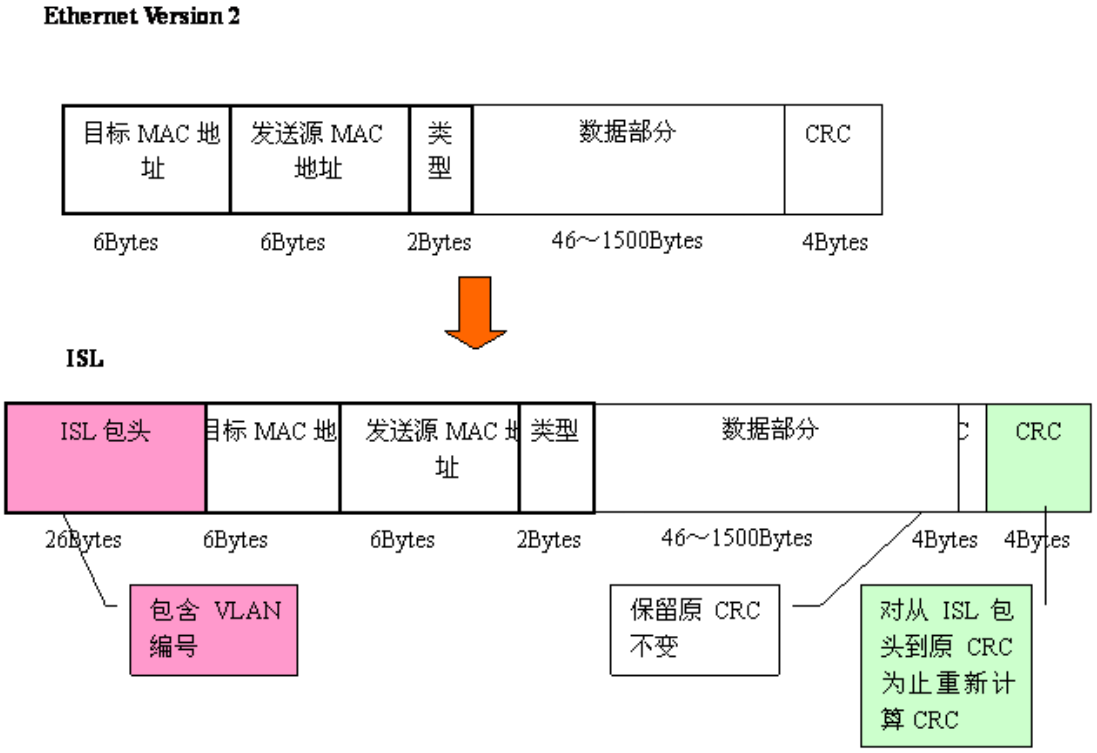


图 2-12 数据帧中加入 VLAN 识别信息（基于 ISL）

ISL 有如用 ISL 包头和新 CRC 将原数据帧整个包裹起来，因此也被称为“封装型 VLAN（Encapsulated VLAN）”。

需要注意的是，不论是 IEEE802.1Q 的“Tagging VLAN”，还是 ISL 的“Encapsulated VLAN”，都不是很严密的称谓。不同的书籍与参考资料中，上述词语有可能被混合使用，因此需要大家在学习时格外注意。 并且由于 ISL 是 Cisco 独有的协议，因此只能用于 Cisco 网络设备之间的互联。

2.6 VLAN 间路由

2.6.1 VLAN 间路由的必要性

根据目前为止学习的知识，我们已经知道两台计算机即使连接在同一台交换机上，只要所属的 VLAN 不同就无法直接通信。接下来我们将要学习的就是如何在不同的 VLAN 间进行路由，使分属不同 VLAN 的主机能够互相通信。

首先，先来复习一下为什么不同 VLAN 间不通过路由就无法通信。在 LAN 内的通信，必须在数据帧头中指定通信目标的 MAC 地址。而为了获取 MAC 地址，TCP/IP 协议下使用的是 ARP。ARP 解析 MAC 地址的方法，则是通过广播。也就是说，如果广播报文无法到达，那么就无从解析 MAC 地址，亦即无法直接通信。

计算机分属不同的 VLAN，也就意味着分属不同的广播域，自然收不到彼此的广播报文。因此，属于不同 VLAN 的计算机之间无法直接互相通信。为了能够在 VLAN 间通信，需要利用 OSI 参照模型中更高一层--网络层的信息（IP 地址）来进行路由。关于路由的具体内容，将在后面章节中详细介绍。

路由功能，一般主要由路由器提供。但在今天的局域网里，我们也经常利用带有路由功能的交换机--三层交换机（Layer 3 Switch）来实现。接下来就让我们分别看看使用路由器和三层交换机进行 VLAN 间路由时的情况。

2.6.2 使用路由器进行 VLAN 间路由

在使用路由器进行 VLAN 间路由时，与构建横跨多台交换机的 VLAN 时的情况类似，我们还是会遇到“该如何连接路由器与交换机”这个问题。路由器和交换机的接线方式，大致有以下两种：

1）将路由器与交换机上的每个 VLAN 分别连接

2）不论 VLAN 有多少个，路由器与交换机都只用一条网线连接

最容易想到的，当然还是“把路由器和交换机以 VLAN 为单位分别用网线连接”了。将交换机上用于和路由器互联的每个端口设为访问链接，然后分别用网线与路由器上的独立端口互联。如图 2-13 所示，交换机上有 2 个 VLAN，那么就需要在交换机上预留 2 个端口用于与路由器互联，路由器上同样需要有 2 个端口，两者之间用 2 条网线分别连接。

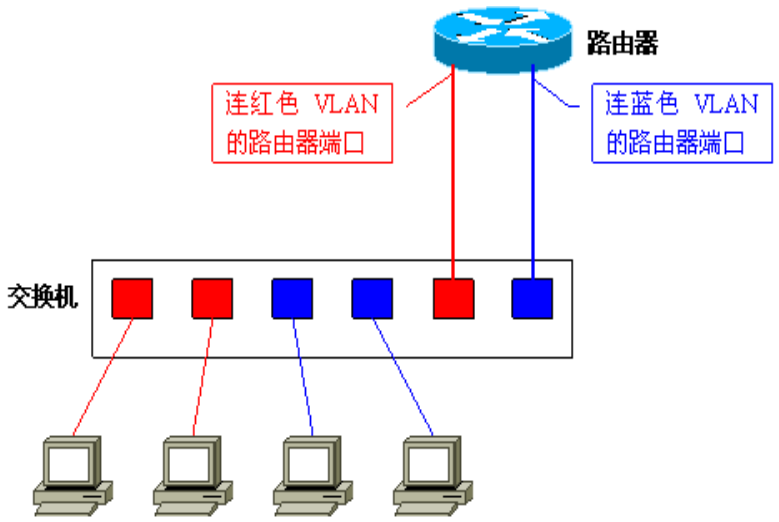


图 2-13　路由器与交换机上的每个 VLAN 分别连接

如果采用这个办法，大家应该不难想象它的扩展性很成问题。每增加一个新的 VLAN，都需要消耗路由器的端口和交换机上的访问链接，而且还需要重新布设一条网线。而路由器，通常不会带有太多 LAN 接口的。新建 VLAN 时，为了对应增加的 VLAN 所需的端口，就必须将路由器升级成带有多个 LAN 接口的高端产品，这部分成本、还有重新布线所带来的开销，都使得这种接线法成为一种不受欢迎的办法。

那么，第二种办法 “不论 VLAN 数目多少，都只用一条网线连接路由器与交换机”是如何做的呢？当使用一条网线连接路由器与交换机、进行 VLAN 间路由时，需要用到汇聚链接。

具体实现过程为：首先将用于连接路由器的交换机端口设为汇聚链接，而路由器上的端口也必须支持汇聚链路。双方用于汇聚链路的协议自然也必须相同。接着在路由器上定义对应各个 VLAN 的“子接口（Sub Interface）”。尽管实际与交换机连接的物理端口只有一个，但在理论上我们可以把它分割为多个虚拟端口。 如图 2-14 所示。

VLAN 将交换机从逻辑上分割成了多台交换机，因而用于 VLAN 间路由的路由器，也必须拥有分别对应各个 VLAN 的虚拟接口。

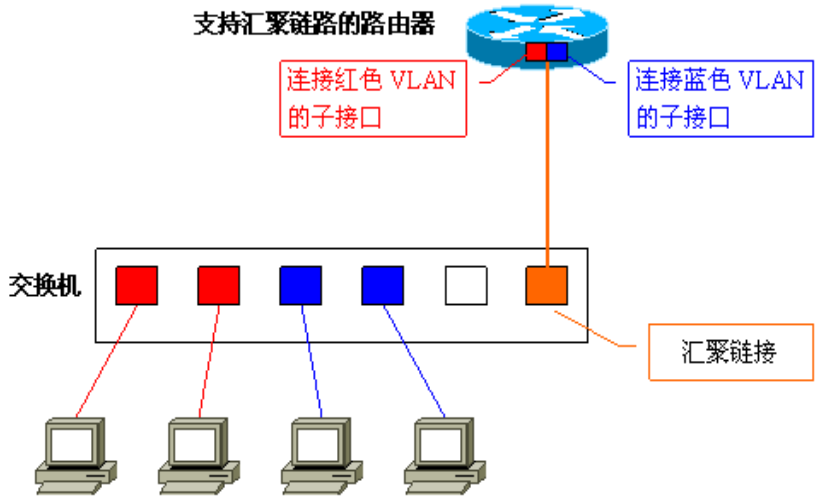


图 2-14　路由器与交换机只用一条网线连接

采用这种方法的话，即使以后在交换机上新建 VLAN，仍只需要一条网线连接交换机和路由器。用户只需要在路由器上新设一个对应新 VLAN 的子接口就可以了。与前面的方法相比，扩展性要强得多，也不用担心需要升级 LAN 接口数不足的路由器或是重新布线。

1、同一 VLAN 内的通信

接下来，我们继续学习使用汇聚链路连接交换机与路由器时，VLAN 间路由是如何进行的。如图 2-15 所示，为各台计算机以及路由器的子接口设定 IP 地址。

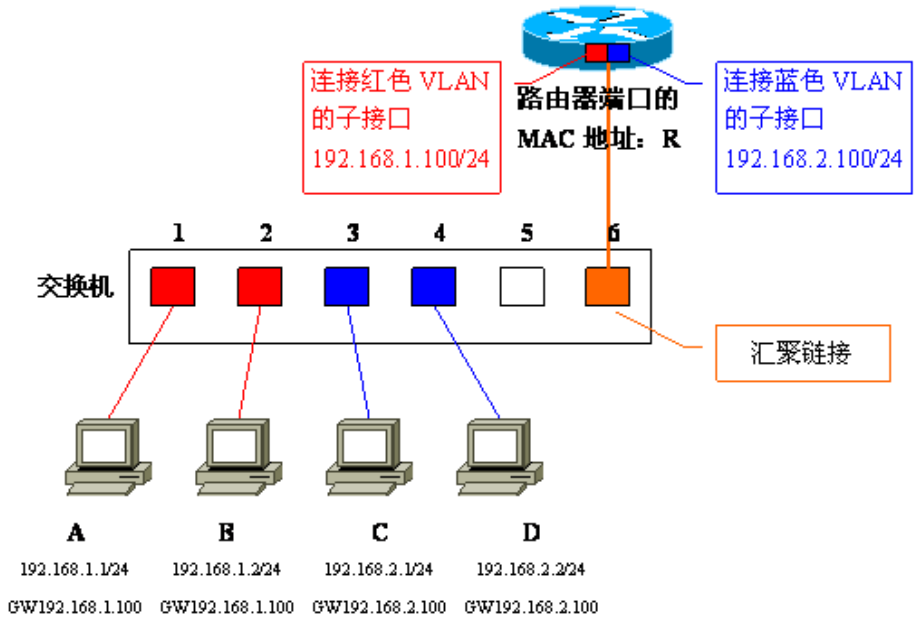


图 2-15　设置对应各个 VLAN 的虚拟接口

红色 VLAN（VLAN ID=1）的网络地址为 192.168.1.0/24，蓝色 VLAN（VLAN ID=2）的网络地址为 192.168.2.0/24。各计算机的 MAC 地址分别为 A/B/C/D，路由器汇聚链接端口的 MAC 地址为 R。交换机通过对各端口所连计算机 MAC 地址的学习，生成一个 MAC 地址列表。

首先考虑计算机 A 与同一 VLAN 内的计算机 B 之间通信时的情形。

计算机 A 发出 ARP 请求信息，请求解析 B 的 MAC 地址。交换机收到数据帧后，检索 MAC 地址列表中与收信端口同属一个 VLAN 的表项。结果发现，计算机 B 连接在端口 2 上，于是交换机将数据帧转发给端口 2，最终计算机 B 收到该帧。收发信双方同属一个 VLAN 之内的通信，一切处理均在交换机内完成。 如图 2－C16 所示。

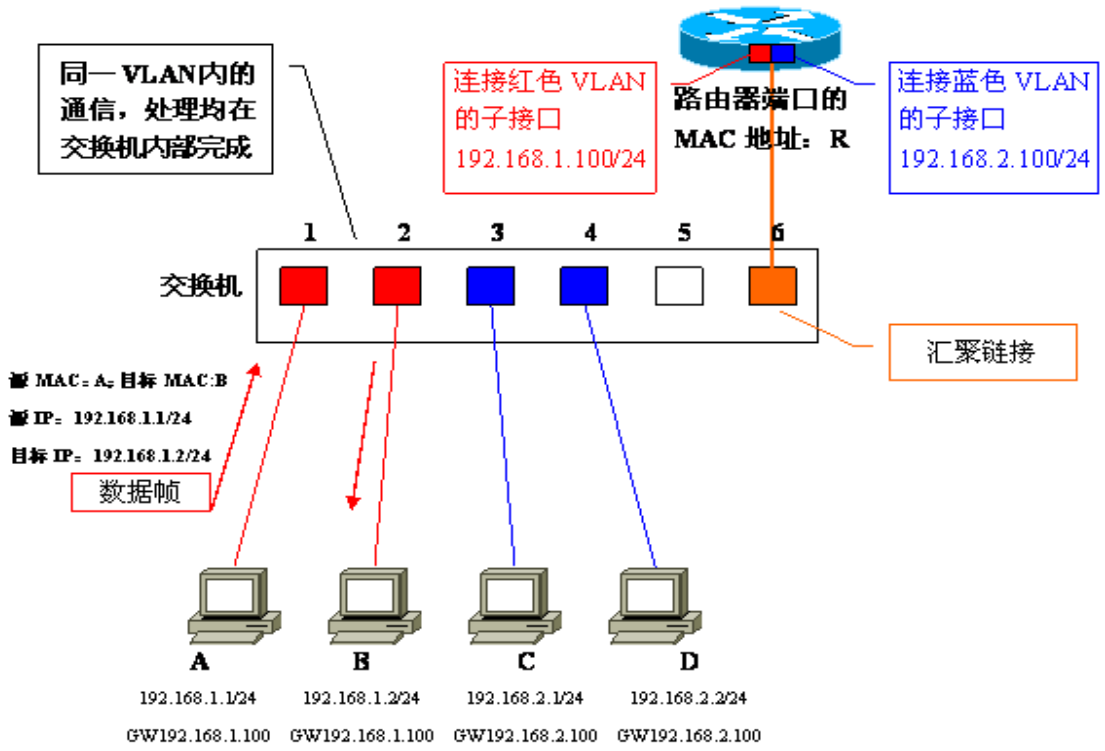


图 2-16　同一 VLAN 中的数据传输

2、不同 VLAN 间通信时数据的流程

这是这一 VLAN 的核心内容，它就是不同 VLAN 间的通信问题。让我们来考虑一下计算机 A 与计算机 C 之间通信时的情况。

计算机 A 从通信目标的 IP 地址（192.168.2.1）得出 C 与本机不属于同一个网段。因此会向设定的默认网关（Default Gateway，GW）转发数据帧。在发送数据帧之前，需要先用 ARP 获取路由器的 MAC 地址。

得到路由器的 MAC 地址 R 后，接下来就是按图 2-17 中所示的步骤发送往 C 去的数据帧。①的数据帧中，目标 MAC 地址是路由器的地址 R、但内含的目标 IP 地址仍是最终要通信的对象 C 的地址。这一部分的内容，涉及到局域网内经过路由器转发时的通信步骤。

交换机在端口 1 上收到①的数据帧后，检索 MAC 地址列表中与端口 1 同属一个 VLAN 的表项。由于汇聚链路会被看作属于所有的 VLAN，因此这时交换机的端口 6 也属于被参照对象。这样交换机就知道往 MAC 地址 R 发送数据帧，需要经过端口 6 转发。

从端口 6 发送数据帧时，由于它是汇聚链接，因此会被附加上 VLAN 识别信息。由于原先是来自红色 VLAN 的数据帧，因此如图中②所示，会被加上红色 VLAN 的识别信息后进入汇聚链路。路由器收到②的数据帧后，确认其 VLAN 识别信息，由于它是属于红色 VLAN 的数据帧，因此交由负责红色 VLAN 的子接口接收。

接着，根据路由器内部的路由表，判断该向哪里中继。

由于目标网络 192.168.2.0/24 是蓝色 VLAN，，且该网络通过子接口与路由器直连，因此只要从负责蓝色 VLAN 的子接口转发就可以了。这时，数据帧的目标 MAC 地址被改写成计算机 C 的目标地址；并且由于需要经过汇聚链路转发，因此被附加了属于蓝色 VLAN 的识别信息。这就是图中③的数据帧。

交换机收到③的数据帧后，根据 VLAN 标识信息从 MAC 地址列表中检索属于蓝色 VLAN 的表项。由于通信目标--计算机 C 连接在端口 3 上、且端口 3 为普通的访问链接，因此交换机会将数据帧除去 VLAN 识别信息后（数据帧④）转发给端口 3，最终计算机 C 才能成功地收到这个数据帧。

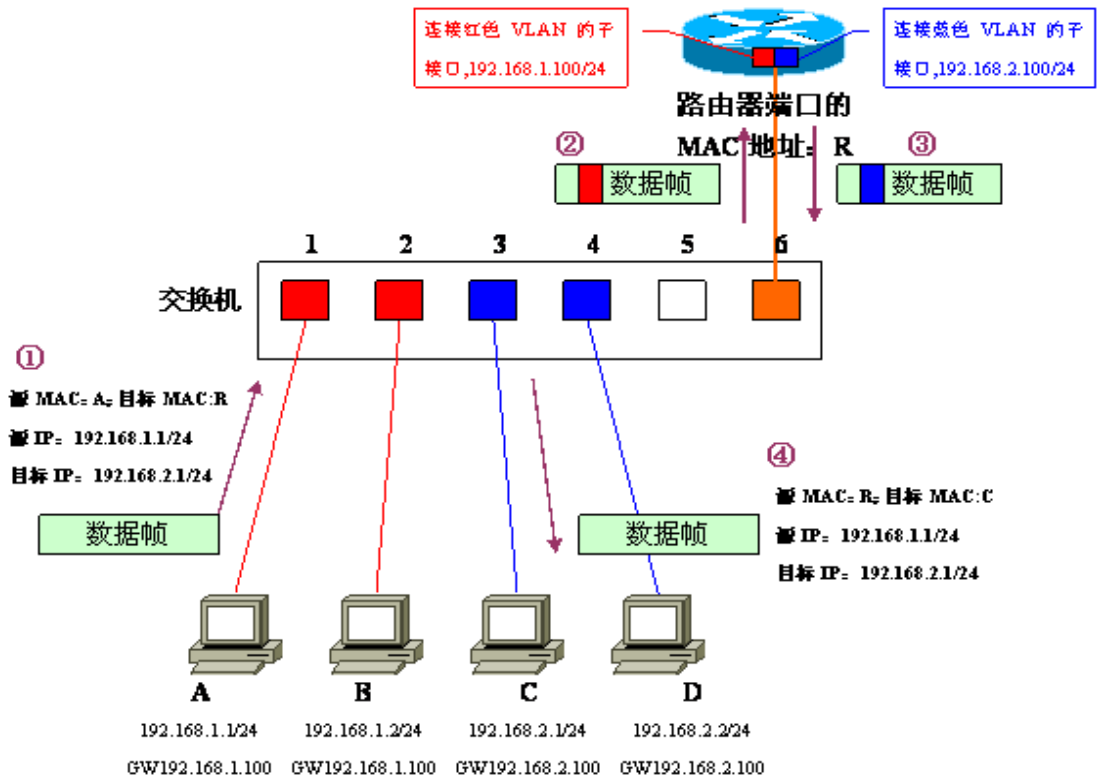


图 2-17　不同 VLAN 间通信时数据的流程

进行 VLAN 间通信时，即使通信双方都连接在同一台交换机上，也必须经过“发送方--交换机--路由器--交换机--接收方”这样一个流程。

2.7　配置 VLAN 实例

配置 VLAN 大致有以下几个步骤：

1）VLAN 配置分析规划，解决配置什么样的问题；

2）VLAN 的具体配置，实现在交换机上 VLAN 配置；

3）VLAN 配置信息的查看、修改，确保配置合理正确；

4）VLAN 配置信息的保存。

VLAN 是以 VLAN　ID 来标识的。在交换机上可以添加、删除、修改 VLAN2 到 VLAN4094。而 VLAN1 则是由交换机自动创建，并且不可删除。可以使用 interface 配置模式来配置一个端口的 VLAN 成员类型、加入、移出一个 VLAN。

2.7.1　Port VLAN 的配置

在特权模式上，通过以下步骤创建或者修改一个 VLAN。

1）configure terminal

2) vlan *vlan-id* 输入一个 VLAN ID 号

3) name *vlan-name*(可选) 为 VLAN 取一个名字。如果没有进行这一步，则交换机会自动取一个名字 VLANxxxx，其中 xxxx 是 0 开头的四位 VLAN ID 号。例如 VLAN0004 是 VLAN 4 的默认名字。如果想把 VLAN 的名字改回默认，输入 no name 命令即可。

4）end

5) show vlan{vlan id} 检查 VLAN 配置是否正确

6) copy running-config startup-config 保存配置文件

例：创建 VLAN 100，并将它命名为 test

switch# conf t

switch# vlan 100

switch# name test

switch# end

在特权模式下，可以删除一个 VLAN，但是不能删除默认 VLAN（即 VLAN 1）

switch# conf t

switch# no vlan 100 删除 vlan 100

switch# end

switch# show vlan 检查 VLAN 是否删除

在特权模式下，利用如下步骤可以将一个端口给一个 VLAN。如果把一个端口分配给一个不存在的 VLAN，则这个 VLAN 将自动被创建。

switch# configure terminal

switch# interface *interface-id* 输入想要加入 VLAN 的端口号

switch# switchport mode access 定义该接口的 VLAN 成员类型（二层 access 口）

switch# switchport access vlan *vlan-id* 将这个接口分配给一个 VLAN

switch# end

switch# show interfaces *interface-id* switchport 检查接口的完整信息

例：把 fastethernet 0/1 作为 access 口加入到 VLAN test 中。

switch# configure terminal

switch# interface fastethernet 0/1

switch# switchport mode access

switch# switchport access vlan 100

switch# end

switch# show interfaces fastethernet 0/1 switchport 检查接口的完整信息

2.7.2 Tag VLAN 配置

1. 配置 VLAN Trunks

Trunk 可以在一个链路上传输多个 VLAN 的流量。Trunk 采用 802.1Q 标准封装。可以把一个普通的以太网端口，如果要把一个接口在 access 模式和 Trunk 模式之间切换。用 switchport mode trunk 将一个接口设置成为 trunk 模式。作为 trunk,该端口要属于一个 native VLAN。所谓 native VLAN，就是指在这个接口上收发的 UNTAG 报文，都被认为是属于这个 VLAN 的。每个 trunk 口的 native VLAN 是 VLAN 1。配置 trunk 链路时，要确认连接链路两端的 trunk 口

属于相同的 native VLAN。二层接口的默认模式是 access。

在特权模式下，利用如下步骤可以将一个端口配置成一个 trunk。

switch# configure terminal

switch# interface *interface-id* 输入想要加入 VLAN 的端口号

switch# switchport mode trunk 定义该接口的类型为二层 trunk 口

switch# switchport trunk native vlan *vlan-id* 为这个接口指定一个 native VLAN

switch# end

switch# show interfaces *interface-id* switchport 检查接口的完整信息

switch# show interfaces *interface-id* trunk 显示这个接口的 trunk 设置

使用 no switchport trunk 接口配置命令，将一个 trunk 口的所有 trunk 的相关属性都恢复成默认值。

习 题

1. 叙述 VLAN 的优点。
2. VLAN 对局域网广播有什么影响？
3. VLAN 有哪几种主要的实现方式？
4. VLAN 帧标记的目的是什么？
5. 比较 Port VLAN 和 Tag VLAN 的优缺点及使用场合。

第3章 交换网络中的冗余链路管理

随着交换技术在网络中的普遍应用，保证各种网络终端包括服务器在内的设备间正常通信成为一项重要的任务，绝大多数情况下我们在交换网络中采用交换设备之间多条链路连接，形成冗余链路来保证线路上的单点故障不会影响正常网络通信。但交换机的基本工作原理导致了这样的设计会在交换网络中产生严重的广播风暴的问题。本章将介绍在交换网络中既能保证冗余链路提供链路备份，又避免广播风暴产生的技术－生成树技术。

3.1 交换机网络中的冗余链路

在许多交换机或交换机设备组成的网络环境中，通常都使用一些备份连接，以提高网络的健全性、稳定性。备份连接也叫备份链路、冗余链路等。备份链路如图 2-1 所示，交换机 SW1 与交换机 SW3 的端口 1 之间的链路就是一个备份连接。在主链路（交换机 SW1 与 SW2 的端口 2 之间的链路或者交换机 SW2 的端口 1 与交换机 SW3 的端口 2 之间的链路）出现故障时，备份链路自动启用，从而提高网络的整体可靠性。

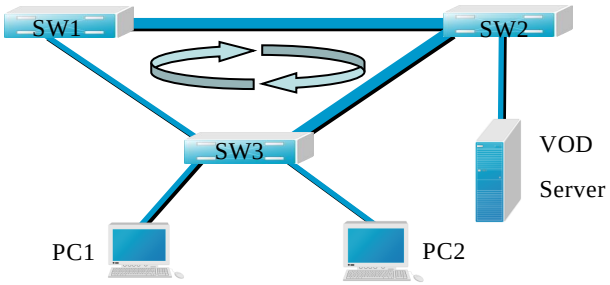


图 3-1　备份链路

使用冗余备份能够为网络带来健全性、稳定性和可靠性等好处，但是备份链路使网络存在环路。图 3-1 中 SW1-SW2-SW3 就是一个环路。环路问题是备份链路所面临的最为严重的问题，环路问题将会导致：广播风暴、多帧复制以及不稳定的 MAC 地址表等问题。

3.2　生成树协议概述

在由交换机构成的交换网络中通常设计有冗余链路和设备。这种设计的目的是防止一个点的失败导致整个网络功能的丢失。虽然冗余设计可能消除的单点失败问题，但也导致了交换回路的产生，它会带来如下问题：

A. 广播风暴

B. 同一帧的多份拷贝

C. 不稳定的 MAC 地址表

因此，在交换网络中必须有一个机制来阻止回路，而生成树协议（Spanning Tree Protocol）的作用正在于此。

生成树协议 Spanning Tree 定义在 IEEE 802.1D 中，是一种桥到桥的链路管理协议，它在防止产生自循环的基础上提供路径冗余。为使以太网更好地工作，两个工作站之间只能有一条活动路径。网络环路的发生有多种原因，最常见的一种是故意生成的冗余，万一一个链路或交换机失败，会有另一个链路或交换机替代。

所以，STP 协议的主要思想就是当网络中存在备份链路时，只允许主链路激活，如果主链路因故障而被断开后，备用链路才会被打开。

生成树协议的发展过程划分成三代:

第一代生成树协议：STP/RSTP

第二代生成树协议：PVST/PVST+

第三代生成树协议：MISTP/MSTP

STP 协议的主要作用：避免回路，冗余备份。

3.3 STP 协议工作原理

3.3.1 生成树协议介绍

生成树协议基于以下几点：（1）有一个唯一的组地址（01-80-C2-00-00-00）标识一个特定 LAN 上的所有的交换机。这个组地址能被所有的交换机识别；（2）每个交换机有一个唯一的标识（Brideg Identifier）；（3）每个交换机的端口有一个唯一的端口标识（Port Identifier）。对生成树的配置进行管理还需要：对每个交换机调协一个相对的优先级；对每个交换机的每个端口调协一个相对的优先级；对每个端口调协一个路径花费。

具有最高优先级的交换机被称为根（root）交换机。每个交换机端口都有一个根路径花费，根路径花费是该交换机到根交换机所经过的各个路段的路径花费的总和。一个交换机中根路径花费的值为最低的端口称为根端口，若有多个端口具有相同的根路径花费，则具有最高优先级的端口为根端口。

在每个 LAN 中都有一个交换机被称为指定（designated）交换机，它属于该 LAN 中根路径花费最少的交换机。把 LAN 和指定交换机连接起来的端口就是 LAN 的指定端口（designated port）。如果指定交换机中有两个以上的端口连在这个 LAN 上，则具有最高优先级的端口被选为指定端口。拓扑结构如图 3-2 所示。

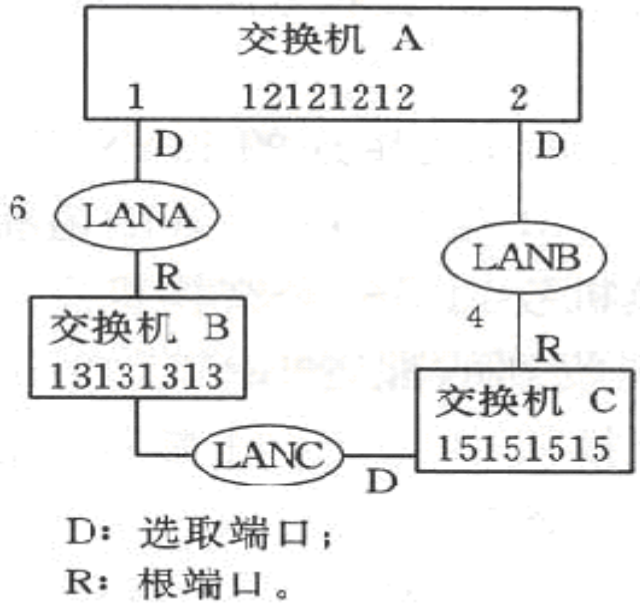


图 3-2 根交换机和根端口

由于交换机 A 具有最高优先级（桥标识最低），被选为根交换机，所以交换机 A 是 LAN A 和 LAN B 的指定交换机；假设交换机 B 的根路径花费为 6，交换机 C 的根路径花费为 4，那么交换机 C 被选为 LAN C 的指定交换机，亦即 LAN C 与交换机 A 之间的消息通过交换机 C 转发，而不是通过交换机 B。LAN C 与交换机 B 之间的链路是一条冗余链路。

3.3.2 BPDU 编码

交换机之间定期发送 BPDU 包，交换生成树配置信息，以便能够对网络的拓扑、花费或优先级的变化做出及时的响应。BPDU 分为两种类型，包含配置信息的 BPDU 包称为配置 BPDU

（Configuration BPDU），当检测到网络拓扑结构变化时则要发送拓扑变化通知 BPDU（Topology cHANGE nOTIFICATION BPDU）。配置 BPDU 编码如图 3-3 所示。

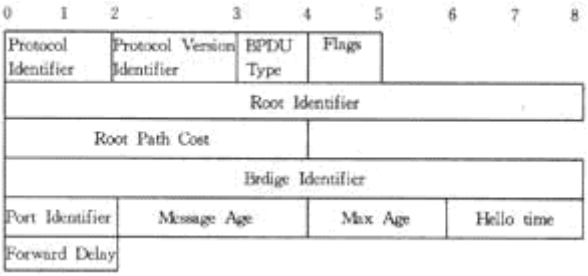


图 3-3　配置 BPDU 编码

拓扑变化通知 BPDU 编码如图 3-4 所示。

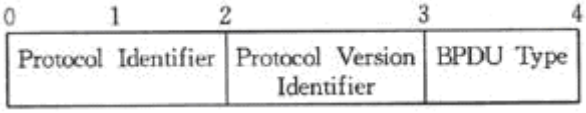


图 3-4　发送拓扑变化通知 BPDU

对于配置 BPDU，超过 35 个字节以外的字节将被忽略掉；对于拓扑变化通知 BPDU，超过 4 个字节以外的字节将被忽略掉。

BPDU 的组成说明:

1.版本号:00(IEEE 802.1D) ;02(IEEE 802.1W)

2.Bridge ID(交换机 ID=交换机优先级+交换机 MAC 地址)

3.Root ID(根交换机 ID)

4.Root Path Cost(到达根的路径开销)

5.Port ID(发送 BPDU 的端口 ID=端口优先级+端口编号)

6.Hello Time(定期发送 BPDU 的时间间隔)

7.Max-Age Time(保留对方 BPDU 消息的最长时间)

8.Forward-Delay Time(发送延迟:端口状态改变的时间间隔)

9.其他一些诸如表示发现网络拓扑变化、本端口状态的标志位。

3.4　形成一个生成树所必需决定的要素

3.4.1　决定根交换机

1、交换机的 BridgeID 由两部分构成：优先级+MAC 地址

2、最开始所有的交换机都认为自己是根交换机；

3、交换机向与之相连的 LAN 广播发送配置 BPDU，其 root_id 与 bridge_id 的值相同；

4、当交换机收到另一个交换机发来的配置 BPDU 后，若发现收到的配置 BPDU 中 root_id 字段的值大于该交换机中 root_id 参数的值，则丢弃该帧，否则更新该交换机的 root_id、根路径花费 root_path_cost 等参数的值，该交换机将以新值继续广播发送配置 BPDU。

3.4.2 决定根端口

一个交换机中根路径花费的值为最低的端口称为根端口。

若有多个端口具有相同的最低根路径花费，则具有最高优先级的端口为根端口。若有两个或多个端口具有相同的最低根路径花费和最高优先级，则端口号最小的端口为默认的根端口。

生成树的选举过程中，应遵循以下优先顺序来选择最佳路径：

1. 比较 Root Path Cost；
2. 比较 Sender’s Bridge ID；
3. 比较 Sender’s Port ID；
4. 比较本交换机的 Port ID。

3.4.3 认定 LAN 的指定交换机

1、开始时，所有的交换机都认为自己是 LAN 的指定交换机。

2、当交换机接收到具有更低根路径花费的（同一个 LAN 中）其他交换机发来的 BPDU，该交换机就不再宣称自己是指定交换机。如果在一个 LAN 中，有两个或多个交换机具有同样的根路径花费，具有最高优先级的交换机被先为指定交换机。在一个 LAN 中，只有指定交换机可以接收和转发帧，其他交换机的所有端口都被置为阻塞状态。

3、如果指定交换机在某个时刻收一了 LAN 上其他交换机因竞争指定交换机而发来的配置 BPDU，该指定交换机将发送一个回应的配置 BPDU，以重新确定指定交换机。

3.4.4 决定指定端口

LAN 的指定交换机中与该 LAN 相连的端口为指定端口。若指定交换机有两个或多个端口与该 LAN 相连，那么具有最低标识的端口为指定端口。

除了根端口和指定端口外，其他端口都将置为阻塞状态。这样，在决定了根交换机、交换机的根端口、以及每个 LAN 的指定交换机和指定端口后，一个生成树的拓扑结构也就产生。

STP 生成树形成方法：

1. 网络中选择了一个交换机为根交换机（Root Bridge）；
2. 除根交换机外的每个交换机都有一个根口（Root Port），即提供最短路径到 Root Bridge 的端口；
3. 每个交换机都计算出了到根交换机（Root Bridge）的最短路径；
4. 每个 LAN 都有了指定交换机（Designated Bridge），位于该 LAN 与根交换机之间的最短路径中。指定交换机和 LAN 相连的端口称为指定端口（Designated port）；
5. 根口（Roor port）和指定端口（Designated port）进入转发 Forwarding 状态；
6. 其他的冗余端口就处于阻塞状态（Blocking 或 Discarding）。

3.5 拓扑变化

拓扑信息在网络上的传播有一个时间限制，这个时间信息包含在每个配置 BPDU 中，即为消息时限。每个交换机存储来自 LAN 指定端口的协议信息，并监视这些信息存储的时间。在正常稳定状态下，根交换机定期发送配置消息以保证拓扑信息不超时。如果根交换机失效了，其他交换机中的协议信息就会超时，新的拓扑结构很快在网络中传播。

当某个交换机检测到拓扑变化，它将向根交换机方向的指定交换机发送拓扑变化通知 BPDU，以拓扑变化通知定时器的时间间隔定期发送拓扑变化通知 BPDU，直到收到了指定交换机发来的确认拓扑变化信息（这个确认信号在配置 BPDU 中，即拓扑变化标志位置位），同时指定交换机重复以上过程，继续向根交换机方向的交换机发送拓扑变化通知 BPDU。这样，拓扑变化的通知最终传到根交换机。根交换机收到了这样一个通知，或其自身改变了拓扑结构，它将发送一段时间的配置 BPDU，在配置 BPDU 中拓扑变化标志位被置位。所有的交换机将会收到一个或多个配置消息，并使用转发延迟参数的值来老化过滤数据库中的地址。所有的交换机将重新决定根交换机、交换机的根端口、以及每个 LAN 的指定交换机和指定端口，这样生成树的拓扑结构也就重新决定了。

3.6 STP 的端口状态

运行生成树协议的交换机上的端口，总是处于下面四个状态中的一个：

1）阻塞：所有端口以阻塞状态启动以防止回路，由生成树确定哪个端口切换为转发状态，处于阻塞状态的端口不转发数据帧但可接受 BPDU。

2）监听：不转发数据帧，但检测 BPDU（临时状态）。

3）学习：不转发数据帧，但学习 MAC 地址表（临时状态）。

4）转发：可以传送和接受数据数据帧。

在正常操作期间，端口处于转发或阻塞状态。当检测到网络拓扑结构有变化时，交换机会自动进行状态转换，在这个期间端口暂时处于监听和学习状态。

生成树经过一段时间（默认值是 50 秒左右）稳定之后，所有端口要么进入转发状态，要么进入阻塞状态。STP BPDU 仍然会定时从各个网桥的指定端口发出，以维护链路的状态。如果网络拓扑发生变化，生成树就会重新计算，端口状态也会随之改变。

当拓扑发生变化，新的配置消息要经过一定的时延才能传播到整个网络，这个时延称为 Forward Delay，协议默认值是 15 秒。在所有网桥收到这个变化的消息之前，若旧拓扑结构中处于转发的端口还没有发现自己应该在新的拓扑中停止转发，则可能存在临时环路。为了解决临时环路的问题，生成树使用了一种定时器策略，即在端口从阻塞状态到转发状态中间加上一个只学习 MAC 地址但不参与转发的中间状态，两次状态切换的时间长度都是 Forward Delay，这样就可以保证在拓扑变化的时候不会产生临时环路。但是，这个看似良好的解决方案实际上带来的却是至少两倍 Forward Delay 的收敛时间！

默认情况下，交换机端口由阻塞状态到侦听状时间为 20 秒。

3.7 STP/MSTP 生成树协议

3.7.1 RSTP 简述

为了解决 STP 协议收敛时间长这个缺陷，在世纪之初 IEEE 推出了 802.1w 标准，作为对 802.1D 标准的补充。在 IEEE 802.1w 标准里定义了快速生成树协议 RSTP（Rapid Spanning Tree Protocol）。RSTP 协议在 STP 协议基础上做了三点重要改进，使得收敛速度快得多（最快 1 秒以内）。

第一点改进：为根端口和指定端口设置了快速切换用的替换端口（Alternate Port）和备份端口（Backup Port）两种角色，当根端口/指定端口失效的情况下，替换端口/备份端口就会无时延地进入转发状态。图 3-1 中所有网桥都运行 RSTP 协议，SW1 是根桥，假设 SW2 的端口 1 是根端口，端口 2 将能够识别这种拓扑结构，成为根端口的替换端口，进入阻塞状态。当端口 1 所在链路失效的情况下，端口 2 就能够立即进入转发状态，无需等待两倍 Forward Delay 时间。

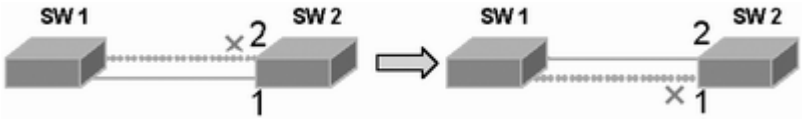


图 3-1 RSTP 冗余链路快速切换示意图

第二点改进：在只连接了两个交换端口的点对点链路中，指定端口只需与下游网桥进行一次握手就可以无时延地进入转发状态。如果是连接了三个以上网桥的共享链路，下游网桥是不会响应上游指定端口发出的握手请求的，只能等待两倍 Forward Delay 时间进入转发状态。

第三点改进：直接与终端相连而不是把其他网桥相连的端口定义为边缘端口（Edge Port）。边缘端口可以直接进入转发状态，不需要任何延时。由于网桥无法知道端口是否是直接与终端相连，所以需要人工配置。

可见，RSTP 协议相对于 STP 协议的确改进了很多。为了支持这些改进，BPDU 的格式做了一些修改，但 RSTP 协议仍然向下兼容 STP 协议，可以混合组网。虽然如此，RSTP 和 STP 一样同属于单生成树 SST（Single Spanning Tree），有它自身的诸多缺陷，主要表现在三个方面。

第一点缺陷：由于整个交换网络只有一棵生成树，在网络规模比较大的时候会导致较长的收敛时间，拓扑改变的影响面也较大。

第二点缺陷：近些年 IEEE 802.1Q 大行其道，逐渐成为交换机的标准协议。在网络结构对称的情况下，单生成树也没什么大碍。但是，在网络结构不对称的时候，单生成树就会影响网络的连通性。

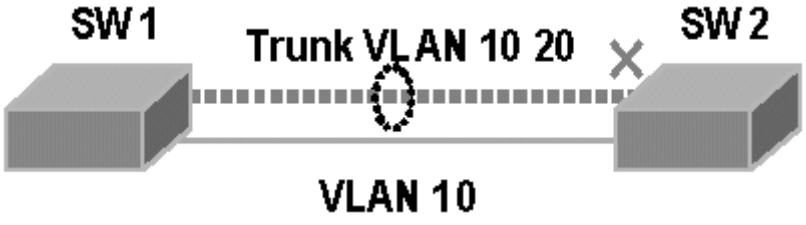


图 3-2 非对称网络示意图

图 3-2 中假设 SW1 是根桥，实线链路是 VLAN 10，虚线链路是 802.1Q 的 Trunk 链路，Trunk

了 VLAN 10 和 VLAN 20。当 SW2 的 Trunk 端口被阻塞的时候，显然 SW1 和 SW2 之间 VLAN 20 的通路就被切断了。

第三点缺陷：当链路被阻塞后将不承载任何流量，造成了带宽的极大浪费，这在环行城域网的情况下比较明显。

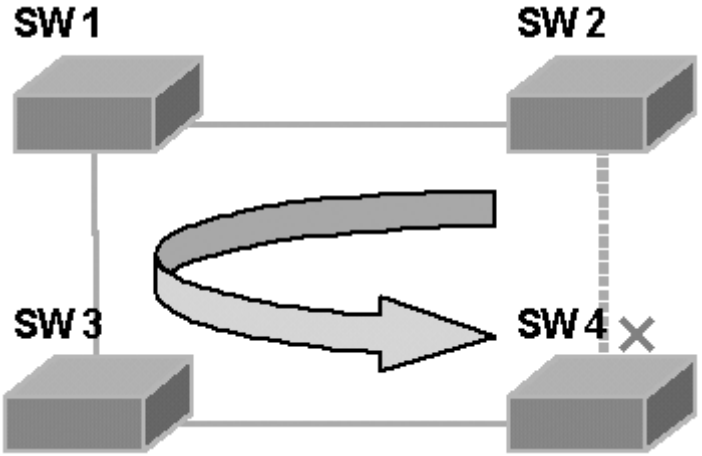


图 3-3　SST 带宽利用率低下示意图

图 3-3 中假设 SW1 是根桥，SW4 的一个端口被阻塞。在这种情况下，SW2 和 SW4 之间铺设的光纤将不承载任何流量，所有 SW2 和 SW4 之间的业务流量都将经过 SW1 和 SW3 转发，增加了其他几条链路的负担。

这些缺陷都是单生成树 SST 无法克服的，于是支持 VLAN 的多生成树协议出现了。

3.7.2 PVST/PVST+

每个 VLAN 都生成一棵树是一种比较直接，而且最简单的解决方法。它能够保证每一个 VLAN 都不存在环路。但是由于种种原因，以这种方式工作的生成树协议并没有形成标准，而是各个厂商各有一套，尤其是以 Cisco 的 VLAN 生成树 PVST（Per VLAN Spanning Tree）为代表。

为了携带更多的信息，PVST BPDU 的格式和 STP/RSTP BPDU 格式已经不一样，发送的目的地址也改成了 Cisco 保留地址 01-00-0C-CC-CC-CD，而且在 VLAN Trunk 的情况下 PVST BPDU 被打上了 802.1Q VLAN 标签。所以，PVST 协议并不兼容 STP/RSTP 协议。

Cisco 很快又推出了经过改进的 PVST＋协议，并成为了交换机产品的默认生成树协议。经过改进的 PVST＋协议在 VLAN 1 上运行的是普通 STP 协议，在其他 VLAN 上运行 PVST 协议。PVST＋协议可以与 STP/RSTP 互通，在 VLAN 1 上生成树状态按照 STP 协议计算。在其他 VLAN 上，普通交换机只会把 PVST BPDU 当作多播报文按照 VLAN 号进行转发。但这并不影响环路的消除，只是有可能 VLAN 1 和其他 VLAN 的根桥状态可能不一致。

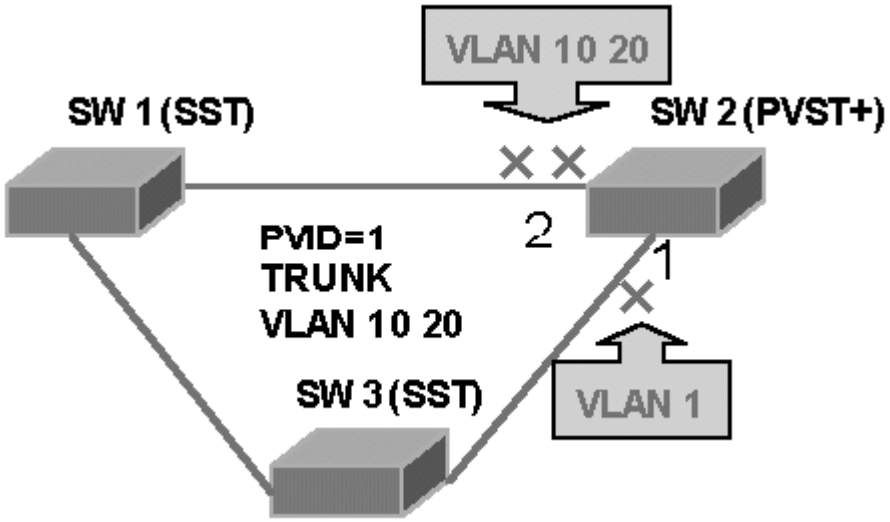


图 3-4　PVST+与 SST 对接示意图

图 3-4 中所有链路默认 VLAN 是 VLAN 1，并且都 Trunk 了 VLAN 10 和 VLAN 20。SW1 和 SW3 运行单生成树 SST 协议，而 SW2 运行 PVST＋协议。在 VLAN 1 上，可能 SW1 是根桥，SW2 的端口 1 被阻塞。在 VLAN 10 和 VLAN 20 上，SW2 只能看到自己的 PVST BPDU，所以在这两个 VLAN 上它认为自己是根桥。VLAN 10 和 VLAN 20 的 PVST BPDU 会被 SW1 和 SW3 转发，所以 SW2 检测到这种环路后，会在端口 2 上阻塞 VLAN 10 和 VLAN 20。这就是 PVST＋协议提供的 STP/RSTP 兼容性。可以看出，网络中的二层环路能够被识别并消除，强制根桥的一致性是没有任何意义的。

由于每个 VLAN 都有一棵独立的生成树，单生成树的种种缺陷都被克服了。同时，PVST 带来了新的好处，那就是二层负载均衡。

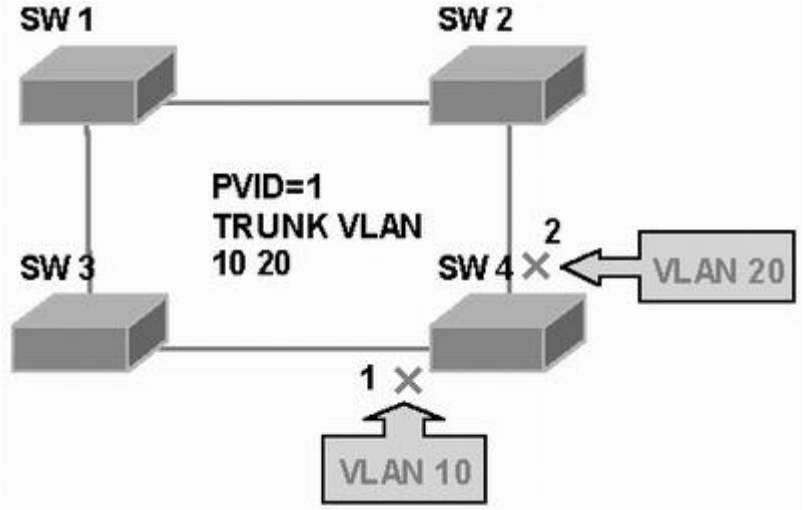


图 3-5　PVST＋负载均衡示意图

图 3-5 中四台设备都运行 PVST＋协议，并且都 Trunk 了 VLAN 10 和 VLAN 20。假设 SW1 是所有 VLAN 的根桥，通过配置可以使得 SW4 端口 1 上的 VLAN 10 和端口 2 上的 VLAN 20 阻塞，SW4 的端口 1 所在链路仍然可以承载 VLAN 20 的流量，端口 2 所在链路也可以承载 VLAN 10 的流量，同时具备链路备份的功能。这在以往的单生成树情况下是无法实现的。

聪明伶俐的 PVST/PVST＋协议实现了 VLAN 认知能力和负载均衡能力，但是新技术也带

来了新问题，PVST/PVST＋协议也有它们的“难言之隐”。

第一点缺陷：由于每个 VLAN 都需要生成一棵树，PVST BPDU 的通信量将正比于 Trunk 的 VLAN 个数。

第二点缺陷：在 VLAN 个数比较多的时候，维护多棵生成树的计算量和资源占用量将急剧增长。特别是当 Trunk 了很多 VLAN 的接口状态变化的时候，所有生成树的状态都要重新计算，CPU 将不堪重负。所以，Cisco 交换机限制了 VLAN 的使用个数，同时不建议在一个端口上 Trunk 很多 VLAN。

第三点缺陷：由于协议的私有性，PVST/PVST＋不能像 STP/RSTP 一样得到广泛的支持，不同厂家的设备并不能在这种模式下直接互通，只能通过一些变通的方式实现，例如 Foundry 的 IronSpan。IronSpan 默认情况下运行的是 STP 协议，当某个端口收到 PVST BPDU 时，该端口的生成树模式会自动切换成 PVST/PVST＋兼容模式。

一般情况下，网络的拓扑结构不会频繁变化，所以 PVST/PVST＋的这些缺点并不会很致命。但是，端口 Trunk 大量 VLAN 这种需求还是存在的。于是，Cisco 对 PVST/PVST＋又做了新的改进，推出了多实例化的 MISTP 协议。

3.7.3 MISTP/MSTP

多实例生成树协议 MISTP（Multi-Instance Spanning Tree Protocol）定义了“实例”（Instance）的概念。简单的说，STP/RSTP 是基于端口的，PVST/PVST＋是基于 VLAN 的，而 MISTP 就是基于实例的。所谓实例就是多个 VLAN 的一个集合，通过多个 VLAN 捆绑到一个实例中去的方法可以节省通信开销和资源占用率。

在使用的时候可以把多个相同拓扑结构的 VLAN 映射到一个实例里，这些 VLAN 在端口上转发状态将取决于对应实例在 MISTP 里的状态。值得注意的是网络里的所有交换机的 VLAN 和实例映射关系必须都一致，否则会影响网络连通性。为了检测这种错误，MISTP BPDU 里除了携带实例号以外，还要携带实例对应的 VLAN 关系等信息。MISTP 协议不处理 STP/RSTP/PVST BPDU，所以不能兼容 STP/RSTP 协议，甚至不能向下兼容 PVST/PVST＋协议，在一起组网的时候会出现环路。为了让网络能够平滑地从 PVST＋模式迁移到 MISTP 模式，Cisco 在交换机产品里又做了一个可以处理 PVST BPDU 的混合模式 MISTP-PVST＋。网络升级的时候需要先把设备都设置成 MISTP-PVST＋模式，然后再全部设置成 MISTP 模式。

MISTP 带来的好处是显而易见的。它既有 PVST 的 VLAN 认知能力和负载均衡能力，又拥有可以和 SST 媲美的低 CPU 占用率。不过，极差的向下兼容性和协议的私有性阻挡了 MISTP 的大范围应用。

MSTP 协议精妙的地方在于把支持 MSTP 的交换机和不支持 MSTP 交换机划分成不同的区域，分别称作 MST 域和 SST 域。在 MST 域内部运行多实例化的生成树，在 MST 域的边缘运行 RSTP 兼容的内部生成树 IST（Internal Spanning Tree）。

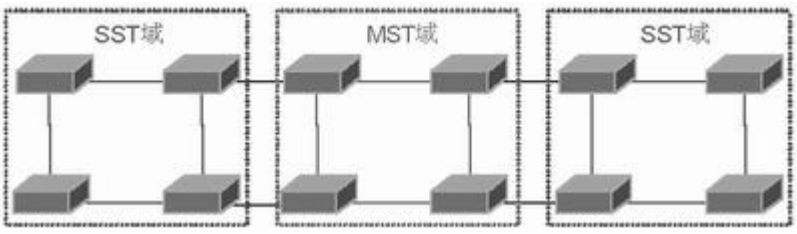


图 3-6　MSTP 工作原理示意图

图 3-6 中间的 MST 域内的交换机间使用 MSTP BPDU 交换拓扑信息， SST 域内的交换机使用 STP/RSTP/PVST＋ BPDU 交换拓扑信息。在 MST 域与 SST 域之间的边缘上，SST 设备会认为对接的设备也是一台 RSTP 设备。而 MST 设备在边缘端口上的状态将取决于内部生成树的状态，也就是说端口上所有 VLAN 的生成树状态将保持一致。

MSTP 设备内部需要维护的生成树包括若干个内部生成树 IST，个数和连接了多少个 SST 域有关。另外，还有若干个多生成树实例 MSTI（MultIPle Spanning Tree Instance）确定的 MSTP 生成树，个数由配置了多少个实例决定。

MSTP 相对于之前的种种生成树协议而言，优势非常明显。MSTP 具有 VLAN 认知能力，可以实现负载均衡，可以实现类似 RSTP 的端口状态快速切换，可以捆绑多个 VLAN 到一个实例中以降低资源占用率。最难能可贵的是 MSTP 可以很好地向下兼容 STP/RSTP 协议。而且，MSTP 是 IEEE 标准协议，推广的阻力相对小得多。

可见，各项全能的 MSTP 协议能够成为当今生成树发展的一致方向是当之无愧的。

3.7.4 配置 STP、RSTP

1、 Spanning Tree 的缺省配置：

关闭 STP，且 STP Priority 是 32768，STP port Priority 是 128。

STP port cost 根据端口速率自动判断；

Hello Time： 2 秒；

Forward-delay Time： 15 秒；

Max-age Time： 20 秒。

2、 打开、关闭 Spanning Tree 协议

可通过 spanning-tree reset 命令让 spanning tree 参数恢复到缺省配置。

Switch(config)#Spanning-tree

如果您要关闭 Spanning Tree 协议，可用 no spanning-tree 全局配置命令进行设置。

3、 配置 Spanning Tree 的类型

Switch(config)#

Spanning-tree mode STP/RSTP

4、 配置交换机优先级

Switch(config)#spanning-tree priority <0-61440> （“0”或“4096”的倍数、共 16 个、缺省 32768)

如果要恢复到缺省值，可用 no spanning-tree priority 全局配置命令进行设置。

5、 配置交换机端口优先级

Switch(config-if)#spanning-tree port-priority <0-240>

(“0”或“16”的倍数、共 16 个、缺省 128)

如果要恢复到缺省值，可用 no spanning-tree port-priority 接口配置命令进行设置。

6、 STP、RSTP 信息显示

SwitchA#show spanning-tree

！显示交换机生成树的状态

```
SwitchA#show spanning-tree  interface  fastthernet 0/1
        ！显示交换机接口
```

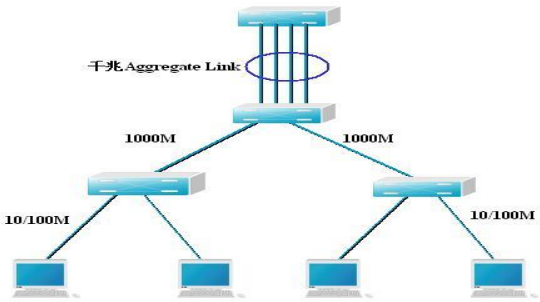
3.8 以太网链路聚合

3.8.1 网络压力

对于局域网交换机之间以及从交换机到高需求服务的许多网络连接来说，100M 甚至 1Gbps 的带宽是不够的。链路聚合技术（也称端口聚合）帮助用户减少了这种压力。

802.3ad 标准定义了如何将两个以上的以太网链路组合起来为高带宽网络连接实现负载共享、负载平衡以及提供更好的弹性。端口聚合将交换机上的多个端口在物理上连接起来，在逻辑上捆绑在一起，形成一个拥有较大宽带的端口，形成一条干路，可以实现均衡负载，并提供冗余链路。

Aggregate Port（以下简称 AP）符合 IEEE802.3ad 标准，它可以把多个端口的带宽叠加起来使用，比如全双工快速以太网端口形成的 AP 最大可以达到 800Mbps，或者千兆以太网接口形成的 AP 最大可以达到 8Gbps。



1. 802.3ad 的主要优点

1）链路聚合技术（也称端口聚合）帮助用户减少了这种压力。

2）802.3ad 的另一个主要优点是可靠性。

3）链路聚合标准在点到点链路上提供了固有的、自动的冗余性。

3.8.2 流量平衡

AP 根据报文的 MAC 地址或 IP 地址进行流量平衡，即把流量平均地分配到 AP 的成员链路中去。流量平衡可以根据源 MAC 地址、目的 MAC 地址或源 IP 地址/目的 IP 地址对。

3.8.3 配置 aggregate port

1. 配置二层 aggregate port

可以通过全局配置模式下的 interface aggregateport 命令手工创建一个 AP。

无论二、三层物理接口，当把接口加入一个不存在的 AP 时，AP 会被自动创建。

无论二、三层物理接口，都可以使用接口配置模式下的 port-group 命令将一个 AP 接口加入。

用户可以使用接口配置模式下的 port-group 命令，将一个以太网接口配置成一个 AP 的成员口。从特权模式出发，按以下步骤将以太网接口配置成一个 AP 接口的成员口。

Switch#configure terminal

Switch(config) # interface *interface-id* 选择端口，进入接口配置模式

Switch(config-if)#port-group *port-group-number* 将该接口加入一个 AP(如果这个 AP 不存在，则同时创建这个 AP)。

Switch(config-if-range)#end 回到特权模式

在接口配置模式下 no port-group 命令删除一个 AP 成员接口。

下面的例子是将二层的以太网接口 0/1 和 0/2 配置成二层 AP 5 成员。

```
Switch#configure terminal
Switch(config) # interface range fastethernet 0/1-2
Switch(config-if-range)#port-group 5
Switch(config-if-range)#end
```

可以在全局配置模式下使用命令 interface aggregatepor n（n 为 AP 号）来直接创建一个 AP（如果 AP n 不存在）。

2. 配置三层 aggregate

默认情况下，一个 aggregate port 是一个二层的 AP，如果要配置一个三层 AP，则需要进行下面的操作。

从特权模式出发，按以下步骤将一个 AP 接口配置成三层 AP 接口。

Switch#configure terminal

Switch(config) #interface aggregate-port *aggregate-port-number* 创建一个 AP

Switch(config-if)#no switchport 将该接口设置为三层模式；

Switch(config-if)#ip address ip-address mask 给 AP 接口配置 IP 地址和子网掩码；

Switch(config-if)#end 回到特权模式。

下面的例子是如何配置一个三层 AP 接口（AP3），并且给它配置 IP 地址（192.168.1.1）。

```
Switch#configure terminal
Switch(config) #interface aggregate-port 3
Switch(config-if)#no switchport
Switch(config-if)#ip address 192.168.1.1 255.255.255.0
Switch(config-if)#end
```

3. 配置 AP 的流量平衡算法

Switch(config) # aggregateport load-balance {*dst-mac* /*src-mac* /*ip*}

dst-mac 根据报文的目的 MAC 地址进行流量分配。

src-mac 根据报文的源 MAC 地址进行流量分配。

ip 根据源 IP 与目的 IP 进行流量分配。在三层条件下，建议采用此流量平衡的方式。

要将 AP 的流量平衡设置恢复到缺省值，可以在全局配置模式下使用：

no aggregateport loag-balance 命令。

4. 显示 aggregate port

可以在特权模式下显示 AP 设置。

show aggregateport [port-number]{load-balance| summary}

5. 配置 aggregate port 的注意事项

1）组端口的速度必须一致；

2）组端口必须属于同一个 VLAN；

3）组端口使用的传输介质相同；

4）组端口必须属于同一层次，并与 AP 也要在同一层次。

第4章　　访问控制列表

4.1 概述

本章介绍如何通过访问控制列表(ACL)在交换机上配置网络安全属性。可以选择对于符合过滤标准的流是丢弃还是转发，因此必须知道你的网络是如何设计的，以及交换机接口是如何在过滤设备上使用的。要通过 ACL 配置网络安全属性，只有通过 CLI 命令(可以通过串口、Telnet 或 Web)来完成配置，无法通过 SNMP 来完成这些设置。

4.1.1　ACL、安全 ACL、Qos ACL 及 ACE

ACL 的全称为访问控制列表(Access Control Lists)，按照其使用的范围，可以分为安全 ACL 和 QoS ACL。

对数据流进行过滤可以限制网络中的通讯数据类型及限制网络的使用者或使用设备。安全 ACL 在数据流通过交换机时对其进行分类过滤，并对从指定接口输入的数据流进行检查，根据匹配条件(conditions)决定是允许其通过(permit)还是丢弃(deny)。

在安全 ACL 允许数据流通过之后，你还可以通过 QoS 策略对符合 QoS ACL 匹配条件的数据流进行优先级策略处理

总的来说，安全 ACL 用于控制哪些数据流允许从交换机通过，QoS 策略在这些允许通过的数据流中再根据 QoS ACL 进行优先级分类和处理。

ACL 由一系列的表项组成，我们称之为访问控制列表表项(Access Control Entry：ACE)。每个访问控制列表表项都声明了选中该表项的匹配条件及行为。

下面我们举例说明交换机、交换机接口、ACL 和 ACE 的关系，由于该例子比较典型，因此

将在本章中全文引用：

有一个国家是 A 国，与 B 国、C 国、D 国和 E 国相邻。如图 4-1：

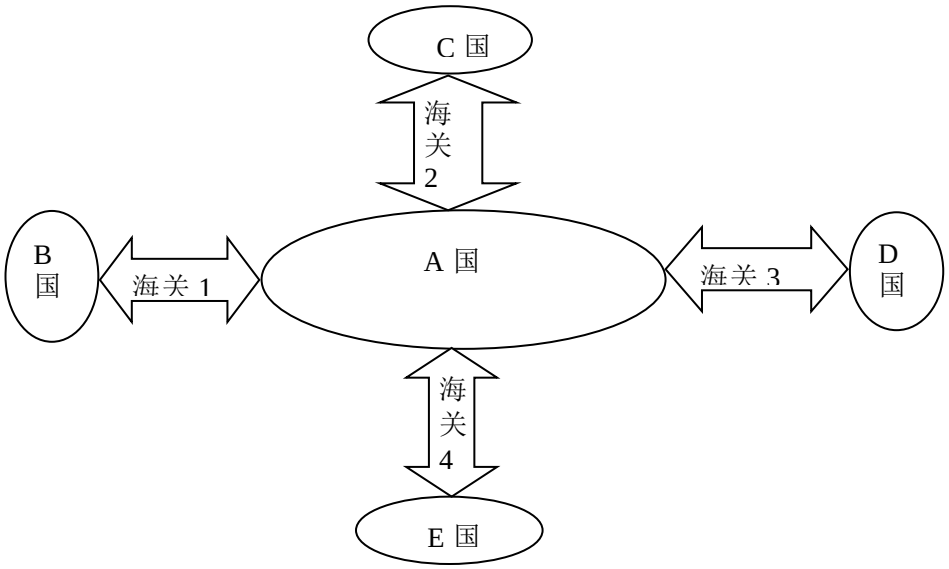


图 4-1　A 国与 B、C、D、E 国相邻

假设 A 国的邻国人员要出国，必须经由 A 国海关过境。即 B、C、D、E 任一国家要到另一个国家，必须经由与 A 国与本国的直通海关入境后，经 A 国其它海关出境到达目的地。A 国对经由本国海关过境人员有严格的身份检查限制，其入境时的过境检查规则如图 4-2 所示：

携带危险物品者->拒绝过境
B 国持旅游护照到 D 国人员->允许过境
C 国持留学护照到 E 国留学人员->允许过境
其它所有人员->拒绝过境

图 4-2　A 国的海关过境规则

A 国的每个海关均有四个出关通道，每个出关通道每天均有出关人数限制。因此 A 国在入境时还根据不同人员的身份进行分类，以便出关时给予不同的待遇。如图 4-3 所示：

B 国持旅游护照的老年人
B 国持旅游护照妇女
C 国路经本国到 D 国留学人员
其它人员

图 4-3　A 国的入境身份识别规则

在上面所举的例子中：A 国就相当于交换机，其四个海关相当于交换机的四个接口，该国的<海关入境规则>就是安全 ACL，其<入境身份识别规则>就是 QoS ACL。

<海关入境规则>的每一条细则就是 ACE，而每一条细则的身份识别条件就是 ACE 的匹配条件，拒绝过境和允许过境两种待遇就相当于 ACE 的行为：permit、deny。在图 4-1 中：<海关入境规则>的第一条细则为：携带危险物品者->拒绝过境。这里“携带危险物品者”就相当于 ACE 的匹配条件，而“拒绝过境”就是行为(deny)，相应的，第二条细则的“B 国持旅游护照到 D 国人员”是匹配条件，“允许入境”为行为(permit)。

同理，图 4-2 的<入境身份识别规则>也是 ACL，其每一条细则也是 ACE，由于是对已入境人员的限制，因此其每一条细则隐含的待遇均是：允许过境，相应的 QoS ACL 也要求其 ACE 的行为为 permit。在 S68 系列交换机中，你不能在 QoS ACL 中定义一个行为为 deny 的 ACE。

在上面的所举的例子中，A 国还可以根据邻国的友好程度制定不同的海关过境规则分别适用于不同的海关。如，A 国与 E 国为兄弟国家，特为其制定<针对兄弟国家 E 的海关过境规则>，这样<海关过境规则>只适用于海关 1－3，而<针对兄弟国家 E 的海关过境规则>只适用于海关 4。同理，对于也可以针对不同的接口，定义不同的 ACL。

4.1.2 理解输入 ACL、输出 ACL

在上面所举的例子中，A 国的<海关过境规则>只在入关时检查入关人员的身份，而 A 国如果想加强其海关安全，则 A 国还可以在所有人员出关时检查出关人员的身份。或者 A 国在入关时不检查入关人员的身份，但在出关时检查出关人员的身份。

输入 ACL，类似于在入关时检查的<海关过境规则>，它在交换机接口接收到报文时，检查报文是否与该接口输入 ACL 的的某一条 ACE 相匹配，而输出 ACL 类似于在出关时检查的<海关过境规则>，它在交换机准备从某一个接口输出报文时，检查报文是否与该接口输出 ACL 的某一条 ACE 相匹配。

4.1.3 理解过滤域模板(masks)和规则(rules)

为了理解过滤域模板，我们还是以上面所举的例子来说明如下：

A 国的<海关过境规则>在制定时是按照如下入关人员的信息来标识入关人员身份的：

1. 国籍
2. 所在省份
3. 目的国家
4. 目的国城市
5. 职业
6. 年龄
7. 所持护照
8. 携带物品

在制定不同的过境细则时，以上 8 条准则可能同时被应用，也可能只应用其中几条。如，细则第一条：携带危险物品者 → 拒绝过境。这里的携带危险物品者，就是只根据入境人员所携带物品来识别的，不分国家、不分其所往目的国及年龄、所持护照等，只要是携带危险物品者就符合该细则的条件。相应的，ACL 的 ACE 也是根据以太网报文的某些字段来标识以太网报文的，这些字段包括：

- 二层字段(Layer 2 fields)：
  - ■48 位的源 MAC 地址(必须声明所有 48 位)

■48 位的目的 MAC 地址(必须声明所有 48 位)

- 三层字段(Layer 3 fields)：

■源 IP 地址字段(可以声明全部 32 位源 IP 地址值，或声明你所定义的子网来定义一类流)

■目的 IP 地址字段(可以声明全部 32 位源 IP 地址值,或声明你所定义的子网来定义一类流)

- 四层字段(Layer 4 fields)：

■可以声明一个 TCP 的源端口、目的端口或者都声明

■ 可以声明一个 UDP 的源端口、目的端口或者都声明

过滤域指的就是你在生成一条 ACE 时，所根据的报文中的哪些字段用以对报文进行识别、分类。过滤域模板就是这些字段的组合。比如，你在生成某一条 ACE 时希望根据报文的目的 IP 字段对报文进行识别、分类，而在生成另一条 ACE 时，希望根据报文的源 IP 地址字段和 UDP 的源端口字段。这样，这两条 ACE 就使用了不同的过滤域模板。就像 A 国的<海关过境规则>的细则，第一条细则只根据入关或出关人员的职业，而第二、第三条细则根据入关或出关人员的国籍、目的国家及所持护照进行身份识别。

规则(rules)，指的是 ACE 过滤域模板对应的值。 比如有一条 ACE 内容如下：

permit tcp host 192.168.12.2 any eq telnet

在这条 ACE 中，过滤域模板为以下字段的集合：

源 IP 地址字段、IP 协议字段、目的 TCP 端口字段

对应的值(rules)分别为：

源 IP 地址＝host 192.168.12.2

IP 协议＝tcp

TCP 源端口＝telnet。

图 4-4 给出了关于对 ACE 的分析：

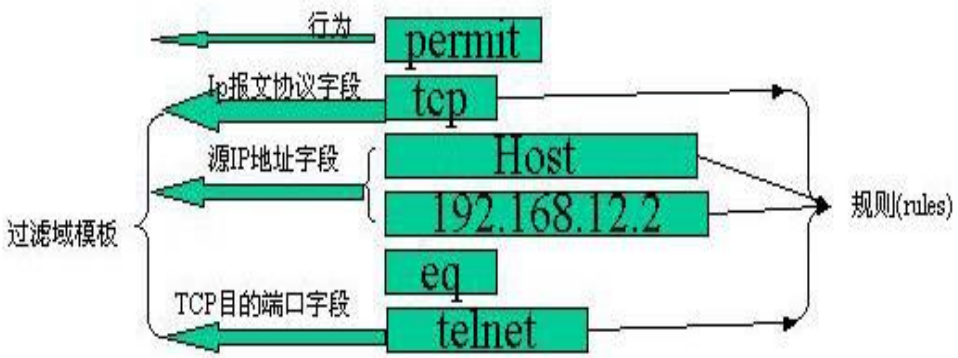


图 4-4：对 ACE：permit tcp host 192.168.12.2 any eq telnet 的分析

4.1.4 在交换机上配置 ACL 的注意事项

1. 在生成 ACL 之后，只有将其应用到某一个接口上，该 ACL 才能生效。就像 A 国的<海关过境

规则>，如果只是制定了该规则，但没有任何海关执行，则该过境规则只是废纸一张。

2. 将 ACL 应用于如下接口：
   a) 二层接口 Switch Ports
   b) 二层接口 Aggregate Port
   c) 三层接口 Routed Port
   d) 三层接口 L3 Aggregate Port
   e) 交换机虚拟接口 SVI(Switch virtual interface)
3. 交换机目前除 SVI 接口允许同时关联一个输出 ACL 外，其他接口只允许关联一个输入 ACL。SVI 接口关联输出 ACL 的目的是控制其他 SVI 接口下的子网访问所关联输出 ACL 的 SVI 下的子网资源的行为，对于该 SVI 下的子网间的访问将不受限制，这种限制只针对 IP 报文，对于其他类型报文将无效。注意：如果你对 SVI 接口关联的子网进行修改或者对 SVI 对应 VLAN 的成员端口发生变化，那么需要删除原有关联的输出或者输入 ACL，然后再重新应用。

4.2 配置安全 ACL

本节简单介绍如何通过 CLI 命令来配置 ACL。

4.2.1 支持的 ACL 类型

本交换机支持以下几种类型的 ACL：

- IP ACL 用于过滤 IP 报文，包括 TCP 和 UDP。
  1. Standard IP access lists (标准 IP 访问控制列表)使用源 IP 地址作为匹配的条件
  2. Extended IP access lists(扩展 IP 访问控制列表)使用源 IP 地址、目的 IP 地址及可选的协议类型信息作为匹配的条件
- Ethernet ACL 用于过滤二层数据流：
  1. MAC Extended access lists(MAC 扩展控制列表)使用源 MAC 地址、目的 MAC 地址及可选的以太网类型作为匹配的条件
- Expert ACL 用于过滤二层和三层、二层和四层、二层和三层、四层数据流：
  1. Expert Extended access lists(专家扩展控制列表)使用源 MAC 地址、目的 MAC 地址、以太网类型、源 IP、目的 IP、及可选的协议类型信息作为匹配的条件。

4.2.2 配置 ACL 的步骤

可以通过如下步骤配置 ACL：

1. 通过声明一个 ACL 的名字及为该 ACL 创建 ACEs(每条 ACE 均由匹配条件和行为构成)来创建一个 ACL。
2. 将该 ACL 应用于某一个交换机接口。

4.3 创建 Standard (标准)及 Extended(扩展)IP ACL

4.3.1 关于 IP 地址的表示

在创建 IP ACL 之前，你有必要了解如何用变量 source、Source-wildcard 及 Destination、Destination-wildcard 来表示 IP 地址。

在 IP ACL 中，在你创建 ACE 时，Source 用于定义报文的源网络或主机。Source-wildcard 是应用于 source 的通配符。Destination 用于定义报文的目的网络或主机。Destination-wildcard 是应用于 destionation 的通配符。

地址通配符的格式与 IP 地址一样，也是 32 位点分十进制格式。地址通配符某一位为 1，则相应的源 IP 地址(对应 source-wildcard)或目的 IP 地址(对应 destination-wildcard)对应位为任意值(即无意义)，地址通配任某一位为 0，则相应的 IP 地址对应位值为你设置的值。可简单地认为地址通配符等于子网掩码按位取反。以下公式可以作为验证地址用：

1) 报文的源 IP 地址*(source-wildcard 按位取反)=ACE 表项的 source*(source-wildcard 按位取反)；
2) 报文的目的 IP 地址*(destination-wildcard 按位取反)=ACE 表项的 destination*(destination-wildcard 按位取反)。

按照该公式，如果你想对源 IP 地址为 192.168.12.2 的主机进行过滤，则你应该设置相应 ACE 的 source=192.168.12.2，source-wildcard=0.0.0.0。如果你想对 192.168.12.0 网段的所有主机进行过滤，则你可以设置 source=192.168.12.x(x 表示 0-255 任意值)，source-wildcard=0.0.0.255。

source，source-wildcard，destination，destination-wildcard 可以以如下三种方式表示：

1) 32 位点分十进制格式
2) 关键字 **any** 是 source 及 source-wildcard 为 0.0.0.0 255.255.255.255(或 destination 及 destinaton-wildcard)的缩写，或者指明为任意源(目的)主机。
3) **host** source 代表源主机 source 及 source-wilcard 为 0.0.0.0，**host** destination 代表目的主机 destiation 及 destination-wildcard 为 0.0.0.0

4.3.2 创建 Standard IP ACL

在特权配置模式，你可以通过如下步骤来创建一条 Standard IP ACL：

	命令	含义
步骤 1	configure terminal	进入全局配置模式。
步骤 2	IP access-list standard { *name*}	用数字或名字来定义一条 Standard IP ACL 并进入 access-list 配置模式。
步骤 3	deny {*source source-wildcard*/***host*** *source*/***any***} or	在 access-list 配置模式，声明一个或多个的允许通过(permit)或丢弃(deny)的条件以用于交换

	permit {*source source-wildcard*/***host*** *source*/***any***}	机决定报文是转发或还是丢弃。 ● **host** source 代表一台源主机，其 source-wildcard 为 0.0.0.0。 ● **any** 代表任意主机，即 source 为 0.0.0.0，source-wild 为 255.255.255.255。
步骤 4	**end**	退回到特权模式。
步骤 5	**show access-lists** [name]	显示该接入控制列表，如果你不指定 access-list 及 name 参数，则显示所有接入控制列表。
步骤 6	**copy running-config startup-config**	保存配置。

在下面的一个例子中，将显示如何创建一条 IP Standard Access-list，该 ACL 名字叫 deny-host192.168.12.x：有两条 ACE，第一条 ACE 拒绝来自 192.168.12.0 网段的任一主机，第二条 ACE 允许其它任意主机。

```
Switch(config)# IP access-list standard deny-host192.168.12.x
Switch(config-std-nacl)# deny 192.168.12.0 0.0.0.255 any
Switch(config-std-nacl)# permit any
Switch(config-std-nacl)# end
Switch # show access-list
```

注意：正如前文所述，如果报文在与指定接口上的 ACL 的所有 ACE 进行逐条比较后，没有任意 ACE 的匹配条件匹配该报文，则该报文将被丢弃。也就是说，任意一条 ACL 的最后都隐含了一条 deny any any 的 ACE 表项。

4.3.3 创建 Extended IP ACL

在特权配置模式，你可以通过如下步骤来创建一条 Extended IP ACL：

	命令	**含义**
步骤 1	**configure terminal**	进入全局配置模式。
步骤 2	**IP access-list extended** { *name*}	用数字或名字来定义一条 Extended IP ACL 并进入 access-list 配置模式。
步骤 3	{**deny**|**permit**}*protocol*{*source source-wildcard*/**host** *source*/**any**}[*operator port*]{*destination destination-wildcard*/**host** *destination*/**any**}[*operator port*]	在 access-list 配置模式，声明一个或多个的允许通过(permit)或丢弃(deny)的条件以用于交换机决定匹配条件的报文是转发或还是丢弃。 ● 以如下方式定义 TCP 或 UDP

		的目的或源端口： 1. 操作符(opeator)只能为 eq。 2. 如果操作符在 source source-wildcard 之后，则报文的源端口匹配指定值时条件生效。 3. 如果操作符在 destination destination-wildcard 之后，则报文的目的端口匹配指定值时条件生效。 4. Port 为 10 进制值，它代表 TCP 或 UDP 的端口号。值范围为 0-65535。 1. protocol 可以为 **IP**、**tcp**、**udp**、**igmp**、**icmp** 协议。
步骤 4	End	退回到特权模式。
步骤 5	show access-lists [*name*]	显示该接入控制列表，如果你不指定 access-list number 及 name 参数，则显示所有接入控制列表
步骤 6	copy running-config startup-config	保存配置。
步骤 7	End	退回到特权模式。

下例显示如何创建一条 Extended IP ACL,该 ACL 有一条 ACE,用于允许指定网络(192.168.x..x)的所有主机以 HTTP 访问服务器 172.168.12.3，但拒绝其它所有主机使用网络。

Switch(config)# IP access-list extended allow_0xc0a800_to_172.168.12.3
Switch(config-std-nacl)# permit tcp 192.168.0.0 0.0.255.255 **host** 172.168.12.3 eq http
Switch(config-std-nacl)#end
Switch # show access-list

4.3.4 创建 MAC Extended ACL

配置 MAC Extended ACL 的过程，与配置 IP 扩展 ACL 的配置过程是类似的。在特权配置模式，你可以通过如下步骤来创建一条 MAC Extended ACL：

	命令	**含义**
步骤 1	configure terminal	进入全局配置模式。

步骤 2	**MAC access-list extended** {*name*}	以名字定义一条 MAC extended acl，并进入 access-list 配置模式
步骤 3	{**deny** | **permit**} {**any** | **host** *source MAC address*} {**any** | **host** *destination MAC address*} [**aarp** |**appletalk** |**decnet-iv** | **diagnostic** | **etype-6000**|**etype-8042** | **lat** | **lavc-sca** | **mop-console** |**mop-dump** | **mumps** | **netbios**|**vines-echo** | **xns-idp**]	在 access-list 配置模式，声明对任意源 MAC 地址或指定的源 MAC 地址、对任意目的 MAC 地址或指定的目的 MAC 地址的报文设置允许其通过或拒绝之的条件。 (可选项)你可以输入如下以太网协议类型： **aarp** | **appletalk** |**decnet-iv** |**diagnostic** | **etype-6000** | **etype-8042** | **lat** | **lavc-sca** |**mop-console** | **mop-dump** | **mumps** | **netbios**|**vines-echo** | **xns-idp**
步骤 4	**End**	退回到特权模式。
步骤 5	**show access-lists** [*name*]	显示该接入控制列表。
步骤 6	**copy running-config startup-config**	保存配置。

你可以用 **no MAC access-list extended** *name* 全局配置命令来删除整条 MAC 扩展 ACL。你也可以单独删除指定 ACL 中的某一条或某几条 ACE。

下例显示如何创建及显示一条 MACExtended ACL，以名字 MACext 来命名之。该 MAC 扩展 ACL 拒绝所有符合指定源 MAC 地址的 **aarp** 报文。

```
Switch(config)# MAC access-list extended MACext
Switch(config-ext-MACl)# deny host 00d0.f800.0000 any aarp
Switch(config-ext-MACl)# permit any any
Switch(config-ext-MACl)# end
Switch # show access-lists MACext
Extended MAC access list MACext
    deny host 00d0.f800.0000 any aarp
    permit any any
```

4.3.5 基于时间的 ACL 应用

你可以使 ACL 基于时间进行运行，比如是 ACL 在一个星期的某些时间段内生效等。为了达到这个要求，你必须首先配置一个 time-range。time-range 的实现依赖于系统时钟，如果你要使用这个功能，必须保证系统有一个可靠的时钟，比如 RTC 等。

从特权模式开始，你可以通过以下步骤来设置一个 time-range：

	命令	含义
步骤 1	**configure terminal**	进入全局配置模式。
步骤 2	**time-range** *time-range-name*	通过一个有意义的显示字符串作为名字来标识一个 time-range，同时进入 time-range 配置模块。名字的长度为 1－32 个字符，不能包含空格
步骤 3	**absolute** {**start** *time date* [**end** *time date*]| **end** *time date* }	设置绝对时间区间(可选) 对于一个 time range，你可以设置一个绝对的运行时间区间，并且只能设置一个区间。基于 time-range 的应用将仅在这个时间区间内有效。
步骤 4	**periodic** *day-of-the-week hh:mm to* [*day-of-the-week*] *hh:mm* **periodic** {**weekdays**	**weekend**	**daily**} *hh:mm to hh:mm*	设置周期时间(可选) 对于一个**time-range**，你可以设置一个或多个周期性运行的时间段。如果你已经为这个**time-range**设置了一个运行时间区间，则将在时间区间内周期性的生效 ***day-of-the-week:*** 一个星期内的一天或几天，**Monday**，**Tuesday**，**Wednesday**，**Thursday**，**Friday**，**Saturday**，**Sunday**。 **Weekdays**： 一周中的工作日，星期一到星期五 **Weekend**：周末，星期六和星期日 **Daily**：一周中的每一天，星期一到星期日
步骤 5	End	回到特权模式。
步骤 6	**show time-range**	验证你的配置。
步骤 5	**copy running-config startup-config**	保存配置(可选)。

可以在全局配置模式下使用no time-range *time-range-name*来删除指定的time-range。

下面的例子以 ACL 应用为例，说明如何在每周工作时间段内禁止 HTTP 的数据流：

```
Switch(config)# time-range no-http
Switch(config-time-range)# periodic weekdays 8:00 to 18:00
Switch(config)# end
Switch(config)# IP access-list extended limit_udp
Switch(config-ext-nacl)# deny tcp any any eq www time-range no-http
Switch(config)# end
```

```
Switch(config-ext-nacl)# exit
Switch(config)# interface fastethernet0/1
Switch(config-if)# IP access-group no-http in
```

下面为 time-range 的显示范例:

```
Switch#show time-range
time-range name: no-http
   periodic Weekdays 8:00 to 18:00

time-range name: no-udp
   periodic Tuesday 15:30 to 16:30
```

4.3.6 创建 Expert Extended ACL

配置 Expert Extended ACL 的过程，与配置 IP 扩展 ACL 的配置过程是类似的。

在特权配置模式，你可以通过如下步骤来创建一条 Expert Extended ACL：

	命令	含义
步骤 1	configure terminal	进入全局配置模式。
步骤 2	expert access-list extended {*name*}	以名字定义一条 expert extended acl，并进入 access-list 配置模式
步骤 3	{**deny**|**permit**}[*protocol*|aarp |appletalk |decnet-iv| diagnostic |etype-6000|etype-8042 | lat | lavc-sca | mop-console|mop-dump | mumps |netbios|vines-echo | xns-idp*][VID vid]*{*source source-wildcard* | **host** *source* | **any**}{ **host** *source MAC address* | **any** } [*operator port*]{*destination destination-wildcard* | **host** *destination* | **any**}{ **host** *destination MAC address* | **any** } [*operator port*] [**time-range** *time-range-name*]	在 access-list 配置模式，声明一个或多个的允许通过(permit)或丢弃(deny)的条件以用于交换机决定匹配条件的报文是转发或还是丢弃。 ● 以如下方式定义 TCP 或 UDP 的目的或源端口： 1. 操作符(opeator)只能为 **eq**。 2. 如果操作符在 source source-wildcard 之后，则报文的源端口匹配指定值时条件生效。 3. 如果操作符在 destination destination-wildcard 之后，则报文的目的端口匹配指定值时条件生效。 4. Port 为 10 进制值,它代表 TCP 或 UDP 的端口号。值范围为 0-65535。 ● protocol 可以为： **IP**、**tcp**、**udp**、**igmp**、**icmp** 等协议 ● vid 指明这个报文所属的 vlan，对于 trunk port 接收到的 tagged 报文，该值

		由报文中的 vid 字段值所决定，对于 untagged 报文，该值等于 native vlan，对于 access port，该值等于该 acces port 所属的 vlan。 ● *time-range-name*(可选) 指明关联的 time-range 的名称 ● **aarp** | **appletalk** |**decnet-iv** |**diagnostic** | **etype-6000** | **etype-8042** | **lat** | **lavc-sca** |**mop-console** | **mop-dump** | **mumps** | **netbios**|**vines-echo** | **xns-idp** (可选项) 你可以输入上述的以太网协议类型。
步骤 4	**End**	退回到特权模式。
步骤 5	**show access-lists** [*name*]	显示该 ACL 列表。
步骤 6	**copy running-config startup-config**	保存配置。

可以用 **no expert access-list extended** *name* 全局配置命令来删除整条专家 ACL，也可以单独删除指定 ACL 中的某一条或某几条 ACE。

下例显示如何创建及显示一条 Expert Extended ACL，以名字 expert 来命名之。该专家 ACL 拒绝源 IP 地址为 192.168.12.3 并且源 MAC 地址为 00d0.f800.0044 的所有 TCP 报文。

tcp 192.168.0.0 0.0.255.255 **host** 172.168.12.3

Switch(config)# expert access-list extended expert

Switch(config-ext-MACl)# deny tcp **host** 192.168.12.3 **host** 00d0.f800.0044 **any any**

Switch(config-ext-MACl)# permit any any any any

Switch(config-ext-MACl)# end

Switch # show access-lists expert

Extended expert access list expert

deny tcp **host** 192.168.12.3 **host** 00d0.f800.0044 **any any**

permit any any any any

4.3.7 应用 ACL 到指定接口上

在创建了一条 ACL 之后，你必须将其应用到所要过滤的接口上，它才能生效。本节分别介绍如何将 IP ACL、MAC Extended ACL 应用到指定接口上。

1、将 IP standard access-list 及 IP extended access-list 应用到指定接口上

在特权模式，通过如下步骤将 IP ACL 应用到指定接口上：

	命令	**含义**
步骤 1	**configure terminal**	进入全局配置模式。

步骤 2	interface *interface-id*	指定一个接口并进入接口配置模式。
步骤 3	IP access-group {*name*} {in|out}	将指定的 ACL 应用于该接口上，使其对输入该接口的数据流进行接入控制. 只有 SVI 接口才能应用 out 参数。
步骤 4	End	退回到特权模式。
步骤 5	show running-config	显示 access-list 配置
步骤 6	copy running-config startup-config	保存配置。

下例显示如何将 access-list deny_unknow_device 应用于接口 2 上：

Switch(config)# interface GigabitEthernet 1/2

Switch (config-if)# IP access-group deny_unknow_device **in**

2、将MAC Extended access-list应用到指定接口上：

在特权配置模式下，通过如下步骤将 MAC Extended access-list 应用到指定接口上：

	命令	含义
步骤 1	configure terminal	进入全局配置模式。
步骤 2	interface *interface-id*	指定一个接口并进入接口配置模式。这里的接口必须为物理接口或 Aggregated Link。
步骤 3	MAC access-group {*name*} {in|out}	将指定的 ACL 应用于该接口上，使其对输入该接口的数据流进行接入控制 只有 SVI 接口才能应用 out 参数。
步骤 4	end	退回到特权模式。
步骤 5	show running-config	显示 access-list 配置
步骤 6	copy running-config startup-config	保存配置。

下例显示如何将 access-list accept_00d0f8xxxxxx_only 应用于 Gigabit 接口 2 上：

Switch(config)# interface GigabitEthernet 1/2

Switch (config-if)# MAC access-group accept_00d0f8xxxxxx_only in

3、将 expert extended access-list 应用到指定接口上

在特权模式，通过如下步骤将专家 ACL 应用到指定接口上：

	命令	含义
步骤 1	configure terminal	进入全局配置模式。

步骤 2	**interface** *interface-id*	指定一个接口并进入接口配置模式。
步骤 3	**expert access-group** {*name*} {**in**|**out**}	将指定的 ACL 应用于该接口上，使其对输入该接口的数据流进行输入输出控制。**out** 只应用在 SVI 接口上。
步骤 4	**end**	退回到特权模式。
步骤 5	**show running-config**	显示 access-list 配置
步骤 6	**copy running-config startup-config**	保存配置。

下例显示如何将 access-list deny_unknow_user 应用于千兆接口 2 上：

Switch(config)# interface GigabitEthernet 1/2

Switch (config-if)# expert access-group deny_unknow_user **in**

下例显示如何将 access-list deny_net1 应用于 VLAN 接口 2 上，以用于禁止 net1 与 vlan2 之间的通讯：

Switch(config)# interface vlan 2

Switch (config-if)# expert access-group access-list deny_net1 out

除 SVI 接口外，你只能将一条 ACL 应用到一个接口上，因此你不可能同时将类型为 IP Standard Access-list、IP Extended Access-list、MAC Extended Access-list、Expert Extended Access-list 的 ACL 应用到某一个接口上。当你将不同类型的 ACL 应用到某一个接口上时，前一个应用的 ACL 将被后一个应用的 ACL 所替换。

关于 SVI 关联 ACL 有一下注意点：

- SVI 接口可以同时关联一条输入的 ACL 和一条输出的 ACL。
- 当 ACL 关联到 SVI 成员接口时可能与 SVI 关联的 ACL 发生冲突，系统将自动报错。
- SVI 在关联输入 ACL 时，将对 SVI 成员接口设置 QOS 产生影响，而 SVI 关联输出 ACL 将不会影响 QOS。
- SVI 关联输入方向的 ACL，其隐含的缺省 ACE 为 deny any any；输入方向的 ACL，其隐含的缺省 ACE 为 deny vid any any.该 VID 为 SVI 所对应的 VID。

4.4 显示 ACL 配置

通过以下命令来显示 ACL 配置：

命令	说明
show access-lists [*name*]	显示所有 ACL 配置或指定名字的 ACL。
show IP access-lists [*name*]	显示 IP ACL
show MAC access-lists [*name*]	显示 MAC ACL
show MAC access-group [**interface** *interface-id*]	显示指定接口上的 MAC ACL 配置
Show IP access-group [**interface**	显示指定接口上的 IP ACL 配置

interface-id]	
show running-config	显示所有配置

以下例子显示名字为 IP_acl 的 Standard IP access-lists 的内容：

```
Switch # show IP access-lists IP_acl
Standard IP access list IP_acl
      Permit host 192.168.12.1
      Permit host 192.168.11.1
```

以下例子显示名字为 IP_ext_acl 的 Extended IP access-lists 的内容：

```
Switch # show IP access-lists IP_ext_acl
Extended IP access list IP_ext_acl
      permit tcp 192.168.0.0 255.255.0.0 host 192.168.1.1 eq www
      permit tcp 192.167.0.0 255.255.0.0 host 192.168.1.1 eq www
```

以下例子显示所有 IP access-lists 的内容：

```
Switch # show IP access-lists
  Standard IP access list IP_acl
    Permit host 192.168.12.1
    Permit host 192.168.11.1
  Extended IP access list IP_ext_acl
    permit tcp 192.168.0.0 0.0.255.255 host 192.168.1.1 eq www
    permit tcp 192.167.0.0 0.0.255.255 host 192.168.1.1 eq www
```

以下例子显示所有 access lists 的内容：

```
Switch # show access-lists
Standard IP access list IP_acl
    Permit host 192.168.12.1
    Permit host 192.168.11.1
Extended IP access list IP_ext_acl
    permit tcp 192.168.0.0 0.0.255.255 host 192.168.1.1 eq www
    permit tcp 192.167.0.0 0.0.255.255 host 192.168.1.1 eq www
Extended MAC access list MACext
    deny host 00d0.f800.0000 any aarp
    permit any any
```

以下例子显示在 Gigabit 接口 1 上的 MAC extended access-list：

```
Switch #show MAC access-group interface GigabitEthernet 1/1
Interface            access-list
-------------------- --------------------------------
Gi1/1                MAC_ext
```

以下例子显示所有接口配置的MAC ACL:

```
Switch #show MAC access-group
Interface            access-list
-------------------- --------------------------------
Gi1/1                MAC_ext
Gi1/2                Not Set
Gi1/3                Not Set
Gi1/4                Not Set
Gi1/5                Not Set
Gi1/6                Not Set
Gi1/7                Not Set
Gi1/8                Not Set
Gi1/9                Not Set
Gi1/10               Not Set
Gi1/11               Not Set
Gi1/12               Not Set
```

第5章　局域网与 Internet 网互联

5.1　概述

随着 Internet 的发展，IP 地址短缺问题已经成为了一个越来越严重的问题，在 IPV6 使用之前，地址转换（Network Address Translation ）技术是解决这个问题的一个最主要的技术手段。

通过地址转换技术可以使用私有地址提供 Internet 访问技术，本章详细描述了地址转换技的技术使用范围组网方案等问题。

地址转换主要是因为 Internet 地址短缺问题而提出的，利用地址转换可以使内部网络的用户访问外部网络（Internet），利用地址转换可以给内部网络提供一种“隐私”保护，同时也可以按照用户的需要提供给外部网络一定的服务，如 WWW、FTP、TELNET、SMTP、POP3 等。

地址转换技术实现的功能是上述的两个方面，一般称为“正向的地址转换”和“反向的地址转换”，在正向的地址转换中，具有只转换地址 NAT 和同时转换地址和端口 NAPT 两种形式。

5.2　地址转换技术介绍

5.2.1　IP 地址短缺问题

所谓 IP 地址就是给每一个连接在 Internet 上的主机分配一个唯一的 32bit 地址，IP 地址是由 Internet Assigned Numbers Authority IANA 组织统一分配的，保证在 Internet 上没有重复的 IP

地址。

IP 地址由网络号码和主机号码两部分组成，为了便于对 IP 地址进行管理，同时还考虑到网络的差异很大，有的网络拥有很多的主机，而有的网络上的主机则很少，因此 Internet 的 IP 地址就分成为五类，即 A 类到 E 类，其中能被使用的是 A、B、C 三类。

A 类 IP 地址的网络号码数不多，目前几乎没有多余的可供分配，现在能够申请到的 IP 地址只有 B 类和 C 类两种。当某个单位申请到 IP 地址时，实际上只是拿到了一个网络号码 net-id。具体的各个主机号码 host-id，则由该单位自行分配，只要做到在该单位管辖的范围内无重复的主机号码即可。

由于当初没有预计到微机会普及得如此之快，各种局域网和局域网上的主机数目急剧增长，另外由于申请 IP 地址的时候是申请的“网络号码”，这样在使用时有时候也有很大的浪费。例如某个单位申请到了一个 B 类地址但该单位只有 1 万台主机，于是在一个 B 类地址中的其余 5 万 5 千多个主机号码就白白地浪费了，因为其他单位的主机无法使用这些号码。地址转换技术就是解决地址短缺问题的一个主要的技术手段。

5.2.2 公有地址和私有地址

Internet 是连接了许多的局域网的一个网络，可以连接各种不同类型的局域网。局域网的类型可以很多，我们在本文讨论的局域网都是使用 TCP/IP 协议连接的局域网，如果局域网采用 TCP/IP 协议连接，局域网的每台机器都必须拥有一个 IP 地址，为了使得局域网的 IP 地址可以被局域网自己规划，IANA 组织在 A、B、C 类 IP 地址中各选出一个网段做为“私有地址” 供各个局域网按照自己的需要自由分配。

私有地址是指内部网络（局域网内部）的主机地址，而公有地址是局域网的外部地址（在因特网上的全球唯一的 IP 地址）。因特网地址分配组织规定以下的三个网络地址保留用做私有地址。

10．0．0．0　　－ 10．255．255．255
172．16．0．0　－ 172．31．255．255
192．168．0．0 － 192．168．255．255

也就是说这三个网络的地址不会在因特网上被分配，但可以在一个企业（局域网）内部使用，各个企业根据在可预见的将来主机数量的多少，来选择一个合适的网络地址，不同的企业的内部网络地址可以相同。如果一个公司选择其他的网段作为内部网络地址，则有可能会引起路由表的混乱。

很明显，私有地址是不会在 Internet 上看见的，在 Internet 上可见的 IP 地址称为公有地址，使用私有地址转换的主机是不能直接访问 Internet 的，同样的道理在 Internet 上也不可能访问到使用私有地址的主机。

5.2.3 地址转换的适用情况

如果某个单位使用私有地址建立局域网，按照主机的用途，局域网内部的主机可以大致分为如下三类：

1) 仅仅只是用来办公使用不需要直接访问 Internet

2) 做为办公使用但是在有些时候需要访问 Internet

3）做为资源存放用途并且可以被 Internet 上的用户访问，例如一个 WEB 服务器。

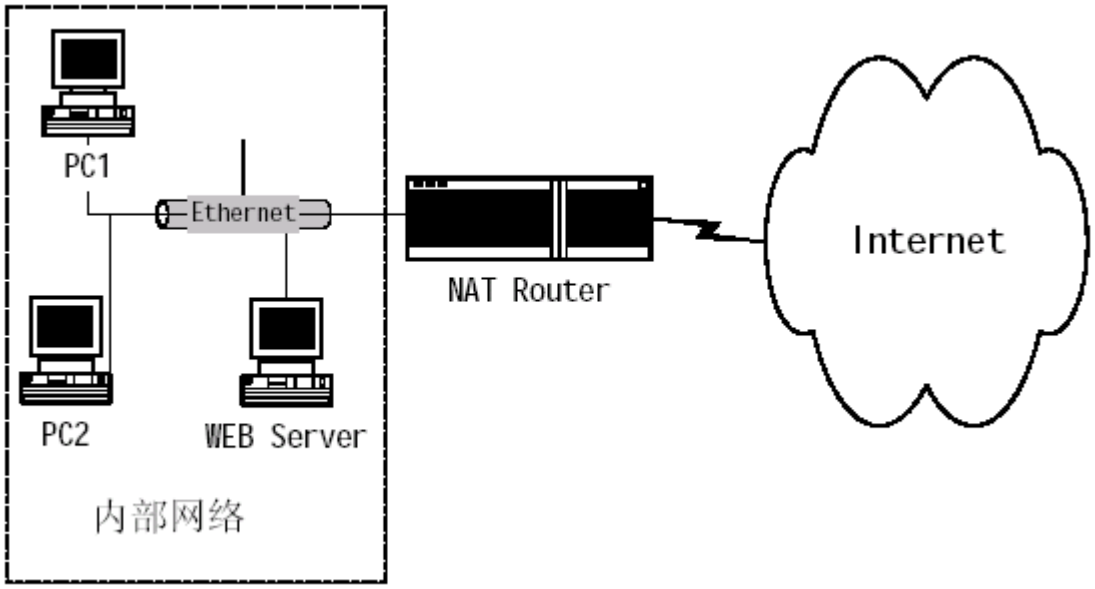


图 5-1　地址转换组网应用示意图

如图 5-1 的内部网络就是使用了一个上述的“私有地址”的内部局域网，其中 PC1 就是属于 **1**）情况描述的主机，它不需要访问 Internet，PC2 属于 **2**）情况描述的主机，它需要在有时候访问 Internet。Web Server 属于 **3**）情况描述的主机是台 WEB 服务器，同时也可以被外部网络访问。该局域网通过一台路由器接入 Internet。

通过地址转换技术，可以使这个内部局域网的所有主机（或者部分主机）可以访问 Internet（外部网络）。只有当内部局域网内部的主机需要访问 Internet 的时候，地址转换技术可以为这台主机分配一个临时的合法的 IP 地址，使得这台主机可以访问 Internet，因此每台内部局域网的主机不需要都拥有合法的 IP 地址就可以访问 Internet 了，这样就大大节约了合法的 IP 地址。

当采用了地址转换技术的内部局域网的主机对 Internet 就是不可见的了，Internet 的主机就不能直接访问内部局域网中的主机，当内部局域网需要给外部网络提供一定的服务的时候，例如提供一个 www 的服务器，可以使用地址转换提供的“内部服务器”功能。

“内部服务器”功能是一种“反向的”地址转换，普通的地址转换是提供内部网络中的主机访问外部网络的，而“内部服务器”功能提供了外部网络的主机访问内部网络中使用私有地址的主机的能力。

5.2.4　NAPT 方式的地址转换

某个局域网用户使用私有地址建立了局域网，当这个局域网准备和 Internet 连接的时候，该局域网拥有的合法 IP 地址数量可能远远小于局域网内部的用户数量，例如某个局域网有 50 台主机需要访问 Internet，而实际的合法 IP 地址只有 5 个。

RG 系列路由器可以提供 NAPT（Port Address Translation）方式的地址转换，NAPT 方式的地址转换使用了 TCP/UDP 的端口信息，这样在进行地址转换的时候使用的是“地址端口”来区分内部局域网的主机对外发起的不同连接。因为 TCP/UDP 的端口范围是 1~65535，一般 1～

1024 端口范围是系统保留端口，因此从理论上计算，通过 NAPT 方式的地址转换，一个合法的 IP 地址可以提供大约 60000 个并发连接。这样，使用 NAPT 方式的地址转换技术，内部局域网的很多用户可以共享一个 IP 地址上网了。由于提出地址转换技术的根本原因就是因为 IP 地址短缺问题，因此 NAPT 方式的地址转换是现在主要的地址转换形式

5.2.5 内部服务器应用

内部服务器是一种“反向”的地址转换，内部服务器功能可以使得配置了私有地址的内部主机可以被外部网络访问。如图 5-1，Web Server 是一台配置了私有地址的机器，通过地址转换提供的配置可以为这台主机映射一个合法的 IP 地址。假设是 202.110.10.10，当 Internet 上的用户访问 202.110.10.10 的时候，地址转换就将访问送到了 Server 上，这样就可以给内部网络提供一种“内部服务器”的应用，RG 路由器对内部服务器的支持可以到达端口级，允许用户按照自己的需要配置内部服务器的端口、协议，提供给外部的端口、协议。例如，在图 5-1 中通过配置 RG 路由器，外部网络的用户可以利用这样的 http://202.110.10.10:8080 地址，来访问内部地址为 10.110.10.10 的 Web 服务器。

5.2.6 利用 ACL 控制地址转换

地址转换功能可以利用访问控制列表决定什么样的地址可以进行地址转换，如果某些主机具有访问 Internet 的权利，而某些主机不能访问 Internet，可以利用 ACL(访问控制列表)定义什么样的主机不能访问 Internet，什么样的主机可以访问 Internet，然后将配置好的 ACL 规则应用在地址转换上，就可以达到利用 ACL 控制地址转换的功能。

如图 5-1，PC1 不需要访问 Internet。那么可以通过访问控制列表限制 PC1 访问 Internet，使得 PC1 只能访问内部局域网的主机。

5.2.7 地址转换应用程序网关

地址转换对一些复杂协议需要做特殊处理，总体上说只要是在数据载荷（“数据载荷”是指除了 IP 头以及 TCP/UDP 头之外的信息）中含有地址或者端口（这里的端口仅仅只 TCP/UDP 的端口）信息的协议，地址转换都需要特殊处理。为了使得地址转换可以支持某种特殊的协议的部分称为应用程序网关，常见的地址转换需要特殊处理的程序有 FTP（包括 PASV 和 PORT 两种模式）、Netmeeting、H323、DNS 等，同时还有一些游戏。

5.2.8 地址转换和代理 Proxy 的区别

地址转换技术和地址代理技术有很类似的地方，都是提供了私有地址访问 Internet 的能力，但是两者还是有区别的，它们区别的本质是在 TCP/IP 协议栈中的位置不同，地址转换是工作在网络层，而地址代理是工作在应用层。

地址转换对各种应用是透明的，而地址代理必须在应用程序中指明代理服务器的 IP 地址。例如使用地址转换技术访问 Web 网页，不需要在浏览器中进行任何的配置。而如果使用 Proxy 访问 Web 网页的时候，就必须在浏览器中指定 Proxy 的 IP 地址，如果 Proxy 只能支持 Http 协议，那么只能通过代理访问 Web 服务器，如果想使用 FTP 就不可以了。因此使用地址转换技术访问 Internet 比使用 proxy 技术具有十分良好的扩充性，不需要针对应用进行考虑。

但是地址转换技术很难提供基于“用户名”和“密码”的验证，在使用 proxy 的时候，可以使用验证功能使得只有通过“用户名”和“密码”验证的用户才能访问 Internet，而地址转换不能做到这一点。

5.2.9 地址转换的优点和缺点

使用地址转换技术主要有以下几个优点：

1) 地址转换可以使内部网络用户方便的访问 Internet。

2) 地址转换可以使内部局域网的许多主机共享一个 IP 地址上网大大节约了合法的 IP 地址。

3) 地址转换可以屏蔽内部网络的用户提高内部网络的安全性。

4) 地址转换同样可以提供给外部网络 WWW、FTP、Telnet 等服务。

5) 地址转换技术可以使得内部局域网的 IP 地址分配变得容易维护，不会因为合法地址转换的缺乏而不容易合理分配内部局域网的 IP 地址，并且当外部有变化的时候也不需要改动内部局域网内部的配置。

地址转换技术主要有以下几个缺点:

1) 地址转换对于报文内容中含有有用的地址信息的情况需要做特殊处理，这种情况的代表协议是 FTP。

2) 地址转换不能处理 IP 报头加密的情况。

3) 地址转换由于隐藏了内部主机地址有时候会使网络调试变得复杂。

5.3 组网应用

5.3.1 内部源地址 NAT 配置

当内部网络需要与外部网络通讯时，需要配置 NAT，将内部私有 IP 地址转换成全局唯一 IP 地址。你可以配置静态或动态的 NAT 来实现互联互通的目的，或者需要同时配置静态和动态的 NAT。

静态 NAT，是建立内部本地地址和内部全局地址的一对一永久映射。当外部网络需要通过固定的全局可路由地址访问内部主机，静态 NAT 就显得十分重要。

动态 NAT，是建立内部本地地址和内部全局地址池的临时映射关系，过一段时间没有用就会删除映射关系。

图 5-2 反映了内部源地址 NAT 的整个过程。

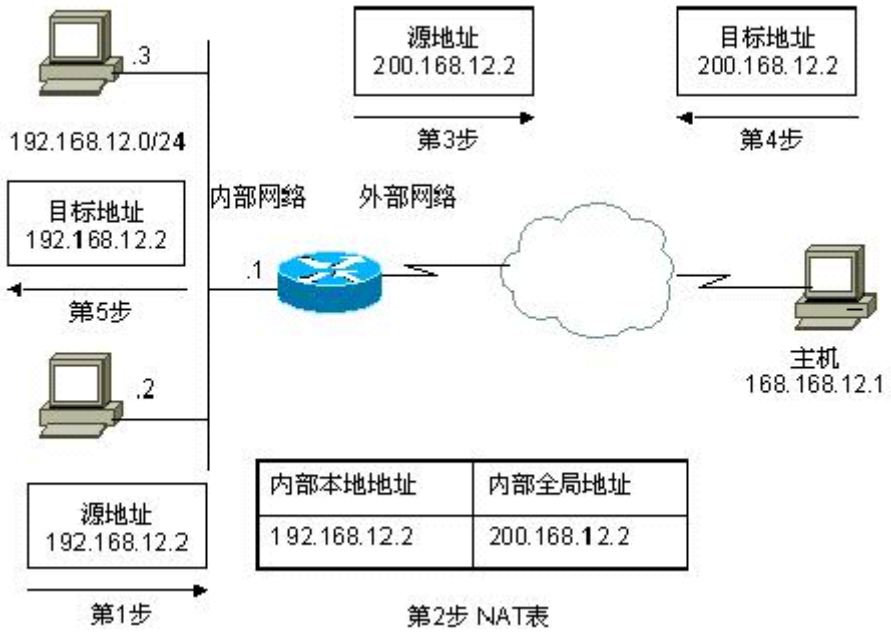


图 5-2　内部源地址 NAT

当内部网络一台主机访问外部网络资源时，详细过程描述如下：

内部主机 192.168.12.2 发起一个到外部主机 168.168.12.1 的连接。当路由器接收到以 192.168.12.2 为源地址的第一个数据包时，引起路由器检查 NAT 映射表。

1、该地址有配置静态映射，就执行第三步；

2、如果没有静态映射，就进行动态映射，路由器就从内部全局地址池中选择一个有效的地址，并在 NAT 映射表种创建 NAT 转换记录。这种记录叫基本记录。

3、路由器用 192.168.12.2 对应的 NAT 转换记录中全局地址，替换数据包源地址，经过转换后，数据包的源地址变为 200.168.12.2，然后转发该数据包。

4、168.168.12.1 主机接收到数据包后，将向 200.168.12.2 发送响应包。

5、当路由器接收到内部全局地址的数据包时，将以内部全局地址 200.168.12.2 为关键字查找 NAT 记录表，将数据包的目的地址转换成 192.168.12.2 并转发给 192.168.12.2。

6、192.168.12.2 接收到应答包，并继续保持会话。第一步到第五步将一直重复，直到会话结束。

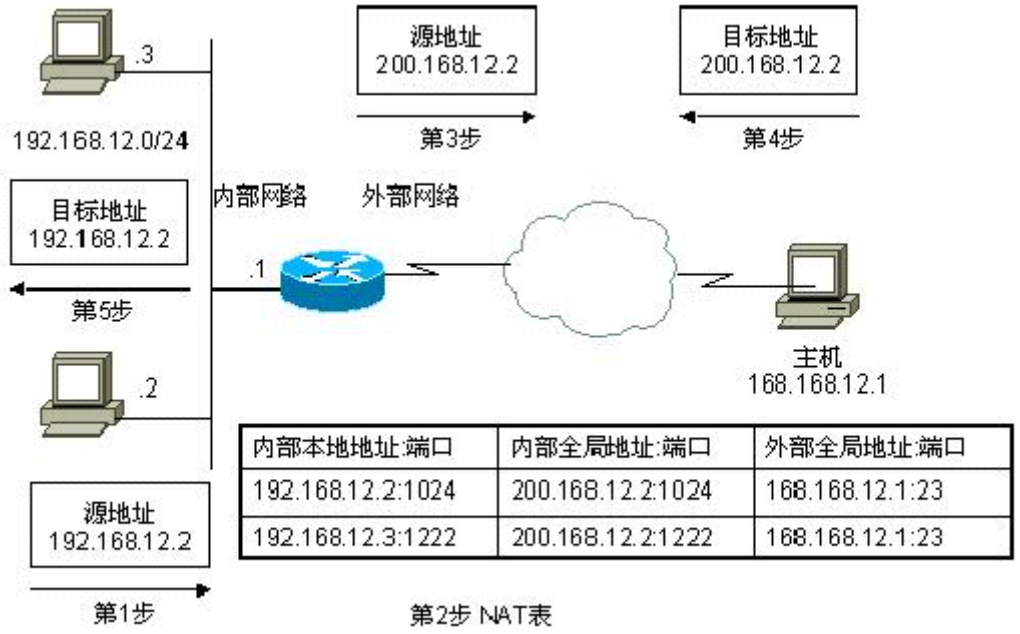
5.3.2　内部源地址 NAPT 配置

传统的 NAT 一般是指一对一的地址映射，不能同时满足所有的内部网络主机与外部网络通讯的需要。使用 NAPT，可以将多个内部本地地址映射到一个内部全局地址，路由器用“内部全局地址+ TCP/UDP 端口号”来对应“一个内部主机地址+TCP/UDP 端口号”。当进行 NAPT 转换时，路由器需要维护足够的信息（比如 IP 地址、TCP/UDP 端口号）才能将全局地址转换回内部本地地址，目前 RGNOS 的 NAT 缺省就是支持 NAPT 转换的。内部源地址 NAPT 配置也有两种情况：

1）内部源地址静态 NAPT，当你内部主机需要对外部网络提供服务，而又缺乏全局地址，或者就没有申请全局地址，就可以考虑配置静态 NAPT，静态 NAPT 的内部全局地址可以是路由器外部(Outside)接口的 IP 地址，也可以是向 CNNIC 申请来的地址；

2）内部源地址动态 NAPT，允许内部所有主机可以访问外部网络，动态 NAPT 的内部全局地址可以是路由器外部(Outside)接口的 IP 地址，也可以是向 CNNIC 申请来的地址。

图 5-3 反映了内部源地址 NAPT 的整个过程。



内部本地地址:端口	内部全局地址:端口	外部全局地址:端口
192.168.12.2:1024	200.168.12.2:1024	168.168.12.1:23
192.168.12.3:1222	200.168.12.2:1222	168.168.12.1:23

图 5-3 内部地址 NAPT 配置

上图所示，主机 168.168.12.1 以为是在跟同一台设备通信，实际上是分别与内部网络两台地址不同的主机通信。以下详细描述了内部网络 NAPT 的整个过程：

内部主机 192.168.12.2 发起一个到外部主机 168.168.12.1 的连接。当路由器接收到以 192.168.12.2 为源地址的第一个数据包时，引起路由器检查 NAT 映射表：

1、如果 NAT 没有转换记录，路由器就为 192.168.12.2 作地址转换，并创建一条转换记录。

2、如果启用了 NAPT，就进行另外一次转换，路由器将复用全局地址并保存足够的信息以便能够将全局地址转换回本地地址。NAPT 的地址转换记录称为扩展记录。

3、路由器用 192.168.12.2 对应的 NAT 转换记录中全局地址，替换数据包源地址，经过转换后，数据包的源地址变为 200.168.12.2，然后转发该数据包。

4、168.168.12.1 主机接收到数据包后，将向 200.168.12.2 发送响应包。

5、当路由器接收到内部全局地址的数据包时，将以内部全局地址 200.168.12.2 及其端口号、外部全局地址及其端口号为关键字查找 NAT 记录表，将数据包的目的地址转换成 192.168.12.2 并转发给 192.168.12.2。

6、192.168.12.2 接收到应答包，并继续保持会话。第一步到第五步将一直重复，直到会话结束。

5.3.3 重叠地址 NAT 配置

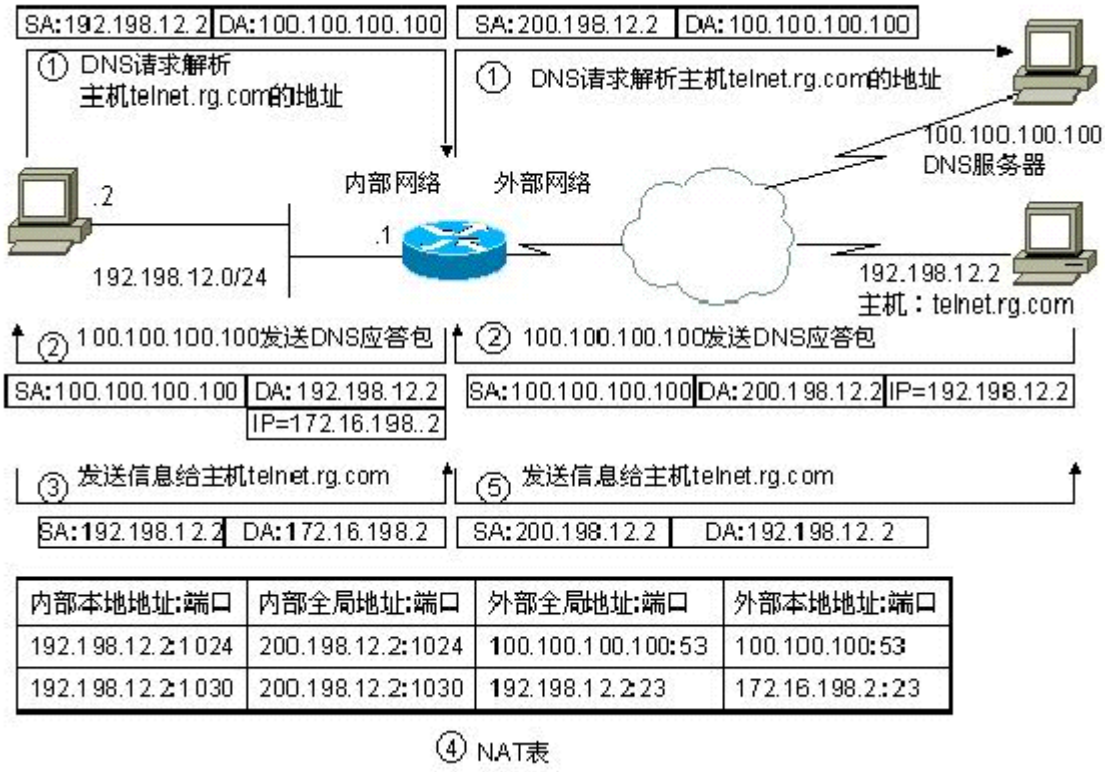
两个需要互联的私有网络分配了同样 IP 地址，或者一个私有网络和公有网络分配了同样的全局 IP 地址，这种情况称为地址重叠。两个重叠地址的网络主机之间是不可能通信的，因为它们相互认为对方的主机在本地网络。重叠地址 NAT 就是专门针对重叠地址网络之间通信的问题，配置了重叠地址 NAT，外部网络主机地址在内部网络表现为另一个网络主机地址，反

之一样。重叠地址 NAT 配置分为两个部分内容：

1）内部源地址转换配置，

2）外部源地址转换配置，只有与内部网络地址重叠的外部网络需要配置外部源地址转换，外部源地址转换可以采用静态 NAT 配置或动态 NAT 配置。在本配置描述中，将只描述外部源地址转换如何配置。

图 5-4 显示了 NAT 如何对重叠地址网络进行地址转换。



内部本地地址:端口	内部全局地址:端口	外部全局地址:端口	外部本地地址:端口
192.198.12.2:1024	200.198.12.2:1024	100.100.100.100:53	100.100.100:53
192.198.12.2:1030	200.198.12.2:1030	192.198.12.2:23	172.16.198.2:23

④ NAT表

图 5-4　重叠地址 NAT 配置

上图是发生地址重叠时，内部网络主机访问重叠地址主机时的典型应用过程，

以下对该过程进行详细描述：

1、内部主机通过 Telnet 远程登录主机 telnet.rg.com，首先向 DNS 服务器 100.100.100.100 发送地址解析请求。该过程包含了内部源地址转换。

2、路由器截获 DNS 响应包，检查响应包中解析后返回的 IP 地址是否属于重叠地址（即与内部网络地址相同）。如果是重叠地址，就进行地址转换，上图中将 192.198.12.2 转换成 172.16.198.2，然后将 DNS 响应包发送给内部网络主机 192.198.12.2。

3、内部主机 192.198.12.2 获知 telnet.rg.com 主机的 IP 地址为 172.16.198.2，就向 172.16.198.2 的 TCP 23 号端口发送连接请求包。

4、路由器接收到该 TCP 连接请求包，就建立转换映射记录，内部本地地址为 192.198.12.2，内部全局地址为 200.198.12.2，外部本地地址为 172.16.198.2，外部全局地址为 192.198.12.2。

5、根据 NAT 映射记录，将数据包的源地址置换为 200.198.12.2，目标地址置换为 192.198.12.2，然后将数据包发送给外部主机 192.198.12.2。

6、主机 telnet.rg.com 接收到数据包，发送确认包给内部主机。

7、路由器接收到数据包，以外部全局地址及其端口号、内部全局地址及其端口号为关键字，

检索 NAT 映射表，用外部本地地址、内部本地地址分别置换源地址和目标地址，然后转发给内部主机 192.198.12.2。

8、内部主机接收到数据包，重复 3）~7）步骤，直到会话结束。

5.3.4 TCP 负载均衡

当内部网络某台主机 TCP 流量负载过重时，可能需要多台主机进行 TCP 业务的均衡负载。这时，你可以考虑用 NAT 来实现 TCP 流量的负载均衡，NAT 创建了一台虚拟主机提供 TCP 服务，该虚拟主机对应内部多台实际的主机，然后对目标地址进行轮询置换，达到负载分流的目的。但是对于其它的 IP 流量，不做任何的改变，除非 NAT 作了其它配置。

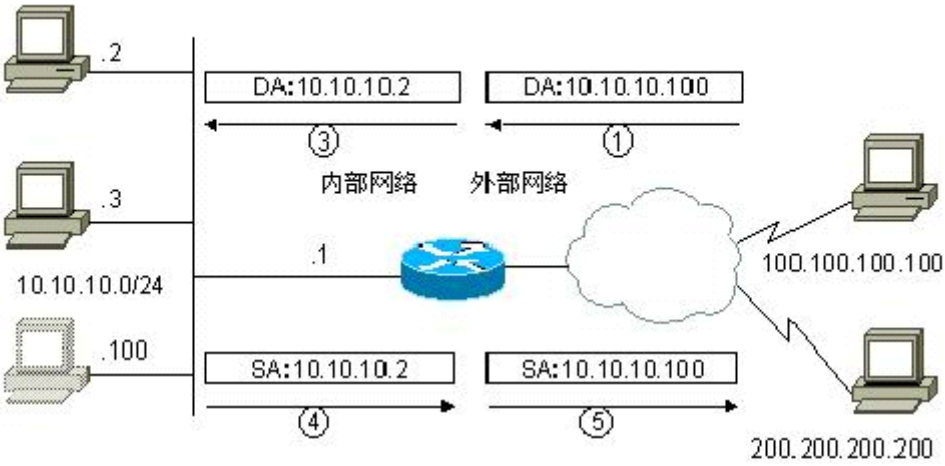
配置 NAT 实现 TCP 负载均衡，内部网络的地址可以是合法的全局地址，也可以是私有网络地址。但是虚拟主机地址必须为合法的全局地址。

图 5-5 显示了 TCP 负载均衡工作流程。

在图中，实际提供 TCP 服务的主机有两台，地址分别为 10.10.10.2 和 10.10.10.3，对外提供了一个虚拟 IP 地址 10.10.10.100，外部网络通过 10.10.10.100 访问 TCP 服务。以下为 NAT 实现 TCP 负载均衡过程的详细描述：主机 100.100.100.100，向 10.10.10.100 发起 Telnet 连接服务。

路由接收到 Telnet 连接请求包，建立一个 NAT 转换记录，为内部全局地址 10.10.10.100 分配一个内部实际主机地址 10.10.10.2。路由器用实际的内部主机地址替换目标地址，然后将数据包转发到实际主机。实际主机 10.10.10.2 接收到数据包并发送应答包。路由器接收到应答包，以内部本地地址及端口号和外部全局地址及端口号为关键字，在 NAT 映射表查找匹配转换记录。然后将数据包的源地址转换为虚拟主机地址，并转发数据包。

如果再来一个 TCP 连接请求，路由器将按照轮询分配方式将 10.10.10.3 的地址作为内部本地地址，建立一个不同的 NAT 转换记录，从而达到负载均衡的目的。



协议	内部本地地址:端口	内部全局地址:端口	外部全局地址:端口
TCP	10.10.10.2:23	10.10.10.100:23	100.100.100.100:1688
TCP	10.10.10.3:23	10.10.10.100:23	200.200.200.200:1556

② NAT表

说明：
SA:源地址 DA:目标地址

图 5-5　TCP 负载均衡

5.4　静态与动态 NAT 配置命令

5.4.1　配置静态 NAT

➢Red-Giant(config)#**ip nat inside source static** *local-address global-address* ●定义内部源地址静态转换关系

➢Red-Giant(config)# **interface** *interface-type interface-number*

➢Red-Giant(config-if)#**ip nat inside** ●定义该接口连接内部网络

➢Red-Giant(config)# **interface** *interface-type interface-number*

➢Red-Giant(config-if)#**ip nat outside** ●定义接口连接外部网络

5.4.2　配置动态 NAT

➢Red-Giant(config)#**ip nat pool** *address-pool start-address end-address* {**netmask** *mask* | **prefix-length** *prefix-length*} ●定义全局 IP 地址池

➢Red-Giant(config)#**access-list** *access-list-number* **permit** *ip-address wildcard* ●定义

访问列表，只有匹配该列表的地址才转换

➢Red-Giant(config)#**ip nat inside sourcelist** *access-list-number* **pool** *address-pool* ●定义内部源地址动态转换关系

➢Red-Giant(config)# **interface** *interface-type interface-number*

➢Red-Giant(config-if)#**ip nat inside** ●定义该接口连接内部网络

➢Red-Giant(config)# **interface** *interface-type interface-number*

➢Red-Giant(config-if)#**ip nat outside** ●定义接口连接外部网络

5.4.3 配置静态 NAPT(或 PAT)

➢Red-Giant(config)#**ip nat inside source static** {**UDP** | **TCP**} *local-address port global-address port* ●定义全局 IP 地址池

➢Red-Giant(config)# **interface** *interface-type interface-number*

➢Red-Giant(config-if)#**ip nat inside** ●定义该接口连接内部网络

➢Red-Giant(config)# **interface** *interface-type interface-number*

➢Red-Giant(config-if)#**ip nat outside** ●定义接口连接外部网络

5.4.4 配置静态 NAPT(或 PAT)

➢Red-Giant(config)#**ip nat pool** *address-pool start-address end-address* {**netmask** *mask* | **prefix-length** *prefix-length*} ●定义全局 IP 地址池，对于 NAPT，一般就定义一个 IP 地址

➢Red-Giant(config)#**access-list** *access-list-number* **permit** *ip-address wildcard* ●定义访问列表，只有匹配该列表的地址才转换

➢Red-Giant(config)#**ip nat inside sourcelist** *access-list-number* **pool** *address-pool [**interface** interface-type interface-number]}* **overload**

●定义内部源地址动态转换关系

➢Red-Giant(config)# **interface** *interface-type interface-number*

➢Red-Giant(config-if)#**ip nat inside** ●定义该接口连接内部网络

➢Red-Giant(config)# **interface** *interface-type interface-number*

➢Red-Giant(config-if)#**ip nat outside** ●定义接口连接外部网络

5.4.5 NAT 的监视和维护命令

➢显示命令

```
show ip nat statistics
show ip nat translations [verbose]
```

➢清除状态命令

```
clear ip nat translation *
clear ip nat translation outside local-address global-address
```

习 题

1. NAT 的作用是什么？
2. 在 NAT 中有哪四种地址？
3. 因特网地址中的私有地址是什么？
4. 最常用的网络地址转换模式有哪几种？
5. NAPT 和 NAT 的主要区别是什么？

第6章 地址解析协议

我们知道，当在浏览器里面输入网址时，DNS 服务器会自动把它解析为 IP 地址，浏览器实际上查找的是 IP 地址而不是网址。那么 IP 地址是如何转换为第二层物理地址（即 MAC 地址）的呢？在局域网中，这是通过 ARP 协议来完成的。ARP 协议对网络安全具有重要的意义。通过伪造 IP 地址和 MAC 地址实现 ARP 欺骗，能够在网络中产生大量的 ARP 通信量使网络阻塞。所以网络管理人员应深入理解 ARP 协议。

6.1 什么是 ARP 协议

ARP 协议是“Address Resolution Protocol”（地址解析协议）的缩写。在局域网中，网络中实际传输的是“帧”，帧里面是有目标主机的 MAC 地址的。在以太网中，一个主机要和另一个主机进行直接通信，必须要知道目标主机的 MAC 地址。但这个目标 MAC 地址是如何获得的呢？它就是通过地址解析协议获得的。所谓“地址解析”就是主机在发送帧前将目标 IP 地址转换成目标 MAC 地址的过程。ARP 协议的基本功能就是通过目标设备的 IP 地址，查询目标设备的 MAC 地址，以保证通信的顺利进行。

6.2 ARP 协议的工作原理

6.2.1 ARP 的工作过程

在每台安装有 TCP/IP 协议的电脑里都有一个 ARP 缓存表，表里的 IP 地址与 MAC 地址是一一对应的，如图 6-1 所示所示。

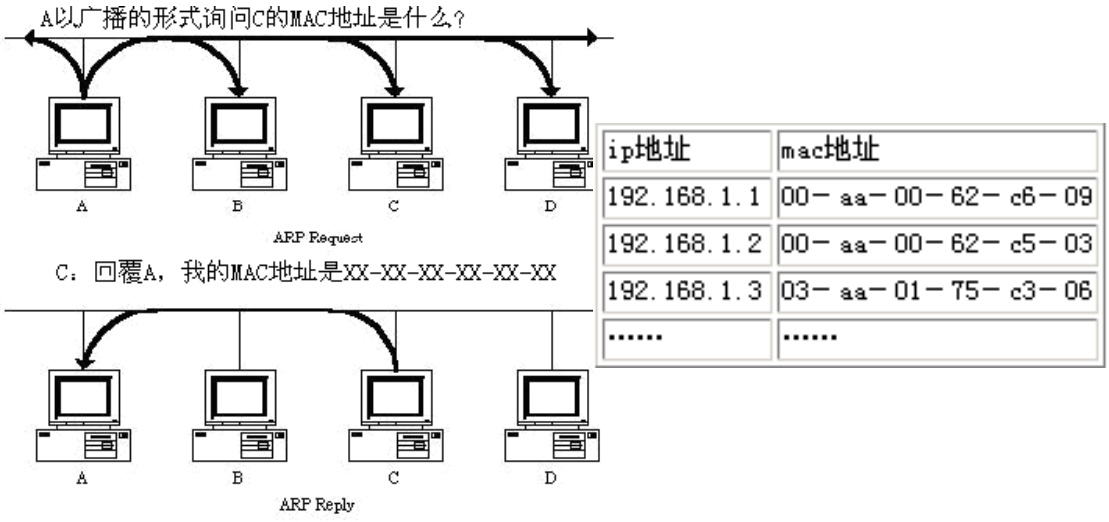


图 6-1 ARP 缓存表

在图 6-1 中，我们以主机 A（192.168.1.5）向主机 C（192.168.1.1）发送数据为例。当发送数据时，主机 A 会在自己的 ARP 缓存表中寻找是否有目标 IP 地址。如果找到了，也就知道了目标 MAC 地址，直接把目标 MAC 地址写入帧里面发送就可以了；如果在 ARP 缓存表中没有找到相对应的 IP 地址，主机 A 就会在网络上发送一个广播，目标 MAC 地址是“FF.FF.FF.FF.FF.FF”，这表示向同一网段内的所有主机发出这样的询问：“192.168.1.1 的 MAC 地址是什么？”。网络上其他主机并不响应 ARP 询问，只有主机 C 接收到这个帧时，才向主机 A 做出这样的回应：“192.168.1.1 的 MAC 地址是 00-aa-00-62-c6-09”。这样，主机 A 就知道了主机 C 的 MAC 地址，它就可以向主机 C 发送信息了。同时它还更新了自己的 ARP 缓存表，下次再向主机 C 发送信息时，直接从 ARP 缓存表里查找就可以了。ARP 缓存表采用了老化机制，在一段时间内如果表中的某一行没有使用，就会被删除，这样可以大大减少 ARP 缓存表的长度，加快查询速度。

6.2.2 ARP 的查询过程

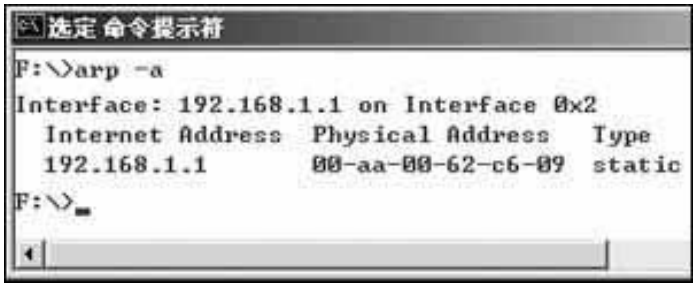
前面说的 ARP 表格，只有在 TCP/IP 协议被载入核心之后才会建立，如果 TCP/IP 协议被卸载或关闭机器，那么表格就会被清空，到下次协议载入或开机的时候再重新建立，而同时会向网路发出一个 ARP 广播，告诉其它机器它的目前地址是什么，以便所有机器都能保持最正确的资料。

然而，ARP cache 的大小是有所限制的，如果超过了界限，那么越长时间没被使用过渡资料就必须清理掉，以腾出空间来储存更新的资料。所以，当机器收到 ARP request 封包时，如果查询对象不是自己，则不会根据发送端地址资料来更新自己的 ARP 表格，而是完全忽略该封包。同时，每笔存在 cache 中的资料，都不是永久保存的。每笔资料再更新的时候，都会被赋

予一个存活倒数计时值，如果在倒数时间到达的时候，该资料就会被清掉。然而，如果该资料在倒数时间到达之前被使用过，则计时值会被重新赋予。在 windows 操作系统或一些网络设备里默认情况下 ARP cache 缓存保留的时间值为 20 分钟。

当然，ARP 尚有一套机制来处理当 ARP 表格资料不符合实际地址资料的状况(例如，在当前连线尚未结束前,收到目的端的地址资料更新讯息),或是目的主机太忙碌而未能回答 ARP 请求等状况。

1．如何查看 ARP 缓存表



ARP 缓存表是可以查看的，也可以添加和修改。在命令提示符下，输入“arp -a”就可以查看 ARP 缓存表中的内容了，如附图所示。

用“arp -d”命令可以删除 ARP 表中某一行的内容；用“arp -s”可以手动在 ARP 表中指定 IP 地址与 MAC 地址的对应。

6.3 ARP 欺骗

6.3.1 ARP 欺骗概述

ARP 协议的作用是在处于同一个子网中的主机所构成的局域网部分中将 IP 地址映射到 MAC 地址。网络上的每一个设备至少有两个地址：媒体存取控制地址和 Internet 协议（IP）地址。MAC 地址是设备中网络接口卡的物理地址，它在该设备服务的寿命期限内不会发生改变。如果机器移动到网络的其它地方，IP 地址就会发生改变。ARP 用于将 IP 地址匹配到或解析至恰当的 MAC 地址（反之亦然）。ARP 通过向连接到以太网中的所有主机发出一个数据包的办法进行工作。数据包中含有发送者需要连接的 IP 地址。大多数主机会忽略该数据包。目标机器识别出数据包中的 IP 地址与自己匹配，所以就会作出响应。ARR 是一个非常简单的协议，仅有四种类型的基本信息组成：

- ARP 询问—计算机 A 发出询问：“哪台计算机拥有该 IP 地址？”
- ARP 应答—计算机 B 向计算机 A 发出信息：“我拥有哪个 IP 地址，我的 MAC 地址是 123.123.123.123”。
- 逆向 ARP 询问（RARP）—是与 ARP 询问一样的概念，但计算机 A 询问：“哪台计算机拥有该 MAC 地址？”
- 逆向 ARP 应答—计算机 B 向计算机 A 发出信息：“我拥有那个 MAC 地址，我的 IP 地址是 123.123.123.123”。

所有的网络设备都有一张 ARP 表,里面临时记忆着该设备已经匹配起来的所有的 IP 地址和 MAC 地址。ARP 表能够确保该设备不需要向已经与自己进行过通信的计算机重复 ARP 询问。当有人在未获得授权时就企图更改 MAC 和 IP 地址的 ARP 表格中的信息时,就发生了 ARP 攻击。通过这种方式，黑客们可以伪造 MAC 或 IP 地址，以便实施如下的两种攻击：

（1）服务拒绝

黑客很容易就可以将一个在操作上有效的 IP 地址与虚假的 MAC 地址联系起来。例如黑客可以发出 ARP 应答将用户的网络路由器 IP 地址与一个不存在的 MAC 地址联系起来。用户计算机认为它们知道其默认网关的位置，但实际上它们在发送目的地址不在本地的数据包，而是在天空中的一个巨大的“位存储桶”。只此一步，黑客就已经切断了用户网络与 Internet 的连接。

（2）中间人

黑客可以使用 ARP 投毒的办法来截取用户网络中两设备间的通信。例如，黑客想知道 IP 地址为 123.123.123.123 的用户计算机与用户 Internet 路由器之间的所有通信。首先，黑客会向客户的路由器发送恶意的 ARP 应答，将其计算机 MAC 地址与 IP 地址 123.123.123.123 联系起来。

ARP 协议的基本功能就是通过目标设备的 IP 地址，查询目标设备的 MAC 地址，以保证通信的进行。

基于 ARP 协议的这一工作特性，黑客向对方计算机不断发送有欺诈性质的 ARP 数据包，数据包内包含有与当前设备重复的 MAC 地址，使对方在回应报文时，由于简单的地址重复错误而导致不能进行正常的网络通信。一般情况下，受到 ARP 攻击的计算机会出现两种现象:

1）不断弹出“本机的 XXX 段硬件地址与网络中的 XXX 段地址冲突”的对话框。

2）计算机不能正常上网，出现网络中断的症状。

因为这种攻击是利用 ARP 请求报文进行“欺骗”的，所以防火墙会误以为是正常的请求数据包，不予拦截，因此普通的防火墙很难抵挡这种攻击

6.3.2 ARP 欺骗技术实现原理分析

当你给一个系统打补丁时，只是安全措施里的一个很基本的步骤而已，通常一个 hacker 要进入你的系统，他所要做的并不是你打补丁就可以避免的，象这些欺骗都要求你必须掌握相当的网络底层知识和合理安排物理布线才可阻止得了。特别是多种手法混用的时候，特别要说明的是:有些人往往以为会使用某些工具入侵就觉得自己是个 hacker,其实这只是入门而已(有些是连门都找不到)，通过本节的介绍，我们应该知道，一个 hacker 在真正入侵系统时，他并不是依靠别人写的什么软件，而更多的是靠对系统和网络的深入了解来达到这个目的。

首先还是得说一下什么是 ARP ，如果你在 UNIX Shell 下输入 arp -a (Windows 9x 下也是)，其输出看起来应该是这样的：

```
Interface: xxx.xxx.xxx.xxx
Internet Address   Physical Address   Type
```

xxx.xxx.xxx.xxx　　00-00-93-64-48-d2　　dynamic

xxx.xxx.xxx.xxx　　00-00-b4-52-43-10　　dynamic

....

这里第一列显示的是 IP 地址，第二列显示的是和 IP 地址对应的网络接口卡的硬件地址（MAC），第三列是该 IP 和 MAC 的对应关系类型。

可见，ARP 是一种将 IP 转化成以 IP 对应的网卡的物理地址的一种协议，或者说 ARP 协议是一种将 IP 地址转化成 MAC 地址的一种协议，它靠维持在内存中保存的一张表来使 IP 得以在网络上被目标机器应答。

为什么要将 IP 转化成 MAC 呢？简单的说，这是因为在 TCP 网络环境下，一个 IP 包走到哪里，该怎么走是依靠路由表来定义的，但是，当 IP 包到达该网络后，哪台机器响应这个 IP 包却是依靠该 IP 包中所包含的 MAC 地址来识别，也就是说，只有机器的 MAC 地址和该 IP 包中的 MAC 地址相同的机器才会应答这个 IP 包，因为在网络中，每一台主机都会有发送 IP 包的时候，所以，在每台主机的内存中，都有一个 ARP--> MAC 的转换表。通常这种转换表是动态的转换表（注意在路由中，该 ARP 表可以被设置成静态表），也就是说，该对应表会被主机在需要的时候刷新，这是由于以太网在子网层上的传输是靠 48 位的 MAC 地址而决定的。

通常主机在发送一个 IP 包之前，它要到该转换表中寻找和 IP 包对应的 MAC 地址，如果没有找到，该主机就发送一个 ARP 广播包，其形式如下：

“我是主机 xxx.xxx.xxx.xxx ， MAC 是 xxxxxxxxxxx ，IP 为 xxx.xxx.xxx.xx1 的主机请告之你的 MAC ”

IP 为 xxx.xxx.xxx.xx1 的主机响应这个广播，应答 ARP 广播为：

“我是 xxx.xxx.xxx.xx1，我的 MAC 为 xxxxxxxxxx2”

于是，主机刷新自己的 ARP 缓存，然后发出该 IP 包。

了解这些常识后，现在就可以说明在网络中如何实现 ARP 欺骗了，可以先来看这样一个例子：

一个入侵者想非法进入某台主机，他知道这台主机的防火墙只对 192.0.0.3(假设)这个 IP 开放 23 口(telnet)，而他必须要使用 telnet 来进入这台主机，所以他要这么做：

1）他先研究 192.0.0.3 这台主机，想方设法让这台机器不能工作。

2）这时，主机发到 192.0.0.3 的 IP 包将无法被机器应答，系统开始更新自己的 ARP 对应表。将 192.0.0.3 的项目删去。

3）这段时间里，入侵者把自己的 IP 改成 192.0.0.3

4）他发一个 ping(icmp 0)给主机，要求主机更新主机的 ARP 转换表。

5）主机找到该 IP，然后在 ARP 表中加上新的 IP-->MAC 对应关系。

6）防火墙失效了，入侵的 IP 变成合法的 MAC 地址，可以 telnet 了。

7）现在，假如该主机不只提供 telnet ， 它还提供 r 命令（rsh，rcopy，rlogin 等），那么，所有的安全约定将无效，入侵者可以放心的使用这台主机的资源而不用担心被记录什么。

有人也许会说，这其实就是冒用 IP 嘛。是冒用了 IP，但决不是 IP 欺骗，IP 欺骗的原理比这要复杂的多，实现的机理也完全不一样。

上面就是一个 ARP 的欺骗过程，这是在同网段发生的情况，但是，提醒注意的是，利用交换集线器或网桥是无法阻止 ARP 欺骗的，只有路由分段是有效的阻止手段（也就是 IP 包必须经过路由转发）。在有路由转发的情况下，ARP 欺骗如配合 ICMP 欺骗将对网络造成

极大的危害，从某种角度讲，入侵者可以跨过路由监听网络中任何两点的通讯，如果设置防火墙，请注意防火墙有没有提示过类似:“某某 IP 是局域 IP 但从某某路由来”等这样的信息。

在有路由转发的情况下，发送到达路由的 IP 的主机其 ARP 对应表中，IP 的对应值是路由的 MAC。

比如， 在 ping www.cns111.com 后，那么在我的主机中，www.cns111.com 的 IP 对应项不是 cns111 的 MAC ，而是路由的 MAC。其 IP 也是路由的 IP。(有些网络软件通过交换路由 ARP 可以得到远程 IP 的 MAC)

所以，要有效阻止 ARP 的欺骗，必须深入理解 ARP 协议，才能阻止 hacker 的入侵。

那么，如何防止 ARP 欺骗呢？

1） 不要把你的网络安全信任关系建立在 IP 基础上或 MAC 基础上，(RARP 同样存在欺骗的问题)，理想的关系应该建立在 IP+MAC 基础上。
2） 设置静态的 MAC-->IP 对应表，不要让主机刷新你设定好的转换表。
3） 除非很有必要，否则停止使用 ARP，将 ARP 做为永久条目保存在对应表中。
4） 使用 ARP 服务器,通过该服务器查找自己的 ARP 转换表来响应其他机器的 ARP 广播。确保这台 ARP 服务器不被黑。
5） 使用“proxy”代理 IP 的传输。
6） 使用硬件屏蔽主机。设置好你的路由，确保 IP 地址能到达合法的路径。(静态配置路由 ARP 条目)，注意，使用交换集线器和网桥无法阻止 ARP 欺骗。
7） 管理员定期用响应的 IP 包中获得一个 RARP 请求，然后检查 ARP 响应的真实性。
8） 管理员定期轮询，检查主机上的 ARP 缓存。
9） 使用防火墙连续监控网络。注意有使用 SNMP 的情况下，ARP 的欺骗有可能导致陷阱包丢失。

第7章　　园区网安全设计

计算机网络最早出现在军事网，在它诞生之后的几十年间，主要用于在各科研机构的研究人员之间传送电子邮件，以及共同合作的职员间共享打印机。早期的计算机网络应用得非常简单，在当时的环境下，网络的安全性未能引起人们的足够的关注。随着信息技术的迅猛发展，特别是进入二十一世纪的近几年，网络正在以惊人的速度改变着人们的工作效率和生活方式，从各类机构到个人用户都将越来越多地通过各种网络处理工作、学习、生活方方面面的事情，网络也将以它快速、便利的特点给社会、个人带来了前所未有的高效速度，所有这一切正是得益于互联网络的开放性和匿名性的特征。在此背景下发展起来的园区网络，由于其开放性和匿名性的特征，不可避免地存在着各种各样的安全隐患，若不解决这一系列的安全隐患，势必对园区网的应用和发展，以及网络用户的利益造成很大的影响。

本章主要介绍园区安全性方面存在的隐患及其相应的解决方法，也就是通过交换机端口安全、路由器配置访问控制列表 ACL、防火墙包过滤技术来实现。

7.1 园区网安全隐患

网络安全的隐患是指计算机或其它通信设备利用网络进行交互时可能会受到的窃听、攻击或破坏，它是指具有侵犯系统安全或危害系统的潜在的环境、条件或事件。计算机网络和分布式系统很容易受到来自非法入侵者和佥用户的威胁。

7.1.1 园区网常用安全隐患

园区网安全隐患包括的范围比较广，如自然火灾、意外事故、人为行为（如合用不当、安全意识差等）、黑客行为、内部泄密、外部泄密、信息丢失、电子监听（信息流量分析、信息窃取等）和信息我　战等。所以，对网络安全隐患的分类方法也比较多，如根据威胁对象可分为对网络数据的威胁和对网络设备的威胁；根据来源可　分为内部威胁和外部威胁。

安全隐患的来源一般可分为　以下几类：

1）非人为或自然力造成的硬件故障、电源故障、软件错误、火灾、水灾、风暴和工业事故等。

2）人为但属于操作人员无意的失误造成的数据丢失或损坏。

3）来自园区网外部和内部人员的恶意攻击和破坏。

其中安全隐患最大的是第三类。外部威胁主要来自一些有意或无意的对网络的非法访问，并造成了网络有形或无形的损失，其中的黑客就是最典型的代表。

还有一种网络威胁来自园区网系统内部，这类人熟悉网络的结构和系统的操作步骤，并拥有合法的操作权限。中国首例“黑客”操纵股价案例便是网络案例隐患中策略失误和内部威胁的典型实例。

7.1.2 常见解决隐患的方案

为了防止来自各方面的园区网安全威胁的发生，除进行宣传教育外，最主要的就是制定一个严格的安全策略，这也是网络安全中的核心和关键。

但是由于我国的信息安全技术起步晚，整体基础薄弱，特别是信息安全的基础设施和基础部件几乎全部依赖国外技术。所以，我国的网络安全产品，总的来说是自主开发少，软硬件技术受制于人。近几年来，我国的信息技术得到了迅猛发展，国家性的一些关键部门，如银行和电信等，很多都采用了国外的信息产品特别是操作系统、数据库和骨干网络设备。这些部门要么采用国外的产品，要么就根本不采用任何安全措施，这些都给国家安全和人们的日常生活留下了严重的安全隐患。

现在，我国的网络信息安全领域也得到了迅猛的发展，除了专注于安全产品研发的公司外，国产化的网络设备供应商也越来越重视新产品安全功能的应用。在国内公司开发　的新产品中都注重了网络安全的应用，可以通过交换机端口安全、配置访问控制列表 ACL、在防火墙实现包过滤等技术来实现一套可行的园区网安全解决方案。

7.2 交换机端口安全

7.2.1 交换机端口安全概述

网络的交换机有些有端口安全功能，利用端口安全这个特性，可以实现网络接入安全，具

体可以通过限制允许访问交换机上某个端口的 MAC 地址以及 IP 地址（可选）来实现严格控制对该端口的输入。当你为安全端口打开了端口安全功能并配置了一些安全地址后，除了源地址为这些安全地址的包外，这个端口将不转发其它任何包。此外，你还可以限制一个端口上能包含的安全地址最大个数，如果你将最大个数设置为 1，并且为该端口配置一个安全地址，则连接到这个端口的工作站（其地址为配置的安全地址）将独享该端口的全部带宽。

为了增强安全性，你可以将同 MAC 地址和 IP 地址绑定起来作为安全地址。当然你也可以指定 MAC 地址而不绑定 IP 地址，。

如果一个端口被配置了一个安全端口，当其安全地址的数目已经达到允许的最大个数时，如果该端口收到一个源地址不属于端口上的安全地址的包时，一个安全违例将产生。当安全违例产生时，你可以选择多种方式来处理违例，例如丢弃收到的报文，发送违例通报或关闭相应端口等。

当设置了安全端口上安全地址的最大个数后，可以使用下面几种方式加满端口上的安全地址：

可以使用接口配置模式下的命令 switch port-security mac-address *mac-address* 来手工配置端口的所有安全地址。

也可以让该端口自动学习地址，这些自动学习到的地址将变成该端口上的安全地址，直到达到 IP 最大个数。需要注意的是，自动学习的安全地址均不会绑定地址，如果在一个端口上，你已经配置了绑定 IP 地址的安全地址，则将不能通过自动学习来增加安全地址。

也可以手工配置一部分安全地址，剩下的部分让交接交换机自己学习。

当违例产生时，可以设置下面几种针对违例的处理模式：

Protect 当安全地址个数满后，安全端口将丢弃未知名地址（不是该端口的安全地址中的任何一个）的包。

RestrictTrap 当违例产生时，将发送一个 Trap 通知。

Shutdown 当违例产生时，将关闭端口并发送一个 Trap 通知。

7.2.2 端口安全的默认配置

端口安全的具体内容有四项，它的默认配置如表 7-1 所示。

表 7－1 端口安全的默认设置

内容	设置
端口安全开头	所有端口均关闭端口安全功能
最大安全地址个数	128
安全地址	无
违例处理方式	保护（protect）

7.2.3 配置端口安全的限制

配置端口安全时有如下一些限制：

■一个安全端口不能是一个 aggregate port；

■一个安全端口只能是一个 access port 。

一个千兆接口上最多支持 20 个同时申明 IP 地址和 MAC 地址的安全地址。另外，由于 这种同时申明 IP 地址和 MAC 地址的安全占用的硬件资源与 ACL 等功能所占用的系统硬件资源共享，因此当您在某一端口上应用了 ACL，则相应地该端口上所能设置的申明 IP 地址的安全

地址个数将会减少。

建议一个安全端口上的安全地址的格式保持一致，即一个端口上的安全地址或者全是绑定了 IP 地址的安全地址，或者都是不绑定 IP 地址的安全地址。如果一个安全端口同时包含管两种格式的安全地址，则不绑定 IP 地址的安全地址失效（绑定 IP 地址的安全地址优先级最高），这时如果你想使端口上不绑定 IP 地址的安全地址生效，你必须删除端口上所有的绑定了 IP 地址的安全地址。

7.2.4 配置端口及违例处理方式

从特权模式开始，可以通过以下步骤来配置一个安全端口和违例处理方式：

1） configure terminal

2） interface interface-id

3） switchport modes access 设置接口为 access 模式。

4） switchport port-security 打开该接口的端口安全功能。

5） switchport port-security maxinum *value* 设置接口上安全地址的最大个数，范围是 1－128，默认是 128。

6） switchport port-security violation{protect|restrict|shutdown} 设置处理违例的方式：

Protect 保护端口，当安全地址个数满后，安全端口将丢弃未知名地址（不是该端口的安全地址中的任何一个）的包。

RestrictTrap 当违例产生时，将发送一个 Trap 通知。

Shutdown 当违例产生时，将关闭端口并发送一个 Trap 通知。当端口因为违例而被关闭后，可以在全局配置模式下使用命令 errdisable recovery 来将接口从错误状态中恢复过来。

7） End

8） Show port-security interface[interface-id] 验证你的配置。

在接口配置模式下，你可以使用命令 no switchport port-security 来关闭一个接口端口安全功能。使用命令 no switchport port-security maxinum 恢复默认个数。使用命令 no switchport port-security violation 将违例处理置为默认模式。

下面的例子说明了如何使用 gigabitethernet 1/3 接口上的端口安全功能，设置最大地址个数为 8，设置违例方式为 protect。

```
switch#conf  t
switch(config)# switchport modes access
switch(config)#switchport port-security
switch(config)#switchport port-security maxinum 8
switch(config)#switchport port-security violation protect
switch(config)#end
```

7.2.5 配置安全端口上的安全地址

从特权模式开始，可以通过以下步骤来手工配置一个安全端口上的安全地址。

1） configure terminal

2） interface interface-id

3） switch port-security mac-address mac-address[ip-address ip-address] 手工配置接口上的安全地址。ip-addree：可选 IP 为这个安全地址绑定的地址。

4） End

5） Show port-security address 验证你的配置。

在接口配置模式下，你可以使用命令 no switchport port-security mac-address mac-address 来删除该接口的安全地址地

下面的例子说明了如何为接口 gigabitethernet 1/3 配置一个安全 MAC 地址：00d0.f800.073c，并为其绑定一个地址 IP：192.168.12.202。

```
switch#conf t
switch(config)# interface gigabitethernet 1/3
switch(config-if)# switchport modes access
switch(config-if)#switchport port-security
switch(config-if)#switchport port-security mac-address 00d0.f800.073c ip-address 192.168.12.202
switch(config-if)#end
```

7.2.6 配置安全地址的老化时间

你可以为一个接口上的所有安全地址配置老化时间。打开这个功能，你需要设置安全地址的最大个数，这样，你就可以让交换机自动的增加和删除接口上的安全地址。

从特权模式开始，可以通过以下步骤来配置一个安全端口和违例处理方式：

1） configure terminal

2） interface interface-id

3） switchport port-security aging{static|time time}

static:加上这个关键字，表示老化时间将同时应用于手工配置的安全地址和自动学习的地址，否则只应用于自动学习的地址。Time：表示这个端口上安全地址的老化时间，范围是 0－1440，单位是分钟。如果设置为 0，则老化功能实际上被关闭。老化时间按照绝对的方式计时，也说是一个地址成为一个端口的安全地址后，经过 Time 指定的时间后，这个地址就将被自动删除。Time 的默认值为 0。

4） End

5） Show port-security interface[interface-id] 验证你的配置。

可以在接口配置模式下，使用命令 no switchport port-security aging time 来关闭一个接口的安全地址老化功能（老化时间为 0）。使用命令 no switchport port-security aging static 来使老化时间仅应用于动态学习到的安全地址。

下面的例子说明了如何配置一个接口 gigabitethernet 1/3 上的端口安全的老化时间，老化时间设置为 8 分钟，老化时间应用于静态配置的安全地址。

switch#conf t

switch(config)# interface gigabitethernet 1/3

switch(config-if)#switchport port-security aging time 8

switch(config-if)#switchport port-security aging static

switch(config-if)#end

7.2.7 查看端口安全信息

从特权模式开始，可以通过以下步骤来查看端口安全信息：

show port-security interface[interface-id] 查看接口的端口安全配置信息。

show port-security address 查看安全地址信息

show port-security [interface-id] address 显示某个接口上的安全地址信息。

show port-security 显示所有安全端口的统计信息，包括最大安全地址数，当前安全地址数以及违例处理方式等。

下面的例子显示了接口 gigabitethernet 1/3 上的端口安全配置：

switch# show port-security interface gigabitethernet 1/3

interface:Gi1/3

port security:Enabled

port status:down

violation mode:shutdown

Maxinum MAC Address:8

Total MAC Address:0

configured MAC Address:0

Aging time:8 mins

secureStatic address aging:Enabled

下面的例子显示了系统中的所有安全地址：

switch# show port-security address

Vlan	Mac Address	IP Address	Type	Port	Remaining Age(mins)
1	00d0.f800.073c	192.168.12.202	configured	Gi1/3	8
1	00d0.f800.3cc9	192.168.12.5	configured	Gi1/1	7

也可以只显示一个接口上的安全地址，下面的例子显示了接口 gigabitethernet 1/3 上的安全地址：

switch# show port-security address interface gigabitethernet 1/3

Vlan	Mac Address	IP Address	Type	Port	Remaining Age(mins)
1	00d0.f800.073c	192.168.12.202	configured	Gi1/3	8

下面的例子显示的是安全端口的统计信息：

switch# show port-security

Secure Port	MaxSecureAddr(count)	CurrentAddr(count)	Security Action
Gi1/1	128	1	Restrict
Gi1/2	128	0	Restrict
Gi1/3	8	1	Protect

7.3 在路由器中配置访问控制列表 ACL

7.3.1 访问控制列表 ACL 概述

访问控制列表 ACL（Access Control List）最直接的功能便是包过滤。通过接入控制列表可以在路由器、三层交换机上进行网络安全属性配置，可以实现对进入到路由器、三层交换机的输入数据流进行过滤。

认证输入数据流的定义可以基于网络地址、TCP、UDP 的应用等。可以选择对于符合过滤标准的流是丢弃还是转发，因此必须知道网络是如何设计的，以及路由器接口是如何在过滤设备上使用的。要通过 ACL 配置网络安全属性，只有通过命令来完成配置，无法通过 SNMP 来完成这些设置。

7.3.2 访问控制列表的类型

访问控制列表的类型主要分为 IP 标准访问控制列表和 IP 扩展访问控制列表，主要动作为允许（Permit）和拒绝（Deny），主要的应用方法是入栈应用（In）和出栈应用（Out）。

1. 基于编号的访问控制列表

在路由器上可配置编号的访问控制列表。

1）IP 标准访问控制列表（Standard IP ACL）

标准访问控制列表是对基本 IP 数据包中的 IP 地址（源地址）进行控制，所有的访问控制列表都是在全局配置模式下生成的。

IP 标准访问控制列表的格式为：

access-list *listnumber* {permit|deny} *address* [*wildcard-mask*]

例如：

(config)#access-list 2 permit 172.16.0.0　0.0.255.255

(config)#access-list 2 Deny 192.168.10.0　0. 0.0.255

2）IP 扩展访问控制列表（Extended IP ACL）

扩展访问控制列表不仅可以对源 IP 地址加以控制，还可以对目的地址、协议以及端口号进行控制。

扩展访问控制列表的格式为：

access-list *listnumber* {permit|deny} *protocol SourceAddress source-wildcard-mask* DestinationAddress *destination-wildcard-mask [operator operand]*

其中：

listnumber：表示规则序号，范围是 100－199；

protocol: 表示指定的协议，主要是 TCP、UDP、IP；

SourceAddress：表示源地址；

source-wildcard-mask：表示源地址的反掩码；

DestinationAddress：表示目的地址；

destination-wildcard-mask：表示目的地址的反掩码；

operator operand：表示端口范围，默认为全部端口号 0－65535。

2. 基于命名的访问控制列表

在三层交换机上配置命名的 ACL，可以采用创建 ACL、接口上应用 ACL、查看 ACL 这三个步骤进行。

在特权配置模式，可以通过如下步骤来创建一个 Standard IP ACL

1) conf t
2) ip access-list standard {*name*} 用名字来定义一条 Standard IP ACL 并进入 access-list 配置模式。
3) deny { *SourceAddress source-wildcard-mask|host-source|any*} 或 permit { *SourceAddress source-wildcard-mask|host-source|any*}

   其中：

   host-source：表示一台源主机，其 *source-wildcard-mask* 为 0.0.0.0；

   *any:*表示任意主机，即 *SourceAddress* 为 0.0.0.0， *source-wildcard-mask* 为 255. 255. 255. 255
4) show access-list [*name*]显示接入控制列表，如果你不指定 access-list 和 name 参数，则显示所有该接入控制列表。

在特权配置模式，可以通过如下步骤来创建一个 Extended IP ACL

1) conf t
2) ip access-list extended {*name*} 用名字来定义一条 Extended IP ACL 并进入 access-list 配置模式。
3) {deny|permit} protocol { *SourceAddress source-wildcard-mask|host-source|any*}[operator port]
4) { DestinationAddress *destination-wildcard-mask|host-destination|any*}[operator port]
5) show access-list [*name*]显示接入控制列表，如果你不指定 access-list 和 name 参数，则显示所有该接入控制列表。

7.4 防火墙基础

7.4.1 防火墙概述

在网络时代，当一个网络接入 Internet 以后，它的用户就可以与外部世界相互通信。为安全起见，人们在该网络和 Internet 之间插入一个中介系统，竖起一道安全屏障。这道屏障作为扼守本网络的安全和审计的关卡，可以阻断来自外部世界的威胁和入侵，这种中介系统也叫防火墙或防火墙系统。

当园区网连接到 Internet 上时，防止非法入侵、确保园区内部网络的安全至关重要。最有效的防范措施是在园区内部网络和外部网络之间设置一个防火墙，实施网络之间的安全访问控制，以确保园区内部网络的安全。防火墙是一种综合性的技术，它涉及计算机网络技术、密码技术、安全技术、软件技术、安全协议、网络标准化组织（ISO）的安全规范以及安全操作系统等多方面。防火墙是用一个或一组网络设备，在两个或多个网络间加强访问控制，以保护一个网络不受来自另一个网络攻击的安全技术。它是一种非常有效的网络安全技术。在 Internet 上，通过它来隔离风险区域（即 Internet 或有一定风险的网络）与安全区域（内部网，如 Intranet）的连接，但不妨碍人们对风险的访问。防火墙可以监控进出网络的通信数据，从而完成仅让安全和核准的信息进入，同时又抵制对园区网构成威胁的数据进入的任务，包过滤便是有效的实

现方法。

防火墙作为不同网络或网络安全域之间信息的出入口，能根据企业的安全策略控制出入网络的信息流，且本身具有较强的抗攻击能力。它是提供信息安全服务，实现网络和信息安全的基础设施。在逻辑上，防火墙是一个分离器、限制器和分析器，可以有效监控内部网和 Internet 的任何活动，以保证内部网络的安全。防火墙通常是放在外部因特网和内部网络之间，以保证内部网络的安全。因此，防火墙的作用是防止不希望的、未授权的通信进出被保护的网络，迫使单位强化自己的网络安全政策。一般的防火墙都可以达到以下目的：一是可以限制他人进入内部网络，过滤掉不安全服务和非法用户；二是防止入侵者接近你的防御设施；三是限定用户访问特殊站点；四是监视 Internet 安全提供方便。由于防火墙假设了网络边界和服务，因此可以看成相对独立的网络，例如 Intranet 等种类相对集中的网络。防火墙正在成为控制对网络系统访问的非常流行的方法。事实上，在 Internet 上的 Web 网络中，超过三分之一的 Web 网站都是由某种形式的防火墙加以保护，这是对黑客防范最严、安全性较强的一种方式，任何关键性的服务器，都建议放在防火墙之后。

7.4.2 防火墙的结构

目前防火墙从结构上讲，可分为两种：

1）应用网关结构

内部网络<->代理网关（Proxy Gateway）<->Internet

2）路由器加过滤器结构

内部网络<->过滤器（Filter）<->路由器（Router）<->Internet

总的说来，应用网关结构的防火墙系统在安全控制方面更加细致，多数基于软件系统，用户界面更加友好，管理控制较为方便；路由器加过滤器结构的防火墙系统多数基于硬件或软硬件结合，速度比较快，但是一般仅控制到第三层和第四层协议，不能细致区分各种不同业务；有一部分防火墙结合了包过滤和应用网关两种功能，形成复合型防火墙，具体使用防火墙则应该根据本企业实际情况加以选择。

7.4.3 防火墙的基本类型

如今市场上的防火墙多种多样，有以软件形式运行在普通计算机之上的，也有以固件形式设计在路由器之中的。总的说来可以分为三种：包过滤防火墙、应用代理（网关）防火墙和基于状态检查的包过滤防火墙。

1）包过滤防火墙

工作在 OSI 的 L3，常见的路由器、通过 ACL 处理 IP 包头。

无法对数据包及上层的内容进行检查，因此无法过滤审核数据包的内容。

不能对数据传输状态进行判断。

所有可能用到的端口都必须静态放开，极大地增加了被攻击的可能性。

2）应用代理（网关）防火墙

基于软件的防火墙，工作在 OSI 的 L7，是中介、代理。

3）基于状态检查的包过滤防火墙

在 OSI 底层对接收到的数据包进行审核，当收到的数据包符合访问控制要求时，将该数据包传送到高层进行应用级别和状态的审核，如果不符合要求，则丢弃。

7.4.4 防火墙的初始配置

本节以锐捷 RG-WALL 150 防火墙为例，介绍 RG-WALL 系列防火墙的初始配置。将 PC 的 COM1 口连接到防火墙的 Console 口，并将 PC 机网卡连接到防火墙的 Forcethernet 口，然后进行配置。

在初始设置过程中，首先通过防火墙的控制口(Console)登录进入防火墙进行一些初步设置，然后启动已注册管理员的 PC 的浏览器(Web Browser)，在地址栏中输入 RG-WALL 的内网接口 IP 地址，由此可进入防火墙的图形化配置界面，对防火墙估进一步的配置。具体的配置如下例所示。

1. 登录防火墙

```
****************************************
**RG-OS V1.0       http://www.red-giant.com.cn**
****************************************
RG-Wall-150 login :   root
Password : rg-wall123
```

以上是系统的默认 ID 和口令值

```
/ >si
```

按任意键进入默认设置阶段，设置系列号、feature code 以及授权号。

RG-WALL 的第一步系统将提示输入系列号、feature code 以及授权号。按照“产品使用授权书”上提供的信息输入序列号，区分大小写。序列号的格式以 SW-xx-xxxxx 以及 SK-xx-xxxxx 输入，例如：

SW-03-91004

输入完序列号再输入 feature code 的内容，feature code 是设置 RG-WALL 可使用功能的编码（厂商提供的 16 位编码）。授权号与序列号和 feature code 相同。

2. 选定路由模式或网桥模式

按任意键继续。下一阶段将决定 RG-WALL 在安装网络中要起的作用。并且这一阶段的选择决定以后的设置工作。在这里将说明路由模式下的设置方法。

在最后的输入提示中键入“P/p”时将取消当前设置和之前阶段的设置，进入前一个设置阶段。键入“C/c”时将取消当前设置的内容，重新开始当前设置过程。输入任意键将应用当前设置内容并进入下一个阶段。这些设置阶段的取消以及移动的方法在其他安装步骤中也相同。

3. 输入管理员 ID 和密码

完成防火墙模式设置以后，输入要启用的管理员 ID 和密码。这里的主管理员表示带有停止/启动系统的、授权其他管理员权限的主要系统负责人员。默认将 admin 作为管理员帐号，管理员密码必须是英文和数字的混合格式并且必须大于 6 个字。如输入密码：admin123。两次密码输入完全匹配时才可以进入下一步操作。

4. 设置系统名称以及语言

接下来输入系统名称，例如：Host.firewall.com。

下一阶段选择 CLI Terminal 识别的语言，默认值是中文。

5. 设置时间

下一阶段是设置系统时间。所有的日志和报表以及计划任务的作业都会根据这里设置的时间来形成，因此必须正确设置当前时间。

选择[0]进入下一个阶段。

6. 指定管理员 PC 的 IP 地址

要 RG-WALL 的 GUI 和 CLI 必须注册管理员 PC 的 IP 地址。管理员的 IP 地址最多可以输入 10 个并且每个 IP 地址之间用“,”和空格隔开。例如：192.168.1.1, 192.168.1.2。输入完管理员 IP 地址进入下一阶段。

以下的步骤基本上都可以通过进入防火墙的图形化配置界面后进行配置。

7. 网络接口构成

为了使 RG-WALL 的网络连接正常必须按照计划书的方案分配各接口地址。各接口　的区域分配可以修改，但是必须设置 Internal 和 External 并且启用 HA 时也必须设置 HA Link。

8. VLAN 构成

如果要构成 VLAN 并通过 802.1Q 方式访问时必须设置各 VLAN 的 IP 地址以及子网掩码和 MTU 信息。RG-WALL 共提供 6 个 VLAN 接口。设置完 VLAN 后选择[0]进入下一个阶段。

输入 VLAN 设置的接口号开始设置 VLAN。

9. Static Route

如果计划在路由模式下启用 OSPF 可以跳过这一阶段进入下一个 OSPF 设置阶段，或者以后 WEB 方式设置。

10. 设置 OSPF

路由模式下可以设置该值，或者以后通过 WEB 方式设置。

11. 设置 HA Zone

架设路由模式下高可用结构时首先要确定是否启用虚 IP 地址、配置什么样的虚 IP 以及是否使用 4 层交换机来实现高层同步模式。

在此输入组成 HA Zone 的 RG-WALL 组名。默认值为 Default。

12. 设置虚 IP 地址

首先构成 VIG（Virtual Interface Group）。选择[2]可以确认当前的 VIG 以及各接口的虚 IP 地址信息。

13. 设置 DNS

在此输入域名，输入完成按回车键进入下一阶段。

14. 选择基本规则

最后一个阶段是设置初始规则阶段。在这个阶段选择需要的基本规则即可，基本设置完毕后通过 GUI 进一步设置。

15. 应用系统设置

基本安装设置已经完成，按任意键重新启动系统的同时应用当前设置。重新启动后出现登录画面，登录操作系统。这时会出现 RG-WALL 的登录提示符。

登录 RG-WALL 系统后出现 CLI 基本菜单。继续通过 CLI 进行作业可以选择[2]或者[3]。

16. Reinstall

RG-WALL 的重新安装提供了路由模式设置和网桥模式设置中的所有设置项。

在 CLI 命令提示符上输入 reinstall 重新设置系统。

17. 确认安装是否正常

进入 RG-WALL CLI 模式并输入以下命令:

[admin:E:W] RG-WALL>ping “与各接口连接的对方设备 IP 地址”

邻接网络设备的 ping 测试成功以后可以再测试 ping 管理员 PC、DMZ 的主要服务器以及外网常用的 IP 地址。

18. GUI 安装

RG-WALL 的 GUI 通过 JAVA 技术实现，因此兼具客客户端软件管理方式和 WEB 浏览器管理方式的优点，支持多种语言，与管理工作站的操作系统无关。

为了运行 JAVA 类程序，管理员工作站需要具备 SUN 公司的免费软件 Java Runtime Environment(JRE)。这一插件可以通过 RG-WALL 的 WEB 管理界面安装。

在管理员工作站上启动 WEB 浏览器后，在地址栏中输入 RG-WALL Internal 接口的 IP 地址。

注意：在初始配置中，关键是要设置管理员 ID、密码和 IP 地址，并设置至少一个接口的 IP 地址，其余配置可以在进入 WEB 配置界面后设置。

第8章　　常见网络故障分析及处理

对于以太网故障，根据经验大多数的网络故障都与硬件有关，例如电缆、中继器、HUB、Switch 和网卡等。对于以太网典型故障的查找，一般过程如下:

(1) 收集一切可以收集到的有价值的信息,分析故障的现象.

(2) 将故障定位到莫一特定的网段,或者单一独立动能组(模块),也可以是某一用户.

(3) 确定到底是属于特定的硬件故障还是软件故障.

(4) 动手修复故障.

(5) 验证故障确实被排除.

一般来说,最好的方法是先把故障细分或隔离在一个小的功能段上,即首先排除最大的简单段,从任何一个方便的,靠近问题的站点出发,利用二分法隔离障碍,再继续使用二分法直至把故障划分到最小的单位.网管人员不要过多的指望用户会给出准确的故障情况描述,最好由自己亲自来确认一下当然也可以由用户演示所发现的问题。由于网络故障带来的压力和混乱，人们经常忽略一些细节问题。如果某个部件出了问题，最好不要立即去替换它，除非能肯定故障的来源。

故障查找要注意一些事项，由于以太网采用通用总线拓扑结构以及物理层可扩展的潜在问题，所以某个特定物理层的问题会以不同的方式显现出来，由于采用的测试手段、位置和环境不同，显示出的现象也常常矛盾。

为了避免被假象误导，应按以下两个故障查找步骤操作：

1）沿网段多做测试，如果故障现象随测试点的不同还保持一样，就可以依照所测试出来的故障现象去排除。如故障现象在一些或所有的测试点都不同，就要把查找故障的方向定在物理层（除非有特别提示），例如查找坏的电缆、噪声环境、接地循环等故障。

2）提高测试质量，在测试的同时，要把测试仪器设置成至少可同时发送较低的流量。

8．1 物理层故障分析与处理

1．本地故障

在进行硬件故障查找之前，要确定其他用户也不能到这台机器上，这就排除了用户帐号的错误。对一个单一的站点来说，典型的故障多发生在坏的电缆、坏的网卡、驱动软件、或是工作站设置的不正确等问题上。

2．电缆连接问题

目测连接性：检查连接性常见的方法就是检查 HUB、收发器以及近期出产的网卡上的状态灯。如果是 10Base5 的电缆，要检查所有的 AUI 电缆是否牢固的连接，划锁要同时锁牢，很多问题只要简单的把未接牢的部分重新紧一下就解决了。

受损的电缆或连接部件：在检查物理层的问题时要注意受损的电缆、当前任务使用的电缆方式（必须正确地使用交叉、全反连接以及直通连接方式的电缆）电缆的终端方式是否不对、未打好的 RJ-45 水晶头或未接牢的 BNC 头。没有接上电缆，电缆链接到了错误的端口上等。对怀疑有问题的电缆可以用一般的电缆测试仪进行测试。

（1）劣质网线导致动作站无法接通

为了降低信号的干扰，双绞线电缆中的每一线对都是由两根绝缘的通道线相互扭绕而成，而且同一电缆中的不同线对扭绕的圈数是不一样的。在绕线方向上标准双绞线电缆中的线对是按逆时针方向扭绕的。不合标准的线缆会引起双绞线之间的相互干扰，从而使传输距离达不到要求。

（2）不正确的网线线序造成上网不正常

按照 568B 标准制作的网线对电磁干扰的屏蔽更好，这种接法也称为 100m 接法，是指它能满足 100m/s 带宽的通信速率。100m/s 网线未按照 568B 标准制作网线接头，网线的外皮与水晶头没有紧密衔接，线缆松散，造成传输的数据帧出错上网不正常。

（3）五类双绞线强行运行在千兆以太网上从而影响连通性

理论上五类双绞线可以运行在千兆以太网上的。但实际上在五类双绞线上运行千兆以太网经常出现断续或连接不上。说明千兆以太网对五类双绞线的参数要求更为严格。如需要在五类双绞线上运行千兆以太网（将 100m/s 以太网升级为千兆以太网，又不想重新布线），则必须对五类双绞线进行严格的测试（按国际 cat-5n 标准），如果测试合格，可以在五类双绞线上运行千兆以太网。否则必须使用超五类线来运行千兆以太网。

（4）双绞线的连接距离

双绞线的标准连接长度一直被确定为 100m ,但在五类和超五类双绞线出现后，一些网络制造商在自己的产品宣传资料中称自己的双绞线或 HUB 实际的连接距离可以超过 100m，一般能达到 130~150m 左右。虽然有这种产品可以达到，但值得注意的是，即使一些双绞线能够在大于 100m 的状态下工作，但其通信能力将会大打折扣，甚至可能会影响网络的稳定性，一定要慎用。

8．2 数据链路层故障分析与处理

8.2.1 检查链路层的问题

碰撞问题：如果平均碰撞率大于 10%或者观察到非常高的碰撞，就需要进一步的测试了。如果可能，试着通过减少网段规模（将网络分成小块）并随时检测碰撞的变化以隔离出发生问题的区域。为了追踪碰撞情况，就必须知道网络的流量。可以使用背景流量发生器来加入适当的流量（100 帧/秒，100 字节长的流量），并同时观察网络的统计显示。某些与介质有关的故障是与流量的大小成正比的。可以在用控制键改变流量同时观察碰撞与错误的改变。这种做法要特别小心，因为很容易给网络加入很重的流量。解决与碰撞有关的问题常常是很费劲的，因为测试的情况在很大程度上取决于观察的位置。也许在同一网段相距几尺远的不同观察点看到的情况就不同，要多找几个点来观察并留意所发生的变化。

如果碰撞和流量成正比，或碰撞几乎是 100%，或几乎没有正常的流量，则可能是布线系统出了问题。对于 UTP 布线可以在 HUB 上端开电缆然后进行电缆测试。对于铜轴电缆就要进行阻抗测试，可以使用数字表或其他仪表的直流通断功能进行测试。如果电缆两端都有端接器，从 t 型接头应测的大约 25 欧姆，如果从电缆的一端将会测的 50 欧姆。

帧级错误：如果出现帧级错误，就要运行错误统计测试，并通过详细功能把有问题的工作站的 MAC 地址找出，然后经过测试把故障确定下来。可以试着将驱动程序用“干净”的原盘重新装入工作站，要确认各项配置安全。如果这一切仍不奏效，可以使着把有疑问的网卡换掉。

利用率过高：如果利用率过高（平均值大于 40%，瞬间峰值高于 60%），那么网段负荷就过重了。因当考虑安装网桥和路由器以减少在网段中的流量或把网段分成若干小的网段。

8.2.2 故障检查过程

1．有故障时首先检查网卡

在局域网中，网络不通的现象常有发生，一旦遇到类似这样的问题时，我们首先因该认真检查各联入网络的机器中，网卡设置是否正常。检查时，我们可以用鼠标依次打开“控制面板/系统/设备管理器/网络适配器”设置窗口，在窗口中检查一下有无中断号及 I/O 地址冲突（最好把各台机器的中断设为相同，以便于对比），直到网络适配器的属性中出现”该设备运转正常“，并且在”网上邻居“中至少能找到自己，说明网卡的设置没有问题 。

2．确认网线和网络设备工作正常

当检查网卡没有问题时，此时可以通过网上邻居来看看网络中的其他计算机，如果还不能看到网络中的其他机器，这种情况说明可能是由于网络连线中断的问题。网络连线故障通常包括网络线内部断裂、双绞线、RJ-45 水晶头接触不良，或者网络连接设备本身质量有问题，或者连接有问题。这时，我们可以用测线仪来检查一下线路是否断裂，然后用替代的方法来测试一下网络设备的质量是否有问题。在网线和网卡本身都没有问题的情况下，我们再看看是不是软件设置方面的问题，例如如果中断号不正确也有可能导致故障出现。

3．检查驱动程序是否完好

对硬件进行检查和确认后，再检查驱动程序本身是否损害，如果没有损害，看看安装是否正确。如果这些可以判断正确，设备也没有冲突，就是不能连入网络，这时候可以将网络适配器在系统配置中删除，然后重新启动计算机，系统就会检测到新硬件的存在，然后自动寻找驱动程序再进行安装。

4．正确对网卡进行设置

在确定网络介质没有问题，但还是不能接通的情况下，再返回网卡设置中。看看是否有设备资源冲突，在许多时候冲突也不是都有提示的。可能发生的设备资源冲突有：NE2000 兼容网卡和 COM2 有冲突，都使用 IRQ3,（Realtek RT8029）PCI Ethernet 网卡和显卡都“喜欢”IRQ10。为了解决这种设备的冲突，可以按照如下操作步骤来进行设置：首先在设置窗口中将 COM2 屏蔽，并强行将网卡中断设为 3；如果遇到 PCI 接口的网卡和显卡发生冲突时，可以采用不分配 IRQ 给显卡的办法来解决，就是将 CMOS 中的 Assign IRQ for VGA 一项设置为 Distable。

8．3 网络层故障分析与处理

网络层常见的故障包括：

1．没有启用路由选择协议，或路由选择协议配置不正确

2．不正确的网络 IP 地址

3．不正确的子网掩码

4．DNS 和 IP 的不正确的绑定

对以上问题，应首先检查并校正本机的 IP 地址和子网掩码、DNS 设置，然后检测本机与网关的连通性、本机与其他网络的连通性，如果不能与其他网络连通，则应检查并纠正路由协议的配置。

8．4 传输层及高层故障分析与处理

8.4.1 协议故障

协议故障通常表现为以下几种情况：

1．电脑无法登录到服务器。

2．电脑在”网上邻居“中既看不到自己，也无法在网络中访问其他电脑。

3．电脑在”网上邻居“中既看到自己和其他电脑，但无法访问其他电脑。

4．电脑无法统过局域网接入 Internet。

故障原因分析：

1．协议未安装，实现局域网通信，需要安装 NetBEUI 协议。

2．协议配置不正确， TCP/IP 协议涉及到的基本参数有 IP 地址、子网掩码、DNS、网关，任何一个设置错误，都会导致故障发生。

排除步骤：

（1） 检查电脑是否安装 TCP/IP 和 NetBEUI 协议，如果没有，建议安装这两个协议，并把 TCP/IP 参数配置好，然后重启系统。

（2） 在控制面板的网络属性中，单击文件及打印共享按钮，在弹出的文件及打印共享按钮对话框中检查一下，看看是否选中了“允许其他用户访问我的文件“和”允许其他用电脑使用我的打印机“复选框，或者其中一个。如果没有，全部选中或选中其中一个，否则将无法使用共享文件夹。

（3） 系统重新启动后，双击“网上邻居”，将显示网络中的其他电脑和共享资源。如果仍看不到其他电脑，可以使用查找命令，能找到其他电脑就可以了。

（4） 在网络属性的标示中重新命名该电脑，使其在网络中具有唯一性。

8.4.2 配置故障

配置错误也是导致故障发生的重要原因之一。网络管理员对服务器、路由器等的不当设置自然会导致网络故障，电脑的使用者对电脑设置的修改，也往往会产生一些令人意想不到的访问错误。

配置故障排错：首先检查发生故障电脑的相关配置。如果发现错误，修改后再测试相关的网络服务能否实现。如果没有发现错误，则测试系统内的其他电脑是否有类似的故障，如果有同样的故障，说明问题出在网络设备上，如交换机。反之，检查被访问电脑对该访问电脑所提供的服务作认真的检查。

故障：不能访问服务器或某项服务。在这里设定服务器或某项服务以前是正常的，并且已经做过如下的工作：

1．重新冷启动 PC 机（热启动不能复位全部的适配卡）。

2．确认 PC 机本身没有硬件故障

3．确认所有的网络电缆都连接正确

4．确认所有的网卡驱动都工作正常，没报告工作错误

5．确认服务器或某项服务没有改变，例如重新配置增加硬件或软件。

要测试一下这一故障是否只影响该工作站（本地故障）还是会影响其他站点（大范围故障），可以通过其他工作站装入服务器或服务来证明这一点。这些工作站要在同一网段或 HUB 上。如果故障在在同一网段或 HUB 上的其他站点也存在，就试着从其他的网段或 HUB 上的站点进行测试。

8.4.3 操作系统故障

操作系统故障也是导致故障发生的主要原因之一。用户对计算机设置的修改或删除，也往往会产生一些令人意想不到的访问错误。

（1）许多机器可以成功登陆网页，但没法浏览信息，或者总是出现“该页无法显示”。
首先应检查 TCP/IP 协议是否已安装，还有其设置是否正确。打开控制面板的网络项，双击 TCP/IP 的属性，检查 IP 地址、DNS、配置、网关等是否设置正确。接着检查 IE 浏览器的“连接”一项，不要设置为用代理服务器连接，如果这么做后，还是无法浏览网页，那肯定是操作系统有问题，这时可考虑重装或修复操作系统和 ie 浏览器。

（2）所有电脑都有“网上邻居”图标，但是打开“网上邻居”后，什么也没有。
这种问题多发生在自己的电脑上，此时可检查设备管理器中的网络适配器属性中的驱动程序是否正常。

（3）服务器或服务的可达性：

如果使用协议分析仪，就要捕获 3~4 分钟的数据包来分析，看一下是否有从服务器发出的延时请求，并找出是哪个服务器发出的，如果有延时请求，则表明服务器不能完全处理所加载的任务，每个延时请求作废一个任务请求。

8.4.4 由于病毒产生的问题

蠕虫病毒对网络速度的影响越来越重。这种病毒导致被感染的用户只要一连上网就不停地

往外发邮件，病毒选择用户个人电脑的随机文档附加在用户机子上的通信簿的随机地址进行邮件发送。造成网络瘫痪，个人电脑无法使用，严重破坏计算机操作系统。因此，我们应时常注意各种新病毒通告，了解各种病毒特性；及时升级所有的杀毒软件。计算机也要及时升级、安装系统补丁程序，以提高系统的安全性和可靠性。

实验一　Frame-relay 交换机

一、实验介绍

1、实验名称：Frame-relay 交换机实验

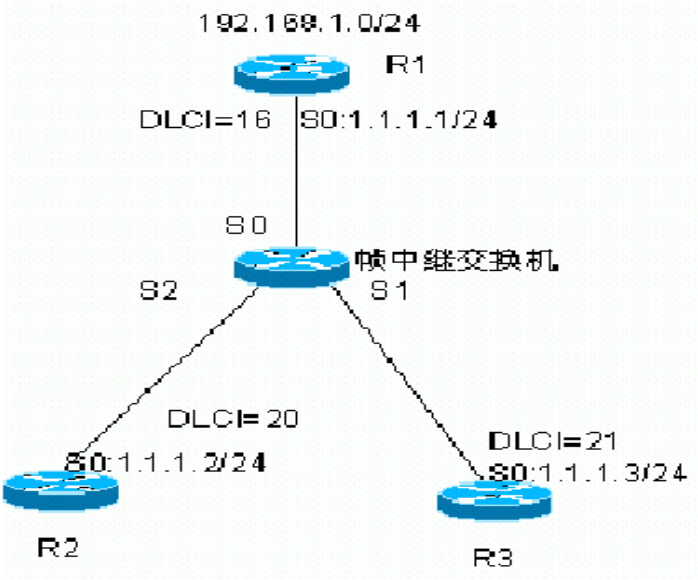
2、实验目的：掌握路由器作为帧中继交换机配置技术

3、实验设备：2621 路由器、V35DCE、V35DTE

4、实验时间：30 分钟

二、实验拓扑

• 连接两个路由器之间的链路称为永久性虚电路（ PVC），一个永久性虚电路在它的每一端包括一个独立的数据链路连接标识（ DLCI: Data Link Connection Identifier）。



拓扑说明：

四台路由器，其中的一台路由器仿真成帧中继交换机，使用帧中继交换的功能。R1 路由器封装帧中继并且用多个 IP 地址静态映射，路由器 R2、R3 在物理层接口上封装帧中继，都工作在 DTE 方式，DLCI 号在 R1 上分别是 16，R2 的 DLCI 号是 20，R3 的 DLCI 号是 21。然后，路由器 R1 将被作为点到多点的帧中继接口。路由器 R2 和 R3 分别映射到中心路由器 R1。

三、帧中继交换机路由器配置

Route(config)#frame-relay switching　允许帧中继交换使能

Red-Giant(config)#**interface serial0**

Red-Giant(config-if)#**encapsulation frame-relay**

Red-Giant(config-if)#**frame-relay intf-type dce**

Red-Giant(config-if)#**frame-relay route** 16 **interface Serial1** 21

Red-Giant(config-if)#**frame-relay route** 17 **interface Serial2** 20

！在串口 serial0 配置层上，首先将封装帧中继，指定封装格式 DCE，然后配置本地的 DCLI 号 16 serial1 的 DCLI 21 进行交换，配置本地的 DLCI 17 和 serial2 的 DCLI 20 进行交换。

Route(config)#**interface Serial1**

Red-Giant(config-if)#**encapsulation frame-relay**

Red-Giant(config-if)#**frame-relay intf-type dce**

Red-Giant(config-if)#**frame-relay route** 21 **interface Serial**0 16

！在接口 seiral1 上，首先配置帧中继接口类型 DCE，然后配置本地的帧中继的 DCLI 号 21 和接口 serial0 的 DCLI 16 进行交换。

Route(config)#**interface Serial2**

Red-Giant(config-if)#**encapsulation frame-relay**

Red-Giant(config-if)#**frame-relay intf-type dce**

Red-Giant(config-if)#**frame-relay route** 20 **interface Serial**0 17!在接口 seiral2 上，首先配置帧中继接口类型 DCE，然后将本地的帧中继的 DCLI 号 20
和接！口 serial0 的 DCLI 17 进行交换。

四、实验配置 R1 路由器配置

R1(config)#interface serial0
R1(config-if)#ip address 1.1.1.1 255.255.255.0
R1(config-if)#encapsulation frame-relay ietf
R1(config-if)#frame-relay map ip 1.1.1.2 16
R1(config-if)#frame-relay map ip 1.1.1.3 17

R2 路由器配置：

R2(config)#interface serial0
R2(config-if)#ip address 1.1.1.2 255.255.255.0
R2(config-if)#encapsulation frame-relay ietf
R2(config-if)#frame-relay map ip 1.1.1.1 20

R3 路由器配置：

R3(config)#interface serial0
R3(config-if)#ip address 1.1.1.3 255.255.255.0
R3(config-if)#encapsulation frame-relay ietf
R3(config-if)#frame-relay map ip 1.1.1.1 21

五、验证命令

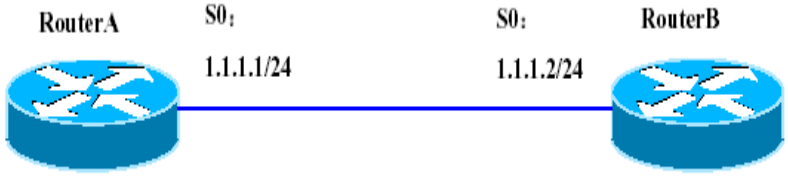
Show frame-relay route
Show frame-relay pvc
Show frame-relay map
Debug frame-relay

实验二　PPP CHAP 实验

一、实验介绍

1、实验名称：PPP CHAP 实验
2、实验目的：掌握路由器 PPP CHAP 认证技术
3、实验设备：R2621 路由器、V35DCE、V35DTE
4、实验时间：30 分钟

二、实验拓扑



拓扑说明：

本实验说明了 PPP CHAP 认证的配置，其中，Router A 为认证方，IP 地址为 1.1.1.1/24,主机名为 RouterA,要求口令为 Router,建立的用户列表中包括 RouterB 的主机名；Router B 为认证方，IP 地址为 1.1.1.2/24,主机名为 RouterB,口令发送为 Router。

三、实验配置

RouterA 配置：

Red-Giant#config terminal

!设置主机名

Red-Giant(config)#hostname RouterA

!设置用户名和密码的列表

RouterA(config)#username RouterB password 0 Router

RouterA(config)#username RouterC password 0 Router

RouterA(config)#interface serial0

!封装协议

RouterA(config-if)#encap ppp

RouterA(config-if)#bandwidth 2000000

RouterA(config-if)#clock rate 64000

!设置 IP 地址

RouterA(config-if)#ip address 1.1.1.1 255.255.255.

RouterA(config-if)#ppp chap hostname RouterA

RouterA(config-if)#ppp chap password 0 Router

RouterB 配置：

Red-Giant(config)#hostname RouterB

!以对方的主机名作为用户名，密码和对方路由器的密码设定的一致

RouterB(config)#username RouterA password 0 Router

RouterB(config)#interface serial0

!封装协议

RouterB(config-if)#encap ppp

RouterB(config-if)#ppp auth chap!设置 IP 地址

RouterB(config-if)#ip address 1.1.1.2 255.255.255.0

四、验证命令

Show interface Serial0

Debug ppp authentication

实验三　PPP PAP 认证

一、实验介绍

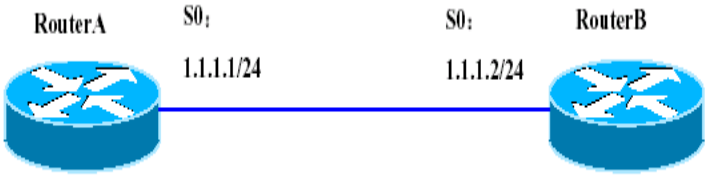
1、实验名称：PPP PAP 认证

2、实验目的：掌握路由器 PPP PAP 认证技术

3、实验设备：R2621 路由器、V35DCE、V35DTE

4、实验时间：30 分钟

二、实验拓扑



拓扑说明：

本实验是 PAP 配置，用户名为 Red-Giant,设定密码 Router，认证方的 IP 地址为 1.1.1.1/24，被认证方的 IP 地址为 1.1.1.2/24，要求设定的用户名和密码和认证方一样。Router A 为被认证方，Router B 为认证方。

三、实验配置

RouterA 配置：

Red-Giant#config terminal

Red-Giant(config)#interface Serial0

!配置 IP 地址

Red-Giant(config-if)#ip address 1.1.1.2 255.255.255.0

!封装 PPP 协议

Red-Giant(config-if)#encapsulation ppp

Red-Giant(config-if)#bandwidth 2000000

Red-Giant(config-if)#clock rate 64000

!设置 PAP 认证的用户名和密码 Red-Giant(config-if)#ppp pap sent-username Red-Giant password 0 Router

RouterB 配置：

Red-Giant#config terminal

Red-Giant(config)#username Red-Giant password 0 Router

Red-Giant(config)#interface Serial0

!配置 IP 地址

Red-Giant(config-if)#ip address 1.1.1.1 255.255.255.0

!封装 PPP 协议

Red-Giant(config-if)#encapsulation ppp

!设定 PPP 的认证方式

Red-Giant(config-if)#ppp authentication pap

四、验证命令

Show interface Serial0

Debug ppp authentication

实验四　RIP 动态路由

一、实验介绍

1、实验名称：RIP 动态路由

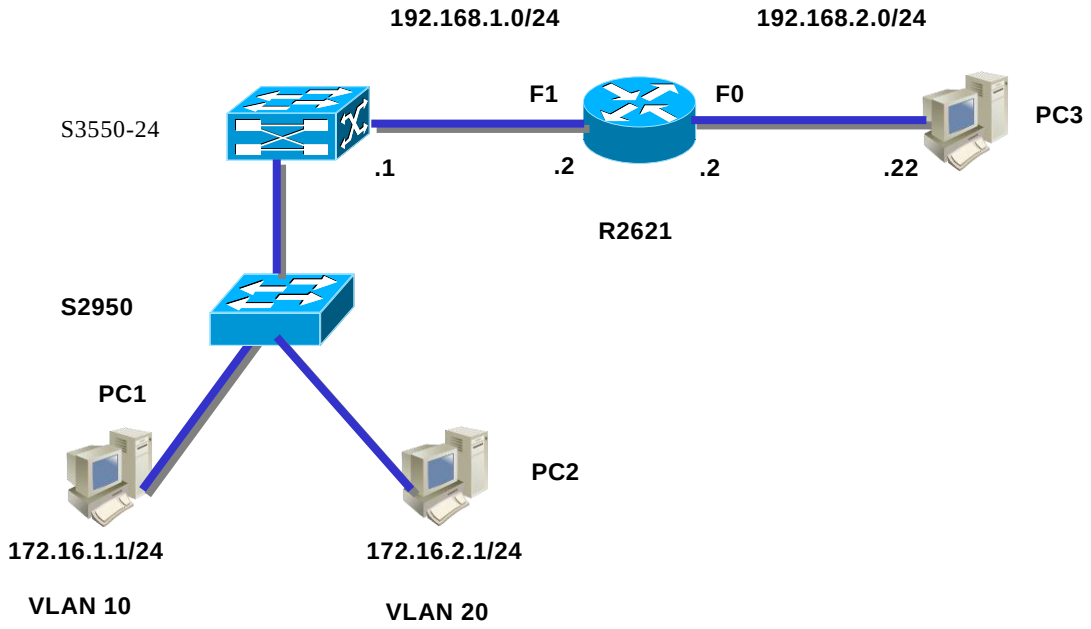
2、实验设备：R2621、S3550-24 与 S2950 各 1 台

3、实验目的：通过 RIP 动态路由，使路由器和三层交换机具有非直连子网的路由信息，进而实现非直连子网的互相通信。

4、实验时间：60 分钟

二、实验拓扑

描述：假设校园网通过交换机 S3550-24 及 S2950 互连，并通过 路由器 R2621 连接到外网的一台主机 PC3，现要实现 PC1 与 PC3 的相互通信。



三、实验理论

1．RIP 动态路由协议工作特点：

1）定期向邻居路由器发送路由表的副本并且计算距离向量。

2）使用 UDP 协议 520 端口发送路由信息。

2．显示路由表的信息：Router#show ip route

四、实验配置

本实验假设已配置了 VLAN 10 和 VLAN 20 ，并对路由器和三层交换机已做了基本配置，以下的配置仅仅列出了路由部分的配置。

路由器 R2621 上的 RIP 路由协议配置：

R2621(config)#router rip

注：启用路由器 R2621 的 RIP 进程

R2621(config-router)#network 192.168.1.0

R2621(config-router)#network 192.168.2.0

注：

1．公布主类网络 192.168.1.0 和 192.168.2.0

2．包含在 192.168.1.0 和 192.168.2.0 主类内的接口发送和接收 RIP 路由信息

三层交换机 S3550-24 上的 RIP 路由协议配置：

S3550(config)#router rip

注：启用 S3550-24 的 RIP 进程

R2621(config-router)#network 192.168.1.0

R2621(config-router)#network 172.16.0.0 注：

1．公布主类网络 192.168.1.0 和 172.16.0.0 及其子网

2．包含在 192.168.1.0 和 172.16.0.0 主类内的接口发送和接收 RIP 路由信息

五、测试结果

1．路由器和三层交换机应该看到全网路由。

2．主机 192.168.2.22 能够访问主机 172.16.1.1。

六、验证命令

- show run
- show int
- show ip int brief
- show ip route
- show ip protocols
- ping

实验五　OSPF 动态路由

一、实验介绍

1、实验名称：OSPF 动态路由

2、实验设备：　R2621、S3550-24 与 S2950 各 1 台

3、实验目的：通过 OSPF 动态路由，使路由器和三层交换机具有非直连子网的路由信息，进而实现非直连子网的互相通信。

4、实验时间：60 分钟

二、OSPF 路由协议简介

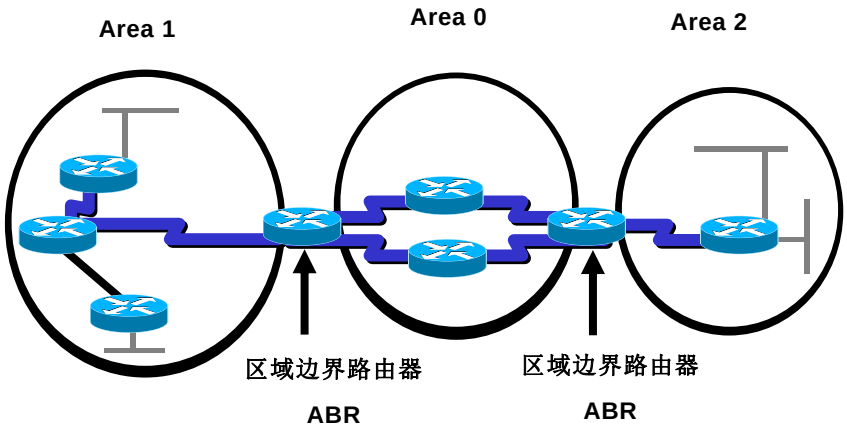
•链路状态路由协议，克服了 RIP 的两个致命弱点：

　　- 收敛速度慢（240 秒以上）

　　- 规模限制，只有 15 跳

•分区域概念：

　　- 骨干区域 Area 0，非骨干区域 Area N



OSPF 基本配置：

•创建 OSPF 路由进程

　　- 每个进程都有个进程号。

•定义与该 OSPF 路由进程关联的 IP 地址范围

　　- 接口 IP 地址落在该地址范围，就属于后面定义的区域。

•该范围 IP 地址所属的 OSPF 区域

三、实验拓扑

本实验的实验拓扑结构与实验四相同。

四、实验配置

本实验假设已配置了 VLAN 10 和 VLAN 20 ，并对路由器和三层交换机已做了基本配置，以下的配置仅仅列出了路由部分的配置。

路由器 R2621 上的 OSPF 路由协议配置：

R2621(config)#router ospf 10

注：启用路由器 R2621 的 OSPF 进程，进程号定义为 10

R2621(config-router)#network 192.168.0.0 0.0.255.255 area 0

注：

1. 定义与该 OSPF 路由进程关联的 IP 地址范围,接口 IP 地址落在该地址范围内，就属于后面定义的区域
2. 定义该范围 IP 地址所属的 OSPF 区域

三层交换机 S3550-24 上的 OSPF 路由协议配置：

S3550(config)#router ospf 50

注：启用路由器 R2621 的 OSPF 进程，进程号定义为 50

R2621(config-router)#network 192.168.0.0 0.0.255.255 area 0

R2621(config-router)#network 172.16.0.0 0.0.255.255 area 0

注：

1. 定义与该 OSPF 路由进程关联的 IP 地址范围,接口 IP 地址落在该地址范围内，就属于后面定义的区域
2. 定义该范围 IP 地址所属的 OSPF 区域

五、验证命令

- show run
- show int
- show ip int brief
- show ip route
- show ip protocols
- ping

实验六　ACL 的应用

一、实验介绍

1、实验名称：ACL 的应用

2、实验设备：R2621、S3550-24 与 S2950 各 1 台

3、实验目的：通过访问控制表 ACL 的设置，掌握 Access-list 表项的设置方法和应用领域。

4、实验时间：60 分钟

二、IP ACL 的基本准则

1) 一切未被允许的就是禁止的。

2) 路由器或三层交换机缺省允许所有的信息流通过；而防火墙缺省封锁所有的信息流，然后对希望提供的服务逐项开放。

3) 按规则链来进行匹配。

4) 使用源地址、目的地址、源端口、目的端口、协议、时间段进行匹配。

5) 从头到尾，至顶向下的匹配方式。

6) 匹配成功马上停止。

7) 立刻使用该规则的“允许、拒绝”。

三、IP 标准访问列表的配置格式

1.定义标准 ACL

基于编号的标准访问列表

Router(config)#access-list <1-99> {permit|deny} 源地址 [反掩码]

基于命名的标准访问列表

ip access-list standard { name}

deny{source source-wildcard|host source|any}or

permit {source source-wildcard|host source|any}

2.应用 ACL 到接口

Router(config-if)#ip access-group <1-99>|{name} { in | out }

四、IP 扩展访问列表的配置格式

1. 定义扩展的 ACL

基于编号的扩展 ACL

Router(config)#access-list <100-199> { permit /deny } 协议 源地址 反掩码 [源端口] 目的地址 反掩码 [目的端口]

基于命名的扩展 ACL

ip access-list extended { name}

{deny|permit} protocol {source source-wildcard |host source| any}[operator port] {destination destination-wildcard |host destination |any}[operator port]

2. 应用 ACL 到接口

Router(config-if)#ip access-group <100-199> { in | out }

下面显示如何创建一条 Extended IP ACL，该 ACL 有一条 ACE，用于允许指定网络（192.168.x..x）的所有主机以 HTTP 访问服务器 172.168.12.3，但拒绝其它所有主机使用网络。

Switch （config）# ip access-list extended allow_0xc0a800_to_172.168.12.3

Switch （config-std-nacl）# permit tcp 192.168.0.0 0.0.255.255 host 172.168.12.3 eq www

Switch （config-std-nacl）#end

Switch # show access-lists

五、访问列表的验证

显示全部的访问列表

Router#show access-lists

显示指定的访问列表

Router#show access-lists <1-199>

显示接口的访问列表应用

Router#show ip interface <接口名称><接口编号>

六、基于时间的 IP ACL

首先需要校正路由器时钟；

定义时间范围，先通过绝对，后判断周期；

absolute — 绝对的时间段

periodic — 周期性时间段

关联 IP ACL 与时间范围

七、实验内容

1. 在下面这个例子中,以太网口 E0 上的 UDP 数据包被限制在 2005 年一月一日上午 8:00 到 2005 年 12 月 31 日下午 6:00 之间的周末(星期六与星期日)可以发送。

配置如下：

```
#interface ethernet 0
#ip access-group 101 out
!
#time-range test
  #absolute start 8:00 1 January 2005 end 18:00 31 December 2005
  #periodic weekends 00:00 to 23:59
!
#access-list 101 permit udp any any time-range test
```

2. 规定：(1)192.168.1.0 网段允许访问 WEB；(2) 192.168.2.0 网段允许访问 WEB 和电子邮件；(3) 192.168.3.0 网段什么都可以做。

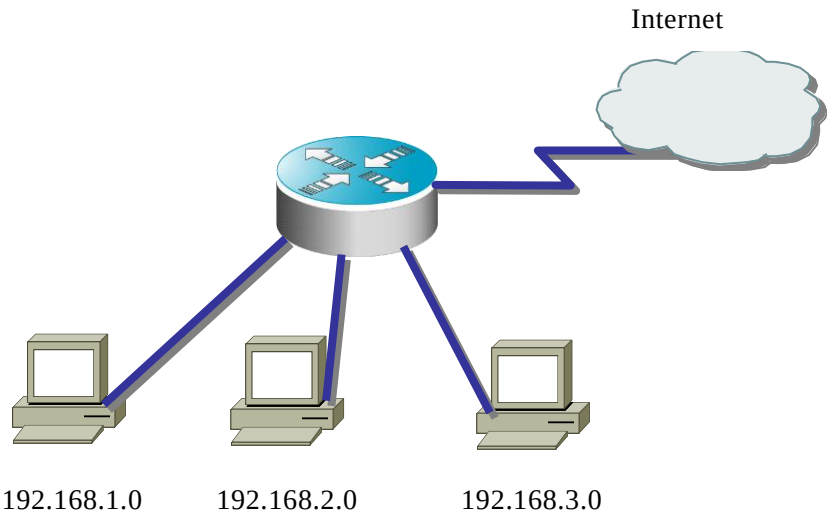
配置如下：

(1)access-list 101 permit tcp 192.168.1.0 0.0.0.255 any eq 80

(2)access-list 101 permit tcp 192.168.2.0 0.0.0.255 any eq 80

access-list 101 permit tcp 192.168.2.0 0.0.0.255 any eq 25

(3)access-list 101 permit ip 192.168.3.0 0.0.0.255 any



3.规定：(1)所有人可上网但不能 QQ；(2)192.168.2.0 主机只可访问 WEB，其他不能做。

配置如下：(将路由器换成交换机)

(1) IP access-list standard qq

deny UDP any any eq 4000

deny UDP any any eq 8000

permit ip any any

(2) permit tcp host 192.168.2.0 any any eq 80

deny ip host 192.168.2.0 any

permit ip any any

4.规定：（1）192.168.1.0 网段星期一至五可访问 WEB，其他时间不能访问 WEB；

（2）192.168.2.0 周末 8：00 至 18：00 不能访问 TFP。

配置如下：

（1）(config)#time-range student

#periodic weekdays 00:00 to 23:59

(config)#time-range teacher

#periodic weekend 08:00 to 18:00

#access-list 101 permit tcp 192.168.1.0 0.0.0.255 any eq 80 time-range student

#access-list 101 deny tcp 192.168.2.0 0.0.0.255 any eq ftp time-range

teacher

综合实验

一、实验介绍

1、实验名称：综合实验

2、实验设备：R2621　2 台，S3550-24 与 S2950 各 1 台

3、实验目的：

本实验是如下知识点的综合练习：

VLAN 创建；

VLAN 的汇聚链接；

建立 RSTP 生成树；

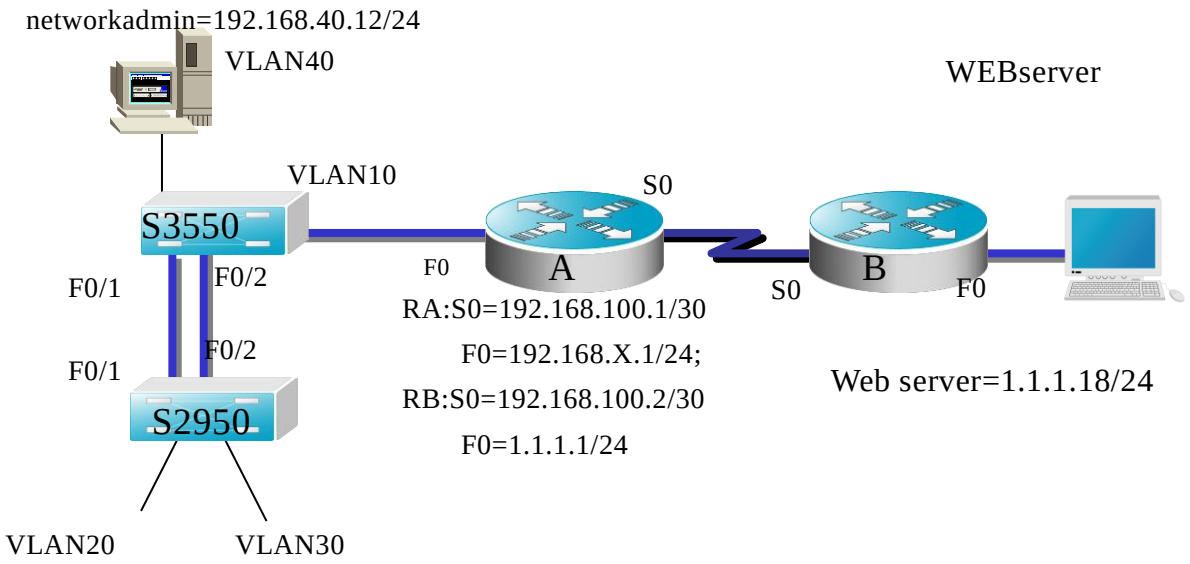
PPP PAP 认证；

访问控制列表 ACL；

路由动态协议 RIP。

4、实验时间：120 分钟

二、实验拓扑



S3550 :

VLAN20=192.168.20.1/24

VLAN30＝192.168.30.1/24

VLAN40=192.168.40.1/24

S2950 :VLAN1=192.168.X.3/24

S3550: VLAN1=192.168.X.2/24

三、实验内容

1. 在 S3550 上建立四个 VLAN，分别是 VALN10，VLAN20，VLAN30，VLAN40；
2. 在 S2950 上建立二个 VLAN，分别是 VLAN20，VLAN30；
3. 在 S3550 和 S2950 之间建立冗余链路（使用 F0/1 口和 F0/2 口）；
4. 在路由器 A 与路由器 A 之间建立 PPP 链路并进行 PAP 认证；
5. 在路由器 A 中建立防火墙，控制 VLAN20 和 VLAN30 中的主机访问 WEBserver。

四、实验配置

```
s2950#configure terminal
s2950 (config)#vlan 20
s2950 (config-vlan)#name student
s2950 (config-vlan)#exit
s2950 (config)#vlan 30
s2950 (config-vlan)#name teacher
s2950 (config-vlan)#exit

s2950 (config)#interface range fastethernet 0/5-10
s2950 (config-if-range)#switchport access vlan 20
s2950 (config-if-range)#exit
s2950 (config)#interface range fastethernet 0/11-15
s2950 (config-if-range)#switchport access vlan 30
s2950 (config-if-range)#exit

s2950 (config)#enable secret level 1 0 ruijie
s2950 (config)#enable secret level 15 0 ruijie
s2950 (config)#interface vlan 1
s2950 (config-if)#ip address 192.168.1.1 255.255.255.0
s2950 (config-if)#no shutdown
s2950 (config-if)#exit

s2950 (config)#interface range fasthernet 0/1-2
s2950 (config-if-range)#switchport mode trunk
s2950 (config-if-range)#exit

s2950 (config)#spanning-tree
s2950 (config)#spanning-tree mode rstp

s3550#configure terminal
s3550(config)#vlan 10
```

```
s3550(config-vlan)#exit
s3550(config)#vlan 20
s3550(config-vlan)#exit
s3550(config)#vlan 30
s3550(config-vlan)#exit
s3550(config)#vlan 40
s3550(config-vlan)#exit

s3550(config)#interface fastethernet 0/24
s3550(config-if)#switchport access vlan 10
s3550(config-if)#exit

s3550(config)#interface fastethernet 0/20
s3550(config-if)#switchport access vlan 40
s3550(config-if)#exit

s3550(config)#interface range fastethernet 0/1-2
s3550(config-if-range)#switchport mode trunk
s3550(config-if-range)#exit

s3550(config)#enable secret level 1 0 ruijie
s3550(config)#enable secret level 15 0 ruijie
s3550(config)#interface vlan 40
s3550(config-if)#ip address 192.168.40.1 255.255.255.0
s3550(config-if)#no shutdown
s3550(config-if)#exit

s3550(config)#spanning-tree
s3550(config)#spanning-tree mode rstp
s3550(config)#spanning-tree priority 0

s3550(config)#interface vlan 20
s3550(config-if)#ip address 192.168.20.1 255.255.255.0
s3550(config-if)#no shutdown
s3550(config-if)#exit
s3550(config)#interface vlan 30
s3550(config-if)#ip address 192.168.30.1 255.255.255.0
s3550(config-if)#no shutdown
```

```
s3550(config)#interface vlan 10
s3550(config-if)#ip address 192.168.10.2 255.255.255.0
s3550(config-if)#no shutdown
s3550(config-if)#exit

s3550(config)#router rip
s3550(config-router)#network 192.168.10.0
s3550(config-router)#network 192.168.20.0
s3550(config-router)#network 192.168.30.0
s3550(config-router)#network 192.168.40.0
s3550(config-router)#version 2
s3550(config-if)#exit

R1#configure terminal
R1(config)#interface fastethernet 0
R1(config-if)#ip address 192.168.10.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit

R1(config)#interface serial 0
R1(config-if)#encapsulation ppp
R1(config-if)#clock rate 64000
R1(config-if)#ip address 192.168.100.1 255.255.255.252
R1(config-if)#no shutdown
R1(config-if)#ppp authentication pap
R1(config-if)#exit
R1(config)#username ruijie password 123

R1(config)#router rip
R1(config-router)#network 192.168.10.0
R1(config-router)#network 192.168.100.0
R1(config-router)#version 2
R1(config-router)#no auto-summary
R1(config-router)#

R1(config)#time-range vlan20
R1(config-time-range)#periodic  weekdays 00:00 to 23:59
```

```
R1(config-time-range)#exit
R1(config)#time-range vlan30
R1(config-time-range)#periodic weekend 00:00 to 23:59
R1(config-time-range)#exit
R1(config)#access-list 101 permit tcp 192.168.20.0 0.0.0.255 host 1.1.1.18
eq 80 time-range vlan20
R1(config)#access-list 101 deny tcp 192.168.30.0 0.0.0.255 host 1.1.1.18 eq
80 time-range vlan30
R1(config)#access-list 101 permit tcp 192.168.30.0  0.0.0.255 host 1.1.1.18
eq 80

R1(config)#interface fastethernet 0
R1(config-if)#ip access-group 101 in

R2#configure terminal
R2(config)#interface fastethernet 0
R2(config-if)#ip address 1.1.1.1 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#exit

R2(config)#interface serial 0
R2(config-if)#encapsulation ppp
R2(config-if)#ip address 192.168.100.2 255.255.255.252
R2(config-if)#no shutdown
R2(config-if)#ppp pap sent-username ruijie password 123
R2(config-if)#exit

R2(config)#router rip
R2(config-router)#network 192.168.100.0
R2(config-router)#network 1.1.1.0
R2(config-router)#version 2
R2(config-router)#no auto-summary
```

五、验证

1. 从 VLAN20、VLAN30 中 ping 主机 WEBserver；
2. 从 VLAN20、VLAN30 中分时间段访问 WEBserver 网页。

附录：

常见故障排除方法

1．关于交换机基础配置的常见问题及故障排除方法

A、超级终端不显示配置界面

解答：要将超级终端的波特率设置为 9600，点击“还原默认值”就好，这个问题往往出现在配置交换机的初期。

B、配置远程登录只能进入到用户模式

解答：要在配置完登录密码后,enable secret level 1 0 star 不要忘记配置 enable secret level 15 0 star 。

C、PC 机不能远程登录到交换机

解答：远程登录的主机是否和交换机的管理地址在一个网段；交换机的管理 VLAN 是否运行了 no shutdown 这个命令。

D、关于二层交换机的管理地址

在操作时发现给 VLAN1 配置了管理地址后，发现无法登陆，查看 VLAN1 状态已经 UP。

解答：经过查看配置发现，学生主机连接交换机的端口属于 VLAN20，而学生要通过 TELNET 管理交换机，无法连接。需要设置 VLAN20 的管理 IP，并将其 no shutdown。

E、关于二层交换机的多管理地址

解答：学生在实验时给多个 VLAN 配置 IP 地址，在二层交换机里只允许有一个管理 IP 地址生效。也就是哪一个 VLAN 的 IP 地址最后 no shutdown，哪一个 VLAN 的地址就生效。

F、关于跨 VLAN 管理交换机

解答：二层交换机的管理地址是在 VLAN20 上，而用户现在需要通过 VLAN30 进行登陆管理交换机。需要通过三层交换机实现 VLAN 间路由。同时在二层交换机上设置

Ip default-gateway 1.1.1.1 将交换机的网关指向三层交换机的 VLAN20 的 IP 地址。

2．关于 VLAN 的实验常见问题及故障排除方法。

A、VLAN 模式下不能进行其他 VLAN 的创建

解答：这个问题出现的情况不会很多，要清楚各种命令在什么模式下输入，VLAN 的建立是在全局模式下，创建完 VLAN 就进入了 VLAN 配置模式，要创建其他的 VLAN 需要退出 VLAN 模式，返回全局模式。

B、TRUNK 链路不传递多个 VLAN 信息

解答：TRUNK 链路的建立要在交换机两端建立 TRUNK 接口，TRUNK 接口的 NATIVE VLAN 必须相同。

C、TRUNK 链路不传递某个 VLAN 信息

解答:一些学生会在 TRUNK 接口下运行 switchport trunk allowed vlan remove（vlan 号），

禁止了某个 VLAN 信息的传输而自己的确不知道。可以用 switchport trunk allowed vlan all 这条命令来恢复。

D、跨越交换机同一网段不能通信

解答：首先确定两台交换机之间是否建立了相同的 VLAN，然后确定接入主机的交换机端口是否 UP。

3. 关于生成树协议的实验常见问题及故障排除方法

A、生成树协议开启的错误

解答：生成树协议有两步，spanning－tree 首先开启生成树协议，这个时候生成树的默认模式是 MSTP。实验中做到的是 STP 以及 RSTP。所以不要忘记第二步，确定生成树协议的模式，spanning－tree mode （stp 或者 rstp）。

B、两条链路都断掉，主机之间还能通信

解答:只有一种可能，就是主机之间并没有通过这两条链路通信，一般情况下是物理线缆插错。

4. 三层交换机 3550 上做 VLAN 间路由常见问题及解决方法

VLAN 间不能通信

解答：1）三层交换机上的路由功能虽然默认情况下是打开的，但是不排除被学生误关的情况，这里在全局模式下用 ip routing 命令打开路由。

2）每个 VLAN 的 SVI 地址是否建立，每个 VLAN 的 SVI 是否被 no shutdown 开启。

3）每个 VLAN 下的主机是否设置了网关，并且网关地址是否指向了主机所在的 VLAN。

5. 交换机和路由器开机无法进入用户模式

解答：1）交换机和路由器在启动过程的最后一步是加载保存在设备里的配置文件，使其生效，当交换机和路由器发现没有配置文件时，会自动启动一个配置向导，来进行一些基本功能的配置，一般情况下只需按“Ctrl+C”终止配置向导就会出现命令行操作模式。

2）交换机和路由器的操作系统被删除，因此设备无法启动，可以通过 TFTP 服务器上传相应版本的操作系统。

6. 路由器基本配置实验常见问题及解决办法

A、远程登录配置后只能进入用户模式，不能进入特权模式，当要进入特权模式的时候提示没有配置特权密码

解答：在配置完登录密码之后，不要忘记要配置用户模式进入特权模式的密码 enable password star 或者 enable secret star(二者可选其一)。

B、两台路由器通过广域网线路连接，物理层正常，数据链路层不正常

解答：1)可能一端广域网接口地址没有正确配置；DCE 端没有配置时钟速率；远端路由器接口没有开启；路由器的接口封装模式不一样。

2)可能是路由器两端接口封装类型不一致。

3)可能是封装类型为 PPP 时验证没通过，检查设置的验证方式，和验证密码。

C、假设路由器一个接口配置了 192.168.1.0 /24 的地址，另一个接口配置相同网段的地址却不能配置。

解答：路由器每一个接口是一个广播域，每一个接口的地址不能在相同的广播域内。

7. 静态路由配置实验常见错误及解决办法

A、静态路由的出口配置本地接口的地址不能被设置

解答：当数据包要把某个本地接口作为路由出口的时候，要指定本地接口的名称，而不是本地接口的地址。

B、连接在两台路由器下的主机在静态路由正确配置的情况下不能正常通信。

解答：主机上的网关未配置。

8. 动态路由协议 RIP V1 及 RIP V2 实验常见问题及解决办法。

A、声明了本地直连网段，对方没有学习到路由信息

解答：在动态路由中经常犯的一个错误就是忘记在两台路由器上都要声明主干网段的地址段（连接两台路由器的那个网段）。

B、RIPv2 容易忘记的命令

解答：由版本 1 转换成版本 2 要记得是 VERSION 2 这条命令；在大多数情况下要手动关闭自动汇总： no auto-summary。

9. **IP 访问控制列表实验常见问题及解决办法**

A、没有禁止的网段的数据包不能被传输

解答：在访问控制列表的最后隐含着拒绝所有的命令，所以不要忘记 permit any 这条命令在访问控制列表最后。

B、访问控制列表建立了，却没有效果

解答：可能没有在接口下应用；在接口下应用了，但是数据流的方向却没有想清楚，所以控制数据流的方向上要分析清楚。