第 3 章
了解网络硬件

交换机和路由器是几乎所有局域网络都要使用的基本设备。其中，交换机将其他网络设备（例如其他交换机、路由器、网络防火墙、无线接入点等）和所有终端设备（例如计算机、服务器、网络摄像头、网络打印机等）连接在一起，实现彼此之间的通信，而路由器用于实现局域网之间以及局域网与 Internet 的互连，将所有的网络连接在一起。可见，对于任何局域网络而言，交换机和路由器都是必不可少的网络硬件设备。

3.1 认识交换机

如果把网络布线系统比喻为一条条宽阔的道路，那么，网络交换机（Switch）就像是一座立交桥，将通往各个方向的道路汇连在一起，实现彼此之间的互连互通。无需红绿灯，等待，四通八达，任意驰骋。

3.1.1 交换机的功能

交换机是构建局域网络不可或缺的集线设备。作为局域网通信的重要枢纽和节点，其主要功能就是连接设备。所谓局域网络（Network），简单地说，其实就是若干计算机的集合，而这些计算机就是借助交换机相互连接在一起的。

交换机最主要的功能就是连接计算机、服务器、网络打印机、网络摄像头、IP 电话等终端设备，并实现与其他交换机、无线接入点、网络防火墙、路由器等网络设备的互连，从而构建局域网络，实现所有设备之间的通信。如图 3.1 所示，就是交换机与终端设备和网络设备的连接方式。

作为局域网络的核心与枢纽，交换机的性能决定着网络性能，交换机的带宽决定着网络带宽。因此，局域网络的升级往往就是交换机的升级。当然，前提条件是网络布线必须能够满足网络传输的需要。

3.1.2 交换式网络的传输性能

可以形象地把计算机比喻为写字楼或工厂，把网络布线比喻为城市马路或高速公路，把网络应用比喻为不同类型的汽车，各种数据则是装在这些汽车上的货物，而交换机就是连接来自所有道路的立交桥。毫无疑问，立交桥都拥有多向多车道，可以从任何一条路转向另外其他一

条路，而且所有车辆都可以自行其道，相互之间没有阻碍和影响。

而由交换机构建的局域网络，计算机之间的通信可以同时进行，彼此不受影响干扰，并且每个通信都可以“独享”带宽，即拥有端口所能提供的传输速率。这就好像在限速 80km/h 的立交桥上，每辆车都可以占用一个车道，都可以跑到 80km/h 的速率。如图 3.2 所示，为多台计算机同时通信的情形。

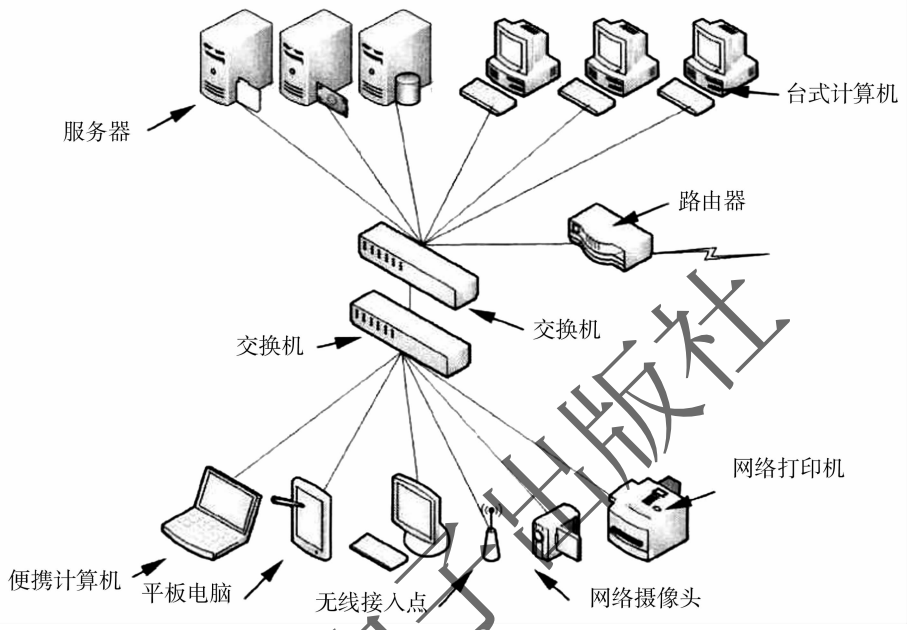

图 3.1 交换机的功能

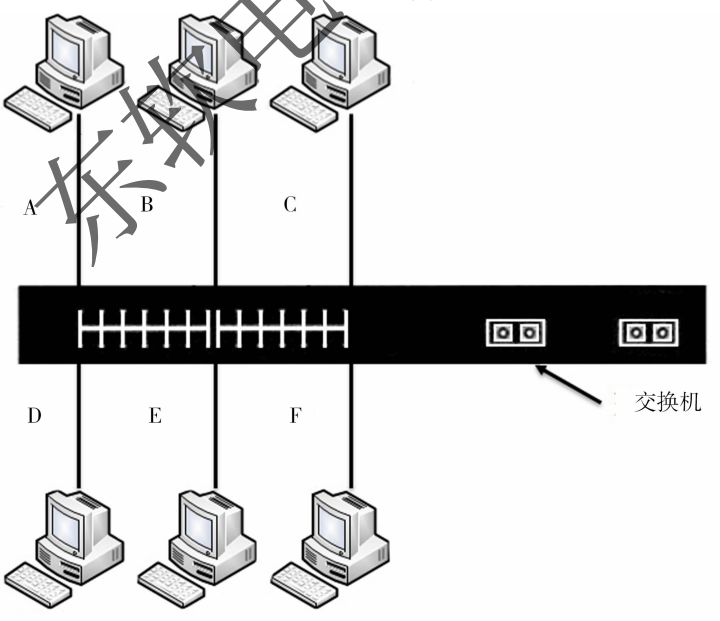

图 3.2 多台计算机同时通信

由交换机构建的网络称为“交换式网络”。交换式网络的工作模式通常为“全双工”(Full Duplex)，即终端设备可以同时接收和发送数据，数据流是双向的，如图 3.3 所示。

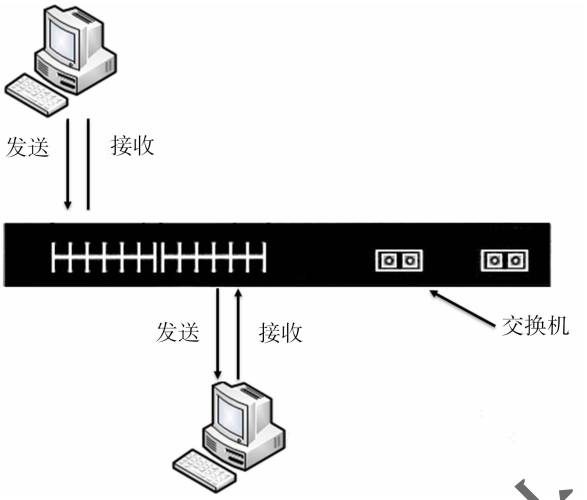

图 3.3　全双工示意图

对于 100Mbps 端口而言，在全双工工作模式下，接收和发送数据的速率均为 100Mbps，总带宽即可达到 200MbPs；对于 1000Mbps 端口而言，在全双工工作模式下，接收和发送数据的速率均为 1000Mbps，总带宽即可达到 2000Mbps；同样，对于 10Gbps 端口而言，在全双工工作模式下，接收和发送数据的速率均为 10Gbps，总带宽将达到惊人的 20Gbps。

3.1.3　交换机的工作原理

交换机位于 OSI 参考模型中的数据链路层（即第二层），是一种基于 MAC 地址（Media Access Control，即介质访问控制）是别的且用于完成数据封装及转发的网络设备。交换机可以“学习”MAC 地址，并将其存放在内部的地址列表中，通过在数据帧的始发者和目标接收者之间建立临时的交换路径，是数据帧直接由源地址到达目的地址。因此，交换机就像是一个业务熟练的调度员，能够准确地将转载数据的汽车从出发路口直接派送到目的地路口。当然，要完成这样繁重和智能化的工作，交换机也需要一个学习和记忆的过程。

计算机借助网卡连接到局域网络，而每块网卡都有其与生俱来的“胎记”，即 MAC 地址。交换机通过“学习”，会把连接到每个端口的 MAC 地址记住，形成一个端口与 MAC 地址的对应表。

提示：MAC 地址是识别局域网节点的标识，所有网络设备（包括每块网卡、交换机和路由器的每个端口）都有二个唯一的 MAC 地址，通常是由网卡生产厂家直接烧入 EPROM 中的，是传输数据对真正用以标识发出数据的设备和接收数据的设备的标志。

交换机的工作过程如下所示：

（1）当交换机从某个端口收到一个数据包时，先读取包头中的源 MAC 地址，从而建立源端口与源 MAC 地址的对应关系，并将其添加到地址表。由于交换机能够自动根据收到的以太网帧中的源 MAC 地址更新地址表的内容，所以交换机使用的时间越长，学习到的 MAC 地址就越多，未知的 MAC 地址就越少，因而广播的包就越少，处理速度就越快。

（2）读取包头中的目的 MAC 地址，并在地址表中查找相应的端口。

（3）如果地址表中有与该目的 MAC 地址对应的端口，则把数据包直接复制到这个端口上。由于不是将该帧发送到所有端口，从而使那些既非源端口、又非目的端口的端口之间认可进行

相互通信，进而提供了更高的传输速率。

(4)如果在 MAC 地址表中没有找到该 MAC 地址，也就是说，该目的 MAC 地址是首次出现，则将该帧发送到所有其他端口(源端口除外)，相当于该帧是一个广播帧。拥有该 MAC 地址的网卡在接收该广播帧后，将立即做出应答，从而使交换机将“端口号-MAC 地址”对照表添加到地址表。

不断重复上述过程，交换机即可实现所有数据的转发，并逐步学习和记忆整个网络中的 MAC 地址，不断丰富和完善自己的 MAC 地址表。

人类的记忆会随着时间的流逝而淡忘。那么，交换机是否会永久性地记住所有的端口号与 MAC 地址关系呢？答案同样是否定的。由于交换机中的内存有限，因此，能够记忆的 MAC 地址数量也是有限的。既然不能无休止地记忆所有的 MAC 地址，那么，也必须赋予其相应的忘却机制，从而吐故纳新。实际上，交换机设计了一个自动老化时间(Auto-aging Time)机制，若某个 MAC 地址在一定时间内(默认为 300 秒)不再出现，那么，交换机将自动把该 MAC 地址从地址表中清除。当下一次该 MAC 地址重新出现时，将会被当作新地址处理。另外，由于地址表是保存在内存中的，因此，当交换机断电或重新启动之后，地址表数据将会全部丢失，必须重新学习。

交换机可以在任意一对端口之间建立临时专用通道，不同端口间的转发可以并行操作。这就像是在各个端口间建立了一座立交桥，形成立体交叉结构，不同流向的数据各行其道，每个端口均能够独享固定贷款，传输速率几乎不受计算机数量的影响。另外，当两个或两个以上的端口与目的端口进行通信时，交换机将把这些数据帧保存在缓存中，然后根据顺序对其逐一处理和转发，从而实现“多”对“一”的通信。

由此可见，交换机的工作过程可以概括为“学习—记忆—接收—查找—转发”。通过广播方式“学习”网卡 MAC 地址，并将“MAC 地址—端口号”的对应关系创建为一个地址表“记忆”在内存中。从源端口“接收”到数据后，在地址与表中“查找”与目的 MAC 地址相对应的端口，然后将数据帧“转发”至目的端口。

3.1.3 交换机端口类型

交换机的功能就是用于连接其他网络设备(例如交换机、路由器、网络防火墙等)，以及网络终端设备(例如计算机、网络打印机、IP 电话机、网络摄像头等)，从而实现相互之间的通信，构建局域网络。因此，交换机必须都拥有大量的端口。由于网络环境和网络需求非常复杂，所以交换机也就不得不拥有多种类型的端口。大致可以将端口分为 5 种类型，即光纤端口、双绞线端口、GBIC 插槽、SFP 插槽和 10GE 插槽。

1.光纤端口

光纤在局域网络中拥有无可比拟的优势。第一，光纤的有效传输距离最远，几百米至几千米都没有问题，因此被广泛应用于楼宇之间、楼层之间的连接。第二，光纤的抗电磁干扰能力强，无论多么恶劣和复杂的环境，都丝毫不受影响。第三，传输速率高，1Gbps 甚至 10Gbps 都可以轻松实现，最适宜高速设备之间的连接。

2.双绞线端口

双绞线端口是应用最多、也是最廉价的端口类型。双绞线网络的优点有 4 个：

- 一是价格低廉，这正是其被广泛采用的原因之一；
- 二是连接简单，将跳线两端的水晶头插入 RJ-45 端口，即可成设备之间的连接；
- 三是传输速率高，可以轻松实现 1000Mbps 的高速连接；
- 四是自适，可以智能判断对端设备的传输速率和工作模块，自动进行协商，建立所能达到的最高的传输速率。

缺点有两个：

- 一是传输距离较短，100Mbps 和 1000Mbps 网络只能传输 100m。不过，对于一般的网络连接而言，这样的距离也已经足够；
- 二是抗干扰能力差，要求外界环境不能有太多的电磁干扰。

3.1GE 模块与插槽

1GE 模块与插槽的类型主要包括两种，即 GBIC 和 SFP。具体介绍如下：

(1)GBIC 模块与插槽。

GBIC(Gigastack Gigabit Interface Converter)是一个通用的、低成本的千兆位以太网连接标准，用于提供交换机与其他设备之间的高速(00Mbps)连接。借助不同的 GBIC 模块，既可建立高密度端口的叠堆，又可实现由服务器或者远程主干网络的高速连接，因此具有非常大的灵活性。

GBIC 模块分为四种：

- 一是 1000BasE-T GBIC 模块，适用于超五类或六类双绞线，最长传输距离为 100m；
- 二是 1000BasE-SX GBIC 模块，适用于多模光纤(MMF)，最长传输距离为 500m；
- 三是 1000BasE-LX/LH GBIC 模块，适用于单模光纤(SMF)，最长传输距离为 10km；
- 四是 1000BasE-ZX GBIC，适用于长波单模光纤，最长传输距离为 70 至 100km。

由此可见，只需更换 GBIC 模块，交换机就能够适用于各种传输介质和网络环境，为用户提供高速连接和应用。

(2)SFP 模块与插槽。

SFP(Small Form-factor Pluggable)可以简单地理解为 GBIC 的升级版本，同样能够提供高达 1000Mbps 的连接。实际上，SFP 已经取代 GBIC，成为了新的千兆位接口标准，而 GBIC 则基本上已经退出市场。

SFP 插槽所占用的位置比 GBIC 模块减少一半，因此，可以在面积相同的面板上设置多一倍的端口数量，由于 SFP 模块在功能上与 GBIC 基本一致，只是体积相对更为“迷用户”，因此，也被称为迷用户 GBIC。

SFP 模块的类型与 GBIC 非常相似，也可分别应用于双绞线、多模光纤和单模光纤，从而使网络连接变得更加灵活，适应更为复杂的网络环境。SFP 的类型也与 GBIC 一样，主要分为 1000BasE-T、1000BasE-SX、1000BasE-LH/LX 和 1000BasE-ZX 等 4 种类型。

4.10GE 模块与插槽

10-Gbps 端口是当今速度最快、价格最昂贵的端口，因此，10Gbps 端口通常用于实现重点业务的汇聚层交换机与核心层交换机之间的连接。10Gbps 端口通常借助于不同标准的插槽和模块实现，主要包括 XENPAK、X2、XFP 和 SFP+等 4 种。

(1)XENPAK。

XENPAK 是面向万兆位以太网的第一代模块。根据 XENPAK 多方协议提议，收发器模

块采用了 XAUI 接口。其中 1310nm 串行收发器，传输距离可达 10km，使用了直接调制激光器技术，不再需要传统的调制器、冷却器或复杂的光复用器。这种模块具有良好的抗 EMI 和散热性能，每个线路卡最多可实现 8 个端口的高密度配置，其面板热插拔特性使 4 种物理层介质设备收发器都能实现即插即用。

(2)X2。

X2 和 XPAK 是 XENPAK 模块的直接改进版，体积缩小了 40%，光接口、电接口都与原来保持一致。X2 模块目前应用最普遍，Cisco Catalyst 3560-E、Catalyst 3750-E 和 Catalyst 4900 系列，以及 Catalyst 4500-E 和 Catalyst 6500-E 系列中，X2 插槽都被大量应用。

(3)XFP。

XFP(10-Gigabit Small Form-factor Pluggable)支持局域网 PHY 和广域网 PHY，具有可插拔、尺寸更加小巧、价格更有竞争力等特点。因此，大多数最新的设计全都采用了 XFP 模块，这是因为它的物理尺寸的小型化可以达到很高的端口密度。可以预见，使用 XFP 模块的产品很快会成为试产的新宠。XFP 更多地被应用于路由器模块。

(4)SFP+。

SFP+(Small Form-factor Pluggable Plus)适用于 10Gbps 以太网的最新型可插拔模块尺寸规格，最多可提供 11.1Gbps 的速率。

SFP+得名于 SFP，并与 SFP 模块采用相同的物理尺寸，因此，能够与旧的 SFP 模块在同样的插槽中工作。SFP+模块比 XFP 更小，由此也把每个线卡的密度从 XFP 的 16 个提高到至少 24 个。

SFP+模块可用于替代目前的 XFP、XENPAK 和 X2 等万兆位模块。SFP+相对于这些万兆位模块而言，其主要优势如下：

- 体积优势。SFP+体积与 SFP 一样，相对于其他类型的万兆位模块，体积大大减小，有利于在更小的体积上实现更多的万兆位端口。
- 成本优势。由于 SFP+模块相对于 XFP 模块而言，删除了 CDR(时钟数据恢复模块)，因此，在成本上会有降低。
- 电源功耗降低。XENPAK 的功耗最低为 9W，X2 功耗为 4W，XFP 的功耗为 2.5～3.5W，而 SFP+的功耗只有 1W，从而无需专门的散热部件降低了整板时功耗及对散热的要求。

5.复用端口

有些级联端口虽然是独立的、端口类型不同的两个端口，但是，这两个端口中只能使用其中的一个，不能同时用于连接设备。这类端口被称之为复用端口，设计的目的是为了提高网络设备的可用性。

6.10GE 转换模块

10GE 转换模块主要包含两种常见类型：

(1)TwinGig。

TwinGig 模块用于 Cisco Catalyst 3560-E/3750-E 系列交换机。借助 Cisco TwinGig 转换模块,可以将 10Gb Ethernet 插槽转换成为 2 个 SFP 插槽,实现双 1000Mbps 端口连接。也就是说,借助 Cisco TwinGig 转换模块,可将 2 个 SFP 模块连接到 1 个 10Gbps 插槽。

(2)OneX。

OneX 转换模块是一个可以热插拔的 10Gb Ethernet X2 插槽模块,用于实现 10Gb X2 接口与单 10Gb SFP+接口的转换,支持 Catalyst 3750/4500/4900/6500 等多款交换机平台。

3.1.4　交换机的 VLAN 功能

随着网络内计算机数量的增多,广播包的数量也会急剧增加。当广播包的数量占到通信总数的 30%时,网络的传输效率将会明显下降。所以,当局域网内的计算机达到一定数最后(通常限制在 200 台以内),通常采用划分虚拟网(Virtual Local Area Network,VLAN)的方式将网络分隔开来,将一个大的广播域划分为若干个小的广播域,以减小广播可能造成的损害,子网之间进行通信也必须通过路由设备。

1.VLAN 的意义和作用

在局域网络中使用 VLAN 技术,具有以下重要意义和作用。

- 降低移动和变更的管理成本。VLAN 中的成员与其物理位置无关,既可连接至同一台交换机,也可连接至不同交换机。当需要把一台计算机从一个子网转移到另一个子网时,迁移工作将只是由网络管理员在作为网络管理的计算机上重新定义一下 VLAN 成员即可。
- 控制广播。由于所有的广播都只在本 VLAN 内进行,而不再扩散到其他 VLAN 上,所以将大大减少广播对网络带宽的占用,提高带宽传输效率,并可有效地避免广播风暴的产生。
- 增强安全性。VLAN 的一个重要特点就是提高了网络安全性。由于交换机只能在同一 VLAN 内的端口之间交换数据,不同 VLAN 的端口不能直接相互访问。因此通过划分 VLAN,就可以在物理上防止某些非授权用户访问敏感数据。
- 网络监督和管理的自动化。由于网络管理员可以通过网管软件,查到 VLAN 间和 VLAN 内通信的数据报的细目分类信息,以及应用数据报的细目分类信息,而这些信息对于确定路由系统,和经常遭到访问的服务器的最佳配置十分有用。通过划分 VLAN,这可以使网络管理变得更简单、更轻松、更有效。

VTP(VLAN Trunking Protocol)是一种消息协议,用于在 VTP 域内同步 VLAN 信息(VLAN 的添加、删除和重命名),而不必在每个交换机上配置相同的 VLAN 信息,从而实现 VLAN 配置的一致性。使用 VTP,可以在一个或多个交换机上建立配置修改中心,并自动完成与网络中其他所有交换机的通信,以有效地减少交换网络中的管理事务。

2. VLAN 的类型与适用

当 VLAN 在交换机上划分之后，不同 VLAN 之间的设备就如同是被物理地分隔。也就是说，连接同一交换机，然而处于不同 VLAN 设备，就如同被物理地连接到两个位于不同网段的交换机上一样，彼此之间的通信一定要经过路由设备，否则它们之间将无法得知对方的存在，将无法进行任何联系。

(1)基于端口的 VLAN。

基于端口的 VLAN 是最常使用的划分 VLAN 的方式，几乎被所有的交换机所支持。所谓基于端口的 VLAN，是指由网络管理员使用网管软件或直接设置交换机，将某些端口直接地、强制性地分配给某个 VLAN，如图 3.4 所示。除非网管人员重新设置，否则这些端口将一直保持对该 VLAN 的从属性，即属于该 VLAN，因此这种划分方式也称为静态 VLAN。

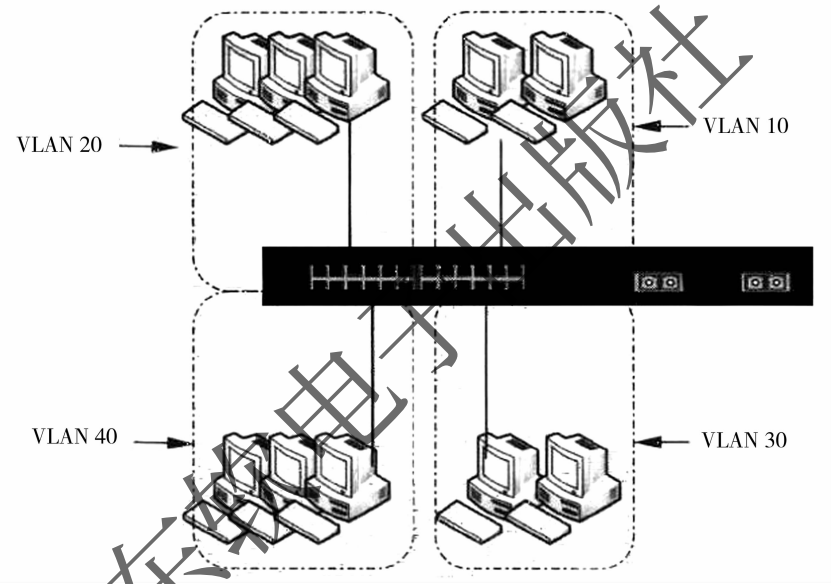

图 3.4 基于端口的 VLAN

这种方法虽然在网络管理员进行 VLAN 划分操作时会比较麻烦，但相对安全，并且容易配置和维护。同时，由于不同 VLAN 之间的端口不能直接相互通信，因此，每个 VLAN 都有自己独立的生成树。此外，交换机之间在不同 VLAN 中的可以有多个并行链路，以提高 VLAN 内部的交换速率，增加交换机之间的带宽。

需要注意的是，不仅可以将同一交换机的不同端口划分为同一 VLAN，而且还可以设置跨越交换机的 VLAN，如图 3.5 所示，即将不同交换机的不同端口划分至同一 VLAN，这就完全解决了位于不同物理位置、连接至不同交换机中的端口处于同一 VLAN 的难题。例如，在一个拥有数十台计算机的企业办公网络中，为了提高网络传输效率，可以将所有用户划分为行政、销售和研发 3 个 VLAN。虽然各个部门位于不同的建筑物内，连接至不同的交换机，但是，仍然能够根据其连接的端口将其划分至同一 VLAN。

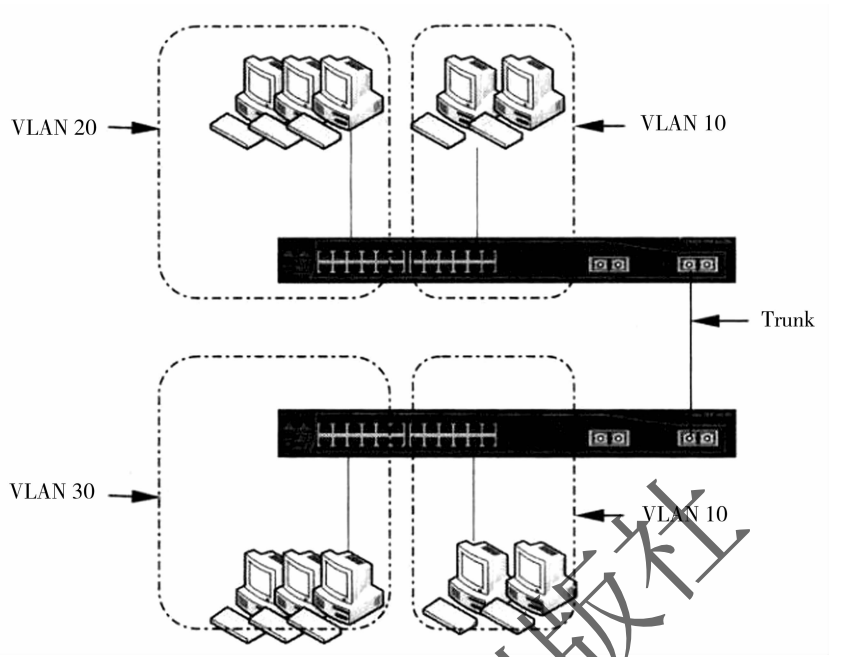

图 3.5　VLAN 与 Trunk

不同交换机上具有相同 ID 的 VLAN 之间，可借助一条链路实现彼此之间的连接。用于连接 VLAN 的链路被称之为 VLAN 中继（VLAN Trunk）。

（2）基于 MAC 的 VLAN。

所谓基于 MAC 的 VLAN，是指借助智能管理软件根据 MAC 地址来划分 VLAN。该划分方式一般用在每一交换机端口只连接一个终端的情况。也就是说，当端口级联集线器或傻瓜交换机时，该种划分方式并不适用。端口借助网络包的 MAC 地址、逻辑地址或协议类型来确定其 VLAN 的从属，将端口划分至不同 VLAN。

当一个网络节点刚连接到交换机时，此时交换机端口尚未分配，于是交换机通过读取网络节点的 MAC 地址，动态地将该端口划入某个虚拟网。一旦动态 VLAN 配置完成，用户的计算机就可以随意改变其连接的交换机端口，而不会由此而改变自己的 VLAN。当网络中出现未定义的 MAC 地址时，交换机可以按照预先设定的方式向网管人员报铃，再由网管人员做相应的处理。

例如，网络管理员有一台笔记本电脑，由于工作性质的关系，需要经常到各部门联机工作。当该笔记本电脑从端口 A 移动到端口 B 时，交换机能够自动识别经过端口 B 的源 MAC 地址，自动把端口 A 从当前 VLAN 中删除，而把端口 B 定义到当前 VLAN 中，如图 3.6 所示。

这种定义方法的优点是当终端在交换式网络中移动时，不必重新定义虚拟网，交换机能够自动进行识别和定义。因此，基于 MAC 的 VLAN 也称为动态 VLAN。由于 MAC 地址具有世界唯一性，因此该 VLAN 划分方式的安全性也较高。

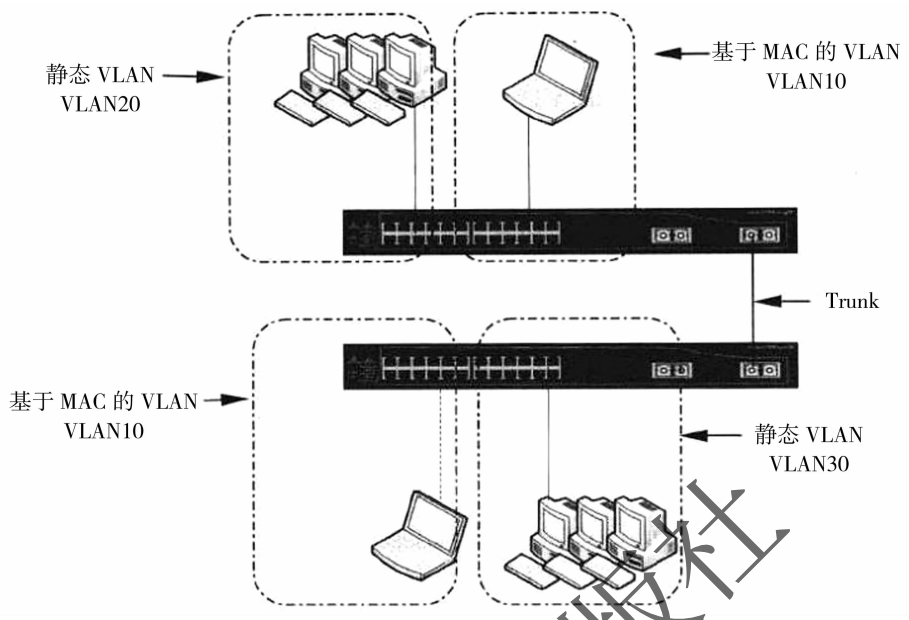

图 3.6　基于 MAC 地址的 VLAN

(3)基于 IP 的 VLAN。

所谓基于 IP 的 VALN,是指根据 IP 地址来划分的 VLAN。交换机属于 OSI 的第二层,因此,这种交换机不能识别帧中的网络层报文,但随着第三层交换机的出现,将第二层的交换功能和第三层的路由功能结合在一起,从而使交换机也能够识别网络层报文,可以使用报文中的 IP 地址来定义 VLAN。因此,当某一用户设置有多个 IP 地址时,或该端口连接到的集线器中拥有多个 TCP/IP 协议用户时,通过基于 IP 的 VLAN,该用户或该端口就可以同时访问多个虚拟网。

在该模式下,位于不同 VLAN 的多个业务部门(每种业务设置成一个虚拟网)既可同时访问同一台网络服务器,也可以同时访问多个虚拟网的资源,还可让多个虚拟网间的连接只需一个路由设备完成。这种定义方法的优点是当某一终端使用的网络层协议或 IP 地址改变时,交换机能够自动识别,重新定义 VLAN,不需要管理员干预。但由于 IP 地址可以人为地、不受约束地自由设置,因此使用该方式划分 VLAN 也会带来安全上的隐患。

(4)基于组播的 VLAN。

基于组播的 VLAN,就是动态地把那些需要同时通信的端口定义到一个 VLAN 中,并在 VLAN 中用广播的方法解决点对多点通信的问题。这种划分方法将 VLAN 扩大到了广域网,因此这种方法具有更大的灵活性,也很容易通过路由器进行扩展,主要适合于不在同一地理范围的局域网用户组成一个 VLAN,不适合局域网,主要是效率不高。

3.了解 VTP 技术

VTP 域(也称 VLAN 管理域)由一个或多个相互连接的、使用相同 VTP 域名的交换机组成。一台交换机能够被配置而且也只能被配置一个 VTP 域。使用命令行界面或 SNMP,可以修改全局 VLAN 的域配置。

关于 VTP 技术，我们需要首先了解一些相关概念，具体介绍如下。

(1)VTP 域。

默认状态下，交换机处于 VTP Server 模式，并且在收到由中继转发的 VTP 通告(VTP Advertisement)或配置至一个管理域之前，一直处于非管理域状态。不能在 VTP 服务器上建立或修改 VLAN，直到管理域名被定或被学习。

如果交换机收到一个从中继连接传来的 VTP 通告，它将继承管理域名和 VTP 配置版本号，并且不再理睬不同的管理域名或更早的配置版本号。

如果将交换机配置了 VTP 透明，以建立可修改的 VLAN，但修改将只影响到个别的交换机。

当修改位于 VTP Server 上的 VLAN 配置时，该修改将传播至 VTP 域中所有的交换机。VTP 通告被发送至所有的中继连接，包括 Inter-Switch-Link(ISL)、IEEE802.1Q、IEEE802.10 和 ATM LAN Emulation(LANE)。

(2)VTP 模式。

可将交换机配置在以下任何一种 VTP 模式下操作：

Server 模式：在 VTP Server(服务器)模式下，可以为整个 VTP 域建立、修改和删除 VLAN，并指定其他配置参数(例如 VTP 版本和 VTP 修剪)。VTP 服务器向其他在相同 VTP 域的交换机通告它们的 VLAN 配置，并同步它们的 VLAN 配置。VTP Server 是默认模式。

Client 模式：VTP Client(客户端)模式在许多行为上与 VTP Server 完全相同，不同之处是不能在 VTP Client 上建立、修改和删除 VLAN。

Transparent 模式：VTP Transparent(透明)交换机不加入到 VTP。VTP Transparent 交换机不通告它的 VLAN 配置，并且不同步它的 VLAN 配置。然而，在 VTP 版本 2 中，Transparent 交换机向其中继端口转发它接收到的 VTP 通告。

(3)VTP 通告。

VTP 域中的每一台交换机都利用保留的多播地址，定期向其每一个中继端口发送通告。VTP 通告被相邻的交换机接收，并必然地更新它们的 VTP 和 VLAN 配置。

在 VTP 通告中，以下全局配置信息被分布。VLAN ID(ISL 和 802.1Q)、Emulated LAN 名(应用于 ATM LANE)、802.10SAID 值(FDDI 网络)、VTP 域名、VTP 配置版本号、VLAN 配置(包括每个 VLAN 的 MTU 大小)，以及帧格式。

(4)VTP 修剪。

VTP 修剪(VTP Pruning)通过减少不必要的泛洪(Flooded Traffic)，例如广播(Broadcast Packet)、多播(Multicast Packet)、未知(Unknown Packet)和泛洪(Flooded Unicast)，从而提高网络带宽。

未启用 VTP 修剪时的泛洪情况，如图 3.7 所示。启用 VTP 修剪后的泛洪情况，如图 3.8 所示。

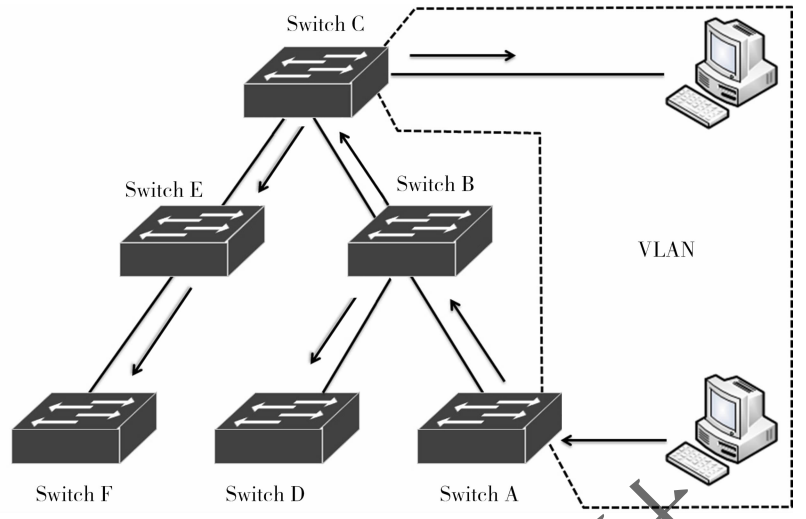

图 3.7 未启用 VTP 修剪

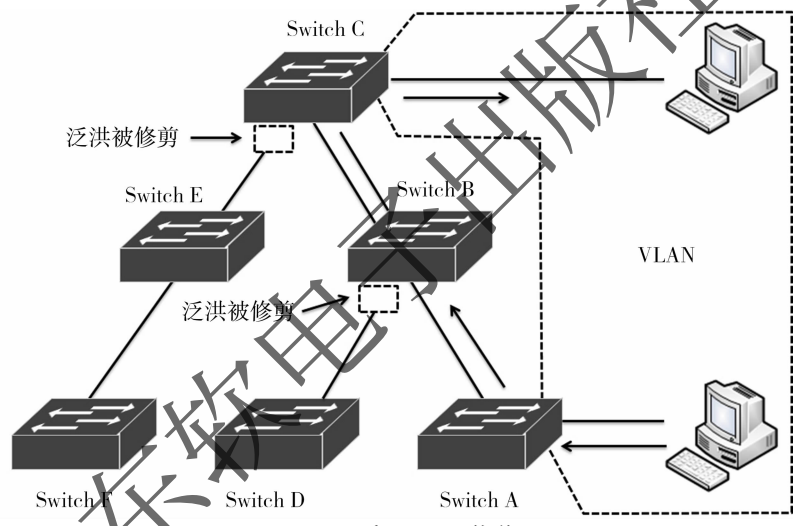

图 3.8 启用 VTP 修剪

VTP 修剪通过访问适当设备的方式，限制了到中继链接的泛洪，增加了网络的有效带宽。默认状态下，VTP 修剪未被启用。在启用 VTP 修剪之前，必须确认管理域中所有的设备都支持该功能。当在 VTPServer 上为整个管理域启用 VTP 修剪后，VTP 修剪将在几秒钟内实现。

4.了解 PVLAN 技术

通过似有虚拟网络技术(Private Virtual Local Area Network，PVLAN)可以实现端口之间相互隔离，满足网络接入用户的安全性要求，避免用户信息和数据的泄露，方式非法攻击和窃取。在使用私有 VLAN 时，各个接入端口之间不可以相互通信，仅可通过上连端口访问网络资源。需要注意的是，第二层交换机和第三层交换机都可以创建 PVLAN。

(1)VLAN 的局限性。

随着局域网络应用的不断丰富，对网络数据通信的安全性将提出更高的要求，注入方式黑客攻击、控制病毒传播等，都要求保证网络用户通信的相对安全性。传统的解决方法是给每个客户分配一个 VLAN 和相关的 IP 子网，通过使用 VLAN，每个用户被从第二层隔离开，可以防

止任何恶意的行为和网络信息探听。然而，这种分配每个客户单一 VLAN 和 IP 子网的模型造成了可扩展性上的局限。主要表现在以下几个方面：

VLAN 的限制。交换机固有的 VLAN 总数支持的限制（例如，Cisco Catalyst 2960 最多支持 255 个 VLAN），导致局域网络不能划分太多数量的 VLAN，从而限制了网络应用。

- 复杂的 STP。对于每个 VLAN 而言，每个相关的 Spanning Tree 拓扑都需要维护管理，复杂繁琐。

IP 地址的紧缺。IP 子网的大量划分势必造成大量 IP 地址的浪费，加之 IP 地址资源紧张，使 IP 地址的分配变得更加困难。

- 路由的限制。每个子网都需要相应的默认网关的配置，管理起来非常麻烦，而且增加了路由的负担，影响网络传输效率。

（2）PVLAN 技术。

同一个 PVLAN 内连接到各端口的计算机彼此相互隔离，即使它们位于同一 IP 地址段，拥有相同的子网掩码和默认网关，也无法实现彼此之间的通信。若欲实现不同端口间的通信，只能经过默认网关，在第三层交换机中实现。

PVLAN 的应用对于保证接入网络的数据通信的安全性是非常有效的，用户只需使用自己的默认网关连接，一个 PVLAN 不需要多个 VLAN 及 IP 子网就提供了具备第二层数据通信安全性的连接。所有用户都接入 PVLAN，从而实现了所有用户与默认网关的连接，而与 PVLAN 内的其他用户没有任何访问。PVLAN 功能可以保证一个 VLAN 中的各个端口相互之间不能通信，但可以穿过 Trunk 端口。这样，即使同一 VLAN 中的用户，相互之间也不会受到广播的影响，如图 3.9 所示。

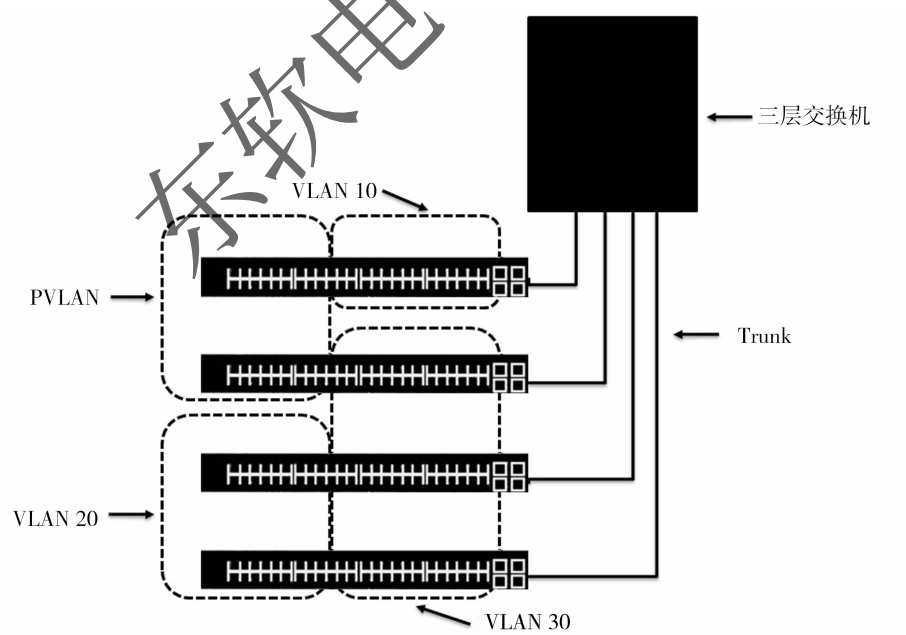

图 3.9　私有虚拟网络技术

由此可见，PVLAN 技术在解决通信安全、防止广播风暴和浪费 IP 地址方面的优势是显而易见的，而且采用 PVLAN 技术有助于网络的优化。另外，PVLAN 的配置也相对简单，不必占

用 VLAN 资源。

3.1.5 各协议层上的交换机

根据工作的协议层，交换机可分为第二层交换机、第三层交换机和第四层交换机。

(1)第二层交换机。

第二层交换机依赖于数据链路层中的信息(例如 MAC 地址)来完成不同端口数据之间的线速交换，所有交换机都能够工作在第二层上。接入层交换机通常全部采用第二层交换机。

(2)第三层交换机。

第三层交换机具有路由功能，将 IP 地址信息用于网络路径选择，并实现不同网段间数据的线速交换。当网络规模足够大，以至于不得不划分 VLAN 以减小广播所造成的影响时，只有借助于第三层交换机才能实现 VLAN 间的线速路由。因此，在大中型网络中，核心层交换机通常都有第三层交换机充当，某些网络应用较为复杂的汇聚层交换机也可以选用第三层交换机。部分固定端口的汇聚层交换机，也往往拥有了三层交换机的功能，例如 Cisco Catalyst 3550 系列、Cisco Catalyst 3560 系列、Cisco Catalyst 3750 系列等。

(3)第四层交换机。

第四层交换机使用传输层包含在每一个 IP 包包头的服务进程/协议(例如 HTTP 是用于传输 Web，FTP 是用于文件传输、Telnet 用于终端通信、SSL 用于安全通信等)进行交换和传输处理，实现带宽分配、故障诊断和对 TCP/IP 应用程序数据流进行访问控制等。由此可见，第四层交换机应当是核心层交换机的当然之选。Cisco Catalyst 4500 系列、Cisco Catalyst 4900 系列和 Cisco Catalyst 6500 系列交换机都支持第四层交换技术。

提示：第二层交换机主要用于实现局域网内主机间的快速信息交流，第三层交换机主要用于实现 VLAN 间的线速转发，第四层交换技术则可以为网络应用资源提供最优分配，实现应用服务质量、负载均衡及安全控制。二、三、四层交换机并不存在谁要取代谁的问题，而是各有其针对的环境和应用的范围。

3.1.6 第二层或第三层交换机的主要参数

局域网交换机是组成网络系统的核心设备。对用户而言，局域网交换机最主要的指标是端口的配置、数据交换能力、包交换速度等。下面将对交换机的一些重要技术参数作一些简要介绍，以便在设计网络拓扑结构和购置交换机时，根据网络的实际需要做出正确的选择。

1.第三层交换机的主要参数

第三层交换机主要被用于核心层交换机，以及大型网络中的汇聚层交换机，承担着网络传输中的大部分数据流量的转发任务，决定着整个网络的传输效率。因此，第三层交换机应当拥有较高的处理性能和可扩展性。Cisco 的 Catalyst 6500、Catalyst 4900、Catalyst 4500 和 Catalyst 4000 系列交换机，以及 Catalyst 3560 和 Catalyst 3550 系列，都是第三层交换机。

(1)转发速率。

网络中的数据是由一个个数据包组成，对每个数据包的处理都要耗费资源。转发速率(也被称为吞吐量)是指在不丢包的情况下，单位时间内通过的数据包数量。吞吐量就像是立交桥的车流量，是第三层交换机最重要的一个参数，标志着交换机的具体性能。如果吞吐量太小，就

会成为网络瓶颈，给整个网络的传输效率带来负面影响。交换机应当能够实现线速交换，即交换速度达到传输线上的数据传输速度，从而最大限度地消除交换瓶颈。对于千兆位交换机而言，若要实现网络的无阻塞传输，要求：

吞吐量(Mbps)＝万兆位端口数量×14.88Mbps＋千兆位端口数量×1.488Mbps＋百兆位端口数量×0.1488Mbps

如果交换机标称的吞吐量大于或等于上述计算值，那么，在第三层交换时，应当可以达到线速。其中，1个万兆位端口在包长为64B时的理论吞吐量为14.88Mbps，1个千兆位端口在包长为64B时的理论吞吐量为1.488Mbps，1个百兆位端口在包长为64B时的理论吞吐量为0.1488Mbps。那么，这些数值是如何得到的呢？

实际上，包转发线速的衡量标准是以单位时间内发送64B的数据包(最小包)的个数作为计算基准的。以千兆位的以太网端口为例，其计算方法如下：

1000,000,000bps/8bit(64＋8＋12)Byte＝1488095pps

当以太网帧为64B时，需要考虑8B的帧头和12B的帧间隙的固定开销。由此可见，线速的千兆位以太网端口的包转发率为1.488Mpps。万兆位以太网的线速端口包转发率，正好为千兆位以太网的10倍，即14.88Mbps；而快速以太网的线速端口包转发率，则为千兆位以太网的十分之一，即0.1488Mpps。

例如，对于一台拥有24个千兆位端口的交换机而言，其满载配置下的吞吐量应达到8×1.488Mpps＝35.71Mpps，才能够确保在所有端口均线速工作时，实现无阻塞的包交换。同样，如果一台交换机最多能够提供176个千兆位端口，那么，其吞吐量应当至少为261.8Mpps(176×1.488Mpps＝261.8Mpps)，这样才是真正的无阻塞结构设计。

如果将一台Cisco Catalyst 4500系列交换机作为中小型网络的核心层，那么，依据所采用的管理引擎不同，其转发速率分别为48Mpbs、75Mpps和102Mpps。对于Cisco Catalyst 4510R而言，尽管最多可以支持384个1000Gbps端口＋48个1000Mbps端口或者68个1000Mbps端口。

如果将一台Cisco Catalyst 6500系列交换机作为大中型网络的核心层，那么，依据所采用的管理引擎不同，其最大转发速率分别为15Mpps、210Mpps和400Mpps。以Cisco Catalyst 6509为例，尽管最多可以支持32个10Gbps端口或386个1000Mbps端口，但是，即使采用性能最好的管理引擎Supervisor Engine 720，400Mbps的转发速率也只能支持26个10Gbps端口，或者268个1000Mbps端口的线速转发。

(2)背板带宽。

带宽是交换机接口处理器或接口卡和数据总线间所能吞吐的最大数据量，就像是立交桥所拥有的车道的总和。由于所有端口间的通信都需要通过背板完成，所以背板所能提供的带宽，就成为端口间并发通信时的瓶颈。带宽越大，提供给各端口的可用带宽越大，数据交换速度越快；带宽越小，给各端口提供的可用带宽越小，数据交换速度也就越慢。也就是说，背板带宽决定着交换机的数据处理能力，背板带宽越大，所能处理数据的能力就越强。因此背板带宽越大越好，特别是对那些汇聚层交换机和中心交换机而言。若要实现网络的全双工无阻塞传输，必须满足最小背板带宽的要求。其计算公式如下：

背板带宽＝端口数量×端口速率×2

Cisco Catalyst 6500 系列交换机依据插槽数量的不同，其背板带宽分别为 32GbPs、256Gbpe 和 720Gbps。根据上述公式计算，256GbpsrtJ 背板只能满足 128 个 1000Mbps 端口的无阻塞并发传输。同理，由于 Cisco Catalyst 506 系列交换机的背板带宽仅为 64Gbps，因此，也就只能满足 32 个 1000Mbpe 端口的无阻塞并发传输。

提示：对于第三层交换机而言，只有转发速率和背板带宽都达到最低要求，才是合格的交换机，二者缺一不可。

(3)可扩展性。

由于第三层交换机往往充当核心层或汇聚层交换机，需要适应各种复杂的网络环境，因此，其可扩展性就显得尤其重要。可扩展性应当包括两个方面。

- 插槽数量。插槽用于安装各种功能模块和接口模块。由于每个接口模块所提供的端口数量是一定的，因此插槽数量也就从根本上决定着交换机所能容纳的端口数量。另外，所有功能模块(如交换引擎模块、IP 语音模块、扩展服务模块、网络监控模块、安全服务模块等)都需要占用一个插槽，因此插槽数量也就从根本上决定着交换机的可扩展性。
- 模块类型。毫无疑问，支持的模块类型(例如 LAN 接口模块、WAN 接口模块、ATM 接口模块、扩展功能模块等)越多，交换机的可扩展性越强。仅以局域网接口模块为例，就应当包括 RJ-45 线卡、GBIC(Giga Bitrate Interface Converter)插槽线卡、SFP(Small Form Pluggable)插槽线卡、X2 插槽线卡等，以适应大中型网络中复杂环境和网络应用的需求。

举例而言，Cisco Catalyst 6513 交换机拥有 13 个插槽，并且支持的模块类型有十几款，具有非常强大的可扩展性，可适用于各种复杂的网络环境，并可满足各种网络应用需求，因此，非常适宜充当大中型网络的核心层交换机。

(4)系统冗余。

第三层交换机作为网络核心，其工作状态的稳定性直接决定着网络的稳定性，而部件的物理损坏又是无法绝对避免的，因此交换机系统的部件冗余就显得尤其重要。通常情况下，电源模块、管理引擎等重要部件都必须提供冗余支持，从而保证所提供应用和服务的连续性，减少关键业务数据和服务的中断。例如，Cisco Catalyst 6507R 交换机就提供了电源模块和管理引擎的冗余。

(5)管理功能。

交换机的管理功能(Management)是指交换机如何控制用户访问交换机，以及用户对交换机的可视程度如何。三层交换机必须支持 SNMP 协议，并且提供友好的设备管理界面。除了可以由厂商提供的网管软件管理外，还必须能够被第三方管理软件进行远程管理，实现与其他网络设备的统一管理，降低管理成本、简化管理操作。

2.第二层交换机的主要参数

第二层交换机根据第二层数据链路层的 MAC 地址和 MAC 地址表来完成端到端的数据交换。第二层交换机只需识别数据帧中的 MAC 地址，直接根据 MAC 地址转发。第二层交换的解决方案，是一个“处处交换”的方案，虽然该方案也能划分子网、限制广播、建立 VLAN，但它的控制能力较小、灵活性不够，也无法控制流量，缺乏路由功能。因此只能被用于充当接入层交换机。Cisco 的 Catalyst 2960 系列、Catalyst 2950 系列、Catalyst 2970 系列和 Catalyst 500

Express 系列，都是二层交换机。

(1)端口类型。

交换机常见的端口有 4 种类型，即光纤端口、双绞线端口、GBIC 插槽和 SFP 插槽。为了增加连接的灵活性，适应更加复杂的网络环境，光纤端口已经逐渐被 SFP 或 GBIC 插槽所取代。由于第二层交换机上要用于接入层，上连同一建筑内的汇聚层交换机，下连普通用户的计算机，传输距离都非常有限，因此通常只需拥有 RJ-45 接口(100BasE-TX 或 1000BasE-T)即可。当然，若要实现与上层交换机(例如核心层交换机或汇聚层交换机)的远程连接，或与其他交换机之间的千兆位连接，也应当拥有 GBIC 或 SFP 插槽。

(2)端口速率。

从端口速率上来看，主要有 100Mbps 和 1000Mbps 两种。常见的搭配形式有 n×10/100Mbps、n×1000Mbps＋m×100Mbps 和 n×1000Mbps 三种。

- n×100Mbps 交换机所有端口全部都为 100Mbps 端口。桌面式交换机通常为 8 个端口，机架式交换机通常为 12、16、24 或 48 个端口。此类交换机是价格低廉的主流产品之一，大多为傻瓜交换机产品，被广泛地作为地段网络中的工作组交换机，为网络内的普通计算机提供接入服务。例如，Cisco Catalyst 2950-12T 接入层交换机拥有 12 个 100Mbps 端口。
- n×1000Mbps＋m×100Mbps 交换机拥有 2 个或 4 个 100Mbps 端口或插槽，以及 12、16、24 或 48 个 100Mbps 端口。由于可实现与其他交换机的千兆位连接，从而有效地解决了交换机之间的互连瓶颈。随着千兆位端口价格的不断下降，该类交换机的性价比越来越高，被广泛应用于对安全性和可管理性要求较高的接入层交换机。例如，Cisco Catalyst3560G 系列接入层交换机，均拥有 2 个 1000Mbps 端口。
- n×1000Mbps 交换机全都采用 1000Mbps 端口或插槽。此类交换机大多只充当着中心交换机或汇聚层交换机的角色，用于连接服务器或其他交换机。毫无疑问，千兆位的带宽能够完美实现任何网络功能，完全满足各种形式的网络需求，是搭建高性能网络的当然之选。例如，Cisco Catalyst 3750G 系列汇聚层交换机的全部端口均为 1000Mbps。

提示：交换机的端口属性主要包括两个方面，一个是端口数量，另一个是端口类型。在选择端口数量时，应当掌握如下两个基本原则：一方面，适当冗余。端口数量越多，交换机的价格越高。所以，应当根据接入计算机的数量来确定端口数量，并为未来计入的用户预留适当数量的端口；另一方面，高密度。由于交换机之间的互连会导致端口的浪费，因此，应当尽量选择 24 或 48 端口的交换机。

(3)延时。

交换机延时(Latency)也称为延迟时间，是指从交换机接收到数据包到开始向目的端口复制数据包之间的时间间隔，所采用的转发技术等因素均会影响延时。延时越小，数据的传输速率越快，网络的效率也就越高。特别是对于多媒体网络而言，较长的数据延迟，往往导致多媒体的短暂中断，所以交换机的延迟时间越短越好。

(4)MAC 地址数。

不同交换机的每个端口所能够支持的 MAC 数量不同。在交换机的每个端口上,都有足够内存(Buffer)记忆多个 MAC 地址,从而"记住"该端口所连接站点的情况。由于 Buffer 容量的大小限制了这个交换机所能够提供的交换地址容量,所以当该端口所容纳的计算机数量超过了地址容量时,目的站点的 MAC 地址将很可能并没有保存在该交换机端口的 MAC 地址表中,那么,该帧即将以广播方式发向交换机的每个端口。当这种情况频频发生时,将在很大程度上影响网络中数据的传输效率。不过,对于接入层交换机而言,由于实施通信的计算机和网络设备的数量有限,所以只要能够记忆 1024 个 MAC 地址基本上就可以了,而一般的交换机通常都能做到这一点。

(5)VLAN 表项。

VLAN 的主要作用有两点,一是将大的网络划分为若干小的子网络,从而减少广播,并提高网络传输效率;二是提高网络安全性,控制用户对某个子网络的访问,有效地保护敏感数据。VLAN 表项限制了网络内可容纳的 VLAN 数量,以及对 VLAN 访问控制的能力。如果 VLAN 表项较小,将限制对 VLAN 的划分,从而不适宜于安全和应用较为复杂的网络。

(6)扩展方式。

交换机扩展端口的方式有两种,一是级联,二是堆叠。采用级联方式时,交换机之间只能借助一个端口通信,从而使得交换机之间的连接成为网络瓶颈。采用堆叠方式时,借助于专用的模块和线缆,可以堆叠交换机间的高速无阻塞连接,并可以实现统一配置与管理。显然,堆叠更适合为大量的计算机提供接入服务,通常被接入层交换机所采用。例如,Cisco Catalyst 2950/2960 系列、Catalyst 3550/3560 系列和 Catalyst 3750 系列交换机,都是既支持级联又支持堆叠。

(7)链路汇聚。

使用端口聚合协议,可以将多个端口绑定在一起,从而成倍地增加连接带宽,并实现链路备份,以及端口间的负载均衡,保证交换机在几秒钟内快速从失败中恢复。

链路汇聚技术是将多台设备之间的多条物理链路捆绑为一个逻辑链路,使得该逻辑链路的容量为所有物理链路的容量之和。同时,当其中一条物理链路中断时,整个逻辑链路也不会中断,大大地提高了网络连接的可靠性。因此,链路汇聚技术也经常被用于接入层交换机与汇聚层交换机之间,尤其是没有千兆位级联的端口的交换机,在提高向上级联带宽的同时,还可以提高网络的稳定性和可用性。如图 3.10 所示,为只拥有 100Mbps 端口的 Cisco Catalyst 2950T-24 采用 4 条链路,连接至 Cisco Catalyst 3550G-24,从而实现接入层交换机与汇聚层交换机之间 400Mbps 的连接带宽,保证了所连接计算机与网络骨干的高速连接。

(8)管理功能。

应用于大中型网络中的交换机。应当都拥有管理功能,并且能够被第三方管理软件所管理。可网管交换机借助 VLAN、扩展树、QoS、端口聚合等,用于实现广播域的划分、冗余链路的智能选择、服务质量控制,以及将若干端口绑定在一起以成倍地增加网络带宽,从而适应大中型网络对网络安全、网络应用、网络控制和网络管理的需要。

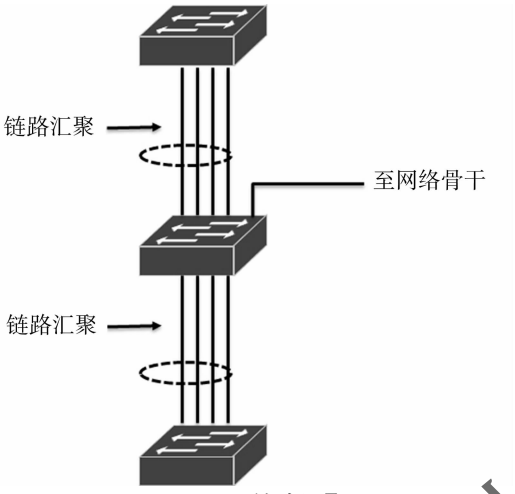

图 3.10　链路汇聚

3.2　认识路由器

路由器是管理数据在网段(或子网)之间的流动的设备。路由器存储其自己的网络接口状态的有关信息以及网络通信可能的问题和目标的列表,并根据这些信息来定向传入数据包和传出数据包。根据环境中使用的硬件设备和应用程序的数目和类型来计划网络通信和路由的需要,可以更好地决定使用专用硬件路由器、基于软件的路由器还是两者的组合。通常,专用硬件路由器在处理较重的路由需求时效果最好,而基于软件的路由器比较便宜,足以处理较轻的路由负载。

在子网之间的通信相对较轻的小型分段网络中,基于软件的路由解决方案(例如 Windows Server® 2008 中的"路由和远程访问"服务)可能比较理想。反之,在拥有大量网段并且性能要求的范围较广的企业网络环境中,可能需要各种基于硬件的路由器来担当网络中的不同角色。

3.2.1　路由器的种类划分

路由器是构成 IP 网络的核心,其本质作用就是连接不同类型的网络,智能选择最佳的信息传送线路。除此以外,路由器还具有访问控制功能。路由器也可以算作是一台专用计算机,而它的价格之所以昂贵,就在于其功能强大的软件,即 IOS(Internet Operation System,即因特网操作系统),可以听懂并翻译各种网络协议,就像一个会讲各种语言的人一样。

路由器的主要功能和一般应用虽然没有明显区别,但是为了满足各种应用需求,也出现过各式各样的路由器,无论是在价格还是在产品性能方面都存在着很大的差异。路由器的分类标准也不是唯一的,根据不同的标准,可以对路由器做不同的分类。

1.按性能划分

从路由性能上,路由器可分为高端、中端、低端和 SOHO 路由器。其中,SOHO 路由器主要适用于 SOHO 网络的 Internet 接入,通常采用固定配置路由器。Cisco 800/500 系列路由器就属于 SOHO 路由器,集成了 Internet 接入、安全和无线服务。

低端路由器主要适用于中小型网络的 Internet 接入或企业分支机构网络远程接入，端口数量和类型、包处理能力都非常有限。Cisco 1500/2500/3500 系列和 Cisco 1900/2900/3900 系列属中低端路由器。其中，Cisco 1800/1900 系列由于其性能和扩展性较差，只适用于较小型的网络，又称为入门级路由器。

中端路由器适用于较大规模的网络，拥有较高的包处理能力，具有较丰富的网络接口，适应较为复杂的网络结构。Cisco7200/7300/7600 系列和 ASR1000 系列属中端路由器，作为可扩展的多用途系统，能够为大中型网络应用提供可靠的第二层和第三层服务，可用于构建企业级数据中心互连平台。

高端路由器主要应用于大型网络的核心路由器，拥有非常高的包处理性能，并且端口密度高、端口类型多，以适应复杂的网络环境。Cisco ASR 1000/9000 和 XR 12000/12000 系列属高端路由器，多被电信级运营商用于构建超大规模的分布式结构网络。

Cisco1900/2900/3900 系列路由器为 ISR G2 路由器，无论是硬件配置，还是功能支持，都比 ISR 路由器有了较大幅度的提升，如表 3.1 所示。

表 3.1　　ISR 与 ISR G2 对比

对比元素	集成多业务路由器(ISR)	第二代集成多业务路由器(ISR G2)
广域网性能	处理服务时最大传输速率为 45Mbps	处理服务时最大传输速率为 150Mbps
网络处理器	单核处理器	多核处理器，支持未来扩展
服务模块性能和容量	1X 倍速和 160GB 存储容量	双核处理器最高支持 7X 倍速；1TB 存储容量
板载 DSP	仅语音	语音和视频就绪 DSP
交换机模块	支持以太网供电(PoE)的快速以太网；基于 Catalyst 3750	支持以太网供电(PoE)的快速以太网/千兆位以太网；基于 Catalyst 3560E/2950
IOS 镜像	多个镜像	仅一个通用 IOS 镜像
服务交付	硬件耦合	随需应变的服务
冗余	单主板	可现场更换的主板
能效	Energy Wise	Energy Wise 搭配基于插槽的控件

2.按结构划分

从结构上分，路由器可分为模块化结构与非模块化结构。通常情况下，几乎所有的中高低端路由器均为模块化结构，可以使用各种类型的模块灵活配置路由器，增加端口的数量、提供丰富的端口类型，以适应企业不断变化的业务需求。

SOHO 路由器多为非模块化结构，只能提供固定类型和数量的端口。

3.按网络位置划分

从路由器在网络中所处的位置划分，可以分为核心路由器、分发路由器和接入路由器，如图 3.11 所示。核心路由器位于数据网络中心，通常选用性能稳定的中高端模块化路由器。要求快速的包转发能力与高速的网络接口，全部为大容量、高性能的模块化结构。

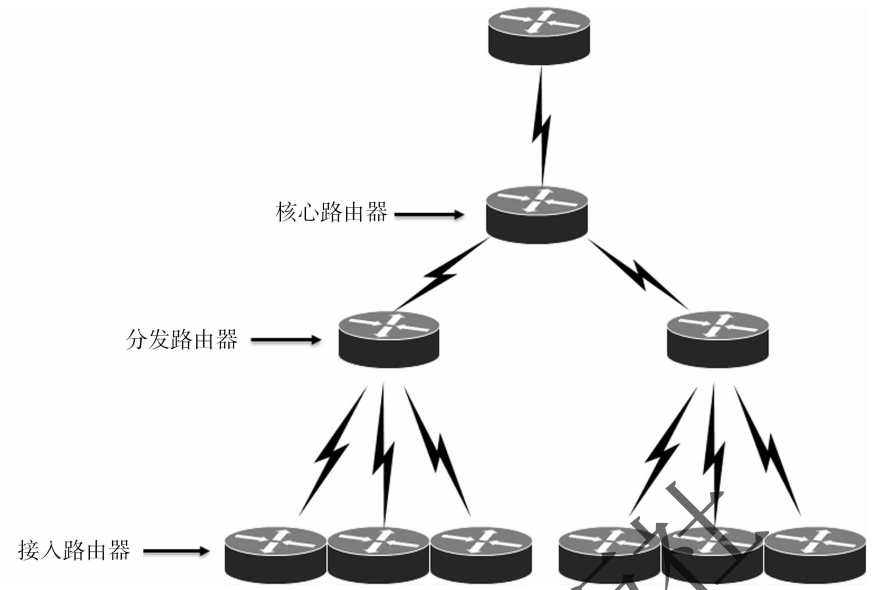

图 3.11　不同网络位置的路由器

分发路由器要用于实现接入路由器的汇接与转发，并接入核心路由器。主要目标是以尽量便宜的方法实现尽可能多的端点互连，并且进一步要求支持不同的服务质量。分发路由器主要采用中低端路由器，主要特点就是端口数量多、价格便宜、应用简单。

4.按功能划分

从路由器的功能方面划分，路由器可分为通用路由器与专用路由器。一般所说的路由器为通用路由器。专用路由器通常为实现某种特定功能对路由器接口、硬件等作专门优化，例如网吧路由器、安全路由器、VPN 路由器等。

5.按转发性能划分

从数据转发性能划分，路由器可分为线速路由器和非线速路由器。通常线速路由器是高端路由器，能以物理链路所支持的最高速率转发数据包；中低端路由器大多是非线速路由器，只能以低于线速的速率转发数据。

6.按网络类型划分

从广义的角度而言，路由器可分为有线路由器和无线路由器两大类。顾名思义，有线路由器就是借助物理连线（光纤、双绞线、同轴线缆等）建立连接的路由器。常见的路由器基本上都是有线路由器。无线路由器是随着无线网络应用的快速普及，在近几年才出现的新产品。无线路由器的功能和有线路由器没有什么区别，同样是用来连接不同的网络或 Internet 接入，不同的是它的连接不是通过有形的连线实现的，而是借助无形的电磁波实现的。

当然，无线路由器除了提供无线接口以外，也提供有线连接端口（以固定端口方式提供，或者借助相应的网络模块提供）。一些中低端路由器通过安装无线路由模块，也可以提供对无线网络的支持。

3.2.2 路由器的规格及选用策略

如今的路由器市场真可谓百家争鸣，不同类型的产品其功能和应用领域也会有所不同，那么如何才能根据自己的网络规模选择一款合适的路由器呢，在选择路由器时，应当考虑哪些因素和参数呢？

1.路由器基本参数

在多种路由器之间进行权衡和选择时，需要参照一些共性的标准，这就是此处要介绍的路由器基本参数。

(1)接口类型。

路由器能支持的接口类型，体现了路由器的通用性。常见的接口类型有：通用串行接口(例如 RS 232 DTE/DCE 接口、V.35 DTE/OCE 接口、X.2 DTE/DCE 接口、RS 449 DTE/DCE 接口和 EIA 530 DTE 接口等)，10Mbps、10/100Mbps、1000Mbps 以太网接口，GBIC 插槽、SFP 插槽和 ATM 接口等。对于模块化路由器而言，业务板类型是否齐全，决定着接口类型是否丰富。

(2)CPU。

对于任何一款路由器产品而言，CPU 都是它的“大脑”。通常在中低端路由器中，CPU 负责交换路由信息、路由表查找以及转发数据包。CPU 的能力直接影响路由器的吞吐量(路由表查找时间)和路由计算能力(影响网络路由收敛时间)。在高端路由器中，通常包转发和查表功能由 ASIC 芯片完成，CPU 只实现路由协议、计算路由以及分发路由表等任务。由于技术的发展，路由器中的许多工作都可由硬件实现(专用芯片)。CPU 性能并不完全反映路由器的性能。路由器性能可由路由器吞吐量、时间延迟和路由计算能力等指标体现。

(3)内存。

路由器中可能有多种内存，例如闪存(Flash)、DRAM 等。内存用于存储配置、路由器操作系统、路由协议软件等。在中低端路由器中，路由表可能存储在内存中。通常来说，路由器内存越大越好(不考虑价格)。但是，与 CPU 能力类似，内存同样不直接反映路由器的性能。因为高效的算法与优秀的软件可能大大节约内存。

为了标语配置和系统升级，许多路由器外置了 Flash 插槽，可以根据需要选择相应容量的内存卡。

(4)背板能力。

背板能力，是指路由器背板容量或者总线带宽能力，体现于路由器的吞吐量。背板能力对于保证整个网络之间的连接速度是非常重要的。如果所连接的两个网络速率都较快，而由于路由器的带宽限制，这将直接影响整个网络之间的通信速度。所以，对于连接较大网络的中高端路由器而言，当网络间的数据流最较大时，应当特别关注路由器的背板容量、背板能力。

(5)端口吞吐量。

端口吞吐量，是指路由器包转发能力，即路由器在某端口上的包转发能力，基本可以衡量路由器的路由性能.以 pps(包每秒)为单位，应当达到线速处理能力。端口吞吐量通常采用两个相同速率接口测试。但是，测试接口可能与接口位置及关系相关。例如，同一插卡端口间测试的吞吐量，可能与不同插卡上端口间吞吐量值不同。

提示：中高端路由器可以使较大的数据包进行正确快速转发；而低端路由器则只能转发小

的数据包，对于那些较大的数据包，则需要拆分成许多小的数据包来分开转发，数据包的转发能力就差了。其实，这与背板容量有非常紧密的关系。

(6)丢包率。

丢包率，是指路由器在稳定的持续负荷下，由于资源缺少在应该转发的数据包中不能转发的数据包所占的比例。丢包率的大小会影响到路由器线路的实际工作速度，严重时甚至会使线路中断。

提示：小型企业网络一般流量不会很大，所以出现丢包现象的机会也很小。因此，低端路由器对该参数不必作太多考虑。

(7)转发时延。

转发时延，是指需要转发的数据包最后一比特进入路由器端口，到该数据包第一比特出现在端口链路上的时间间隔。转发时延较高时，不仅会影响网络传输效率，而且还不能很好地实现视频会议、IP 电话等实时通信。该参数与背板容量、吞吐量等参数紧密相关。

(8)路由表能力。

路由器通常依靠建立及维护的路由表来决定如何转发。路由表能力，是指表内所容纳路由表项数量的极限。一般来说，高端路由器路由表容量应当较大，因为它将面对非常庞大的网络，而中低端路由器通常对路由表能力没有什么要求。原因很简单，其所应用的网络结构相对简单。该参数与路由器自身所带的缓存大小有关。

(9)网络协议。

路由器应当支持开放标准的协议。开放标准的协议是设备互连的良好前提，所支持的协议也意味着设计的灵活和高效。例如，是否支持完全的组播路由协议、是否支持 MPLS、是否支持冗余路由协议 VRRP。此外，如果网络有特殊需求，那么在考虑 IP 路由的同时，还应当考虑路由器对 IPX、AppleTalk 路由的支持能力。

一些设备厂商为了提高效率，会开发出一些私有的协议，用户在选择这些特性上最好根据自己的需要选择，同时应当尽量避免在核心技术上采用此类技术。原因很简单，不标准的协议意味着不同设备供应商之间的不兼容，从而使用户困死在一个设备供应商上。同时，不标准的协议在历史上也往往是被新型的开放协议所取代。

(10)可靠性。

可靠性是指路由器的可用性、负载承受能力、无故障工作时间和故障恢复时间等指标。路由器的可靠性主要体现在接口故障和网络流量增大时的适应能力，保证这种适应能力的方式就是备份，可靠性也是选择路由器应该考虑最多的问题。因为路由器的安全可靠实际上就是网络安全可靠的保障。可靠性也包括多个方面，例如硬件冗余、模块热插拔等。

提示：可靠性通常是由用户口碑、品牌信誉、产品销量、技术先进程度等作为保障的。

(11)安全性。

由于网络黑客和病毒的流行，设备本身的保护和抵御能力也是选择路由器的一个重要因素。已经有部分路由器提供了防止黑客攻击的手段，提供设备全连接 SSH 和安全复制(SCP)功能。另外，路由器本身在使用 RADIUS/TACACS＋等认证的同时，还会使用大量的访问控制列表(ACL)来屏蔽和隔离病毒，因此在选择路由器时应注意 ACL 的控制方式。如果采用 CPU 检查方式，将会降低路由器的运行性能而采用硬件实现的方式，则不会对运行构成额外的负担。

(12)可管理性。

路由器设备可管理性代表了设备监控、维护和管理的重要特性。用户在选择时也必须考虑到设备厂商所能提供的网管系统、对设备本身可管理的方式和方法。

(13)其他功能。

路由器除了应当具备传统的数据传输、包交换功能之外,还要支持数据分类、优先级控制、用户识别和快速自愈等特性。具体来讲,VPN、QoS 能力、组播技术、安全和管理性都要具备。同时,随着语音应用的发展,是否支持语音功能也要视自己的应用情况来决定。Cisco 的集成多业务路由器(简称 ISR),可实现集成语音、安全、视频等主要应用,为中小型企业、大型企业分支机构提供安全、线速的数据、话音、视频和其他高级服务。既满足了客户分支机构更安全地快速访问公司内部数据资源,同时还可以通过选装模块获得诸如 VPN 加速、增强的入侵防护、URL 过滤、话音交换系统等增强性网络服务。

2.路由器性能参数

路由器性能参数主要包括以下几个方面。

(1)全双工线速转发能力。

路由器最基本且最重要的功能是数据包转发。在同样端口速率下转发小包是对路由器包转发能力最大的考验。全双工线速转发能力是指以最小包长(以太网 64B、POS 端口 40B)和最小包间隔(符合协议规定)在路由器端口上双向传输的同时不引起丢包。该指标是路由器性能的重要指标。

(2)设备吞吐量。

这是指设备整机包转发能力,是设备性能的重要指标。路由器根据 IP 包头或 MPIS 标记来进行选路,所以性能指标是每秒转发的包数量。设备吞吐量通常小于路由器所有端口吞吐量之和。

(3)端口吞吐量。

端口吞吐量是指端口包转发能力,通常使用 PPS(包每秒)来衡量,它是路由器在某端口上的包转发能力。通常采用两个相同速率接口测试。但是测试接口可能与接口位置及关系相关。例如同一插卡上端口间测试的吞吐量可能与不同插卡上端口间的吞吐量值不同。

(4)背靠背帧数。

背靠背帧数是指以最小帧间隔发送最多数据包不引起丢包时的数据包数量。该指标用于测试路由器缓存能力。有线速全双工转发能力的路由器该指标值无限大。

(5)路由表能力。

路由器通常依靠所建立及维护的路由表来决定如何转发数据。路由表能力是指路由表内所容纳路由表项数量的极限。由于 Internet 上执行 BGP 协议的路由器通常拥有数十万条路由表项,所以该项口也是路由器能力的重要体现。

(6)背板能力。

背板能力是路由器的内部实现,背板能力体现在路由器的吞吐量上:背板能力通常大于依据吞吐量和测试包场所计算的值。但是背板能力只能在设计中体现,一般无法测试。

(7)丢包率。

丢包率是指测试中所丢失数据包数量占所发送数据包的比率,通常在吞吐量范围内测试。

丢包率与数据包长度及包发送频率相关。在一些环境下可以加上路由抖动、大量路由后测试。

(8)时延。

时延是指数据包第一个比特进入路由器到最后一比特从路由器输出的时间间隔。在测试中通常使用测试仪表发出测试包到收到数据包的时间间隔。时延与数据包长相关,通常在路由器端口吞吐量范围内测试,超过吞吐量测试该指标没有意义。

(9)时延抖动。

时延抖动是指时延变化。数据业务对时延抖动不敏感,所以该指标没有出现在 Benchmarking 测试中。由于 IP 上的多业务,包括语音、视频业务的出现,该指标才有测试的必要性。

(10)VPN 支持能力。

通常路由器都能支持 VPN。其性能差别一般体现在所支持的 VPN 数量上。专用路由器一般支持的 VPN 数量较多。无故障工作时间,该指标按照统计方式指出设备无故障工作的时间。一般无法测试,可以通过主要器件的无故障工作时间计算或者大量相同设备的工作情况计算。

(11)内部时钟精度。

拥有 ATM 端口做电路仿真或者 POS 口的路由器互连通常需要同步。如使用内部时钟则其精度会影响误码率。内部时钟精度级别定义及测试方法可参见相应同步标准。

3.路由器的选用策略

在组建局域网时,路由器的选择也是一项重要的内容。在选购时,要根据用户的实际使用情况,首先确定是选择接入点(AP)级别,家用级别或企业级别的路由器,然后再根据路由器选择方面的基本原则,确定产品的基本性能要求。

在选择路由器时,应当遵循如下基本原则。

(1)协议标准化原则。

必须选择基于国际标准或行业标准的路由器。由于一些特殊路由协议,只有特定厂商的产品才予以支持,因此不太适合充当大型广域网络中的路由设备。

(2)操作简单化原则。

必须选择技术实用、操作简单的路由器。实现的技术越简单,包处理效率越高、越不容易发生故障。操作过程越简单,实现功能的配置和管理就越方便。同一系列产品的路由器操作系统应当与交换机操作系统完全一致或基本一致。从而减轻网络管理员学习和掌握相关技术的难度。例如,不仅所有 Cisco 网络设备(例如交换机、路由器、防火墙甚至无线设备)都采用了 Cisco IOS 操作系统,而且各个业务模块都可以交互使用。同时,不仅路由器系列、交换机系列的模块可以通用,而且路由器和交换机的模块也可以通用。除此之外,Cisco 还分别为交换机、路由器和安全设备提供了图形化配置和管理界面,实现了网络设备的傻瓜化管理。

(3)环境适应化原则。

必须选择环境适应性强的路由器。如果网络规模较大,网络链路形式复杂,网络应用多样,那么,将要求路由器拥有较高的适应能力。同时,路由器还应当具有一定的可扩展性,能够适应网络规模的扩大,或者拓扑结构的改变。也就是说,不仅要提供种类丰富的端口,以满足与远程路由设备的连接,而且,还应当提供丰富的功能,从而实现网络应用所需要的各种服务。

(4)设备可管理原则。

必须选择拥有强大监管和配置能力的路由器。路由器应当能够提供丰富的系统统计信息和运行日志,能够实现对故障的诊断和追踪,实现对深层故障的检测诊断,并能有效地实现设备的远程管理和维护,甚至在故障发生前或故障发生时,及时向网络管理员发出警告。

(5)系统容错冗余原则。

用户在选择路由器时,应充分考虑设备是否支持热插拔,支持备份设置,支持自动切换等功能。对于大型网络中关键应用的核心路由器,应当拥有冗余电源、冗余风扇等模块。例如,Cisco 7613 高可用性路由器,拥有 2 个冗余管理模块,以及 2 个冗余电源模块。

(6)安全可靠性原则。

针对现代网络存在的各种安全隐患,路由器必须具有可靠的安全特性。路由器系统软件本身应当具有简单的 IDS 和 IPS 功能,拥有抵御一般网络攻击的能力,从而保护内部网络不受外部恶意攻击的侵害。当然,如果能够配置相应的功能模块,其安全效果将会更加完美。例如,Cisco 路由器的防火墙模块,可以让路由器所有端口都充当防火墙端口。

除了上述的一些选择原则之外,在选购路由器时,还应认真权衡如下一些因素。

(1)实际需求。

作为电子产品,网络技术成熟周期不断缩短、设备制造成本不断下降、网络需求和网络应用日新月异,因此网络设备的淘汰周期(通常为 5 年左右)也在不断加快。所以,在制订设备购置计划时,应当考虑网络规模和网络应用的实际需要,不要盲目追求高性能、高稳定性,只要能满足实际需求并略有性能储备就可以了。

(2)可扩展性。

充分考虑到近期内(1~3 年内)可能的网络扩展和升级,路由设备(尤其是核心路由设备)的性能和插槽都应当留有一定的扩展余地,以适应网络拓扑结构变化、网络应用服务发展、网络数据传输量增加的需要。

(3)性能和稳定性。

兼顾产品的性能和稳定性,既保证网络数据的高速传输,又保障网络链路的稳定传输,还拥有丰富的功能和充分的安全性。总之,对于作为网络核心(利用路由设备作为核心设备)和网络边界(利用路由器实现与其他网络的连接)的路由器而言,高速、高效、稳定、安全两者缺一不可。

(4)产品性价比。

无论是企事业单位,还是政府机关.在能够满足网络对性能和稳定性要求的前提下,应当尽量压缩开支,选择价格低廉、最具性价比的路由产品。近几年,国内网络设备厂商(例如华为、锐捷等)的技术不断成熟,设备的整体性能已经达到和接近国外知名产品的水平。因此,在性能相近的情况下,建议选择更具价格优势、更加安全的国货产品。

提示:对于大专院校和教育科研部门而言,如果采购进口产品,还可以申请享受免增值税和关税,从而节约大致 20%的费用。

(5)产品品牌。

品牌往往是技术含量和稳定性的保障。通常情况下,应选择知名品牌的产品,因此选择路由器时,不可避免地将涉及品牌因素的产品,以保证设备之间的连通性和兼容性。另外,路由器和交换机应当尽量选择同一厂商以及网络协议和网络技术的一致性。

另外，品牌往往与服务连接在一起。路由器作为一种高科技产品，售前售后的支持和服务显得尤其重要。应尽量选择售后服务方便、快捷的产品。

3.2.3　默认路由、静态路由及动态路由

路由方式分为默认路由、静态路由及动态路由三种。此处将分别解释这三种路由方式的概念。

1.默认路由

默认路由是一种特殊的静态路由，指的是当路由表中与包的目的地址之间没有匹配的表项时路由器能够做出的选择。如果没有默认路由，那么目的地址在路由表中没有匹配表项的包将被丢弃。默认路由在某些时候非常有效，当存在末梢网络时，默认路由会大大简化路由器的配置，减轻管理员的工作负担，提高网络性能。

默认路由和静态路由的命令格式一样。只是把目的地 IP 和子网掩码改成 0.0.0.0 和 0.0.0.2。由于默认路由只能存在末梢网络中，所以只有 R1 和 R3 可用，如图 3.12 所示，配置格式为：

R1(config)#ip route 0.0.0.0 0.0.0.0 10.0.0.2

R3(config)#ip route 0.0.0.0 0.0.0.0 20.0.0.1

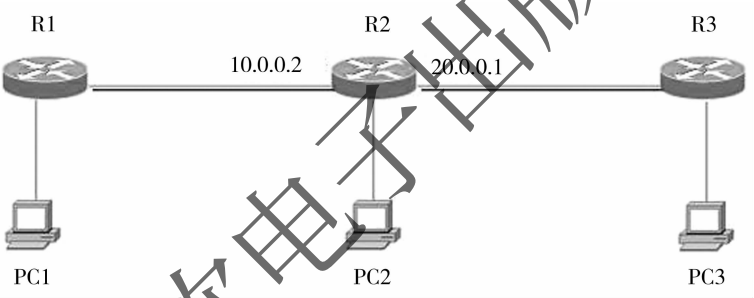

图 3.12　默认路由

默认路由(Default route)，是对IP 数据包中的目的地址找不到存在的其他路由时，路由器所选择的路由。目的地不在路由器的路由表里的所有数据包都会使用默认路由。这条路由一般会连接另一个路由器，而这个路由器也同样处理数据包：如果知道应该怎么路由这个数据包，则数据包会被转发到已知的路由；否则，数据包会被转发到默认路由，从而到达另一个路由器。每次转发，路由都增加了一跳的距离。

当到达了一个知道如何到达目的地址的路由器时，这个路由器就会根据最长前缀匹配来选择有效的路由。子网掩码匹配目的 IP 地址而且有最长的网络会被选择。用无类域间路由标记表示的 IPv4 默认路由是 0.0.0.0/0。因为子网掩码是/0，所以它是最短的可能匹配。当查找不到匹配的路由时，自然而然就会转而使用这条路由。同样地，在 IPv6 中，默认路由的地址是::/0。一些组织的路由器一般把默认路由设为一个连接到网络服务提供商的路由器。这样，目的地为该组织的局域网以外——一般是互联网、城域网或者 VPN 的数据包都会被该路由器转发到该网络服务提供商。当那些数据包到了外网，如果该路由器不知道该如何路由它们，它就会把它们发到它自己的默认路由里，而这又会是另一个连接到更大的网络的路由器。同样地，如果仍然不知道该如何路由那些数据包，它们会去到互联网的主干线路上。这样，目的地址会被认为不存在，数据包就会被丢弃。

主机里的默认路由通常被称作默认网关。默认网关通常会是一个有过滤功能的设备，如防火墙和代理服务器。

若要指定默认路由，可以使用如下命令来实现：

ip route 0.0.0.0 0.0.0.0

ip default-network

ip default-gateway

default-information originate

ip default-gateway

当路由器上的 ip routing 无效时，使用它指定默认路由，用于 RXBoot 模式（no ip routing）下安装 IOS 等。或者关闭 ip routing 让路由器当主机用，此时需要配置默认网关。另外此命令常用于二层交换机上，因为在二层交换机上没有第三层路由表项。

2.静态路由

静态路由是指由用户或网络管理员手工配置的路由信息。当网络的拓扑结构或链路的状态发生变化时，网络管理员需要手工去修改路由表中相关的静态路由信息。静态路由信息在缺省情况下是私有的，不会传递给其他的路由器。当然，网管员也可以通过对路由器进行设置使之成为共享的。静态路由一般适用于比较简单的网络环境，在这样的环境中，网络管理员易于清楚地了解网络的拓扑结构，便于设置正确的路由信息。

在一个支持 DDR（dial-on-demand routing）的网络中，拨号链路只在需要时才拨通，因此不能为动态路由信息表提供路由信息的变更情况。在这种情况下，网络也适合使用静态路由。

使用静态路由的另一个好处是网络安全保密性高。动态路由因为需要路由器之间频繁地交换各自的路由表，而对路由表的分析可以揭示网络的拓扑结构和网络地址等信息。因此，网络出于安全方面的考虑也可以采用静态路由。不占用网络带宽，因为静态路由不会产生更新流量。

大型和复杂的网络环境通常不宜采用静态路由。一方面，网络管理员难以全面地了解整个网络的拓扑结构；另一方面，当网络的拓扑结构和链路状态发生变化时，路由器中的静态路由信息需要大范围地调整，这一工作的难度和复杂程度非常高。

路由器在执行路由过程中，需要查看路由表来决定如何转发数据包，用静态路由一个个地配置，繁琐易错。如果路由器有个邻居知道怎么前往所有的目的地，可以把路由表匹配的任务交给它，省去了很多麻烦。

例如，网关会知道所有的路由，如果一个路由器连接到网关，就可以配置默认路由，把所有的数据包都转发到网关。

为什么默认路由是 0.0.0.0 呢？在匹配 IP 地址时，0 表示通配（wildcard），也就是说，任何值都可以。所以 0.0.0.0 和任何目的地址匹配都会成功，造成默认路由要求的效果。

3.动态路由

动态路由，简单来说动态路由是指路由器能够自动地建立自己的路由表，并且能够根据实

际情况的变化适时地进行调整。

动态路由器上的路由表项是通过相互连接的路由器之间交换彼此信息，然后按照一定的算法优化出来的，而这些路由信息是在一定时间间隙里不断更新，以适应不断变化的网络，以随时获得最优的寻路效果。为了实现 IP 分组的高效寻路，IETF 制定了多种寻路协议。其中用于自治系统（AS：Autonomous System）内部网关协议有开放式最短路径优先（OSPF：Open Shortest Path First）协议和寻路信息协议（RIP：Routing Information Protocol）。所谓自治系统是指在同一实体（例如学校、企业或 ISP）管理下的主机、路由器及其他网络设备的集合。还有用于自治域系统之间的外部网络路由协议 BGP-4 等。

运行这些路由协议的软件就是我们通常说的路由软件，Linux 下常见的路由软件有 gated 和 zebra。前者既有 GPL 版本的发行，又有收费的版本；而后者则是日本某组织开发的完全 GPL 的高效的路由软件。Linux 的发行里面一般默认就有 gated 这个软件，我们下面主要介绍它的配置和使用方法。

动态路由机制的运作依赖路由器的两个基本功能：对路由表的维护；路由器之间适时的路由信息交换。

路由器之间的路由信息交换是基于路由协议实现的。交换路由信息的最终目的在于通过路由表找到一条数据交换的“最佳”路径。每一种路由算法都有其衡量“最佳”的一套原则。大多数算法使用一个量化的参数来衡量路径的优劣，一般来说，参数值越小，路径越好。

该参数可以通过路径的某一特性进行计算，也可以在综合多个特性的基础上进行计算。几个比较常用的特征是：路径所包含的路由器结点数（hop count）、网络传输费用（cost）、带宽（bandwidth）、延迟（delay）、负载（load）、可靠性（reliability）和最大传输单元 MTU（maximum transmission unit）。

3.2.4　路由信息协议（RIP）

RIP（Routing Information Protocol，即路由信息协议）路由协议是一种相对古老，在小型及同介质网络中得到了广泛应用的路由协议。RIP 采用距离向量算法，是一种距离向量协议。RIP 在 RFC 1058 文档中定义。

RIP 使用 UDP 报文交换路由信息，UDP 端口号为 520。通常情况下，RIPv1 报文为广播报文；而 RIPv2 报文为组播报文，组播地址为 224.0.0.9。RIP 每隔 30s 向外发送一次更新报文。如果路由器经过 180s 没有收到来自对端的路由更新报文，则将所有来自此路由器的路由信息标志为不可达，若在 240s 内仍未收到更新报文就将这些路由从路由表中删除。

RIP 使用跳数来衡量到达目的地的距离，称为路由量度。在 RIP 中，路由器到与它直接相连网络的跳数为 0；通过一个路由器可达的网络的跳数为 1，其余依此类推；不可达网络的跳数为 16。

如表 3.2 所示，给出了 RIP 的默认配置。

表 3.2 RIP 的默认配置

特性	默认设置
自动摘要	启用
初始默认信息	无
默认 metric	Built-in;自动翻译
IP RIP 认证关键链	未认证 认证模式:clear text(清除文本)
IP RIP 接收版本	取决于路由器配置命令版本
IP RIP 发送版本	取决于路由器配置命令版本
IP RIP triggered	取决于路由器配置命令版本
IP RIP horizon	使用媒体分类
邻居	未定义
网络	未指定
Offset 列表	禁用
输出延迟	0ms
基本时钟	更新:30s 无效:180s Hold-down:180s Flush:240s
无效更新源	禁用
版本	接收 RIP 版本 1 和版本 2 数据包;发送版本 1 数据包

若要配置 RIP 路由,必须为一个网络启用 RIP 路由器,并且选择性地配置一些相关参数。在特权 Exec 模式下开始执行如下操作,以此来启用并配置 RIP。

(1)进入全局配置模式。

Router # configure terminal

(2)启用 IP 路由器。

Router(config)# ip routing

(3)启用 RIP 路由,进入路由器配置模式。

Router(config)# router rip

(4)使用 RIP 路由器程序连接一个网络。

Router(config)# network network number

(5)(可选)定义一个相邻路由器,以交换路由信息至该路由器。

Switch(config)# neighbor ip-address

(6)(可选)偏移量设置,是对通过 RIP 学习和通告的路由进行路由量度的增加设置。通过应用匹配访问列表,可以对某个指定接口的某些进站和出站路由进行偏移量设置,而其他路由偏移量保持不变。

Router(config)# offset list [accesS-list number | name] {in | out} offset [type number]

提示：设置 RIP 偏移量，需要注意当量度值为 16 时，该路由将被看作无效路由，此偏移量的取值十分重要。偏移量设置适当，也可以用于过滤路由。

(7)(可选)调整路由协议时钟，其中：

- update：路由更新时间，定义路由器发送路由更新报文的周期，默认为 30s。
- invalid：路由无效时间，定义路由表中路由因没有更新而变为无效的时间，默认为 180s。
- holddown：路由拒绝时间，在该时间内，路由器不会接受其他路径的路由，默认为 180s。
- flush：路由清除时间，该时间过后，该路由将被清除出路由表，默认为 240s。

Router(config)# timers basic update invalid holddown flush

提示：通过调整以上时钟，可能会加快路由协议的收敛时间及故障恢复时间。

(8)(可选)配置接收和发送 RIP 版本 1 或 RIP 版本 2 数据包。默认情况下，只接收版本 2 发送版本 1。

Router(config)# version {1 | 2}

(9)(可选)禁用自动汇总。RIP 路由自动汇总，就是当子网路由穿越有类网络边界时，将自动汇总成有类网络路由。RIPv2 默认值情况下将进行路由自动汇总，RIPv1 不支持该功能。RIPv2 路由自动汇总的功能提高了网络的伸缩性和有效性。如果有汇聚路由存在，则在路由表中将看不到包含在汇聚路由内的子路由，这样可以大大缩小路由表的规模。

通过汇聚路由，会比通告单独的每条路由更有效率，主要有以下因素：

- 当查找 RIP 数据库时，汇聚路由会得到优先处理。
- 当查找 RIP 数据库时，任何子路由将被忽略，减少了处理时间。

有时可能希望学到具体的子网路由，而不愿意只看到汇总后的网络路由，这时需要关闭路由自动汇总功能。

Router(config)# no auto summary

(10)(可选)禁止 RIP 路由源地址验证配置。默认情况下，RIP 会对进站的路由更新报文源地址进行验证，如果源地址无效，RIP 就会丢弃该报文。判断源地址是否有效，就是判断源 IP 地址是否与接口 IP 地址在相同的网络内。如果是无编号 IP 地址接口，将不会进行有效性验证。

Router(config)# no validatE-updatE-source

(11)(可选)增加 RIP 更新发送延迟。

Router(config)# output-delay delay

(12)返回特权 Exec 模式。

Router(confiG-router)# end

(13)校验配置。

Router # show ip protocols

(14)保存配置。

Router # copy runninG-config startup-config

禁用 RIP 路由时，使用“no router rip”全局配置命令。

若要显示活动路由器协议的参数和目前的状态，可以使用“show ip protocols”特权 Exec 命

令。使用“show ip rip database”特权 Exec 命令，可以显示 RIP 数据库中的地址。

3.2.5 路由器的网络地址转换(NAT)功能

网络地址转换(Network Address Translation，NAT)被广泛应用于各种类型的 Internet 接入方式和各种类型的网络。原因很简单，NAT 不仅完美地解决了 IP 地址不足的问题，而且还能有效地避免来自网络外部的攻击，隐藏并保护网络内部的计算机。虽然 NAT 也可以借助于某些代理服务器实现，但考虑到运行成本，很多时候都是在路由器 L 实现。

随着接入 Internet 计算机数量的不断猛增，IP 地址资源也就愈加显得捉襟见肘。事实上，除了中国教育和科研计算机网(CERNET)外，用户几乎根本申请不到整段的 C 类 IP 地址了。在其他 ISP 那里，即使是拥有几百台的计算机大型网络接入 Internet，分配给用户的也只有几个或十几个 IP 地址。显然，这几个少得可怜的 IP 地址根本无法满足网络用户需求，于是就产生了 NAT 技术。

借助于 NAT，私有(保留)地址的“内部”网络通过路由器发送数据包时，私有地址被转换成合法的 IP 地址，从而只需使用少量 IP 地址(甚至是 1 个)，即可实现私有地址网络内所有计算机与 Internet 的通信。也就是说，在网络内的计算机数量大于 ISP 提供的合法 IP 地址时，NAT 就有了自己的用武之地。

NAT 将自动修改 IP 报文头中的源 IP 地址和目的 IP 地址，IP 校验则在 NAT 处理过程中自动完成。有些应用程序将源 IP 地址嵌入到 IP 报文的数据部分中，所以还需要同时对报文进行修改，以匹配 IP 头中已经修改过的源 IP 地址。否则，在报文数据部分嵌入 IP 地址的应用程序就不能正常工作。令人遗憾的是，尽管 NAT 的 Cisco 版本可以处理许多应用，但它毕竟也不是万能的，还是有一些应用无法被支持。如表 3.3 所示，列举了 Cisco NAT 支持的和不支持的应用。

表 3.3　　Cisco NAT 支持和不支持的应用

支持的应用	不支持的应用
任何非源和目的的 TCP/UDP 报文	IP 组播
在 IP 报文的数据部分中的 IP 地址	路由表更新
ICMP	
FTP	DNS 域的迁移
TCP 上的 NetBIOS(会话服务除外)	BOOTP
RealAudio	Talk，ntalk
White Pines CUSeeMe	SNMP
Streamworks	NetShow
DNS(“A”和“PTR”查询)	
H.323	
NetMeeting	
VDOLive	
Vxtreme	

NAT 的实现方式有 3 种，即静态转换、动态转换和端口多路复用。

静态转换：是指将内部网络的私有地址转换为公用 IP 地址时，IP 地址对是一对一的，是一成不变的，某个私有 IP 地址只能转换为某个公用 IP 地址。借助于能态转换，可实现外部网络

对内部网络中某些特定设备(如服务器)的访问。

动态转换:是指将内部网络的私有 IP 地址转换为公用 IP 地址时,IP 地址对是不确定的、是随机的,所有被授权访问 Internet 的私有 IP 地址,可随机转换为任何指定的合法 IP 地址。也就是说,只要指定哪些内部地址可以进行转换,以及用哪些合法地址作为外部地址时,就可以进行动态转换。动态转换可以使用多个合法外部地址集。当 ISP 提供的合法 IP 地址略少于网络内部的计算机数量时,可以采用动态转换的方式。

端口多路复用,是指改变外出数据包的源端口并且端口转换完成,即端口地址转换(Port Address Translation,PAT)。采用端口多路复用方式,内部网络的所有主机均可共享一个合法外部 IP 地址以实现对 Internet 的访问,从而可以最大限度地节约 IP 地址资源。同时,又可隐藏网络内部的所有主机,有效避免来自 Internet 的攻击。因此,目前网络中应用最多的就是端口多路复用方式了。

在配置网络地址转换实现的过程之前,首先必须搞清楚内部接口和外部接口,以及在哪个外部接口上启用 NAT。通常情况下,连接到企业网络的接口是 NAT 内部接口,而连接到外部网络(例如 Internet)的接口是 NAT 外部接口,如图 3.13 所示。

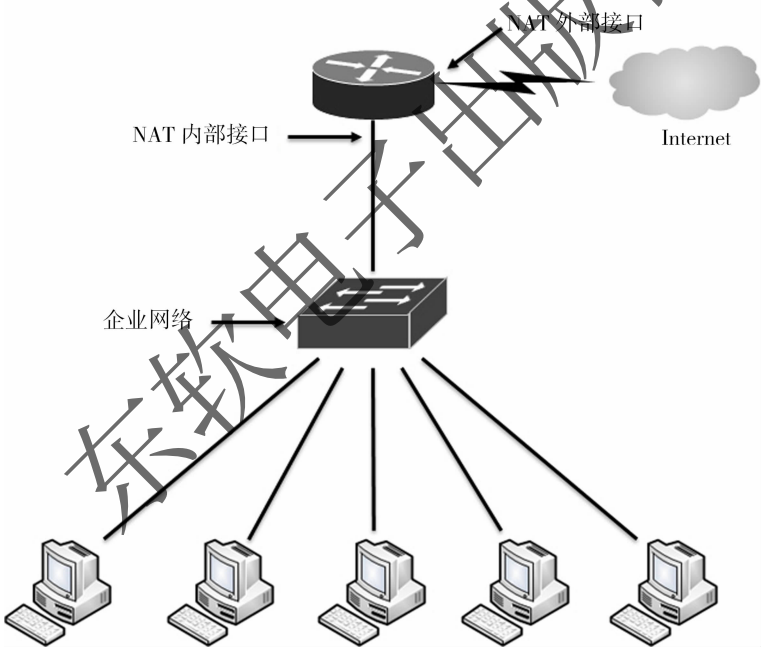

图 3.13　网络地址转换

NAT 地址转换的实现方式包括三种,一种是静态地址转换,另一种是动态地址转换,还有一种是端口复用地址转换。我们将逐一进行大体介绍。

- 静态地址转换:所谓静态地址转换,是指将合法的 IP 地址一一对应地转换为内部私有 IP 地址。如果企业网获得了多个合法的 IP 地址,可以借助静态地址转换方式来将合法 IP 地址转换为内部服务器的 IP 地址,从而实现对企业网络和 Internet 对服务器的访问。
- 动态地址转换:所谓动态地址转换,是指将内部私有 IP 地址动态地转换为合法 IP 地址池内的 IP 地址,对应关系是不固定的。如果企业网络获得多个合法 IP 地址,可以借助动态地址转换方式,实现 Internet 连接共享。

- 端口复用地址转换：所谓端口复用地址转换，是指通过复用 TCP 端口的方式，使用一个合法 IP 地址实现 Internet 连接共享。如果企业网络只获得一个合法的 IP 地址，则应当采用端口复用地址转换方式。

3.2.6 Windows Server 中的软件路由

Windows Server® 2008 操作系统中的路由和远程访问服务使远程用户可以通过虚拟专用网络(VPN)或拨号连接访问专用网络上的资源。配置了“路由和远程访问”服务的服务器可以提供局域网(LAN)和广域网(WAN)路由服务，用来连接小型办公网络中的网段或通过 Internet 连接两个专用网络。

正如“路由和远程访问”服务的名称所表述的那样，“路由和远程访问”服务的主要功能包括远程访问和路由，具体介绍如下。

(1)远程访问。

通过将“路由和远程访问”配置为充当远程访问服务器，可以将远程工作人员或流动工作人员连接到组织网络上。远程用户可以像其计算机物理连接到网络上一样进行工作。

利用远程访问连接可以使用通过 LAN 连接的用户通常可用的所有服务(包括文件共享和打印机共享、Web 服务器访问和消息传递)。例如，在运行“路由和远程访问”的服务器上，客户端可以使用 Windows 资源管理器来建立驱动器连接和连接到打印机。由于远程访问完全支持驱动器号和通用命名约定(UNC)名称，因此大多数商用应用程序和自定义应用程序不必进行修改即可使用。

运行“路由和远程访问”的服务器提供两种不同类型的远程访问连接：

- 虚拟专用网络(VPN)：
  - VPN 可以跨专用网络或公用网络(例如 Internet)创建安全的点对点连接。VPN 客户端使用基于 TCP/IP 的特殊协议(称为隧道协议)对 VPN 服务器上的虚拟端口进行虚拟呼叫。虚拟专用网络的最佳示例是与连接到 Internet 的远程访问服务器建立 VPN 连接的 VPN 客户端。远程访问服务器应答虚拟呼叫，对呼叫者进行身份验证，并在 VPN 客户端与公司网络之间传输数据。
  - 与拨号网络相反，VPN 始终是通过公用网络(例如 Internet)在 VPN 客户端与 VPN 服务器之间建立的逻辑间接连接。为了确保隐私安全，必须对通过该连接发送的数据进行加密。
- 拨号网络：
  - 在拨号网络中，远程访问客户端使用电信提供商的服务(例如模拟电话和 ISDN)与远程访问服务器上的物理端口建立非永久的拨号连接。拨号网络的最佳示例是拨打远程访问服务器的一个端口的电话号码的拨号网络客户端。
  - 基于模拟电话或 ISDN 的拨号网络是拨号网络客户端与拨号网络服务器之间的直接物理连接。可以对通过该连接发送的数据进行加密，但并非必须。

(2)路由。

路由器是管理数据在网段(或子网)之间的流动的设备。路由器存储其自己的网络接口状态的有关信息以及网络通信可能的源和目标的列表，并根据这些信息来定向传入数据包和传出

数据包。根据环境中使用的硬件设备和应用程序的数目和类型来计划网络通信和路由的需要，可以更好地决定使用专用硬件路由器、基于软件的路由器还是两者的组合。通常，专用硬件路由器在处理较重的路由需求时效果最好，而基于软件的路由器比较便宜，足以处理较轻的路由负载。

在子网之间的通信相对较轻的小型分段网络中，基于软件的路由解决方案（例如 Windows Server® 2008 中的“路由和远程访问”服务）可能比较理想。反之，在拥有大量网段并且性能要求的范围较广的企业网络环境中，可能需要各种基于硬件的路由器来担当网络中的不同角色。

1.路由和远程访问服务的用途

路由和远程访问适用于对支持下列远程访问和路由方案感兴趣的网络和系统管理员：

- 允许远程访问客户端通过 Internet 连接到专用网络的远程访问（VPN）。
- 允许远程访问客户端通过拨入调制解调器组或其他拨号设备连接到专用网络的远程访问（拨号）。
- 网络地址转换（NAT），与专用网络上的计算机共享 Internet 连接以及在公用网络与专用网络之间转换流量。
- 保护两个专用网络之间的连接，以便通过 Internet 安全发送专用数据。
- 在两个网络之间路由，用于配置简单路由、多路由器或请求拨号路由拓扑。

2.路由和远程访问服务的新增功能

在 Windows Server 2008 中，路由和远程访问服务增加了如下所示的一些新功能：

（1）服务器管理器。

服务器管理器是一项新增功能，用于指导信息技术（IT）管理员顺利安装、配置和管理 Windows Server 2008 中所包含的服务器角色和功能。在管理员完成初始配置任务中所列的任务后，服务器管理器将会自动启动。之后，当管理员登录到服务器时，它便会自动启动。

（2）SSTP 隧道协议。

安全套接字隧道协议（SSTP）是一种新形式的虚拟专用网络（VPN）隧道，具备允许数据通过阻止 PPTP 和 L2TP/IPsec 数据的防火墙的功能。SSTP 提供了一种机制，可封装通过 HTTPS 协议的 SSL 通道的 PPP 流量。PPP 的使用允许支持强身份验证方法，例如 EAP-TLS。HTTPS 的使用意味着数据将流经 TCP 端口 443（通常用于 Web 访问的端口）。安全套接字层（SSL）可通过增强的密钥协商、加密和完整性检查提供传输级别的安全性。

安全套接字隧道协议（SSTP）是虚拟专用网络（VPN）隧道的一种新形式。SSTP 提供了一种机制，可以封装通过 HTTPS 协议的 SSL 通道传输的 PPP 通信。使用 PPP 可以支持强大的身份验证方法（例如 EAP-TLS）。使用 HTTPS 意味着通信将流经 TCP 端口 443（常用于 Web 访问的端口）。安全套接字层（SSL）通过增强的密钥协商、加密和完整性检查，提供传输级别的安全性。在 Windows Server 2008 和带 SP1 的 Windows Vista 中支持使用 SSTP。

使用 SSTP 封装的通信可以通过阻止 PPTP 和 L2TP/IPsec 通信的防火墙。

（3）网络访问保护的 VPN 强制。

VPN 强制为所有通过 VPN 连接访问网络的计算机提供有限网络访问权限。具有网络访问保护（NAP）的 VPN 强制在功能上类似于网络访问隔离控制（Windows Server 2003 中的一项功能），只不过 VPN 强制更容易部署。

NAP 是 Windows Vista® 客户端操作系统和 Windows Server 2008 操作系统中包含的一种客户端健康策略创建、实施和更新技术。使用 NAP，系统管理员可以建立并自动实施健康策略，这包括软件要求、安全更新要求、所需的计算机配置以及其他设置。

在进行 VPN 连接时，未遵从健康策略的客户端计算机将具有受限的网络访问权限，直到其配置得以更新并遵从策略为止。根据用户选择部署 NAP 的方式，未遵从策略的客户端可以自动进行更新，以便用户无需手动更新或重新配置其计算机，便可快速重新获取完全网络访问权限。

(4)IPv6 支持。

Windows Server 2008 和 Windows Vista 支持 Internet 协议版本 6(IPv6)的下列增强功能：

- 协议：
  - PPPv6。本机 IPv6 流量现在可以通过基于 PPP 的连接进行发送。例如，PPPv6 支持允许用户通过可用于宽带 Internet 访问的拨号或基于以太网上 PPP(PPPoE)的连接与基于 IPv6 的 Internet 服务提供商(ISP)进行连接。
  - 通过拨号以太网以及 VPN 隧道的 PPPv6
  - 通过 IPv6 的 L2TP
  - DHCPv6 中继代理
- 无状态筛选，基于以下参数：
  - 源 IPv6 地址/前缀
  - 目标 IPv6 地址/前缀
  - 下一跃点类型(IP 协议类型)
  - 源端口号(TCP/UDP)
  - 目标端口号(TCP/UDP)
- 通过 IPv6 传输的 RADIUS

默认情况下，路由和远程访问将配置为仅接受 Internet 协议版本 4(IPv4)连接。在 Windows Server 2008 中，用户可以使用路由和远程访问 Microsoft 管理控制台(MMC)来配置 IPv6 路由和连接。

(5)新的加密支持

为了适应政府安全要求以及安全行业支持更强大的加密的趋势，Windows Server 2008 和 Windows Vista 对 PPTP 和 L2TP VPN 连接支持下列加密算法：

对于 PPTP 而言，可支持的加密算法包括：

- 只支持 128 位 RC4 加密算法。
- 取消了对 40 位 RC4 和 56 位 RC4 的支持，但是可以通过更改注册表项来添加。

对于 L2TP/IPsec 而言，取消了支持 Message Digest 5(MD5)完整性检查的数据加密标准(DES)加密算法，但是可以通过更改注册表项来添加。可支持的加密算法包括：

- IKE 主模式将支持：
  - 高级加密标准(AES)256(新增)、AES 192(新增)、AES 128(新增)和 3DES 加密算法。
  - 安全哈希算法 1(SHA1)完整性检查算法。
  - 用于主模式协商的 DiffiE-Hellman(DH)组 19(新增)和 20(新增)。

- IKE 快速模式将支持：
  - AES 256(新增)、AES 192(新增)、AES 128(新增)和 3DES 加密算法。
  - SHA1 完整性检查算法。

3.3　了解介质类型

网络传输介质是网络中发送方与接收方之间的物理通路，它对网络的数据通信具有一定的影响。常用的传输介质有：双绞线、同轴线缆、光纤、无线传输媒介。

任何信息传输和共享都需要有传输介质，计算机网络也不例外。对于一般计算机网络用户来说，可能没有必要了解过多的细节，例如计算机之间依靠何种介质、以怎样的编码来传输信息等。但是，对于网络设计人员或网络开发者来说，了解网络底层的结构和工作原理则是必要的，因为他们必须掌握信息在不同介质中传输时的衰减速度和发生传输错误时如何去纠正这些错误。

3.3.1　介质类型及其特征

网络传输介质是指在网络中传输信息的载体，常用的传输介质分为有线传输介质和无线传输介质两大类。

- 有线传输介质是指在两个通信设备之间实现的物理连接部分，它能将信号从一方传输到另一方，有线传输介质主要有双绞线、同轴线缆和光纤。双绞线和同轴线缆传输电信号，光纤传输光信号。
- 无线传输介质指我们周围的自由空间。我们利用无线电波在自由空间的传播可以实现多种无线通信。在自由空间传输的电磁波根据频谱可将其分为无线电波、微波、红外线、激光等，信息被加载在电磁波上进行传输。

不同的传输介质，其特性也各不相同。他们不同的特性对网络中数据通信质量和通信速度有较大影响。

除了上述的大体分类之外，还可按照网络传输介质的物理特性来进行细分，主要包括如下所述的几种类型。

(1)双绞线。

双绞线简称 TP，将一对以上的双绞线封装在一个绝缘外套中，为了降低信号的干扰程度，线缆中的每一对双绞线一般是由两根绝缘铜导线相互扭绕而成，也因此把它称为双绞线。双绞线分为非屏蔽双绞线(UTP)和屏蔽双绞线(STP)。

非屏蔽双绞线价格便宜，传输速度偏低，抗干扰能力较差。屏蔽双绞线抗干扰能力较好，具有更高的传输速度，但价格相对较贵。双绞线需用 RJ-45 或 RJ-11 连接头插接。

市面上出售的 UTP 分为 3 类、4 类、5 类和超 5 类四种：

- 3 类：传输速率支持 10Mbps，外层保护胶皮较薄，皮上注有“cat3”。
- 4 类：网络中不常用。
- 5 类(超 5 类)：传输速率支持 100Mbps 或 10Mbps，外层保护胶皮较厚，皮上注有“cat5”。

超 5 类双绞线在传送信号时比普通 5 类双绞线的衰减更小，抗干扰能力更强，在 100M 网络中，受干扰程度只有普通 5 类线的 1/4，这类较少应用。

STP 分为 3 类和 5 类两种，STP 的内部与 UTP 相同，外包铝箔，抗干扰能力强、传输速率高但价格昂贵。

双绞线一般用于星型网的布线连接，两端安装有 RJ-45 头（水晶头），连接网卡与集线器，最大网线长度为 100 米，如果要加大网络的范围，在两段双绞线之间可安装中继器，最多可安装 4 个中继器，如安装 4 个中继器连 5 个网段，最大传输范围可达 500 米。

(2)同轴线缆。

同轴线缆由绕在同一轴线上的两个导体组成。具有抗干扰能力强，连接简单等特点，信息传输速度可达每秒几百兆位，是中、高档局域网的首选传输介质。

同轴线缆由一根空心的外圆柱导体和一根位于中心轴线的内导线组成，内导线和圆柱导体及外界之间用绝缘材料隔开，如图 3.14 所示。

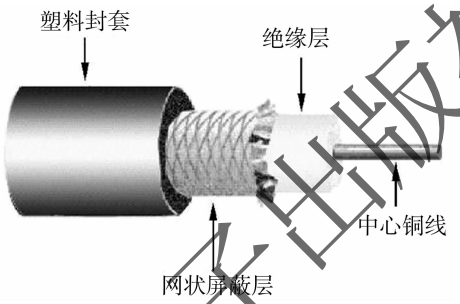

图 3.14　同轴线缆

按直径的不同，可将同轴线缆划分为粗缆和细缆两种：

- 粗缆：传输距离长，性能好但成本高、网络安装、维护困难，一般用于大型局域网的干线，连接时两端需终结器。粗缆具有如下特征：粗缆与外部收发器相连；收发器与网卡之间用 AUI 线缆相连；卡必须有 AUI 接口（15 针 D 型接口）；每段 500 米，100 个用户，4 个中继器可达 2500 米，收发器之间最小 2.5 米，收发器线缆最大 50 米。
- 细缆：与 BNC 网卡相连，两端装 50 欧的终端电阻。用 T 型头，T 型头之间最小 0.5 米。细缆网络每段干线长度最大为 185 米，每段干线最多接入 30 个用户。如采用 4 个中继器连接 5 个网段，网络最大距离可达 925 米。细缆具有如下特征：细缆安装较容易，造价较低，但日常维护不方便，一旦一个用户出故障，便会影响其他用户的正常工作。

根据传输频带的不同，可分为基带同轴线缆和宽带同轴线缆两种类型：

- 基带：数字信号，信号占整个信道，同一时间内能传送一种信号。
- 宽带：可传送不同频率的信号。

提示：同轴线缆需用带 BNC 头的 T 型连接器连接。

(3)光纤。

光纤又称为光缆或光导纤维，由光导纤维纤芯、玻璃网层和能吸收光线的外壳组成，是由一组光导纤维组成的用来传播光束的、细小而柔韧的传输介质。应用光学原理，由光发送机产生光束，将电信号变为光信号，再把光信号导入光纤，在另一端由光接收机接收光纤上传来的光信号，并把它变为电信号，经解码后再处理。与其他传输介质比较，光纤的电磁绝缘性能好、信号

衰小、频带宽、传输速度快、传输距离大。主要用于要求传输距离较长、布线条件特殊的主干网连接。具有不受外界电磁场的影响，无限制的带宽等特点，可以实现每秒几十兆位的数据传送，尺寸小、重量轻，数据可传送几百千米，但价格昂贵。

光纤分为单模光纤和多模光纤：

- 单模光纤：由激光作光源，仅有一条光通路，传输距离长，20～120km。
- 多模光纤：由二极管发光，低速短距离，2 千米以内。

提示：光纤需用 ST 型头连接器连接。

(4)无线电波。

无线电波是指在自由空间(包括空气和真空)传播的射频频段的电磁波。无线电技术是通过无线电波传播声音或其他信号的技术。

无线电技术的原理在于，导体中电流强弱的改变会产生无线电波。利用这一现象，通过调制可将信息加载于无线电波之上。当电波通过空间传播到达收信端，电波引起的电磁场变化又会在导体中产生电流。通过解调将信息从电流变化中提取出来，就达到了信息传递的目的。

(5)微波。

微波是指频率为 300MHz～300GHz 的电磁波，是无线电波中一个有限频带的简称，即波长在 1 米(不含 1 米)到 1 毫米之间的电磁波，是分米波、厘米波、毫米波和亚毫米波的统称。微波频率比一般的无线电波频率高，通常也称为“超高频电磁波”。微波作为一种电磁波也具有波粒二象性。微波的基本性质通常呈现为穿透、反射、吸收三个特性。对于玻璃、塑料和瓷器，微波几乎是穿越而不被吸收。对于水和食物等就会吸收微波而使自身发热。而对金属类东西，则会反射微波。

(6)红外线。

红外线是太阳光线中众多不可见光线中的一种，由德国科学家霍胥尔于 1800 年发现，又称为红外热辐射，太阳光谱中，红光的外侧必定存在看不见的光线，这就是红外线。也可以当作传输之媒介。太阳光谱上红外线的波长大于可见光线，波长为 0.75～1000μm。红外线可分为三部分，即近红外线，波长为 0.75～1.50μm 之间；中红外线，波长为 1.50～6.0μm 之间；远红外线，波长为 6.0～l000μm 之间。

3.3.2　干扰网络介质的因素

即使是简单的非屏蔽双绞线，它对数据的传输能力在过去十年左右的时间里也经历了漫长的发展。在 20 世纪 80 年代末期，很多专家认为 UTP 布线不可能支持超过 10Mbps 的数据传输。而现在已经可以在 100 米长的 UTP 上支持 1.2Gbps 甚至更高的数据传输，而且 UTP 的传输速度可能在将来得到进一步提高。

由于更高传输速率的要求，线缆设计的复杂性也在增加。随着数据速率的提高，线缆中的实际情况变得越来越神秘，而且数据信号在高速传输时出现错误的可能性也增大了。因此这完全不是个简单的事情。随着数据速率的提高，线缆的电气特性会改变，信号变形的程度更大，信号能够传输的距离变短。当人们设计 1000Base-T(千兆以太网)和支持超过 l00MHz 的线缆时，却发现在一些低速时不会产生的问题。这些问题是不同类型的串扰以及不同线对的传输延迟。

电流流过线缆就是线缆里的电子移动和互相撞击，就像多米诺骨牌那样。为了保证接收端能够正确地接收信号，线缆的发送端与接收端之间必须有足够多的电子产生相互关系。当信号的频率提高时（也就会提高数据传输速率），线缆里就会产生一些阻碍信号传输的现象（也就是影响数据的传输）。这些现象对于负责线缆购买和测试线缆的人员都是很重要的。

5e 类和 6 类线缆的当前规范描述了其中的一些现象，并且定义了线缆需要满足的最大（或最小）参数值。

由于 1000BasE-T 以太网使用的调制技术很复杂，TIA 指定的布线性能规范超出了初始测试规范的内容。这些性能特征包括功率总和、线对之间的串扰、时滞、返回损耗和 ELFEXT。其中一些参数与串扰相关，因此是很重要的。虽然串扰在所有技术领域里都是很重要的，但像 1000BasE-T 这样的高速技术对于串扰更加敏感，因为它使用全部四对双绞线进行数据传输。

所有这些需求都属于线缆标准的当前版本 ANSI/TIA/EIA-568-B。

很多传输要求都是以数学公式表达的。为了方便那些不善于计算对数的人，标准里根据相应的频率列出了预先计算好的数值。但是这些特性必须通过全频段的彻底测试，因此性能必须在指定频率范围之内的任意频率上都与公式一致。

下面是通信线缆的主要测试参数及分类：

- 与衰减（信号损耗）相关的
  - 导线电阻
  - 分布电容
  - 返回损耗
  - 阻抗
- 与噪声相关的
  - 非平衡阻抗
  - 非平衡电容
  - 近端串扰（NEXT）
  - 远端串扰（FEXT）
  - 功率总和 Next
  - 功率总和 FEXT
- 其他
  - 衰减串扰比（ACR）
  - 传播延时
  - 时滞

接下来，我们将介绍其中一些比较重要的干扰因素。

1.衰减

正如前面说过的，衰减就是信号的损失。信号在线缆里传输时，不是所有的信号都能到达线缆的接收端，因此就产生了信号的损失。线缆长度超过一定数值时，由于信号损失得太多，信号在线缆里传输时，不是所有的信号都能线缆越长，损失的信号越多。

衰减以分贝（dB）进行测量，而且测量是在导线的接收端进行的。因此如果发送器输出 10dB 信号而在接收端测量到的信号是 3dB，那么衰减就是 3－10＝－7dB，结果中的负号通常被

忽略，因此衰减就是信号损失了 7dB。如果发送端输出 10dB，因此如果发送器输 6dB，那么衰减只是 4dB。因此衰减越小越好。

衰减会随着信号频率的提高而增加。举例来说，一根 100 米长的线缆工作于 1MHz 时衰减是 2dB，而工作于 100MHz 时衰减是 20dB。

温度升高也会增加衰减。温度每升高一摄氏度，3 类线缆的衰减增加 1.5%，5e 类线缆的衰减增加 0.4%。线缆安装在金属管道里时衰减也会增加 2%至 3%。

当信号到达接收端时，信号必须能够给接收端识别，因此线缆的衰减值十分重要。不同类型的线缆，衰减不同，工作于不同频率的线缆，衰减也不同。另外，虽然 5 类、5e 类和 6 类线缆基本上都是工作于 100MHz，但当线缆的带宽增加时，允许的衰减值就会减小。

下面详细介绍影响衰减产生的因素。

(1)导线电阻。

导线电阻会限制电子在导体内的运动，从而阻碍信号的传输。电阻式信号的一些能量变成热量浪费掉了，但局域网布线系统的电流和电压都很低，因此产生的热量是可以忽略的。线缆越长，导体直径越小，电阻就越大。在一定尺寸下，电阻基本上就是导线材料的固定属性。铜、黄金、白银具有较低的电阻，经常用作导体。

(2)分布电容。

当线缆中包含多根导线并且彼此距离很近时，就会产生这种电子现象。包裹导线的绝缘材料会在两个导线之间形成电容，从而保存部分信号能量。绝缘材料具有一个名为绝缘常数的特性，它对分布电容具有很大影响。不同材料具有不同的绝缘常数，这个数值越小，信号的损失越小。FEP 和 HDPE 具有较小的绝缘常数，同时其他性能也不错，因此适用于高频线缆。

(3)阻抗。

阻抗是电阻、电容和电感的组合，以欧姆表示。典型 UTP 线缆的阻抗是 85 到 115 欧姆。美国使用的 3 类、5 类、5e 类和 6 类 UTP 线缆的阻抗是 100＋15 欧姆。在测试线缆的故障、短路和匹配问题时，阻抗的数值是很有用的。线缆测试仪能够显示三种可能的阻抗，从而表示存在的问题：

- 阻抗数值不位于 85 到 115 欧姆之间表示线缆或组件的类型不匹配。这很可能是由于安装了不正确的连接器，或是线路中交叉连接了不同类型的线缆。
- 阻抗为无穷大表示线缆是开路的或被切断了。
- 阻抗为零表示线缆被短路了。

有些电子在传输过程中可能由于导线阻抗不匹配或导线存在的一些瑕疵而被反射回发送端，这种现象被称为返回损耗。如果电子在线缆中传输了很长距离之后才被反射，返回损耗可能根本不会被注意到，因为返回的信号可能在到达发送端之前由于衰减而消失了。如果反射信号的强度足够大，它就会在高速技术中产生影响。

2.噪声

线缆里除了信号以外的所有与电相关的都是噪声，它们会危胁信号的完整性。线缆内部和外部存在着很多噪声源。控制噪声对于线缆和连接器设计人员是十分重要的，因为缺少控制的噪声可能会淹没数据信号，从而导致网络无法工作。

双绞线使用平衡的信号传输方式。信号在导线对中一根导线里传输的路径与信号在另一根导线里向相反方向传输的路径基本上是相同的(同轴线缆的传输方式就不是这样,它的中心导线为信号提供了一个很好的路径,但它的网状和金属箔屏蔽形成的导体的效率比较低,对于信号来说不是一个很好的路径)。

当信号在导线对里传输时会形成一个电场。当两根导线完全对称时,信号就会流畅地传输。然而铜线直径、绝缘层厚度、中心导体的微小变化都会导致电场受到干扰,这被称为失衡。电子失衡意味着噪声。

导线对的两根导线直径不一致时会产生电阻失衡。不匹配的导线、制作工艺较差的导线或在安装过程中被拉长的导线都会产生电阻失衡。

电容失衡也与直径相关,但它与包裹导线的绝缘材料的直径相关。如果一根导线的绝缘层比另一根导线的厚,就会产生电容失衡。或者,如果生产过程没有得到很好的控制,导线没有处于绝缘层的中央,也会产生电容失衡。

上述两种噪声源通常由生产厂商进行了很好的控制,它们与串扰相比是比较小的。

很多人在使用电话时有过串扰的经历,也就是在电话里听到了其他人的谈话。当一对导线里传输的信号泄露到其他导线对时就会产生串扰。

在使用导线对传输信号时会形成电场,这个电场随着信号的传输会在相邻导线对上产生感应电压。导线平行的部分越多,这种现象越严重;信号频率越高,产生串扰的可能性越大。将导线对的两根导线相互缠绕在一起可以耦合异相信号的能量,从而消除这种电场,这样的结果是减少了信号的传输。但是缠绕必须是对称的,也就是说,两根导线必须相互缠绕,而不是一根导线缠绕另一根,而且两对相邻导线不应具有相同的缠绕密度。为什么要这样呢?因为这些扭曲点都是适合信号传输的点,就像是小溪里的垫脚石。一般来说,缠绕的密度越高,对电场的消除效果就越好,串扰就越少。这就是为什么5类和更高类别的线缆具有很高的缠绕密度。串扰以分贝为单位,其数值越高表示线缆的串扰越小。

3.近端串扰(NEXT)

如果在信号发送端测试到了串扰,就表示发生了近端串扰。NEXT 最常发生在距离发送端 20 米到 30 米的位置。

对于 10BasE-T 和 100BasE-TX 来说,主要的问题来自于设计不良和安装不良导致的串扰。如果安装正确,则 NEXT 对于 1000BasE-T 来说不是什么问题,因为设计人员采取了一些技术消除 NEXT。这种技术对于 1000BasE-T 来说是必需的,因为线缆内四对导线都要进行数据发送和接收。

4.远端串扰(FEXT)

远端串扰(FEXT)与 NEXT 类似,只是它发生在与数据发送端相反的另一端。由于衰减的原因,导致远端的信号强度比近端的要低得多。

FEXT 的测量用于计算“等效远端串扰(ELFEXT)”。FEXT 在短线缆上要比在长线缆上要明显。因为这时信号还没有因为衰减而变得很小。

5.等效远端串扰(ELFEXT)

等效远端串扰(ELFEXT)是在与数据源相对的另一端测试的导线对之间的信号耦合,从而

计算信号的损失。ELFEXT 是计算出来的，而不是测量出来的。计算方法是用被干扰导线对的远端串扰(FEXT)减去干扰导线对的衰减值。这个计算描述了干扰与信号的比值，也是另一种信噪比。从另一个角度来看，这个数值说明了远端信号串扰造成的噪声与接收端信号的比值。ELFEXT 还可以比作远端 ACR(衰减串扰比)。

任意两对导线组合之间都需要进行测量，因为每对导线的衰减是略有不同的。如果 ELFEXT 的值很高，就表明线缆衰减过大或远端串扰很严重。

6.线对与线对之间的串扰

对于近端串扰和远端串扰来说，一种测量串扰的方法是测量线对与线对之间的影响。在进行线对与线对的测量时，把信号输入一对导线(干扰者)，测量另一对导线(被干扰者)上被耦合的信号。在四对双绞线的线缆中，需要测试下面六种线对之间的组合：

- 第 1 对与第 2 对
- 第 1 对与第 3 对
- 第 1 对与第 4 对
- 第 2 对与第 3 对
- 第 2 对与第 4 对
- 第 3 对与第 4 对

在线缆的另一端还要重复进行这种测试，因此最终会得到 12 个线对组合的测试结果，最差的组合会被记录为线缆的串扰值，如图 3.15 所示。

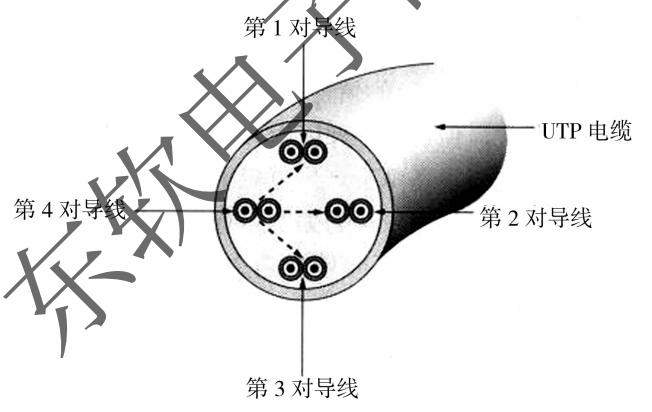

图 3.15　第 4 对导线产生的串扰会影响到其他 3 对导线

7.综合串扰

综合串扰也应用于 NEXT 和 FEXT，而且在实现同时使用多对导线进行数据传输的技术时一定要考虑它。在测试综合串扰时，只有一对导线上(被干扰者)没有信号，然后测量其他所有导线对(干扰者)耦合到被测导线对上的信号强度。

如图 3.16 所示，显示了四对双绞线线缆的剖面图，请注意第 2 对、第 3 对、第 4 对导线上的信号能量都会影响第 1 对导线。这种综合串扰不能超过制定的限制。由于每对导线都受到其他所有导线对的影响，这种测量需要分别进行四次，每次测试一对导线受到其他导线对的影响。同样地，这种测试在线缆的两端都要进行，从而得到八个测试结果。最差的组合会被记录为线缆的综合串扰值。

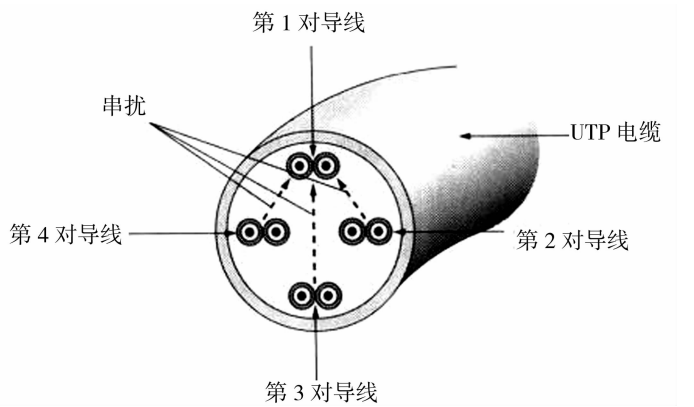

图 3.16　来自第 2、3、4 对导线的串扰都会影响第 4 对导线

8.外部干扰

在数据高速传输的状态下，线缆内的信号可能会受到外部因素的影响。虽然各种线缆的设计人员都会尽量校正这种干扰，但是，这些外部因素并不在线缆设计人员的控制范围之内。包括传输信号的线缆在内，所有电子设备都会产生电磁干扰(EMI)。低功率设备和支持低频率应用的线缆产生的电磁场不具有形成干扰的强度。有些设备会产生广播频率的干扰，居住在电视或广播天线附近的人们在使用电话时就会感觉到这种干扰。

功率较大的设备和线缆产生的 EMI 会影响数据传输。因此，线缆应该铺设在远离这些设备的地点。典型办公环境中常见的电磁干扰源包括：

- 汽车
- 采暖和光空调设备
- 荧光灯
- 激光打印机
- 电梯
- 电力线
- 电视
- 一些医疗设备

在建筑物中进行布线时一定要让线缆与这些设备保持一定距离。不要再铺设电力线的管道里安装线缆。在某些情况下，一些特定的环境也具有很强的电磁干扰，例如机场、医院、军事设施、发电厂等。如果在这些环境中安装线缆，就应该考虑使用屏蔽良好的线缆，或是使用光缆。

9.衰减串扰比(ACR)

衰减串扰比(ACR)表示同一对导线上真正的接收信号比 NEXT(串扰或噪声)大多少。有时 ACR 也被认为是信噪比(SNR)。这是一个计算得到的数值，是不可能“测量”出来的。而且它也不是一个真正的比值，它实际上是在给定频率下，衰减值减去串扰值的结果。从技术角度上来说，SNR 不仅包含由数据传输产生的噪声，还包含外部干扰。从实践的角度来说，除非在电磁干扰很强的情况下，否则 ACR 和真正的 SNR 的功能是一致的。

串扰(噪声)与衰减(信号的损失)之差是很重要的，因为它可以确保信号在传输到接收端时

具有的能量高于串扰或其他噪声造成干扰。

此外，解决与 ACR 相关的问题通常意味着排除 NEXT 带来的问题，因为除了更换线缆之外，减少衰减的唯一方法是缩短线缆长度。

10.传播延时

电子在线缆中以匀速传输，其速度值以光速的百分比表示，这被称为 NVP（标称传输速度）。UTP 线缆的 NVP 通常在 60%到 90%之间。线缆的生产厂商控制着 NVP 的大小，因为这主要是由绝缘材料的绝缘常数决定的。信号输入到发送端与到达线缆另一端之间的时间差被称为传播延时。

11.时滞

时滞是由每对导线的长度不同造成的。为了消除串扰，每对导线被相互缠绕在一起，这样就使得导线的实际长度大于线缆长度。由于每对导线具有不同的缠绕密度，因此各对导线的长度都是不相同的。当信号在两对或更多对导线中传输时，其到达另一端的时间会有些许差别。对于 5 类、5e 类和 6 类线缆的安装来说，时滞不能超过 50ms。

过多的延时或时滞可能会让网络收发器产生时序问题，这样会导致经常需要重新发送数据，从而可能会严重影响链路速度，甚至完全阻塞通信。