1 数据通信简介

1.1 通信和分布式环境

通信系统：

他说一系列硬件软件组合。能支持不同节点间的软件的通信。

主机/服务器：

实现主要的应用功能，并且控制通信系统的系统。

对象/地址/路径：

在分布式系统中，对象代表一个系统，一个进程或一个节点，一个地址代表对象存在的地方。路径告诉你如何到达那里。

数据：

数据是分布式系统最常用的共享资源。

1.2 通信系统功能

通信系统主要功能：

- **命名和寻址**： 通信系统所管理的对象的名字包括进程、端口、邮箱、系统及用户间的会话。通信系统会把这些名字（字符）重新用网络地址形式表达。通信系统有逻辑命到物理名的转换表。
- **分段**：当要传输的信息比网络包大时，往往需要把这些数据分成多个段。以便减少错误率以及提高效率和灵活性。
- **流量控制**：当网络通信超过网络吞吐能力时，流量控制可以协调通信实体间的信息流来优化网络性能。
- **同步**：不同的子进程共享服务器资源时，必须有机制保证这些进程的同步。
- **优先级**：通信系统可以为信息分配优先级以便有区别的进行处理。
- **差错控制**：可靠、无差错的通信系统是主要目标。方法包括纠错，自动重发等来实现。

1.3 分层、协议和接口

1.3.1 通信的分层模型

三层模型：

- **认识层**：人类理解的方式。计算机用户在这一层实现接口。
- **语言层**：用词汇表达概念。计算机使用 ASCII 或 EBCDIC 字符。
- **物理传输层**：通信介质。

1.3.2 客户/服务器运算的分层模型

典型的分布式系统分层：

- **应用层**：最高层。完成进程管理，数据分配，进程内通信等。
- **分布式操作系统层**：为应用层提供全系统分布式服务。支持进程命名、目录、寻址、资源共享、保护与同步、内部通信和恢复。分布式操作系统把分布功能统一成单一逻辑实体，并负责建立单一系统映像（SSI）
- **本地管理和核心层**：支持单独节点上的操作系统。支持本地进程通信、内存和I/O 访、保护剂多任务。
- **通信系统层**：支持以上几层所需要的通信。

分层的好处：

- 层次独立：每一层只需要关心邻近下一层提供的服务。
- 灵活性：某一层变化不影响其他层。
- 易于实现和维护。
- 标准化。

1.3.3 OSI 通信模型的七个分层

数据包（packet）：

网络间数据传输的单位。包括：其实字符、包头（包的来向和去向及类型）、包中的数据、最后的纠错位及介绍字符。数据包结构如下：

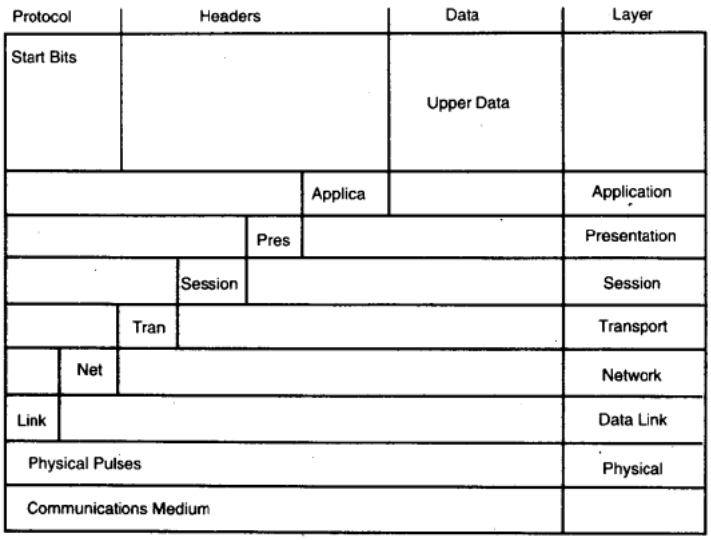


图 1.1 建立一个 OSI 包

- 每一层只会往相邻的层发送或接受信息。
- 每一层只会与不同节点相同的层进行信息交流。

OSI(Open System Interconnection)模型：

一、物理层

产生物理脉冲，数据在网卡通及电缆中传输。

二、数据链路层

收集数据，把数据作为包的第一层处理。组装发送包并进行首次检查。它为发送包增加纠错信息并且为接收包检错。如果包不完整或不正确，会在这里被丢弃。SDLC 和 HDLC 是这一层的两个协议。

三、网络层

局域网（LAN）的规模太大时，就需要划分为较小规模的 LAN 子网。网络层通过多项设备对包进行路径选择以便包达到正确的子网。TCP/IP 中的 IP（互联网协议）在这层工作。

四、传输层

TCP 工作在这层。这是个过渡层。主要管理路由包和错误恢复。

五、会话层

TCP 也在这层工作。为了安全可靠而建立的会话机制。

六、表示层

此层未被完全定义或使用。通常是数据的解压缩和压缩，加密解密等。

七、应用层

处理文件传递，任务传递，虚拟终端协议等。

八、其他层

OSI 有一些拓展，不仅 LAN，也适用于微机大型机等。有些系统增加了第 0 层描述硬件细节。

1.4 客户/服务器连接部件

1.4.1 通信与同步

1.4.2 面向过程的通信

1.5 定义局域网和广域网

广域网：

在地理分布上较广的用户可能要求互连。这就需要快速数据交换的公共远程通信设施。把这些分布较广的用户连接在一起的网络称作广域网（WAN）

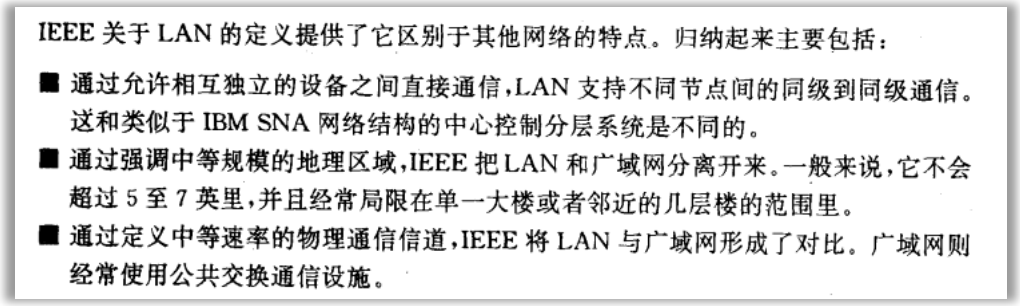
城域网：

为了区分几千英里的 WAN 和一个城市的 WAN，我们把一个城市内运行的专线网络称为城域网（MAN）

局域网：

智能终端间的短距离通信网络被称为局域网（LAN）。IEEE 把 LAN 定义为：中等范围地理区域内，通过中等数据速率的物理通信通道，允许相互独立的设备能够相互通信的数据通信系统。

1.6 LAN 的特点和组成



IEEE 关于 LAN 的定义提供了它区别于其他网络的特点。归纳起来主要包括：

- 通过允许相互独立的设备之间直接通信，LAN 支持不同节点间的同级到同级通信。这和类似于 IBM SNA 网络结构的中心控制分层系统是不同的。
- 通过强调中等规模的地理区域，IEEE 把 LAN 和广域网分离开来。一般来说，它不会超过 5 至 7 英里，并且经常局限在单一大楼或者邻近的几层楼的范围里。
- 通过定义中等速率的物理通信信道，IEEE 将 LAN 与广域网形成了对比。广域网则经常使用公共交换通信设施。

1.7 网络拓扑

1.7.1 网络交换技术

包括电路交换和分组交换。说得狗屁不通，无法理解。

1.7.2 物理拓扑

一、总线型拓扑。

最简单的形式。所有的节点都直接连接到同一根电缆上，每个网络节点都有分配给他的地址，这个地址用来判定是否信息是发给自己的。

优势：

- 实现容易。只需要一根电缆把工作中连接起来。
- 用的电缆少，且较便宜。

劣势：

- 如果一个站点出问题，则有可能会影响到所有站点
- 一个坏工作站发送噪声，可能影响这个总线。
- 对节点数量有限制。过多久需要转发器。

二、星拓型拓扑。

一个中央系统（服务器或者集中器）连接 PC 或工作站。每个节点通过单独的电缆与中央系统连接。

优势：

- 非常安全，一个出现问题，只影响出问题的这个。
- 非常好排查问题。

劣势：

- 太昂贵。消耗的电缆太多。

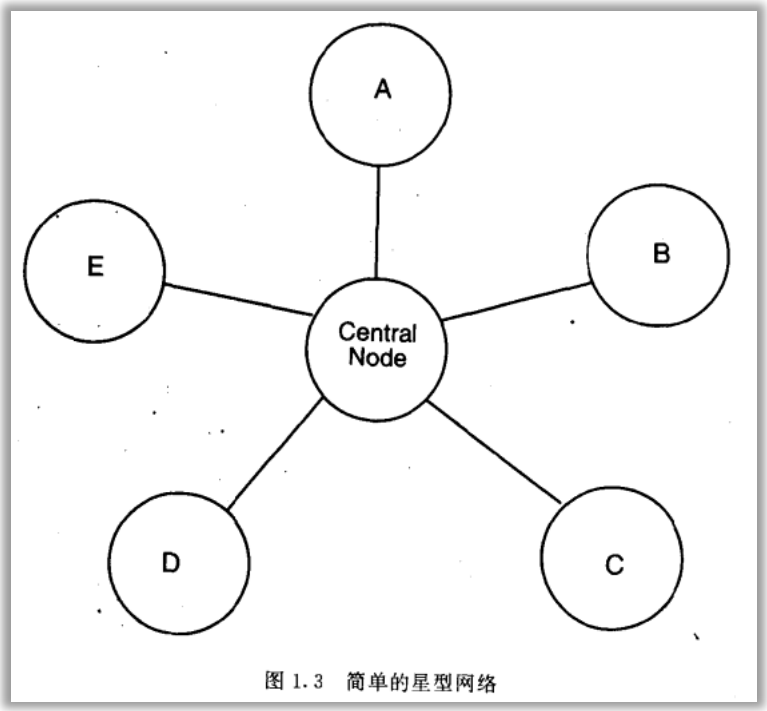


图 1.3　简单的星型网络

三、环形拓扑

所有的节点，服务器，PC，工作站连接到环路中。每个节点接收传递给他的信息，如果发现这个信息不是给自己的，则他会负责转发给下一个节点。

优势：

- 增加节点没问题，因为每个节点都能放大每个报文。

劣势：

- 不能提供网络管理中心点。

适用：

- 局域网一般不采用环形拓扑。
- 适用与大地里范围的网络。可以跨越一个城市的几个地方甚至不同的城市间。

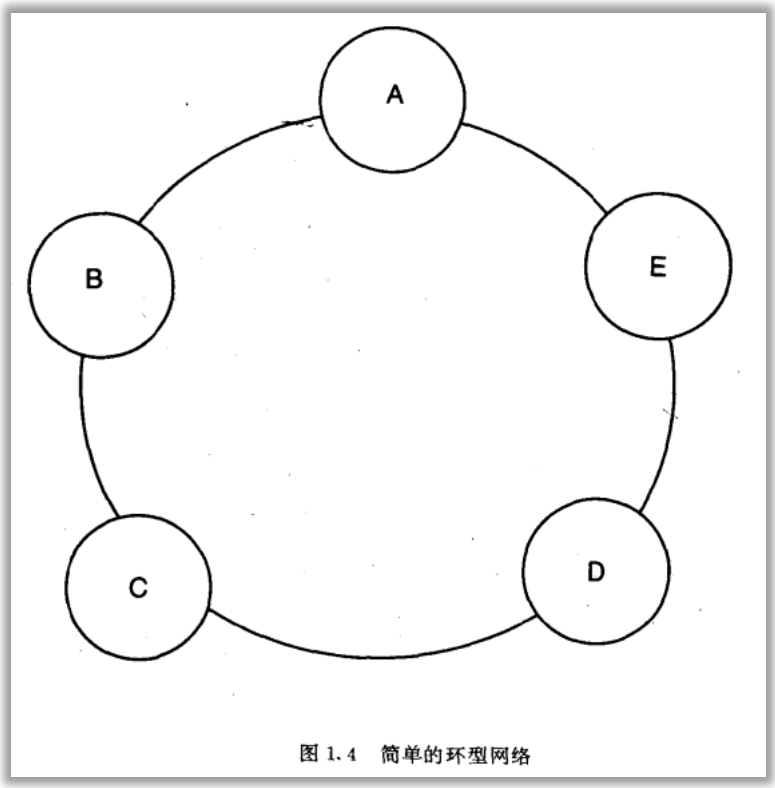


图 1.4　简单的环型网络

1.8　传输和访问控制方法

局域网的信息物理传输用两个范畴来描述：实际的传输介质和介质所使用的方式。

1.8.1 传输介质

目前局域网基本是三种介质：双绞线，同轴电缆，光纤。

传输的技术：

基带传输：

基带传输(Baseband Transmission)使用离散信号(代表 1 或者 0 的电脉冲或者光脉冲)在传输介质上运载信息。这种信号称为数字信号。基带传输使用整个通信能力来传输单一的数据信号。LAN 一般都采用这种数字基带信号。

通过把现有传输时间分段，连接到同一网络的多个工作站可以共享同一条信道。这种技术被称作复用(TDM)。时分复用经常被用于把几个基带信号结合在一起并通过一条高速信道进行传输。

宽带传输：

宽带通信通常采用模拟(不断变化的)信号。通过对载波信号的幅度、频率或相位进行调制,数字信息被编码到模拟波形中。这种方法类似于把多种电视信号结合起来以便在同一CATV 系统中传输。因为信号都是通过电缆上不同的频率来区分,所以这种技术也被称作频分复用(FDM)。

总之,载波信号的频率越高,能够被该信号携带的信息总量就越大。每秒钟能够通过信道的位数被称作数据速率。

普通的 LAN 工作在 10-20Mbps 的数据速率上。当网络足够大时,这个速率可能变得不够快。通常的解决方案是通过宽带网络把基带网络互相连接起来,这样便可以同时传输多个信号。

1.8.2 传输控制

控制分类:

- 中心控制:一个工作站控制整个网络,并给予其他工作站传输许可。

中心访问控制提供了简单的网络协调和管理,它只需简单的工作站到网络的接口。同时,中心化传输控制可能存在单点故障和潜在的网络瓶颈。中心访问控制可以采用下面的访问控制方法:

- 轮询:主站向所有工作站发出通知,指明某个工作站正在准备传输。既然只有轮询到的工作站能够传输,所以避免了工作站之间的冲突。
- 电路交换:在星型拓扑的中心控制 LAN 中,这种方法能够成功地得到实现。此时,中心接到来自从站的请求传输的信息后,在发送方和接收方之间建立相互连接。电路交换在电话技术中被广泛采用,特别是在专用小交换机自动连选业务(PBX)中。
- 时分多重访问(TDMA):为网络上的任一工作站提供了指定的时间片段。工作站只能在指定的时间传输信息。时钟由主站启动和同步。TDMA 能够在总线型拓扑中很好地使用。

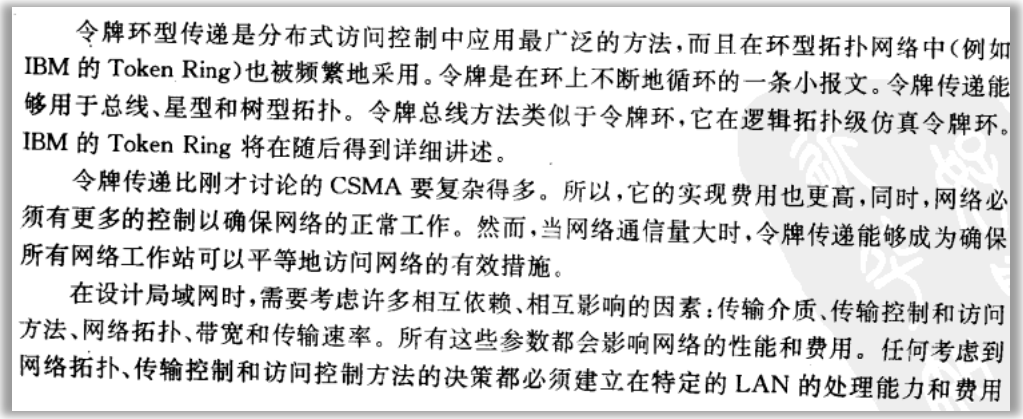
- 随机控制:允许任何工作站进行传输而不用专门的许可。

最著名的随机访问控制技术之一是 Carrier Sense Multiple Access With Collision Detection(CSMA/CD)。使用这种方法时,工作站"有礼貌地"监听以便确定网络是否在使用中。如果网络未被使用,那么该工作站便传输信息。在详细讨论以太网时,这种机制也将得到详细描述。

Apple 的 LocalTalk 网络中使用的 Carrier Sense Multiple Access With Collision Avoidance (CSMA/CA)和 CSMA/CD 访问控制方法非常相似。然而,工作站需采用一些定时策略以便避免冲突发生的可能性。

两种 CSMA 方案的性能都是随机的,因为无法预见哪个工作站试图传输。CSMA 是一种非常简单的访问控制机制,与之相关的网络通信管理工作很少。然而,当网络通信量需求比较大时,随机因素会带来问题,而且在需求接近容量限制时,CSMA 网络性能会急骤下降。

- 分布式控制: 每次只为一个工作站提供许可。



令牌环型传递是分布式访问控制中应用最广泛的方法，而且在环型拓扑网络中（例如IBM 的 Token Ring）也被频繁地采用。令牌是在环上不断地循环的一条小报文。令牌传递能够用于总线、星型和树型拓扑。令牌总线方法类似于令牌环，它在逻辑拓扑级仿真令牌环。IBM 的 Token Ring 将在随后得到详细讲述。

令牌传递比刚才讨论的 CSMA 要复杂得多。所以，它的实现费用也更高，同时，网络必须有更多的控制以确保网络的正常工作。然而，当网络通信量大时，令牌传递能够成为确保所有网络工作站可以平等地访问网络的有效措施。

在设计局域网时，需要考虑许多相互依赖、相互影响的因素：传输介质、传输控制和访问方法、网络拓扑、带宽和传输速率。所有这些参数都会影响网络的性能和费用。任何考虑到网络拓扑、传输控制和访问控制方法的决策都必须建立在特定的 LAN 的处理能力和费用

1.9 IEEE 局域网标准

1.9.1 以太网

1.9.2 环形令牌网

1.10 协议

除了 TCP/IP 协议，还有其他的协议，他们都不同程度支持企业和集团：

- Xerox 网络系统（XNS）
- Novell IPX/SPX
- NetBIOS
- Apple Talk

1.11 其他的 LAN 实现

除了 TCP/IP 的 LAN 实现，还有多种其他实现方法：

- Novell Netware
- Banyan VINES
- SNA

2 TCP/IP 简介

TCP/IP 协议的分类：

TCP/IP 协议族包括互连网协议(IP)、地址分解协议(ARP)、互连网控制信息协议(ICMP)、用户数据报协议(UDP)、传输控制协议(TCP)、路径选择信息协议(RIP)、Telnet、简单邮件转换协议(SMTP)、域名系统(DNS)以及许多其他协议。

2.1 从六个方面理解 TCP/IP

在 TCP/IP 中，所有协议都是以 IP 包的形式通过 IP 互连网传输的。IP 是一种路径选择的协议，意思是在两个节点间使用 IP 协议进行通信时不需要用同一条物理线路连接。在初步理解了信息是怎样通过一个路径选择网络之后，你只需要了解下面这六个问题的答案就可以了：

1. 在这个协议中地址的格式是什么样的？
2. 设备是怎样分到一个地址的？
3. 一个逻辑地址是怎样映射到一个物理地址上的？
4. 终端节点是怎样寻找路径选择器的？
5. 路径选择器是怎样知道网络的拓扑结构的？
6. 用户是怎样在网络中寻求服务的？

本章其余部分回答了这六个问题并通过例子把几个答案结合在一起从而阐述了信息是怎样流过一个 TCP/IP 网的。

2.2 基本的网络概念

2.2.1 寻址

地址的两个部分：

网络（或区域），节点（或主机）。

在互联网中寻址的规则：

- 互联网中的每一个网络都必须有唯一的网络号
- 同一个网络中的每个设备必须有不同的节点号。

两种不同类型的地址：

- 广播地址：同时寻址多个节点。
- MAC 地址：网卡上的物理地址。这是最低层的地址。

2.2.2 包

互联网的信息都是被分快传输的，这些块称为包。

- 便于资源共享。防止某个设备暂用过长的传输时间。
- 易于检错和纠错。

2.2.3 协议

包是一串字符流，通过具体的协议对包进行解读。

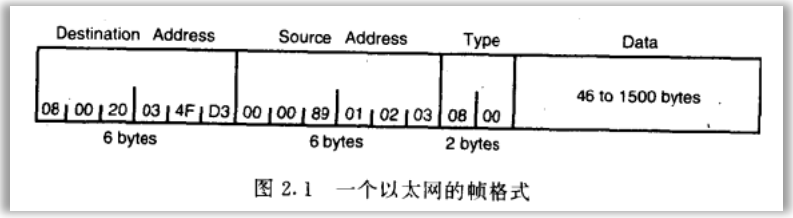


图 2.1 一个以太网的帧格式

2.2.4 路径选择器和端节点

端节点：

工作站、PC 机、打印机、文件服务器等。

路径选择器：

连接网络的设备，负责在整个网络中传递信息。路径选择器连接在多个网络之间。功能就像邮局。

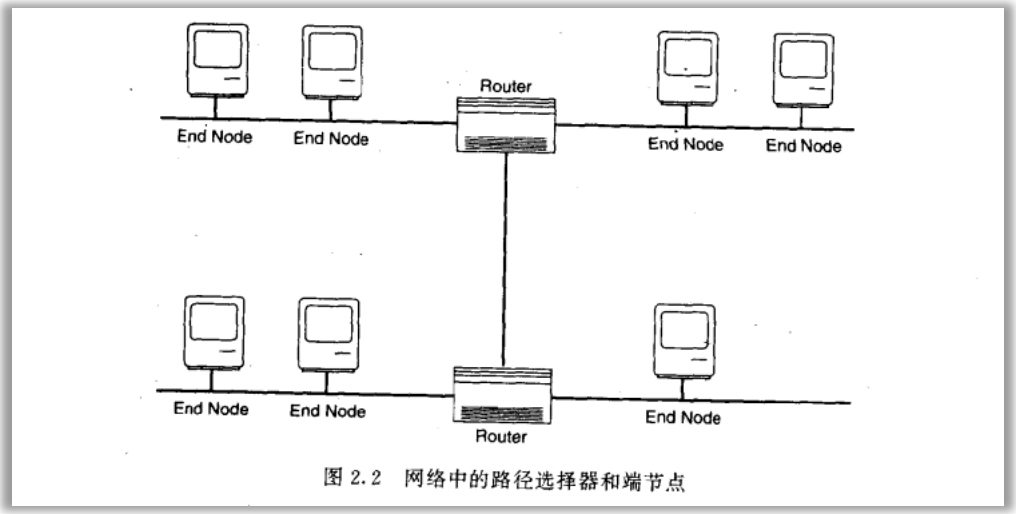


图 2.2 网络中的路径选择器和端节点

2.2.5 端节点的网络发送和接收过程

发送过程：

- 如果源地址与目的地址网络号相同，这两个节点可以直接使用数据链路层进行通信。（例如以太网）。发送方使用 ARP 来分解出接收方节点的 MAC 地址并把 IP 包封装发给目的节点。
- 如果网络号不同，IP 包被封装成数据链路层帧，然后被编址到同一线路的路径选择器的 MAC 地址。再由路径选择器发送到远端。

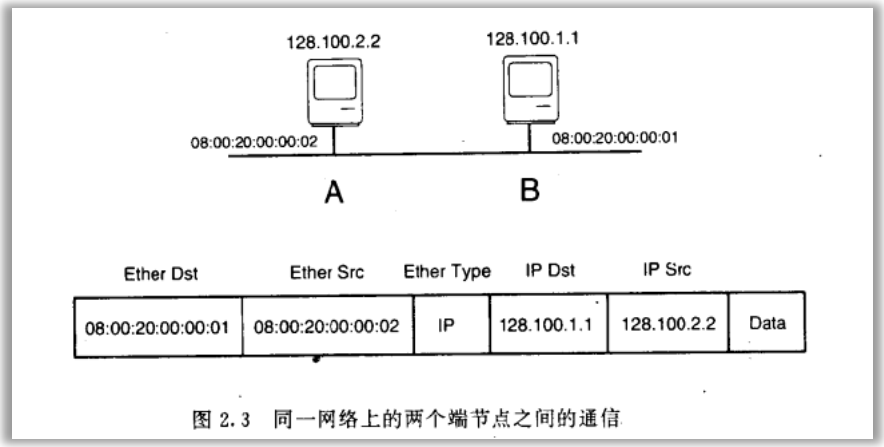


图 2.3　同一网络上的两个端节点之间的通信

接收过程：

一个节点接收到数据包后，会进行目的地址，源地址，广播地址的比较。成功则根据协议解析此包，不成功则丢弃。

2.2.6 路径选择器的发送和接收过程

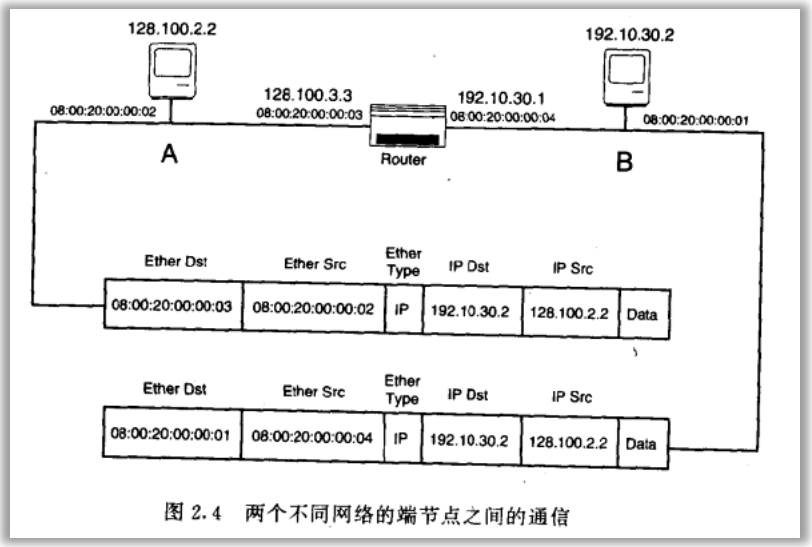


图 2.4　两个不同网络的端节点之间的通信

当一个节点作为一个路径选择器使用并接收到一个 IP 包时，它首先分析出包中的目标 IP 地址并与自己的 IP 地址相比较。如果两个地址相同或目的 IP 地址是 IP 广播地址，那么这个地址是某个端节点的地址，因而这个包将会被处理。如果不是某个端节点的地址，路径选择器自动地不丢掉这些收到的包但不对其寻址。这些包是网络上的端节点发给路径选择器让其往下传到其他网络的包(参看图 2.4)。所有路径选择器都包含表示怎样到达其他网络的路径选择表。路径选择器把目标地址的网络部分与它的路径选择表中的每个网络相比较。如果路径选择器没有在它的路径选择表中找到目标网络，它就查找一个缺省路径选择

(一般为路径选择 0.0.0.0)。如果找不到一个缺省路径选择，这个包就被丢掉(并且把一个不能到达目的地址的 ICMP 信息发给所丢弃的包的源 IP 地址。

如果找到了一条到这个网络的合适的路径选择(或是一条缺省路径选择),路径选择器就测试出到远端网络的距离。如果距离是零,则这个网络是与路径选择器直接相连的网络,在这种情况下,路径选择器发一个 ARP 请求给目标 IP 地址并把 IP 包封装成一个数据链路层帧,这个帧由目的地返回的 ARP 应答中的 MAC 地址所编址。如果路径选择器测出的距离大于零,这个包必须至少再通过一个路由器。在这种情况下,这个路径选择器就利用下一个路径选择器字段发一个 ARP 请求到那个路径选择器,把 IP 包封装成一个数据链路层帧,此帧由下一路径选择器的 MAC 地址进行编址。这样,一个 IP 包就能穿过一个互连网,从头到尾都能保持源和目标 IP 地址的一致,但在每一点上源和目标 MAC 地址不同,一个路径选择器收到一个包后采用的算法如下:

2.3 IP 地址的格式分析

IP 地址格式:

- 由 4 个字节，32bit 组成。
- 标记方法为每个字节表示十进制数并以点号隔开:192.168.1.1.（超过 255 不合法）。
- IP 地址包含网络部分和主机部分。但具体的区分并不是每部分占一半。

IP 地址分类:

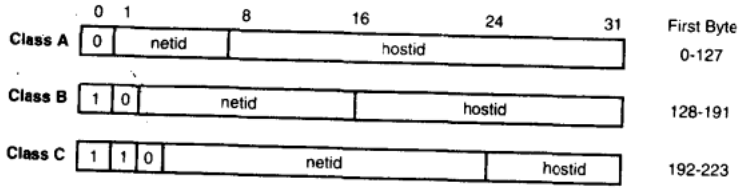


图 2.6 三类 IP 地址

一个 IP 网络通常也被称为一个 IP 地址,其主机部分都是零——例如,10.0.0.0 或 128.37.0.0 或 200.23.45.0。例如,137.103.210.2 就是一个网络部分为 137.103、主机部分为 210.2 的 B 类地址,这个 137.103.0.0 网络上最多有 2^{16}(两个字节)个主机——每个主机必须共享前两个完全相同的字节 137.103,并且主机部分必须不一样。

2.4 为 TCP/IP 设备分配 IP 地址

首先是取得网络号:

可以与 Network Solutions 公司签订服务。他们会提供一个决定唯一的网络号。

再是分配主机 IP 地址:

可以手动，也可以自动。所有的设备网络号一样，但是主机号一定不一样。

2.5 把 IP 地址映射成 MAC 地址

MAC 地址:

独立于 IP 地址。与 IP 地址无关。MAC 地址有时也叫物理地址、硬件地址、链路地址。MAC 地址被设备或者网卡厂商设置到了硬件里。

以太网地址：

其实就是 MAC 地址。以太网地址用十六进制数表示，以冒号隔开。以太网地址是由 IEEE 分配且所有的以太网地址都是唯一的。没有两个设备具备相同的以太网地址。以太网地址有两个独立部分：

- 第一部分：3 个字节构成的厂商代码。
- 第二部分：该厂商生产的产品序号。

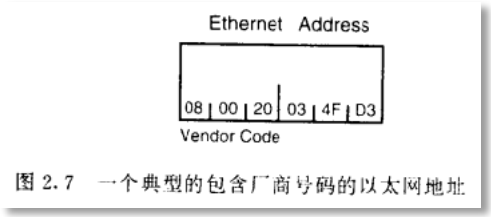


图 2.7　一个典型的包含厂商号码的以太网地址

为啥需要以太网地址和 IP 地址同时存在？

如果每个以太网设备已经有一个唯一地址，那还为什么需要 IP 地址呢？首先，不是每一个设备都是以太网所支持的，IP 地址使得连在光纤、环型令牌网和几条链路上的设备在没有以太网地址时能够使用 IP 协议。其次，以太网地址被设备厂商组织而不由个人组织。一个有效的路径选择方案由设备制造者产生而不是由安装者产生是不可能的。IP 地址基于一个网络的拓扑结构来分配，而不是由设备制造商分配。最后也是最重要的一点是当一个附加地址已经存在时，这个设备就很容易被移走或被代替。如果一块以太网卡坏了，不需要得到一个新的 IP 地址就可以更换这块卡。如果一个 IP 节点从一个网络搬到另一个网络上，不需要更换以太网卡只需配置一个新的 IP 地址就行。

IP 地址到 MAC 地址的映射：

如果在同一个网络，先广播一个 ARP 请求，每一个设备监听者个 ARP 请求，如果发现是发给自己的，则回复 ARP 请求并与请求源建立联系。后续通过 IP 封装成以太网包进行直接的交流。

2.6　终端节点如何找到路径选择器

当目的地址不再同一个网络时，可以根据 ARP 协议首先取得路径选择器的以太网地址。然后将 IP 包发送给路劲选择器，再由路径选择器发送出去。

2.7　路径选择器怎样知道网络的拓扑结构

路径选择器扮演着网络邮局的角色。所以他需要知道能到达哪些网络并且怎样到达那里。这个时候，就需要路径选择表。每个路径选择器都有这样的一张表。

表 2.1　一张含有三个路径选择器的网络的路径选择表

网络	距离	下一路径选择器
路径选择器 1		
1	0	—
2	0	—
3	1	222. 222. 222. 2
4	1	222. 222. 222. 2
5	2	222. 222. 222. 2
6	0	—
路径选择器 2		
1	0	222. 222. 222. 1
2	0	222. 222. 222. 1
3	1	—
4	1	—
5	1	200. 15. 22. 1
6	0	—
路径选择器 3		—
1	0	200. 15. 22. 1
2	0	200. 15. 22. 1
3	1	200. 15. 22. 1
4	0	—
5	0	—
6	1	200. 15. 22. 1

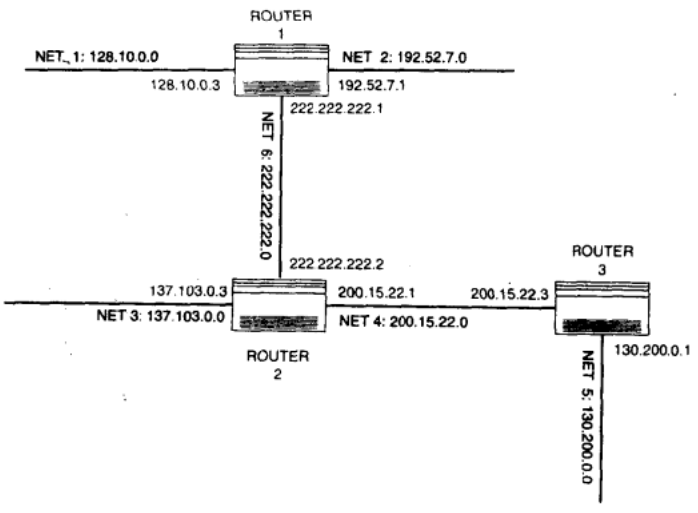


图 2.9　一个有三个路径选择器的网络

如何设置路径选择表：

- 人工设置：太难
- 动态采集：借助多路径选择协议而得到。最常用的是 RIP 协议。

路径选择表里面没有这个网络：

- 包会被丢掉。

- 原因可能是：

  - 发方节点被搞错了或配置错了
  - 路径选择器配置错了不知道这个网络
  - 到达那个网络的所有的路径选择器都不能工作(到达那个网络的路径上有一个路径选择器出了故障)

2.8 寻找和使用服务设施

记住 IP 太难了，而记住名字很容易。有两种常用的方法将名字映射成 IP：

- 定义名称系统 DNS
- 太阳公司的网络信息系统 NIS

输入网址后，发生了什么：

http://www.cnblogs.com/rollenholt/archive/2012/03/23/2414345.html

2.9 TCP 和 UDP

TCP：即为传输控制协议。

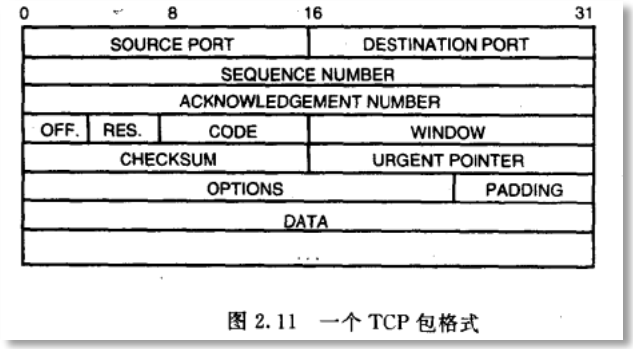


图 2.11 一个 TCP 包格式

UDP：即为用户数据报协议。

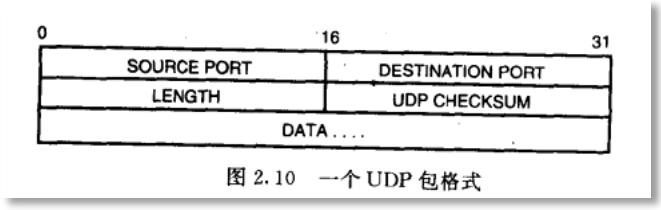


图 2.10 一个 UDP 包格式

端口：一个节点上的每一项服务，都是通过端口来访问的。有时也被称为 socket。

TCP 和 UDP 比较：

TCP	UDP
可靠传输	不可靠传输
效率低，开销大	效率高，开销小

常见应用/协议：NFS，RIP，Trivial 文件传输协议（TFTP），简单网络管理程序（SNMP）	常见应用/协议：FTP，Telnet，SMTP

3 主机名和 Internet 寻址

3.1 TCP/IP 基础

无论是美国邮政总局把邮件送往居民区的个人手中还是送往大公司的有关设施，对你来说差别不大，而这些差别等同于 Internet 地址的差别。下面列出了 Internet 地址的三种主要类型。

- A 型表示有很少的大公司和很多场所（或者说有很少的网络而每个网络上有很多主机）
- B 型与 A 型相比公司较多而场所较少（或者说有更多的网络而每个网络上有较少的主机）
- C 型表示有很多公司和很少场所（或者说有很多网络而每个网络上有很少的主机）

正如上述 C 型一项所表示的那样，可以用网络代替公司而用主机代表场所，如果一座城市只有一个使用邮递站传送邮件的公司，那么邮局便把大量邮件送往很少的位置。但是如果一座城市主要由不相关联的场所组成，那么邮局便把少量的邮件送往多个地址。

> **注解**：还有两类为多信道寻址和未来 Internet 需求而保留。它们开始于 224.0.0.0，直到（不包括全系统通播）255.255.255.255 为止。

3.2 确定寻址方案

要想将你的网络连接到 Internet，你必须要申请一个独一无二的 Internet 地址。这个地址你必须像网络信息中心（NIC）提出申请。至于你被分配到 A 类，B 类，还是 C 类网络地址，这主要取决于你的网络类型。

3.3 广播报文

为了向网络上的所有主机发送报文，TCP/IP 使用特殊的主机地址。这个地址保持网络部分不变，而把主机部分的地址全部改为 0 或者 1. 比如你是 B 型网络 134.135 的成员，那么把报文发往地址：134.135.255.255.

3.4 定义子网掩码

子网掩码用来把数据传送到实体内不同的子网。这样可以避免 Internet 把信息传送到整个网络。

3.5 Internet 域命名约定

域名是访问网络的另一种途径。如果你熟悉 Internet，那么一定熟悉类似于 NETCOM.COM，SPRY.COM 或者 LANTIMES.COM 的名字。这些都是域名，是地址登记的流行形式。

现在有多种多样的高级域扩展。但最流行的应该算是 GOV（政府部门），EDU（教育部门），ARPA（ARPANET 网），COM（商业部门），MIL（军事部门）和 ORG（前面未提及的任何组织）。

3.6 Internet 新闻组命名约定

不知道有什么鸟用

3.7 OSI 堆栈说明

想说明的东西：

数据如何从一台主机到达另一台主机。

协议栈：

描述数据如何在网络中进行传输。

OSI 七层模型：

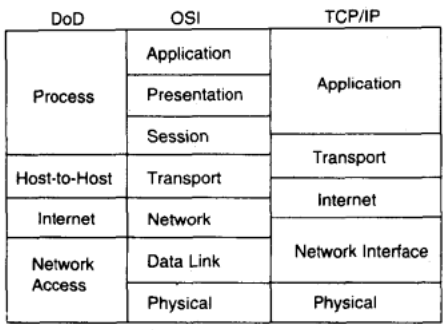


图 3.1 OSI 七层模型和 DoD 四层栈

- 第七层：应用层。这一层主要以程序或应用程序的形式出现，是 OSI 和用户之间的接口层。
- 第六层：表示层。应用程序和终端管理程序在这一层转换。一般通过格式化和数据转换来实现。
- 第五层：会话层。完成与控制相关的应用程序之间的通信。
- 第四层：传输层。完成端数据传输、端到端数据恢复和流量控制。
- 第三层：网络层。在这一层建立、维持和取消连接。这一层使得上面的各层与数据传输及切换技术无关。

■ 第二层：数据链路层。维持同步、差错控制和流量控制以便确保数据能够可靠地通过物理层。

■ 第一层：物理层。这一层可以是以太网或其他介质，是主机之间的物理链路。

TCP/IP 共有五层，在某种程度上它是 OSI 七层模型的派生。这五层也是七层模型的结合，它包括：

■ 第五层：应用层。类似于 ftp，telnet，SMTP 及 NFS 等的应用程序与此层有关。

■ 第四层：传输层。在此层中，TCP 和 UDP 给数据包加入传输数据并把它传递到第三层。

■ 第三层：互连网络层。当你在本地主机上开始将要执行的动作或者响应远端主机（或接收主机）时，该层从第四层中取出包并在把包传递到第二层之前把 IP 的头信息加入其中。

■ 第二层：网络接口层。主机或本地计算机把它看作网络设备，比如/dev/ttyla，/dev/ttys0 或者/dev/wdn0。数据从这一中间层传递到第一层。

■ 第一层：物理层。以太网或者串行线路接口协议（SLIP）本身。

在接收主机处，每次打开一层。信息被传递到下一层，直到再次到达应用层。

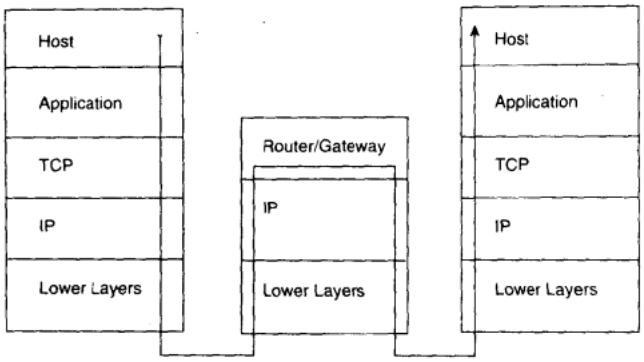


图 3.2　有网关的七层 OSI 模型

3.8　准备 TCP/IP 的安装

硬件网卡的安装？

3.9　安装 TCP/IP

搞鸡毛？

3.10　配置 TCP/IP 连接

/etc/hosts 可以配置哪些主机可以访问本台主机

3.11 测试 TCP/IP 连接

ping 可以用来测试连接的正确性。

4 远程访问和网络文件传送

本章主要了解如何与远程主机进行连接以及传送文件。主要手段是分析常见的实用程序。

4.1 Unix 专用实用程序

4.1.1 rwho

用于显示谁已经在与网络连接的每一台主机上注册了。其实就是显示本地局域网内的所有用户

4.1.2 ruptime

可以查看主机在线时间，以及负载情况。

4.1.3 rlogin

Linux rlogin 命令用于远端登入。执行 rlogin 指令开启终端机阶段操作，并登入远端主机。

4.1.4 前后台切换

为了回到自己的主机：输入~Z
为了返回远端主机：输入 exit

4.1.5 remsh

remsh 命令使您可以在远程系统上执行命令，而无需登录到该系统。
为使用 remsh 做准备
必须按下述方式配置远程系统：
在远程系统上必须有一个登录名与本地登录名相同的帐号。
本地系统名称和本地登录名必须位于远程系统主目录下的 .rhosts 文件中。

4.2 非 Unix 专用的实用程序

这些程序应用更广，不依赖操作系统。

4.2.1 telnet

它既是程序也是协议。

4.2.2 ftp

它同样既是程序也是协议。

ftp 能够在 Internet 内的任何主机上来回拷贝文件。ftp 程序能够运行在使用不同体系结构和操作系统的机器上。在所有主机上 ftp 都能几乎同样工作的事实使其成为非常有用的工具。

4.3 理解 NFS

Network File System(NFS,网络文件系统)是经常与 TCP/IP 联合使用的一个工具。Sun Microsystems 公司开发的 NFS 使你能够安装远程主机的硬盘并且在你的主机上看起来就像本地硬盘一样。

5 TCP/IP 路径选择

独立的网络终将成为历史，LAN 必须要连接到广域网（WAN）或者城域网（MAN）。这个时候，你就会遇到网桥，路由器，网关等待。本章将为你揭开谜底。

5.1 OSI 模型分析

OSI 模型本身并不是任何的通信协议。他只是提供了通信任务的准则。它把复杂的通信任务划分为小规模的，更加简单的子任务。

本章主要了解前三层的模型：

7	应用层
6	表示层
5	会话层
4	传输层
3	网络层
2	数据链路层
1	物理层

图 5.1 OSI 模型

在本章的内容里，解释由 OSI 模型的前三层提供的服务是很重要的：

- 物理层（第 1 层）提供了计算机系统和网络连线间的连接。它指定了电缆引脚分配和线路上的电压等等。这一层的数据单位被称作“位”。
- 数据链路层（第 2 层）为传输提供了数据打包和拆包功能。这一层的数据单位被称作“帧”，帧代表了数据结构（这很像数据库模式）。
- 网络层（第 3 层）提供了通过网络的路径选择。这一层的数据单位被称为“数据报”。

5.2 DoD 模型分析

TCP/IP 协议在 OSI 模型定义前就开发出来了。因而 TCP/IP 并不是采用的 OSI 模型。而是采用的 DoD 模型。

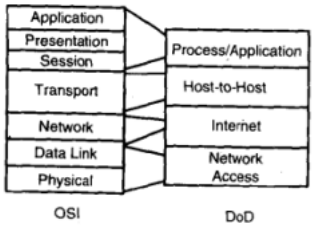


图 5.2 OSI 模型与 DoD 模型的比较

5.3 网络互连设备

TCP/IP 的路径选择决策都是有一张路径选择表进行的。

明了用于显示存储在路径选择表中信息的 netstat－r 命令的输出。

destination	router	refcnt	use	flags	snmp metric	intrf
132.1.16.0	132.1.16.3	1	63	U	－1	lan0
132.1.16.5	132.1.16.4	0	22	U	－1	PPP0
127.0.0.1	127.0.0.1	1	0	UH	－1	lo0
default	132.1.16.1	2	1351	UG	1	lan0

5.3.1 转发器

转发器仅仅用来增强信号并将信号发送出去。如果信号需要传输的距离很长，随着距离变长，信号会变得越来越弱，因此转发器可以帮助提高传输距离。

5.3.2 网桥

网桥经常用于繁忙网络上业务的分离。网桥跟踪了与之直接相连的每一网络中设备的硬件地址，网桥分析帧中的硬件目的地址，而且根据它的表格来决定该帧是否被向前传送。如果该帧需要向前传送，一个新帧便被生成。

注解：网桥是一个“存储并向前传送”的设备，它不把原始信号传送到目的段中。

因为网格能够在数据帧的级别访问信息，所以它操作在 OSI 模型的数据链路层（如图 5.4 所示）。

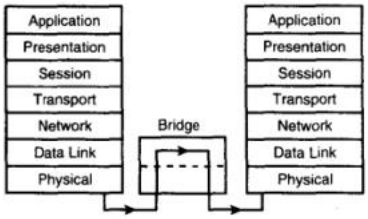


图 5.4 OSI 模型中的网桥

和转发器一样，网桥对协议是透明的。由于网桥操作在数据链路层，它也能够实现物理层的功能。所以，你能够使用网桥来扩展分段的距离。

注解：和转发器不同，网桥不会把错误从一个分段传播到下一个分段。

现有的四种网桥如下：

- 透明网桥：透明网桥是最常见的网桥类型。它不关心连线上的协议。由于它知道它直接相连的设备的硬件地址，所以透明网桥也被称作 Learning 网桥。因为它使用跨越树算法（IEEE802. ID）来管理具有冗余网桥的分段路径，所以它也被看作 Spanning tree 网桥。
- 源路径选择（SR）：在 IBM 环型令牌网中，源路径选择网桥（SR）比较普遍。IBM 使用源路径选择根据帧内的环序号信息来决定其帧是否要穿过网桥。
- 源路径选择透明（SRT）：它是透明网桥和源路径选择网桥的结合。如果数据帧具有 SR 信息，它便进行源路径选择；如果没有，它便进行透明路径选择。
- 转换网桥：一些制造厂生产“转换网桥”，用来把以太网连接到环型令牌网。一个例子是 IBM 的 8209 网桥。

注解：一般说来，网桥连接具有相似拓扑结构的分段，比如环型令牌网到环型令牌网。它们还能够把相同拓扑结构的分段用不同的介质连接起来（这很像转发器）。

5.3.3 路径选择器（路由器）

路径选择器能够决定两个或多个网络之间的最佳路径。路径选择器能够访问网络(软件)地址信息，这意味着它工作在OSI模型的网络层(见图5.5)。由于它需要访问网络地址信息，所以它与协议关系密切。当路径选择器遇到的数据报具有它不支持的协议时，该数据报被丢弃。

例如，如果你的网络之一拥有TCP/IP和NetWare通信业务，而你的路径选择器只支持TCP/IP(或者只有TCP/IP被打开)，那么NetWare业务不会离开那个网络分段进入别的分段。这样通信业务便局限在那个分段内。

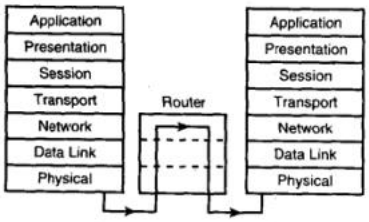


图5.5 OSI模型中的路径选择器

路径选择器与网桥相比要智能化很多，它能够为数据报到达目的地而进行最佳路径选择。这个路径能够依赖于以下的因素而变化：链路的可用性、通信业务级别等等。另一方面，网桥只是简单地决定是否需要传递。

提示：路径选择器不会把错误从一个网络传递到另一个网络。

警告：通过路径选择器访问资源的工作站比通过网桥访问资源的工作站稍慢，而网桥比转发器又稍慢。路径选择器实现的功能比网桥或转发器要复杂，这导致了速度的降低。

在IP领域里，路径选择器传统上被称作网关，这是因为它们很像是与外界联络的“网关”。然而，随着OSI模型被人们的认可以及工业界有关网络互连术语的标准化，网关现在都被称作路径选择器。然而，当你读到RFC的术语时还要小心，因为术语“网关”还在使用。不要把它和下面将要讨论的网关的OSI定义搞混。

5.3.4 网桥路径选择器

网桥路径选择器(bridging router)首先对它能够理解的协议的设备进行路径选择，然后它便试图导通网络通信业务。

某些协议(比如NetBIOS)因为没有网络信息而不能被路径选择。如果你需要把这些协议和TCP/IP一起传递，那么你需要在网络上使用网桥路径选择器。

在大多数情况下，那些基于硬件的路径选择器(例如3COM、Cisco以及Wellfleet)都能作为网桥路径选择器使用。基于软件的路径选择器(例如Novell公司的Multiprotocol Router)都不能(即使是Novell公司的MPR2.11+支持环型令牌网SR网桥)作为网桥路径选择器使用。

注解：检查一下你的路径选择器文档；并非所有的基于硬件的路径选择器都能作为网桥路径选择器使用。

5.3.5 网关

网关是在两种不同的协议(有时候是拓扑)之间进行转换的设备。例如网关可以用于以太网上的 TCP/IP 到环型令牌网上的 SNA 的转换。

> **注解**:网关超向专用于高层协议,例如电子邮件协议。所以,如果你需要在两个主机之间交换电子邮件和打印业务,那么可能需要两台独立的网关。

由于网关转换大多数(如果不是全部的话)协议层,所以它能够覆盖 OSI 模型的全部七层。

5.3.6 确定使用哪种设备

> **提示**:路径选择器需要查看深埋在帧内的软件地址。因此,为了获得信息它需要做更多的工作。网桥只需查看硬件地址(它靠近帧的开始),所以需要较少的工作。因此,作为一条规则,网桥能够比路径选择器更快地传送数据。转发器不会查看任何数据,所以它比网桥还快。

> **警告**:如果(数据链路层)广播通信业务(帧将被发送到网络上的所有设备)是一个重要问题,那么网桥便不是好的网络互连设备。根据定义,广播地址不是"本地的"。因此,广播业务通常跨过网桥传播。这种情况下应使用路径选择器。

5.4 IP 路径选择协议

路径选择器通过两种方式知道其他网络:

- 静态路径选择:管理员手动配置路径表。
- 路径选择协议:
  - 路径选择信息协议(RIP)
  - 首先打开最短的路径(OSPF)
  - 内部网关路径选择协议(IGRP)
  - 互连网控制报协议(ICMP)

5.4.1 路径选择协议分类

- 内部路径选择协议
  - 又叫网关协议。
- 外部路径选择协议
  - 距离-矢量路径选择协议
  - 链路状态路径选择协议

5.4.2 路径选择信息协议（RIP）

属于距离-矢量路径选择协议

5.4.3 配置接口路径选择

可以用 ifconfig 进行配置

5.4.4 分配静态路径选择

5.4.5 内部网关路径选择协议（IGRP）

5.4.6 首先打开最短路径（OSPF）

“首先打开最短路径”(OSPF)是在 1989 年首先推出的链路状态路径选择协议(RFC 1131/1247/1583)。由于 OSPF 比 RIP 的通信业务开销低很多以及它彻底地的排除了“无穷计数”问题，所以越来越多的用户从 RIP 转向了 OSPF。

从费用角度看，OSPF 比 RIP 支持大得多的互连网。记住在基于 RIP 的互连网中，在任意两个网络之间的路径选择器不能超过 15 个，这在有些时候会导致不得不为大型网络采用更多的链路。

与 RIP Ⅰ 相似，OSPF 支持变量长度子网，这使得网络管理员为了网络分段能够使用不同的子网掩码。可变量的子网为单一网络地址大大地增加了灵活性以及子网和主机的数量。OSPF 还支持更新报的判别。

使用费用作为尺度，OSPF 的尺度可达 65,535。

5.4.7 Internet 控制报协议

ICMP 在 1980 年首次推出(RFC 792/1256)。它的功能是用动态方式来确保你的系统具有最新的路径选择表。ICMP 是任何 TCP/IP 网络的组成部分而且无需配置便自动生效。ICMP 提供许多功能，包括路径选择重定向等等。

例如，如果你的工作站把一个包传送到一个路径选择器，而那台路径选择器知道到达目的地的更短的路径，那么该路径选择器会向你的工作站发送一条“重定向”报文以便通知它那条更短的路径。

ICMP(RFC 1256)的新的实现方案包含“路径选择器发现”功能。严格地讲，路径选择器并非只能发现一种路径选择方案，只是它要找到最佳相邻路径选择器。当路径选择器启动时，它便发出路径选择器发现请求(多路广播地址 244.00.2；只有接口不支持多路广播时才进行通播)，请求相邻路径选择器标识它们自己。只有直接与新路径选择器所在的网络相连的路径选择器才响应。

> **注解**：“路径选择器发现”功能是一些相当新的路径选择器才有的功能，而并非所有的路径选择器都支持它。

5.5 IP 包的路径

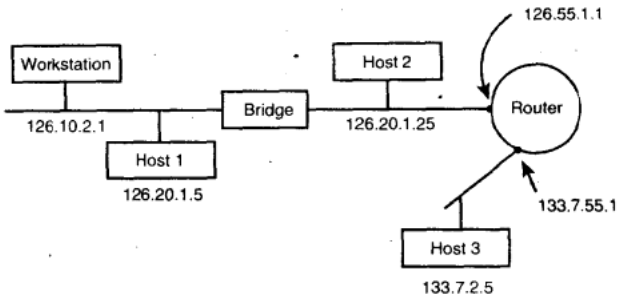


图 5.14 由网桥连接的两个分段以及一个路径选择器连接的分段组成的样例网络

5.5.1 本地段

在图 5.14 中，工作站 Workstation(126.10.2.1)希望与 Host 1(126.20.1.5)通信。Workstation 中的 TCP/IP 软件确定了目的地是在同一个网络上(126.0.0.0)，所以在 Workstation 和 Host 1 之间传送数据不会涉及到路径选择器。

为了在数据链路层组成帧，TCP/IP 软件需要知道 Host 1 硬件地址(也被称作数据链路控制(DLC)地址或者媒体访问控制(MAC)地址)。TCP/IP 软件使用地址分解协议(ARP)可以找到硬件地址。TCP/IP 便将 DLC 地址插入到帧的目的地址字段并把它自己的地址(通过 NIC 得到)插入到源地址字段。然后帧便被传送到线路上。

Host 1 和网桥都“看到”了这一帧。然而网桥根据它知道的地址表，得知 Host 1 和 Workstation 在网络的同一侧，所以网桥便忽略这一帧。

Host 1 在目的字段中看到了自己的地址，所以取走这一帧并处理它。Host 1 在它的应答报中在源地址字段处使用 DLC 地址作为目的地址。用这种方式两项设备都知道了相应的 DLC 地址。

5.5.2 带网桥的网络分段

带网桥的 IP 网络环境中的通信过程和前面讨论过的本地分段情况大不相同。如果数据帧需要通过网桥(bridge)(到达 Host 2)，那么工作站(workstation)使用 ARP 获得 Host 2 的 DLC 地址。工作站在目的字段中使用 DLC 地址，把它自己的地址放入源字段中，然后通过线路将该帧发出。

这种情况下，网桥注意到目的地址列在了它另外的分段中。所以，网桥把帧拷贝一次并把此拷贝放在另一侧(不改变任何东西，包括 DLC 地址)。

5.5.3 带路径选择器的网络分段

在路径选择环境中，数据帧的寻址比前面提到的两种情况都稍微复杂一些。首先，工作站确定目的节点(Host 3)不在自己的网络上，所以它需要使用路径选择器。然而，如果在一个分段上有许多路径选择器，那么应该使用哪一个呢？当你在工作站上安装 TCP/IP 软件时，你总是被请求指定一个缺省的路径选择器。如果你是在本地段内通信。那么这一项不被

使用。然而当你需要在网络外进行通信时，所有的帧都要被寻址到这个缺省路径选择器。

> **提示**：一些工作站软件(比如 Novell 的 LAN WorkPlace for DOS V4.1 以及更高的版本)允许你定义多个缺省的路径选择器，这为你提供了一些备份路径。然而，一定要小心负载均衡指标以便防止某一路径选择器过载。

在前面两个例子中，工作站通过使用 ARP 找到路径选择器 DLC 地址。TCP/IP 网络驱动软件把路径选择器的 DLC 地址而不是 Host 3 的地址放入目的字段中。这个概念是非常重要的——在网桥环境中，路径选择器的 DLC 地址(和 IP 地址)将会被涉及到。

在路径选择器接收到帧后，它通过取走 DLC 信息而"打开"数据帧。路径选择器检查 IP 信息(IP 目的节点地址)并利用路径选择表来弄清楚下一站在哪里。如果目的地在与路径选择器直接相连的网络上(就像前面简单例子中那样)，路径选择器使用 ARP 来确定 Host 3 的 DLC 地址并且使用自己的地址以及 Host 3 的 DLC 地址产生一个新的数据帧。因为数据帧中的源 IP 网络与它自己的网络不同，所以 Host 3 知道该数据帧来自另一台路径选择器。Host 3 回到工作站的应答要经过与上相反的路径。

然而，如果第一台路径选择器没有直接连接到目的节点，那么路径选择器会查看它的路径选择表以便找到下一跳越在哪里，然后使用 ARP 协议确定下一个路径选择器的 DLC 地址，再将具有新信息的帧发送出去。这个过程一直进行下去，直到数据帧到达与目的节点直接相连的路径选择器为止。

现在你已经明白了为什么要保持路径选择器的路径选择表为最新状态。任何沿着数据帧路径的过时的路径选择信息都会导致数据的丢失。在最好的情况下，这将导致数据的重发；在最坏的情况下，这会导致应用程序的崩溃和无法通过互连网进行通信。

6 Frame Relay 和 ATM 综述

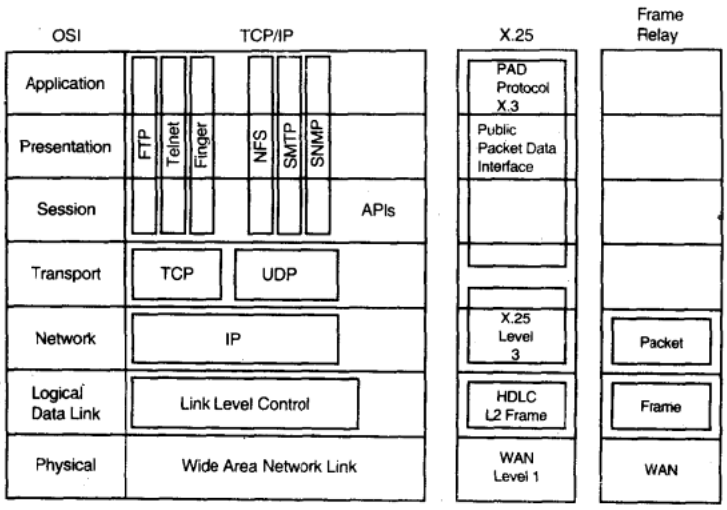


图 6.4　Frame Relay 和 X.25 OSI 的比较

Frame Relay 技术提供了高的吞吐能力、低的等待时间和所需的带宽。现在的技术发展带来了高吞吐量的节点处理机、标准的开放式网桥和路径选择器接口以及支持单元中断和交换的接口。它是企业网络的最佳选择之一。

ATM 技术提供了高带宽、低时延交换和多路复用。与 ATM 单元中断相比，具有较大分组报文长度的传统分组报文交换的主要问题是响应时间和吞吐能力。民意测验的结果是 ATM 将会在九十年代成为标准。高速和宽频带联网中不断变化和进步的技术为"信息高速公路"带来了美好的前景。

7 简单网络管理协议

本 章 要 点

作为网络顾问或者管理员，在安装了网络并且建立了用户帐户及应用程序之后，你的工作并未结束。你的下一项任务便是网络管理，这是一场永不停止的“战斗”。

存在两种类型的网络管理：与软件有关的，比如数据安全及访问许可；还有就是有关硬件的。本章集中讨论第二项内容——使用 SNMP 把硬件作为整体来管理，同时还利用了一些与软件管理有关的概念。本章将 SNMP 划分为下述几节：

- 什么是 SNMP
- 什么是被管理设备
- 什么是网络管理站
- 如何灵活并有效地管理你的网络

- 被管理的节点(或设备)：你希望监控的设备。
- 代理人：用来跟踪被管理设备的状态的特殊软件或者硬件。
- 网络管理站：用来传送和显示不同节点中代理人状态的集中设备。
- 网络管理协议：网络管理站和代理人用来交换管理信息的协议。

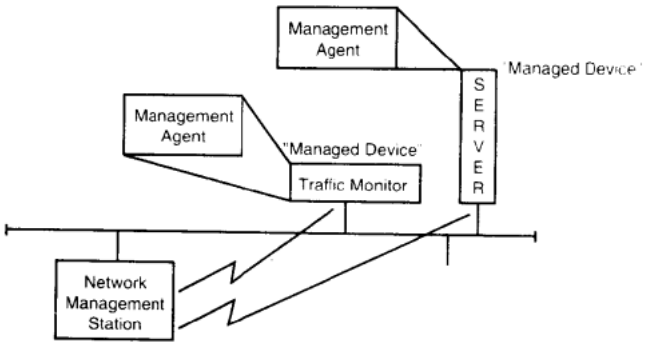


图 7.1　网络管理框图

7.2　什么是 SNMP

简单网络管理协议(SNMP)首先是由 Internet Engineering Task Force(IETF)研究小组开发的，目的是解决 Internet 上的路径选择器管理问题。许多人认为 SNMP 在 IP 上工作，原因是 Internet 运行 TCP/IP。然而，这并不是事实。

SNMP 被设计成为与协议无关，所以它能够用于 IP，IPX，Apple Talk，OSI 和其他必要

8 域名系统

注解:DNS 主要目的是为了解决网络节点名与 IP 地址的对应关系。请不要与“网络信息服务”(“NIS”)相混淆。NIS(当前所常用的为 NIS+)不仅含有网络节点名与网络地址的对应关系,而且它还含有像“用户标识码”(“UID”)及“组标识码”(“GID”)等信息。在 NFS 环境中经常能碰到 NIS 或 NIS+。

表 8.1 高层网络域名

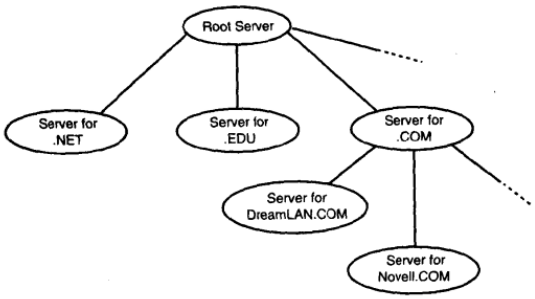
域名	描述
ARPA	高级研究规划局网络(ARPANET)(美国防部 Advanced Research Projects Agency network)
COM	商业组织
EDU	教育学会
GOV	政府机构
MIL	国防机构
NET	网络服务中心,例如 Internet 服务中心
INT	国际组织
ORG	非盈利组织
国家代码	两个字母的国家代码(根据国际标准化组织的 ISO 3166 中的 x.500 标准所定义)

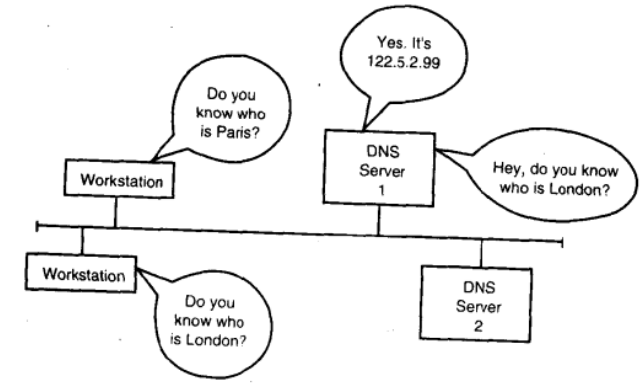
注解:大多数情况下,一个国家必须要使用三个字符的国家代码才能够保证不发生冲突和混淆。

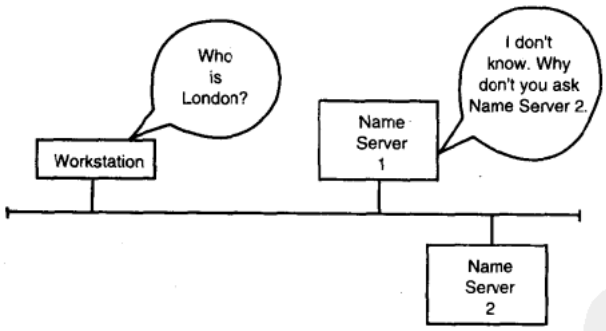
8.3 DNS 域名的解析

在讨论域名服务器时,最简单的方法就是将这些域名服务器排列成树形结构,以表示出这些服务器的层次结构。

树形结构如图 8.4。







9 发送邮件与 SMTP

10 网络安全

绝对安全的系统是不存在的。

10.1 安全的分级

分为四个等级：

- A，B，C，D 等级。
- 每个等级可再细分为多个子集，A1，A2，A3…
- 安全性：
  - An > An-1 >… > A1 >
  - Bn > Bn-1 > … B1 >
  - Cn > Cn-1 >…>C1 >
  - Dn > Dn-1 > … > D1.

市场现状：

- DOS 系统为 D1 级系统，几乎没有任何的安全能力。
- 标准的 UNIX 操作系统属于 C1 级系统。
- 当今流行的 UNIX 如 SCO UNIX 属于 C2 级系统。

- B 级系统目前还没有出现在商业市场上面。

10.2 安全的需求分析

安全是必须的，但并不是越安全越好。而是根据具体的需求，指定合理的安全特性。在易用性和安全性之间取得平衡。

10.3 本地安全

以 UNIX 为例，安全主要包括：

- passwd 文件
- /etc/shadow 文件
- /etc/group 文件

10.4

- 主机等效
- 用户等效

10.5 增加安全的手段

- 利用子网：意外闯入子网时，可以减小受伤的面积。
- 拨号口令：如果采用的是 modem 连接，可以考虑加入拨号口令。
- 口令期：定期更换口令。
- 防火墙：
- 数据加密

11 连接 NetWare

连接不同的网络操作系统，需要考虑的问题：

- 介质。选什么介质，负载是否足够。
- 建立自己的寻址模式。
- 建立用户隶属分区，确定访问权限。

12 连接 DOS 和 Windows