

# 目 录

第一章 网络基础知识.....	6
1.1 网络的发展.....	6
1.2 计算机网络的定义.....	6
1.3 计算机网络的分类.....	7
1.4 网络的拓扑结构.....	8
1.5 网络的传输介质.....	10
1.6 网络操作系统.....	12
1.7 计算机网络通信的基本模式.....	13
1.8 计算机网络通信协议.....	13
1.8.1 标准化组织.....	13
1.8.2 通信协议.....	14
1.9 网络互连设备.....	16
第二章 OSI 参考模型.....	17
2.1 层次化网络体系结构.....	17
2.2 OSI 七层模型功能.....	17
2.3 对等层间的通信.....	19
2.4 数据封装.....	19
2.5 网络互连设备.....	20
2.5.1 网络设备在 OSI 模型中的位置.....	20
2.5.2 中继器 ( Repeater ) .....	21
2.5.3 集线器 ( HUB ) .....	21
2.5.4 网桥 ( Bridge ) .....	22
2.5.5 交换机 ( Switch ) .....	22
2.5.6 路由器 ( router ) .....	23
2.5.7 网关 ( Gateway ) .....	24
第三章 TCP/IP 协议简介.....	25
3.1 TCP/IP 协议层次模型.....	25
3.2 TCP/IP 层次模型协议介绍.....	26
3.3 TCP/IP 应用层协议概述.....	26
3.4 TCP/IP 传输层协议概述.....	27
3.4.1 TCP 协议.....	27
3.4.2 UDP 协议.....	27
3.5 TCP/IP 网络层协议概述.....	28
3.5.1 网际控制报文协议 ( ICMP ) .....	29
3.5.2 地址解析协议 ( ARP ) .....	29
3.5.3 反向地址解析协议 ( RARP ) .....	30
3.6 IP 地址.....	30
3.6.1 IP 地址的分类.....	31
3.6.2 广播地址和组播地址.....	32
3.6.3 子网掩码.....	33
3.6.4 子网规划.....	33

第四章 局域网.....	35
4.1 局域网特点.....	35
4.2 局域网组成.....	35
4.3 决定局域网特性的主要技术.....	36
4.4 局域网体系结构.....	36
4.5 IEEE802 标准.....	37
4.6 典型局域网.....	38
4.6.1 以太网工作原理.....	38
4.6.2 传统的以太网系统.....	38
4.6.3 以太网分段.....	39
4.6.4 以太网电缆使用标准.....	41
4.7 快速以太网.....	42
4.8 千兆以太网.....	42
4.9 万兆以太网.....	42
4.10 以太网标准.....	43
4.11 ATM.....	43
第五章 广域网技术.....	45
5.1 广域网的定义.....	45
5.2 广域网中常用设备.....	45
5.3 广域网的体系结构.....	47
5.4 广域网协议.....	47
5.5 典型广域网.....	47
5.5.1 公用电话交换网 PSTN.....	48
5.5.2 数字数据网 DDN.....	48
5.5.3 分组交换网 X.25.....	49
5.5.4 帧中继 Frame-Relay.....	49
5.5.5 综合业务数字网 ISDN.....	50
5.6 ADSL.....	51
5.7 VDSL.....	52
5.8 HFC 方式.....	52
5.9 VPN 技术.....	53
5.9.1 VPN 概述.....	53
5.9.2 远程访问虚拟网 (AccessVPN).....	53
5.9.3 企业内部虚拟网 (IntranetVPN).....	54
5.9.4 企业扩展虚拟网 (ExtranetVPN).....	55
第六章 路由技术.....	56
6.1 路由器工作原理.....	56
6.1.1 路由器的概念.....	56
6.1.2 路由器作用.....	57
6.1.3 路由器的优缺点.....	57
6.1.4 路由器的工作原理.....	58
6.1.5 路由选择方式.....	58
6.1.6 路由算法.....	59
6.2 路由协议.....	59

6.2.1 RIP 路由协议 .....	59
6.2.2 OSPF 路由协议 .....	60
6.2.3 BGP 协议 .....	60
第七章 网络交换技术 .....	61
7.1 共享式以太网 .....	61
7.2 交换式以太网 .....	62
7.2.1 交换式以太网工作原理 .....	62
7.2.2 交换式以太网的基本结构 .....	63
7.2.3 交换机数据转发方式 .....	63
7.2.4 交换式以太网技术的优点 .....	64
7.2.5 共享式以太网和交换式以太网比较 .....	64
7.2.6 半双工以太网 .....	64
7.2.7 全双工以太网 .....	65
7.2.8 生成树 .....	65
7.3 虚拟局域网 VLAN .....	67
7.3.1 VLAN 的工作原理 .....	67
7.3.2 虚拟局域网的优点 .....	68
7.3.3 VLAN 的分类 .....	69
7.3.4 以端口为中心的 VLAN 的实施 .....	70
7.4 组播 .....	70
7.4.1 组播定义 .....	70
7.4.2 组播技术的原理 .....	72
7.4.3 组管理协议 .....	72
7.4.4 IGMP SNOOPING 协议 (IGMP 监听) .....	72
7.5.1 三层交换机的特点 .....	73
7.5.2 三层交换机的应用 .....	74
7.6 交换机的基本性能参数 .....	74
7.6.1 交换机分类 .....	74
7.6.2 交换机性能参数 .....	75
7.7 联想网络交换机产品线介绍 .....	77
7.7.1 机架式交换机 .....	77
7.7.2 固定配置式交换机 .....	77
第八章 网络管理 .....	78
8.1 网络管理的发展 .....	78
8.2 网络管理功能 .....	78
8.2.1 配置管理 .....	79
8.2.2 性能管理 .....	80
8.2.3 故障管理 .....	80
8.2.4 安全管理 .....	80
8.3 网络管理系统组成 .....	81
8.4 网络管理协议 .....	81
8.4.1 SNMP 协议 .....	81
8.4.2 CMIP 协议 .....	82
8.5 网络管理新技术 .....	82

8.5.1 基于命令行管理技术.....	83
8.5.2 基于 Web 的网络管理技术.....	83
8.5.3 RMON 技术.....	83
8.6 联想 Hyper-manager 网管软件.....	84
8.6.1 Hyper-manger 特点.....	84
8.6.2 Hyper-manger 功能.....	85
8.7 联想 HyperView 网管软件.....	87
8.7.1 Hyperview 系统特点.....	87
8.7.2 Hyperview 系统功能.....	88
8.7.3 HyperManager 与 HyperView 区别.....	89
第九章 网络安全.....	90
9.1 访问控制技术 ACL.....	90
9.2 防火墙.....	91
9.2.1 防火墙功能.....	91
9.2.2 防火墙类型.....	92
9.3 以太网运营.....	92
9.4 认证技术.....	94
9.4.1 PPPoE 认证.....	94
9.4.2 VLAN+Web 认证.....	95
9.4.3 802.1X 认证.....	96
9.5 计费系统概述.....	97
9.5.1 为什么进行计费管理.....	97
9.5.2 联想 Hyper-boss 的特色.....	97
9.5.3 Hyper-boss 的功能.....	98
9.5.4 业务管理.....	100
第十章 企业网络解决方案.....	101
10.1 网络的设计思想.....	101
10.2 网络层次结构.....	101
10.2.1 核心层的功能及设计.....	101
10.2.2 汇聚层的功能及设计.....	102
10.2.3 接入层的功能及设计.....	102
10.3 方案设计.....	103
10.4 联想网络解决方案.....	103
10.4.1 校园网典型方案.....	103
10.4.2 企业网方案.....	104
10.4.3 政务网方案.....	105
10.5 成功案例.....	106
10.5.1 重庆网通信息港解决方案.....	106
10.5.2 贵港政务网方案.....	107
10.5.3 闵行区中小学网络系统.....	108
10.5.4 珠海校校通工程.....	109
10.5.5 武汉市武昌区教育城域网.....	110
10.5.6 上海交大 985 工程.....	111
10.5.7 山东电信城域网.....	112

---

10.5.8 南京广电城域网.....	113
第 11 章 专业名词.....	114
11.1 通信名词.....	114
11.2 IEEE802 标准 .....	116
10.3 交换机涉及参数.....	117

## 第一章 网络基础知识

### 1.1 网络的发展

网络作为一种大众媒体，在现代的信息社会中起着举足轻重的作用。计算机网络主要经历了集中、分化、网络化三个过程。

六十至七十年代，网络的概念主要基于主机构架的低速串行连接，提供应用程序执行，远程打印和数据服务功能（如下图 1-1 所示）。

七十至八十年代，出现了以个人电脑模式为主的商业计算模式。最初，个人电脑是独立的设备，由于认识到商业计算的复杂性，局域网产生了，局域网的出现，大大降低了商业用户打印机和磁盘昂贵的费用（如下图 1-1 所示）。

八十至九十年代，远程计算的需求不断增加，迫使计算机界开发出许多广域网协议，满足不同计算方式远程连接的需求，网与网之间的互连极大的连接起来（如下图 1-1 所示）。

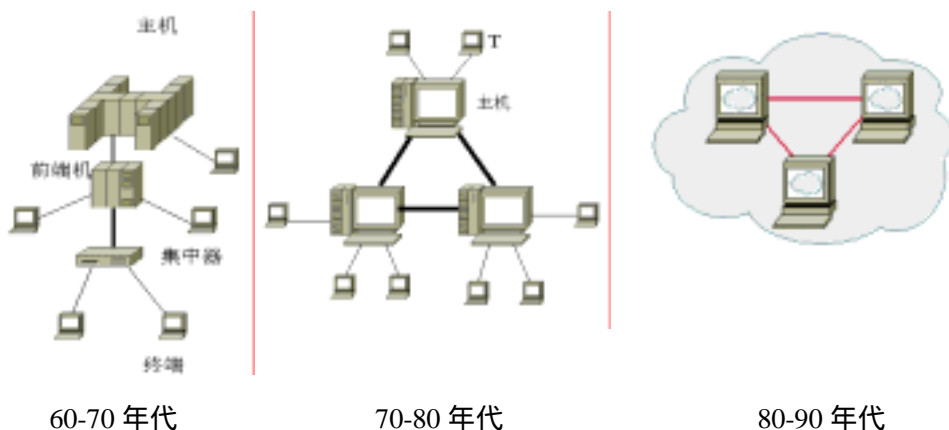


图 1-1 网络的发展

### 1.2 计算机网络的定义

计算机网络是指在网络协议控制下，利用某种传输介质和通信手段，把地理上分散的计算机、通信设备及终端等相互联接在一起，达到相互通信和资源共享（如硬盘、打印机等）的计算机系统。

计算机网络由以下几部分组成：

- 1) 通信设备：传输介质及网络互连设备。
- 2) 用户端设备：主机、服务器、工作站等。

3) 操作系统：网络操作系统。

4) 协议：网络协议软件。

## 1.3 计算机网络的分类

计算机网络的类型，可根据不同的划分标准来分类：

1. 按网络的地理区域分：LAN（局域网），WAN（广域网），MAN（城域网），Internet。

（1）局域网：局域计算机网（LAN, Local Area Network）通常简称为局域网，联网的计算机分布在一个较小的地域范围内（约 10m 至十几公里）内，它能进行高速的数据通信。

局域网在企业办公自动化、企业管理、工业自动化、计算机辅助教学等方面得到广泛的使用。

（2）城域网：联网的计算机之间最远通信距离约几十公里内的网络称为城域网，例如在一个城市范围内建立起来的计算机网络。

（3）广域网：广域计算机网（WAN, Wide Area Network）简称广域网。广域网在地理上可以跨越很大的距离，连网的计算机之间的距离一般在几十公里以上，跨省、跨国甚至跨洲，网络之间也可通过特定方式进行互联，实现了局域资源共享与广域资源共享相结合，形成了地域广大的远程处理和局域处理相结合的网际网系统。世界上第一个广域网是 ARPANET 网，它利用电话交换网互联分布在美国各地的不同型号的计算机和网络。

（4）Internet：Internet 可以传输上千公里，它是全世界各种网络互连得到的网间网。

2. 按照使用范围：公用网、专用网。

（1）公用网：如 CHINANET 等。

（2）专用网：如 CRPAC（铁路分组数据网）。

3. 按信息交换方式分：电路交换、报文交换、分组交换、混合交换、信元交换。

（1）电路交换网：如电话网；

（2）报文交换网：如电报网；

（3）分组交换网：如 X.25 网；

（4）混合交换网（同时采用电路和分组交换）：如帧中继网；

（5）信元交换网：如 ATM 网。

4. 按传输技术分：广播型网络，点到点网络。

（1）广播型网络：如传统以太网（广播、组播）；

（2）点到点网络：如分组交换网。

5. 按拓扑结构分：总线型、星型、环型、网状。

## 1.4 网络的拓扑结构

网络中各站点相互连接的方法和形式称为网络拓扑。拓扑图给出网络服务器、工作站的网络配置和相互间的连接，它的结构主要有星型结构、环型结构、总线结构、网状结构等。

### (1) 星型结构

星型结构为目前使用最普遍的以太网结构,这种结构便于集中控制,因为终端用户之间的通信必须经过中心站,如图 1-2 所示。由于这一特点,也带来了易于维护和安全等优点。端用户设备因为故障而停机时也不会影响其它端用户间的通信,但缺点也是明显的:中心系统必须具有极高的可靠性,因为中心系统一旦损坏,整个系统便趋于瘫痪。对此中心系统通常采用双机热备份,以提高系统的可靠性。

典型应用:以太网交换机、集线器(HUB)、ATM 交换机等,如图 1-3 所示。

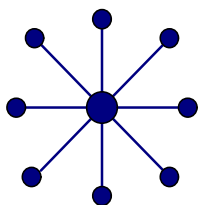


图 1-2 星型拓扑结构

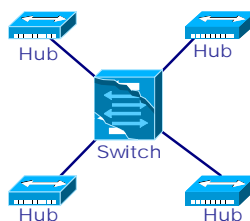


图 1-3 星型拓扑结构的应用

### (2) 总线结构

总线结构是指各工作站和服务均挂在一条总线上,各工作站地位平等,无中心节点控制,其传递方向总是从发送信息的节点开始向两端扩散,如同广播电台发射的信息一样,因此又称广播式计算机网络。如图 1-4 所示。

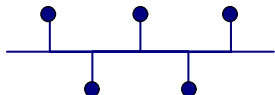


图 1-4 总线拓扑结构

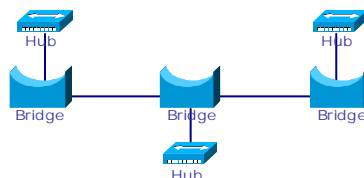


图 1-5 总线拓扑结构的应用

优点:费用低,易扩展,线路利用率高;

缺点:可靠性较低,管理维护困难,传输效率低。

典型应用:早期的局域网,采用网桥和集线器搭建。(如图 1-5 所示)



### (3) 环型结构

环型结构由网络中若干节点通过点到点的链路首尾相连形成一个闭合的环,这种结构使公共传输电缆组成环型连接,数据在环路中沿着一个方向在各个节点间传输,信息从一个节点传到另一个节点。如图 1-6 所示。

环型结构具有如下特点:信息流在网中是沿着固定方向流动的,两个节点仅有一条道路,故简化了路径选择的控制;由于信息源在环路中是串行地穿过各个节点,当环中节点过多时,势必影响信息传输速率,使网络的响应时间延长;环路是封闭的,不便于扩充;可靠性低,一个节点故障,将会造成全网瘫痪;维护难,对分支节点故障定位较难。

典型应用: FDDI 网。如图 1-7 所示。

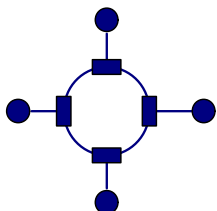


图 1-6 环型拓扑结构

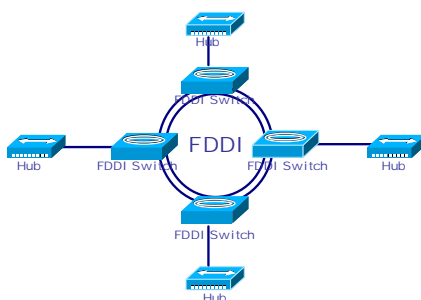


图 1-7 环型拓扑结构的应用

### (4) 网状结构

在网状拓扑结构中,网络的每台设备之间均有点到点的链路连接,如图 1-8。

优点:可靠性高,易扩充,组网方式灵活;

缺点:费用高,结构复杂,管理维护困难。

典型应用:一般用于广域网组网,如 CHINANET 等,如图 1-9。

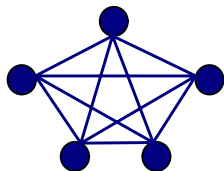


图 1-8 网状拓扑结构

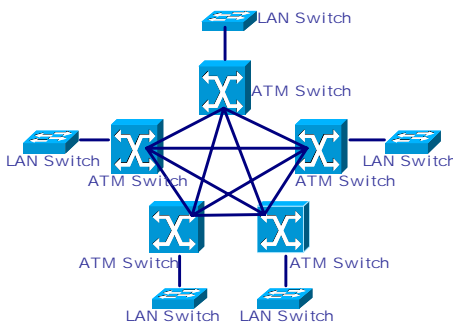


图 1-9 网状拓扑结构应用

## 1.5 网络的传输介质

在计算机网络中，传输所用的媒体介质也是多种多样的。有双绞线、同轴电缆、光纤等有线传输媒体，还有无线传输媒体等，如无线电、微波、激光和卫星等。

### (1) 双绞线

双绞线是最常用的一种传输介质。双绞线是两根相互绝缘的铜导线缠绕在一起所组成的传输媒体，如图 1-10 所示。这两根导线缠绕成螺旋状，以减少邻近线对引起的电磁干扰。

双绞线可分为非屏蔽双绞线(UTP: Unshielded Twisted Pair)和屏蔽双绞线(STP: Shielded Twisted Pair)。在计算机网络中用得更多的是 3 类和 5 类无屏蔽双绞线(Unshielded Twisted Pairs 简称 UTP)，分别称为 UTP-3 和 UTP-5。在以太网局域网中，UTP-3 和 UTP-5 分别作为 10BASE-T 和 100BASE-T 标准的通信线，通信距离为 100m。



图 1-10 双绞线

### (2) 同轴电缆

同轴电缆可分为两种基本类型：基带同轴电缆和宽带同轴电缆。目前常用的基带同轴电缆，其屏蔽线是用铜做成的网状的，特征阻抗为 50 (如 RG-8、RG-58 等)；宽带同轴电缆常用的电缆的屏蔽层通常是用铝冲压成的，特征阻抗为 75 (如 RG-59 等)。如图 1-11 所示。

粗同轴电缆与细同轴电缆是指同轴电缆的直径大还是小。粗缆适用于比较大型的局部网络，它的标准距离长、可靠性高。由于安装时不需要切断电缆，因此可以根据需要灵活调整计算机的入网位置。但粗缆网络必须安装收发器和收发器电缆，安装难度大，所以总体造价高。相反，细缆安装则比较简单，造价低，但由于安装过程要切断电缆，两头须装上基本网络连接头(BNC)，然后接在 T 型连接器两端，所以当接头多时容易产生接触不良的隐患，这是目前运行中的以太网所发生的最常见故障之一。在目前计算机局域网中同轴电缆已不再那么普遍地被使用了，逐渐被双绞线和光纤所取代。

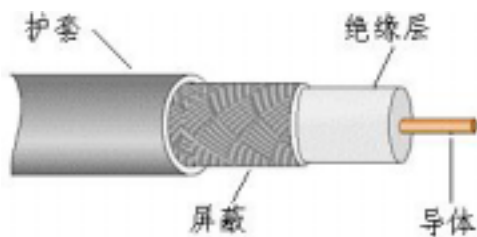


图 1-11 同轴电缆

### (3) 光纤

光纤又叫光缆（光导纤维的简称），它由纤芯、包层和保护层组成，如图 1-12 所示。由于光纤具有损耗低、频带宽、数据传输率高、抗电磁干扰力强等特点，多用于高速的网络主干铺设。

光纤可分单模光纤(Single Mode Fiber)和多模光纤(Multi Mode Fiber)。单模光纤的纤芯直径很小，在给定的工作波长上只能以单一模式传输，传输频带宽，传输容量大。多模光纤是在给定的工作波长上，能以多个模式同时传输的光纤。与单模光纤相比，多模光纤的传输性能较差。

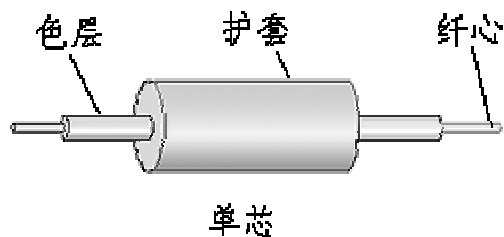


图 1-12 光纤

下面给出三种传输介质的性能比较：

表 1.1 同轴电缆、双绞线、光缆的性能比较

传输媒介	价格	电磁干扰	频带宽度	单段最大长度
UTP	最便宜	高	低	100 米
STP	一般	低	中 等	100 米
同轴电缆	一般	低	高	185 米/500 米
光 缆	最高	没 有	极 高	几十公里

### (4) 无线传输

有线传输的通信线路在经过高山、海洋或岛屿时，施工很难进行，在城市铺设通信电缆也不是一件容易的事情，在远距离通信时铺设的电缆成本昂贵。这样无线传输的出现也就成为现实了。其实，无线传输是一种可以利用无线电波在空中实现传播的通信方式，它包括无

线通信和移动通信等方面。

无线电波广泛应用在各种通信领域中，如收音机收听节目、接收机收到电报信息等。寻呼系统、无绳电话、模拟移动电话、数字移动电话等还在广泛使用中。

## 1.6 网络操作系统

网络操作系统（NOS, Network Operation System）是指能使网络上的计算机方便而有效地共享网络资源，为用户提供所需的各种服务的操作系统软件。网络操作系统除了具备单机操作系统所需的功能外，如内存管理、CPU 管理、输入输出管理、文件管理等，还应提供高效可靠的网络通信能力和多种网络服务功能，如远程管理、文件传输、电子邮件、远程打印等。

当前网络操作系统按其功能可以分为以下三种常见结构：专用服务器结构网络、主从式结构网络、对等式网络。

### 1. 专用服务器结构：(Server—Base)

又称为“工作站 / 文件服务器”结构，由若干台微机工作站与一台或多台文件服务器通过通信线路连接起来组成工作站存取服务器文件，共享存储设备。

文件服务器自然以共享磁盘文件为主要目的。对于一般的数据传递来说已经够用了，但是当数据库系统和其它复杂而被不断增加的用户使用的应用系统到来的时候，服务器已经不能承担这样的任务了，因为随着用户的增多，为每个用户服务的程序也增多，每个程序都是独立运行的大文件，给用户感觉极慢，因此产生了客户机 / 服务器模式。

### 2. 客户机/服务器模式：(client / server)

基于服务器的网络，管理集中在运行网络操作系统（NOS）服务器软件的计算机上。NOS 服务器可以认证用户名和密码信息，确保通过认证的用户能登录并访问资源，同时 NOS 服务器一般为客户机提供应用服务，如多媒体教学系统、ERP、CRM 等。C / S 结构是数据库技术的发展和普遍应用与局域网技术发展相结合的结果。

### 3. 对等式网络：(Peer—to—Peer)

在拓扑结构上与专用 Server 与 C / S 相同。在对等网中，每台计算机既作为客户机又可作为服务器来工作，每个用户都管理自己机器上的资源。

## 1.7 计算机网络通信的基本模式

在通信系统中，传输的信号既可以是模拟信号，也可以是数字信号。模拟信号是指信号的幅度随着时间而连续变化的信号，例如电话线上传递的话音就是一种模拟信号。而数字信号则是指信号在每一时段时间内的幅值只能是离散的有限值，例如计算机系统内传递的数据等。

下面让我们了解一下网络通信的两种基本模式：

### 1、模拟传输方式

传统的电话通信系统是典型的模拟信号传输系统。在电话通信系统中，数以亿计的电话机互相连成网络，通过分级交换技术组成层次结构的通信网络。而这种采用了模拟传输技术的电话网，其使用已持续了近一个世纪，在世界各地几乎都普遍使用。

### 2、数字传输方式

数字传输只传输两个值 0 和 1。数字传输能够把数据、话音、图像或视频等信号复合到同一通信线路上传输，并能通过已有的通信线路获得更高难的数据传输速率，在数字传输过程中信号产生的误码率很低。

尽管模拟传输落后于数字传输，但采用模拟传输技术的电话通信网络仍然在全世界广泛使用。

## 1.8 计算机网络通信协议

### 1.8.1 标准化组织

ISO 是国际标准化组织 ( the International Organization for Standardization)的缩写，该组织成立于 1947 年，总部在瑞士的日内瓦。它是致力于国际标准的、自愿和非赢利的专门机构。

IEEE 是电器和电子工程师协会( IEEE ,The Institute of Electrical and Electronic Engineer )的缩写，是世界上最大的技术专业协会和非盈利性组织。

## 1.8.2 通信协议

设计和开发计算机网络必须遵循相同的网络体系结构,这样才能保证在网络的有效连接和通信。所谓网络体系结构,指的是计算机网络的各层及其协议的集合。目前网络体系结构都采用了分层的技术,既然网络体系结构是分层的,各层之间要有相应的通信协议。那么,通信协议指的是什么?

为了在网络中正确进行数据传输而建立的规则(标准,约定)称为协议。如图 1-13 所示,发送方计算机 A 在发送信息之前,首先要探询对方,然后询问“现在要传送了,准备好了吗?计算机 B 回答“准备好了”,经过上述步骤之后,才能进行信息通讯。在互相通信的两者之间有一种约定,这就是协议。



图 1-13 通信协议举例

目前普遍使用的是 OSI 参考模型、TCP/IP 网络协议、ATM 网络协议和 IEEE 标准。

### (1) OSI 模型

开放系统模型 (OSI, Open System Model) 是一种全新的网络体系结构,是 80 年代初期由 ISO 制定的,作为开放系统互联的国际标准。它能把基于不同网络体系结构的系统互联起来,从而实现不同机种的计算机以及不同的网络系统之间的数据通信。

OSI/RM 模型共有 7 层(如下图 1-14 所示),每层都可以实现一个特定的功能。其具体功能将在第二章介绍。

7	应用层 (Appl icati on)
6	表示层 (Presentati on)
5	会话层 (Sessi on)
4	传输层 (Transport )
3	网络层 (Network)
2	数据链路层 (Data Link)
1	物理层 (Physi cal )

图 1-14 OSI 参考模型的结构

## (2) TCP/IP 协议

TCP/IP 是提供可靠数据传输和无连接数据报服务的一组协议。传输控制协议 TCP(Trans-mission Control Protocol)提供可靠数据传输的协议，网际互联协议 IP(Internet Proto-col)则是提供无连接数据报服务的协议。

TCP/IP 是一种层级式 (Layering) 的结构 (见图 1-15)，可分为 4 层：网络层、网际层、运输层、应用层。每层具体功能将在第三章介绍。

4	应用层 (Application Layer)
3	运输层 (Transport Layer)
2	网际层 (Internet Layer)
1	网络接口 (Network Access Layer)

图 1-15 TCP/IP 协议的分层结构

## (3) ATM 协议

ATM (Asynchronous Transfer Mode) 协议是 80 年代中期 IUT-T (国际电信联盟标准化组织) 为宽带综合业务数字网 (B-ISDN) 制定的“异步传输模式”。它的主要特点是快速分组交换和时分统计复用。ATM 能把实时的语音、图像和非实时的文本、数据等业务综合在一起，并在同一网络上传输。如下图示 1-16。

高层	高层
AAL 层	
ATM 层	
物理层	

图 1-16 ATM 的简化参考模型

## (4) IEEE 标准

IEEE802 标准已被 ANSI 和 ISO 作为国际标准，称之为 ISO802。IEEE802 局域网的参考模型如下图 1-17 所示：

逻辑链路控制子层 (LLC) 的主要功能是保证帧传送的准确和无误等。

介质访问控制子层 (MAC) 负责进行帧的组装和拆卸、帧的发送和接收。

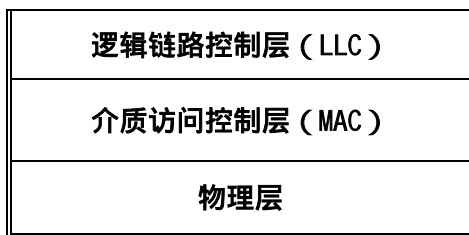


图 1-17 IEEE802 参考模型

## 1.9 网络互连设备

用于网络范围的拓展，实现：

- 局域网之间的互连
- 局域网与广域网之间的互连
- 广域网与广域网之间的互连

网络中主要用到的设备分别为：

- 集线器 (HUB)：工作在物理层，是一种特殊的中继器，随着网络交换技术的发展，集线器正逐步被交换机取代。
- 中继器 (Repeat)，工作在物理层，接收信号进行再生和发送，从而增强信号传输的距离。将多个物理网段连成一个 LAN。
- 网桥 (Bridge)：工作在数据链路层，在 LAN 之间存储和转发帧 (Frame)。
- 交换机 (Switch)：在数据链路层实现互联，在 LAN 之间存储和转发帧 (Frame)。
- 路由器 (Router)：在网络层实现互联，在不同的网络之间存储和转发数据包。
- 网关 (Gateway)：在传输层及以上的层次实现互联，实现不同协议的转换。



## 第二章 OSI 参考模型

### 2.1 层次化网络体系结构

在七十年代末，国际标准化组织 ISO 提出了开放系统互连参考模型，如图 2-1 所示。该模型描述了通过网络传输介质（例如电缆）信息或数据是如何从一台计算机的一个应用程序（例如电子制表软件）到达网络中的另一台计算机的一个应用程序。当信息在一个 OSI 参考模型中逐层传送的时候，它越来越不像人类的语言而变为只有计算机才能明白的数字 0 和 1。

协议分层大大的简化了网络协议的复杂性，网络协议按功能组成一系列层，每一层建筑在它的下层之上，每一层的目的是为上层提供一定的服务，屏蔽低层的细节。如图 2-1 所示。

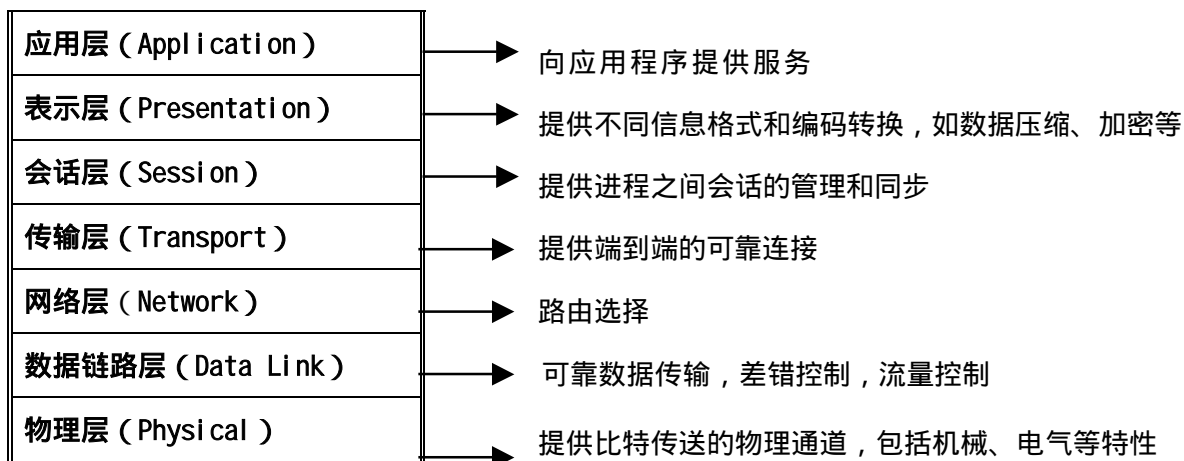


图 2-1 OSI 七层模型及其功能

### 2.2 OSI 七层模型功能

#### (1) 物理层 (physical layer)

物理层作用：

- 承担设备之间的比特流的正确传输。
- 对电压、线路速度、线缆类型进行定义。

物理层设备：集线器、中继器。

#### (2) 数据链路层 (data link layer)

数据链路层作用：

- 将物理层比特流数据封装成数据。（封装的概念请看 2.4 节）
- 采用 MAC 地址对介质访问层进行控制。
- 发现错误，改正错误或通知上层进行更改。

数据链路层设备：交换机和网桥。

### （3）网络层（network layer）

检查网络拓扑，以决定传输报文的最佳路由，其关键问题是确定数据包从源端到目的端如何选择路由。如下图所示，将信息从工作站 A 发送到工作站 B，有多条通路，但我们要选择一条最短的通道来传送消息。

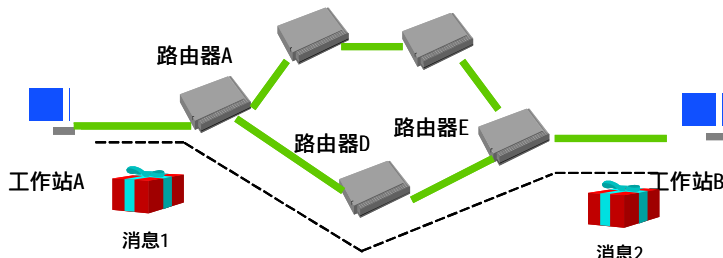


图 2-2 路由选择

网络层设备：路由器和三层交换机。

### （4）传输层（transport layer）

传输层也称为运输层。从会话层接受数据，并且在必要的时候把它分成较小的单元，传输给网络层，并确保到达对方各段的信息准确无误。

### （5）会话层（session layer）

会话层的主要的功能是对话管理，数据流同步和重新同步。图 2-3 显示了两台主机之间对话同步过程。

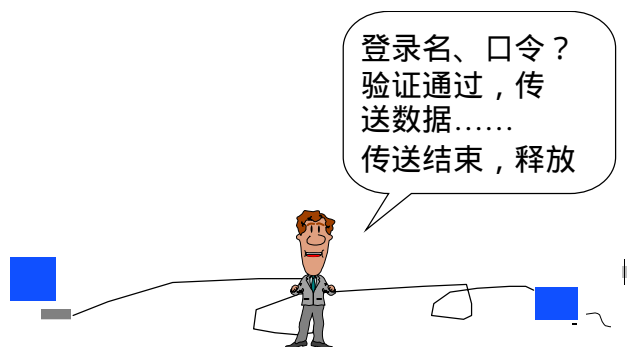


图 2-3 会话管理

### （6）表示层（presentation layer）

将数据转换成计算机应用程序相互理解的格式，如数据压缩、加密、表示等。

### (7) 应用层 (application layer)

应用层包含大量人们普遍需要的协议，并且具有文件传输功能，其任务是显示接收到的信息，把用户的新数据发送到低层。如发送电子邮件、网络管理都是在应用层进行。

## 2.3 对等层间的通信

在 OSI 分层模型中，对等是一个非常重要的概念，因为只有对等层才能相互通信，一方在某层的协议是什么，对方在同一层上也必须是同一协议。如下图 2-4 所示。数据传递都是由上层传到下层，接收由下层到上层，层间是虚通信，最下层为实际通信。



图 2-4 对等层间通讯

## 2.4 数据封装

在网络中发送的信息叫做数据或数据包。如果一台计算机（源主机）要发送数据到另一台计算机（目的主机），数据首先必须打包，该过程叫封装；数据在网络中传输前必须在数据头部加入特定的协议头。数据封装过程如图 2-5 所示。

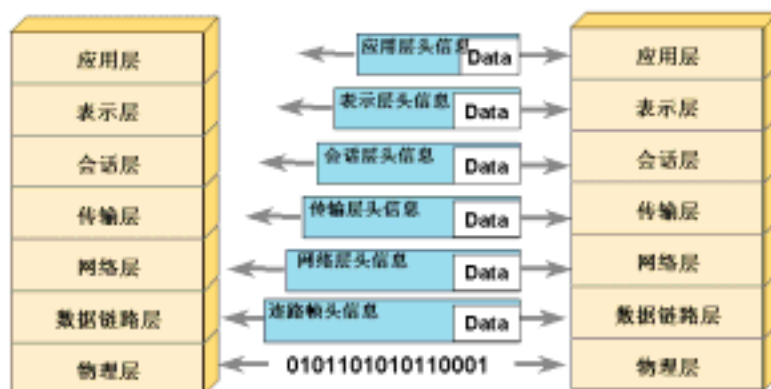


图 2-5 数据封装示意图

具体过程为如下 5 个过程：

- 生成数据：当用户发送信息时，信息中的字符和数字转化成能在互联网中传播的数据。如用户发送电子邮件。
- 打包生成端到端传输的数据：为了在互连网中传输数据，必须给数据打包。由于使用分段，传输层保证在 E-mail 端的主机能可靠的传输数据。
- 在头部加入网络地址：数据打包成数据报，数据报头部含有网络的源地址和目的地址。这些地址帮助网络设备和数据包按选定的路径传输数据。
- 把物理地址加入到数据链路层的数据头部：每一个网络设备必须把数据报打包成数据帧。
- 把信息转换成为比特：为了在物理介质上传输，帧必须转换成 0，1 格式。

例如：E-mail 信息从某个局域网发出，穿过校园骨干网，通过广域网络最后到达目的地或另一个远端局域网。如图 2-6 所示。

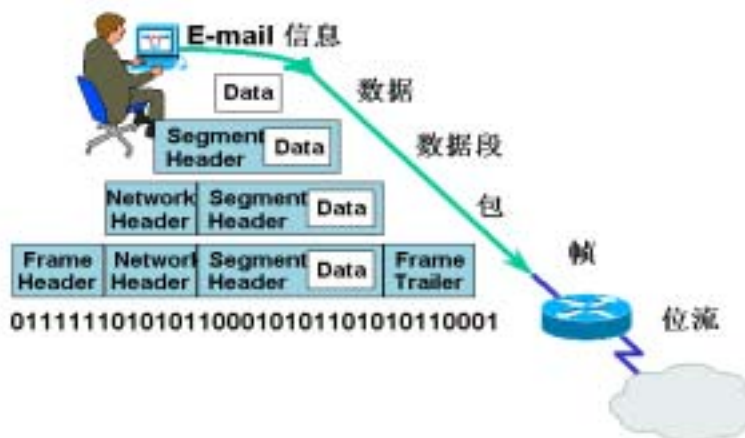


图 2-6 数据封装举例

## 2.5 网络互连设备

### 2.5.1 网络设备在 OSI 模型中的位置

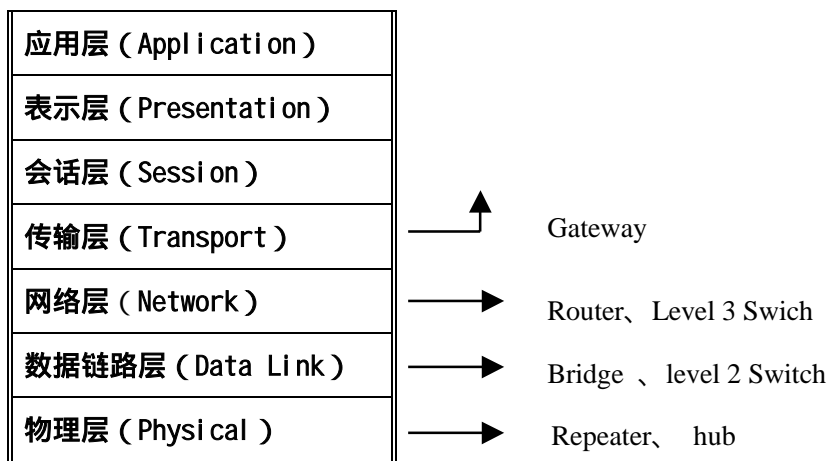


图 2-7 网络设备在层次模型中的位置

## 2.5.2 中继器 (Repeater)

中继器工作在物理层,它可以“延长”网络的距离,在网络数据传输中起到放大信号的作用。如图 2-8 所示。中继器连接的两个网络在逻辑上是同一个网络。

中继器的主要优点是安装简单、使用方便、价格相对低廉。它不仅起到扩展网络距离的作用,还可将不同传输介质的网络连接在一起。

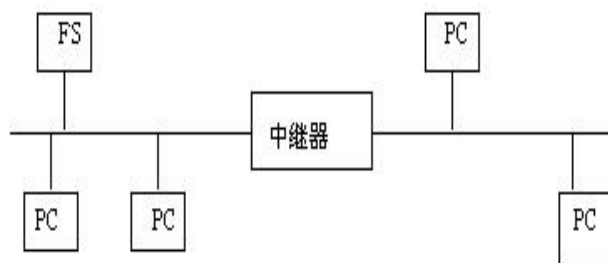


图 2-8 中继器使用方式

## 2.5.3 集线器 (HUB)

集线器,主要指共享式集线器。相当于一个多口的中继器,一条共享的总线,能实现简单的加密和地址保护。如图 2-9 所示,它工作在物理层。主要考虑带宽速度、接口数、智能化(可网管)、扩展性(可级联和堆叠)。

其特点如下:

- 所有的数据转发工作在同一碰撞域(因为都共享一条总线)内进行。如图 2-10 所示。

- 所有连接的设备处于同一广播域里。(广播就是所有设备都能接收到同一信息)
- 所有链路共享同一带宽。

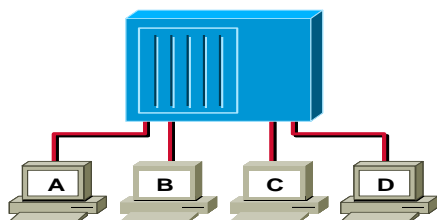


图 2-9 集线器

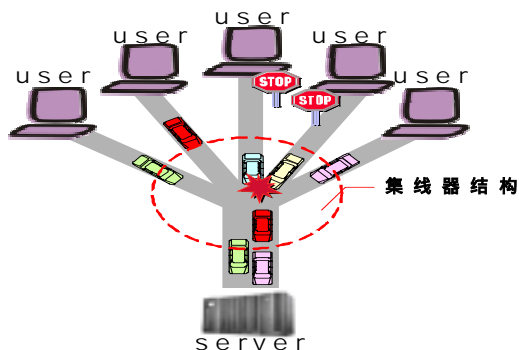


图 2-10 集线器使用方式

## 2.5.4 网桥（Bridge）

网桥工作在数据链路层，将两个 LAN 连起来，在 LAN 之间存储和转发帧（Frame），如下图所示。

其特点如下：

- 每一条链路都属于一个单独的碰撞域。如图 2-12 所示。
- 所有的连接的设备属于同一广播域。

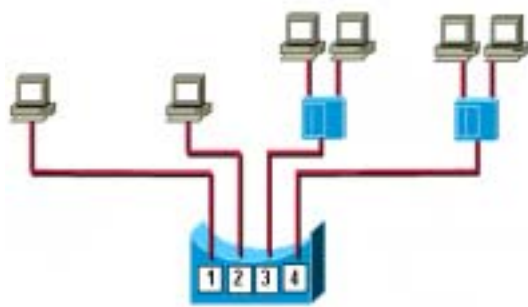


图 2-11 网桥

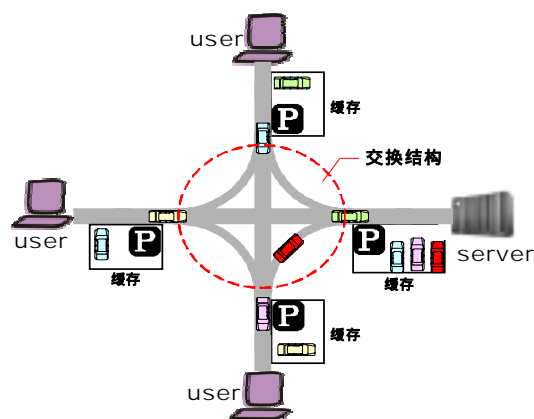


图 2-12 网桥使用方式

## 2.5.5 交换机（Switch）

交换机（Switch）工作在数据链路层，交换机技术现在在不断更新发展，功能不断加强，可以实现网络分段，虚拟子网（VLAN）划分。

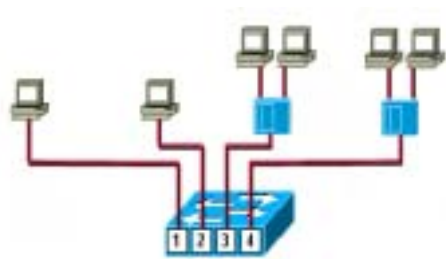


图 2-13 交换机

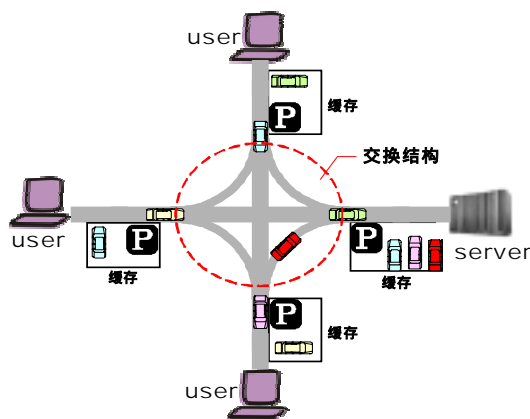


图 2-14 交换机使用方式

其特点如下：

- 每一条链路都属于一个单独的碰撞域。
- 所有的连接的设备属于同一广播域。

那么网桥与交换机到底有何区别呢？

网桥

- 基于软件进行转发控制；
- 一个网桥只能存在一个 STP 域；( STP 称为生成树协议，它主要用于解决环路问题，在第七章将会讲到 )
- 通常的端口数量少于 16 个。

交换机

- 基于硬件（ASIC）的转发方式；
- 一个交换机可以同时存在多个 STP 域；
- 目前交换机可以支持成百上千个的端口。

## 2.5.6 路由器（router）

路由器，工作在网络层。用于连接多个逻辑上分开的网络，几个使用不同协议和体系结构的网络。当一个子网传输到另外一个子网时，可以用路由器完成。它具有判断网络地址和选择路径的功能，过滤和分隔网络信息流。它不仅具有传输能力，而且有路径选择能力。当某一链路不通时，路由器会选择一条好的链路完成通信。另外，路由器有选择最短路径的能力。

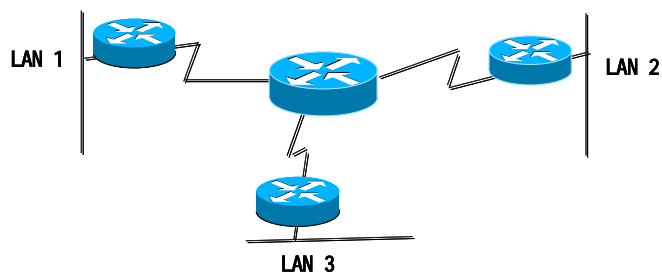


图 2-15 路由器

## 2.5.7 网关 (Gateway)

网关 (Gateway): 又称网间连接器、协议转换器。在传输层及以上的层次实现互联, 实现不同协议的转换。网关既可以用于广域网互连, 也可以用于局域网互连。当连接两个完全不同结构的网络时, 必须使用网关。

- 网关为网络间提供协议转换。
- 网关工作可以工作在 OSI 的任意一层或同时工作几层。一般工作在高层, 如应用层。



## 第三章 TCP/IP 协议简介

### 3.1 TCP/IP 协议层次模型

世界上流行的 TCP/IP 协议的层次并不是按 OSI 参考模型来划分，只跟它有一种大致的对应关系。

使用 TCP/IP 协议的网络可分为 4 层：网络接口、网际层、运输层、应用层,如下图 3-1 所示。

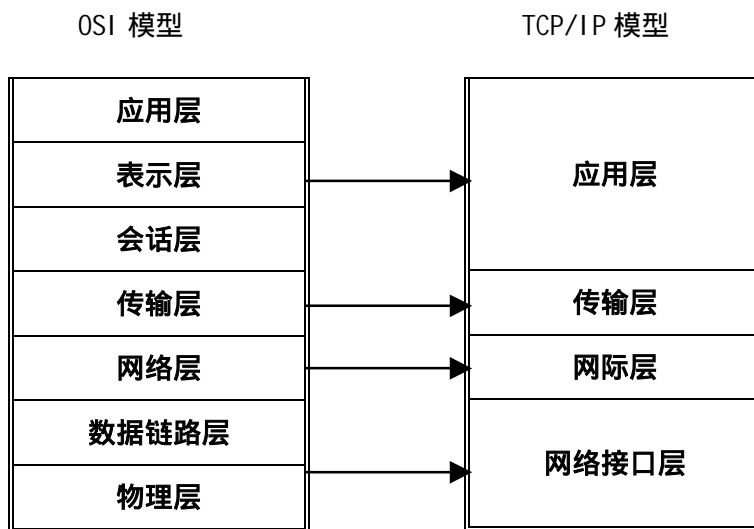


图 3-1 TCP/IP 层次模型与 OSI 模型对照

- (1) 网络接口层。它的作用是传输经过网际层处理过的消息，将 IP 报文封装成网络传输帧，并将 IP 地址映射为网络使用的物理地址。
- (2) 网际层。其使用的协议是 IP 协议，它把运输层送来的消息组装成 IP 数据包，并把 IP 数据包传递给网络接口层。
- (3) 运输层。主要为两台主机上的应用程序提供端到端的通信。运输层主要有 3 个协议：TCP（传输控制协议）、UDP（用户数据报协议）和 ICMP（互联网控制消息协议）。
  - TCP 为两台主机提供可靠的数据传输服务；
  - UDP 只是把称作数据报的分组从一台主机发送到另一台主机，但并不保证该数据报能到达另一端协议提供可靠的数据报传输服务；
- (4) 应用层。为用户提高所需要的各种服务。它提供的主要服务有电子邮件、远程登录、文件传输等方面。

## 3.2 TCP/IP 层次模型协议介绍

网际层主要协议包括 IP 协议、地址解析协议 ARP、反地址解析协议 RARP、网际控制报文协议 ICMP。

传输层定义端到端的协议，它包括传输控制协议 TCP、用户数据报协议 UDP。TCP/IP 不涉及会话层和表示层。

应用层包括所有的高层协议，如虚拟终端协议 Telnet、文件传输协议 FTP，电子邮件协议 SMTP。图 3-2 为每一层上相关协议。

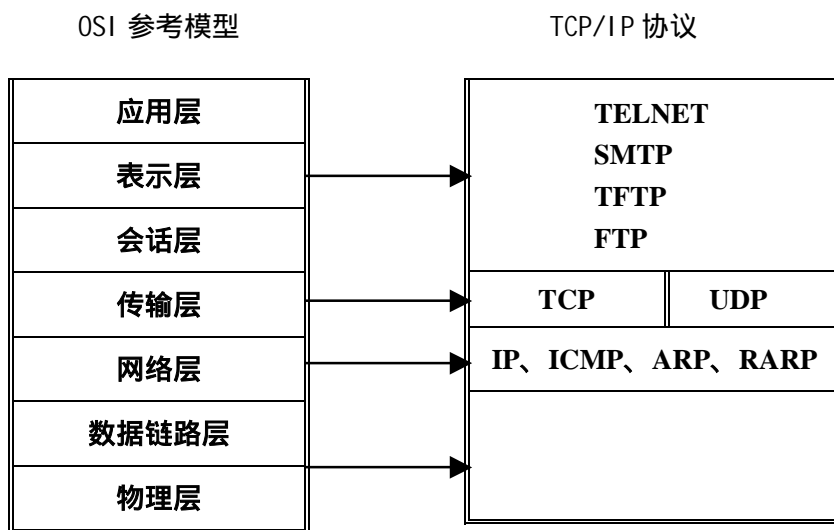


图 3-2 TCP/IP 协议

## 3.3 TCP/IP 应用层协议概述

应用层协议在文件传输、电子邮件和远程登录中发挥着作用。在应用层，网络管理也同样得到了支持，如图 3-3。

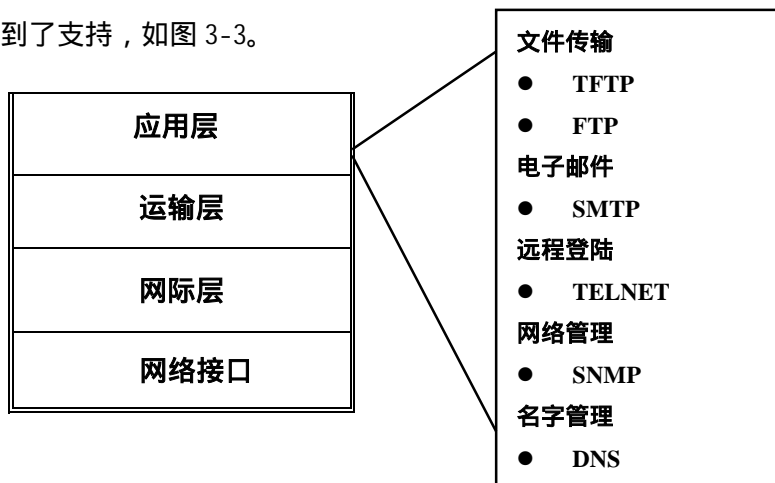


图 3-3 TCP/IP 应用层协议

### 3.4 TCP/IP 传输层协议概述

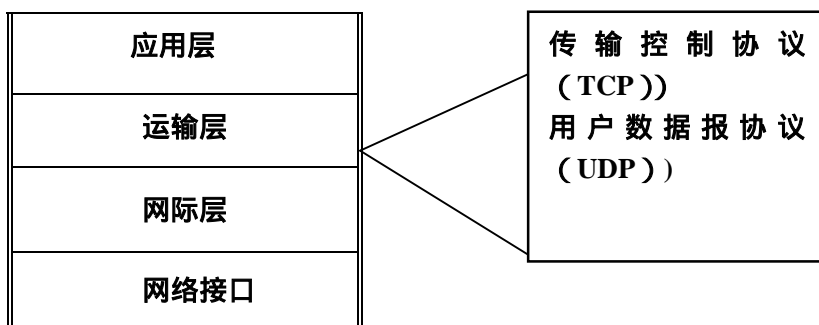


图 3-4 TCP/IP 传输层协议

#### 3.4.1 TCP 协议

TCP 是面向连接的、可靠的协议。它利用端对端错误检测与纠正功能为两台主机提供可靠的数据传输服务。图 3-5 显示了 TCP 传输的过程，这就如同我们打电话，可以进行端到端的通话，那么信息也得到可靠传输。

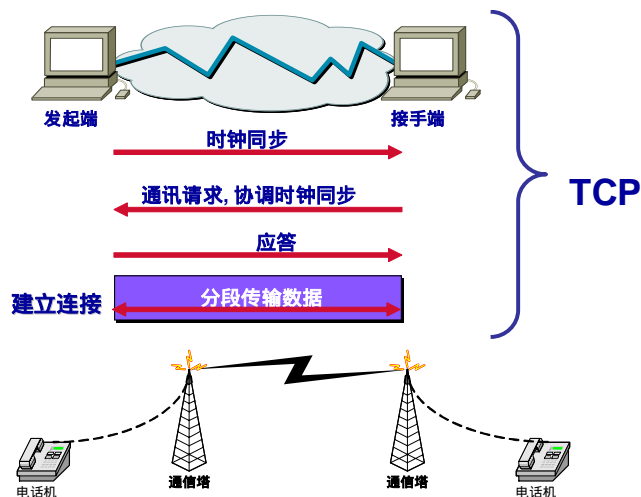


图 3-5 TCP 协议

#### 3.4.2 UDP 协议

UDP 是无连接的，而且“不可靠”。它只是把数据段从一台主机发送到另一台主机，但并不保证该数据段能到达另一端协议提供无连接数据报传输服务。图 3-6 显示了 UDP 的传输

过程，这个过程类似我们平常发信，邮局并不能保证信一定能够到达对方，它是一种不可靠传输。

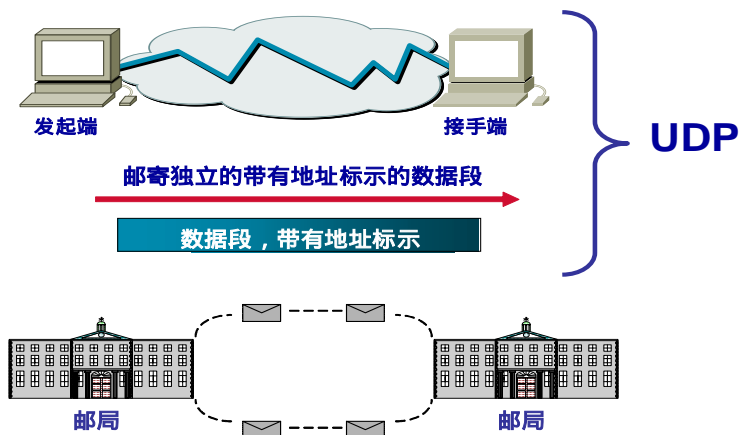


图 3-6 UDP 协议

### 3.5 TCP/IP 网络层协议概述

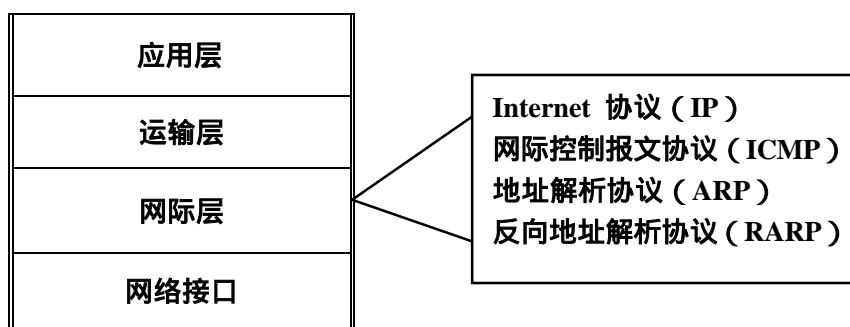


图 3-7 TCP/IP 网络层

IP 协议对数据报进行无连接的最优传送路由选择。它不关心数据报的具体内容，而只是寻找一条能把数据报送到目的端的路径；

ICMP (Internet Control Message Protocol) 则提供了发送差错和控制消息的功能；

ARP (Address Resolution Protocol) 为已知的 IP 地址确定数据链路层的地址 (即 MAC 地址)；

在数据链路层地址已知时，RARP (Reverse Address Resolution Protocol) 确定网络地址 (即 IP 地址)。

### 3.5.1 网际控制报文协议 (ICMP)

ICMP 消息被装载在 IP 数据报里,用来发送差错和控制消息。如果路由器收到一个无法传送到最终目的地的数据包,那么路由器会发送一个“ICMP 主机无法到达”消息给源端(如图 3-8 所示)。如果收到了回声答复,它说明 ping 命令成功了(如图 3-9 所示)。

目的不可达包括主机或端口不可达或网络不可达。

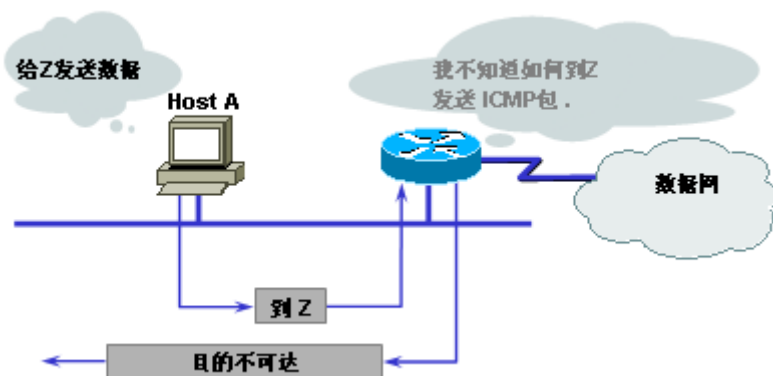


图 3-8 ICMP 测试

ICMP 包含几种不同的信息,其中回声询问由 Ping 命令产生,主机可用它来测试网络的可达性,回声答复表示该节点是可达的。如下图所示。

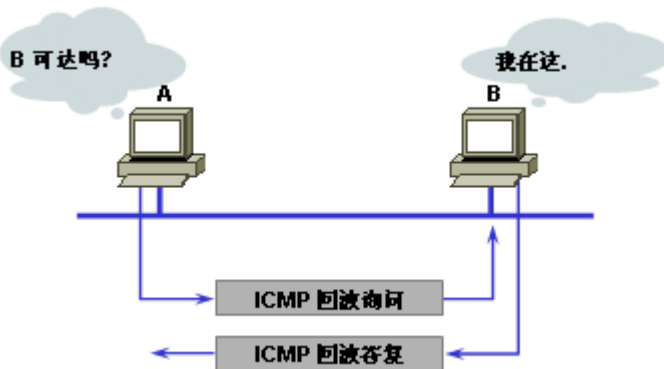


图 3-9 ICMP 检测

### 3.5.2 地址解析协议 (ARP)

地址解析协议 ARP 用来将一个已知的 IP 地址解析或者映射到 MAC 子层地址,以便能在多路访问介质上进行通信,在图 3-10 中,IP 地址为 172.16.3.1 的主机 A 想要寻找 IP 地址为 172.16.3.2 的主机 B,于是它向所有计算机发送广播寻找该 IP 地址,如果找到,B 就把

自己的 MAC 地址发送给 A。

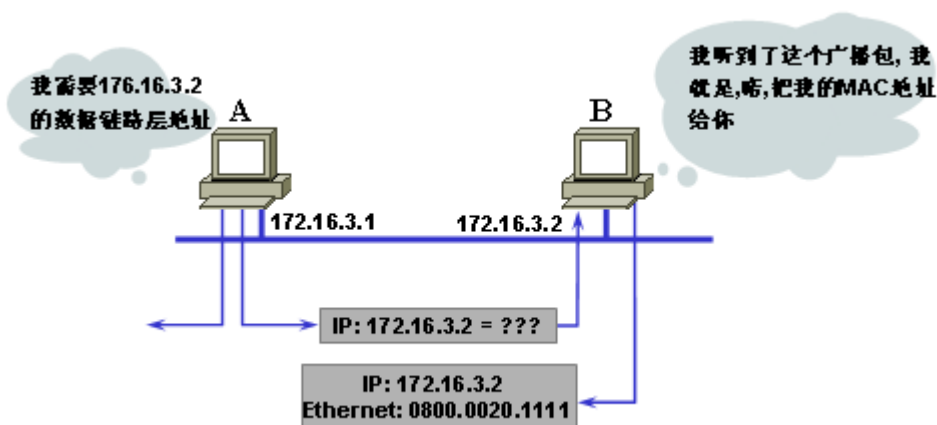


图 3-10 ARP 用于获得 MAC 地址

### 3.5.3 反向地址解析协议 (RARP)

在以太网中传输的数据包还必须包含目的 IP 地址和 MAC 地址。但是当源只知道自己的 MAC 地址而不知道自己的 IP 地址时，此时使用的协议是反向地址解析协议，简称为 RARP。

反向地址解析协议 RARP，要依靠 RARP 服务器来实现。如图 3-11 所示。

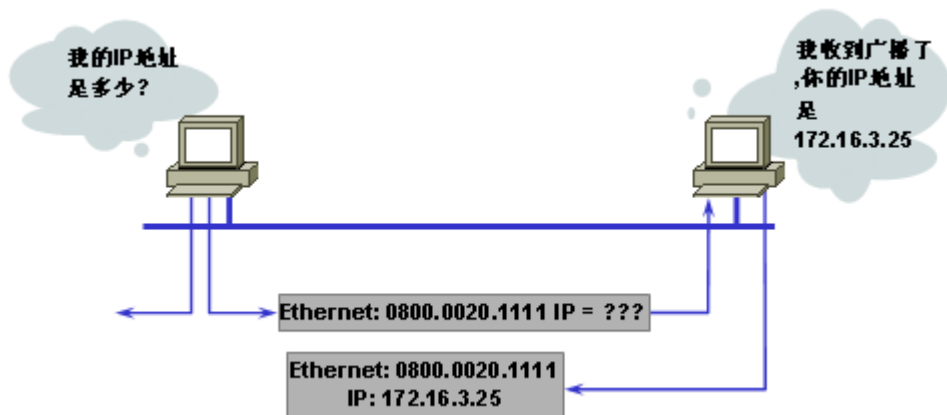


图 3 - 11 通过使用 RARP 请求来获取 IP 地址

## 3.6 IP 地址

在 Internet 上连接的所有计算机，从大型机到微型计算机都是以独立的身份出现，我们称它为主机。为了实现各主机间的通信，每台主机都必须有一个唯一的网络地址。就好像每一个住宅都有唯一的门牌一样，才不至于在传输数据时出现混乱。Internet 是由几千万

台计算机互相连接而成的。而我们要确认网络上的每一台计算机，靠的就是能唯一标识该计算机的网络地址，这个地址就叫做 IP (Internet Protocol 的简写) 地址，即用 Internet 协议语言表示的地址。

### 3.6.1 IP 地址的分类

如图 3-12 所示，每一个 IP 地址都包含两部分，即网络号 (net-id) 和主机号 (host-id)。网络号是用于标识该地址所从属的网络；主机号用于指明该网络上某个特定主机的主机号。

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。

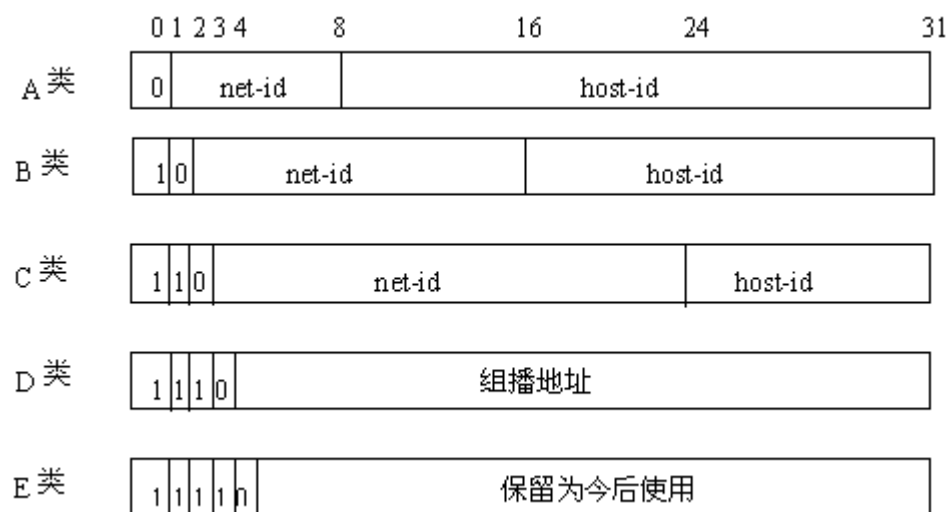


图 3-12 IP 地址的五种类型

#### (1) A 类地址

A 类地址分配给规模特别大的网络使用。A 类网络用第一组数字表示网络本身的地址，后面三组数字作为连接于网络上的主机的地址。分配给具有大量主机（直接个人用户）而局域网网络个数较少的大型网络。例如 IBM 公司的网络。

#### (2) B 类地址

B 类地址分配给一般的中型网络。B 类网络用第一、二组数字表示网络的地址，后面两组数字代表网络上的主机地址。

#### (3) C 类地址

C 类地址分配给小型网络，如一般的局域网和校园网，它可连接的主机数量是最少的，采用把所属的用户分为若干的网段进行管理。C 类网络用前三组数字表示网络的地址，最后

一组数字作为网络上的主机地址。例如，通过中国教育科研网接入 Internet 的北京师范大学计算机中心某主机的 IP 地址为：202.112.92.36。其中前三个数字域组成网络号，最后一个数字域是主机号。

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。当某个单位向 IAB 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。

以下为三类地址的范围比较。

网络类别	最大网络数	第一个可用的网络号码	最后一个可用的网络号码	每个网络中最大主机数
A	126	1	126	16,777,214
B	16,382	128.1	191.254	65,534
C	2,097,150	192.0.1	223.255.254	254

表 3.1 三类地址比较

### 3.6.2 广播地址和组播地址

广播 (broadcast) 地址和组播 (multicast) 地址不是指某一台具体的机器，而是指满足一定条件的一组机器，广播地址和组播地址都只能作为 IP 报文的目的地址，表示报文的一组接受者。

每一设备和接口必须有其主机地址（即 IP 地址的主机部分不能全为 0 或全为 1）。

主机地址部分为全 0 或全 1 的地址称为直接广播地址。使用直接广播地址，主机可以向任何网络直接广播数据。

- 全 1 主机地址保留给 IP 广播使用。例：在网络 176.10.0.0 中，向所有网络上的设备发送的广播地址就是 176.10.255.255。
- 全 0 主机意味着这个网络本身。

组播地址指定一个工作组。它和广播地址的区别在于，广播地址是按主机的物理位置来划分各组，而组播地址指定一个逻辑组，参与该组的机器可能遍布整个 INTERNET 网。



### 3.6.3 子网掩码

TCP/IP 体系规定用一个 32bit 的子网掩码来表示子网号字段的长度。具体的做法是：子网掩码由一连串的“1”和一连串的“0”组成。“1”对应于网络号码和子网号码字段，而“0”对应于主机号码字段（如图 3-13 所示）。

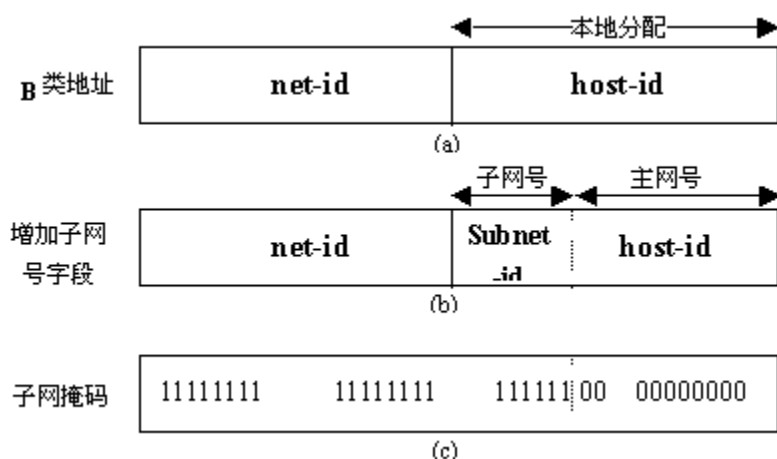


图 3-13 子网掩码格式

默认的网络掩码是根据 IP 地址中的第一个字段确定的。对于 A, B 和 C 类 IP 地址，其对应的子网掩码默认值分别为 255.0.0.0, 255.255.0.0 和 255.255.255.0。

### 3.6.4 子网规划

IP 地址的设计有不够合理的地方。例如，IP 地址中的 A 至 C 类地址，可供分配的网络号码超过 211 万个，而这些网络上的主机号码的总数则超过 37.2 亿个，初看起来，似乎 IP 地址足够全世界来使用（在 70 年代初期设计 IP 地址就是这样认为的）。其实不然。第一，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。第二，IP 地址在使用时有很大的浪费。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。

为了使 IP 地址的使用更加灵活，就引入了子网，各子网之间使用路由器来互连，因而便于管理。需要注意的是，子网的划分纯属本单位内部的，在本单位以外是看不见这样的划分。从外部看，这个单位只有一个网络号码。只有当外面的分组进入到本单位范围后，本单位的路由器在根据子网号码进行选路，最后找到目的主机。若本单位按照主机所在的地理位

置划分子网，那么在管理方面就会方便得多。

例如如果网络分配了一个 C 类地址 201.222.5.0。假设需要 20 个子网，每个子网有 5 台主机。我们需要把后 8 位再分为子网和主机部分，并确定子网掩码是什么。选择子网域大小要使其产生足够的子网。在这个例子中，选择 5 位掩码可以允许有 20 个子网。将所有子网地址选为 8 的倍数（比如 201.222.5.16，201.222.5.32，201.222.5.48）。

在最后百位中剩余的位用于主机域。我们例子中的 3 位允许足够主机以达到每线 5 台主机的要求。主机数字将是 1，2，3 等。主机的最终地址将是网络/子网“线路”的开始地址加上每个主机的号。在 201.222.5.16 子网中的主机地址为 201.222.5.17，201.222.5.18，201.222.5.19 等。

## 第四章 局域网

### 4.1 局域网特点

局域网即一组计算机和其它设备，在物理地址上彼此相隔不远，以允许用户相互通信和共享诸如打印机和存储设备之类的计算资源的方式互连在一起的系统。

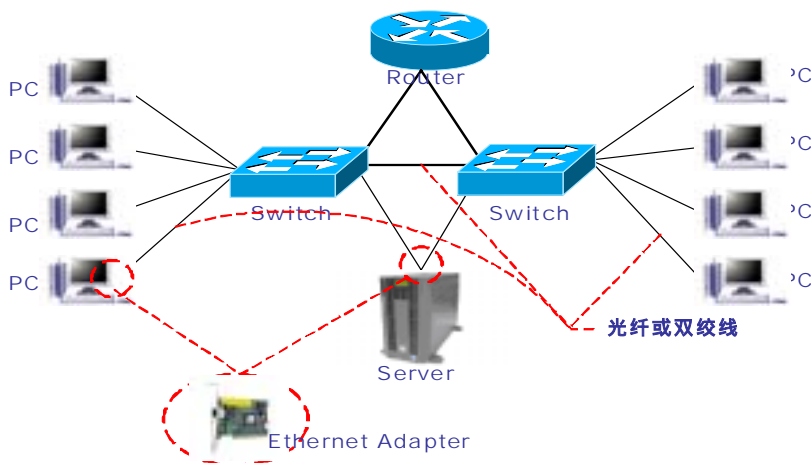
局域网特点：

- (1) 局域网覆盖有限的地理范围，适用于有限范围（一间办公室，一幢办公楼等）内计算机的连网需求；
- (2) 局域网具有高的数据传输速率（10 ~ 100Mbps）低的误码率。
- (3) 局域网的所有权和经营权属于一个单位所有。

### 4.2 局域网组成

局域网由以下部分组成，如图 4-1 所示：

- 计算机终端：主机、工作站，服务器等
- 传输介质：双绞线、光纤等
- 网络适配器：又称网卡。
- 网络连接设备：集线器、交换机、网桥、路由器等。
- 网络操作系统：Win NT、UNIX 等。



网络操作系统，例如：微软的Windows NT以及Novell的Netware和流行的UNIX等

图 4-1 局域网组成

## 4.3 决定局域网特性的主要技术

决定局域网特性的主要技术有以下三方面：用以传输数据的传输介质；用以连接各种设备的拓扑结构；用以共享资源的介质访问控制方法。这三种技术在很大程度上决定了传输数据的类型、网络的响应时间、吞吐量和利用率，以及网络应用等各种网络特性。其中最重要的是介质访问控制方法，它对网络特性具有十分重要的影响。

常见的局域网拓扑结构有星型、总线型、环型等。

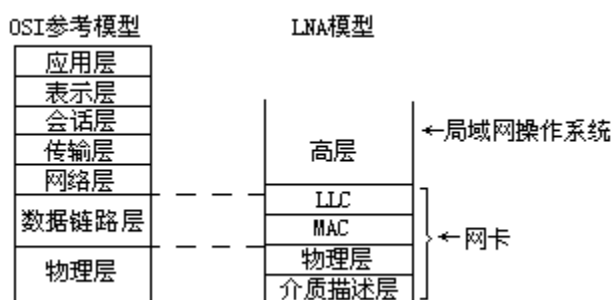
目前被普遍采用并形成国际标准的介质访问控制方法主要有以下三种：

- 带有冲突检测的载波侦听多路访问(CSMA/CD)方法
- 令牌总线(Token Bus)方法
- 令牌环(Token Ring)方法

在以上三种“共享介质”的工作方式中，使用最多的是带有冲突检测的载波侦听多路访问(CSMA/CD)方法。

## 4.4 局域网体系结构

局域网的体系结构包括物理层和数据链路层。其中数据链路层也由两个子层组成：介质访问控制(MAC:Medium Access Control)子层和逻辑链路控制(LLC:Logical Link Control)子层。如下图 4-2 所示。



4-2 局域网体系结构

逻辑链路控制子层(LLC)的主要功能是保证帧传送的完整性与无误性。例如进行流量控制，以保证快速与慢速设备之间帧无误传输。

介质访问控制子层(MAC)的主要功能是：

- (1) 发送时将数据封装成帧；

- (2) 接收时拆卸帧，即将数据帧解除封装，进行地址识别和差错校验；
- (3) 管理链路上的通信。

## 4.5 IEEE802 标准

IEEE 是通信领域的一个国际标准化组织，这个标准化组织有一个 802 委员会，专门研究和制定有关局域网的各种标准，目前已经制定出 12 个标准，如图 4—3 所示。

- (1) IEEE802.1 标准，包括局域网体系结构、网络互连以及网络管理；
- (2) IEEE802.2 标准，逻辑链路控制 LLC；
- (3) IEEE802.3 定义，CSMA/CD 总线介质访问控制方法与物理层规范；
- (4) IEEE802.4，定义令牌总线（Token Bus）介质访问控制方法与物理层规范；
- (5) IEEE802.5，定义令牌环（Token Ring）介质访问控制方法与物理层规范；

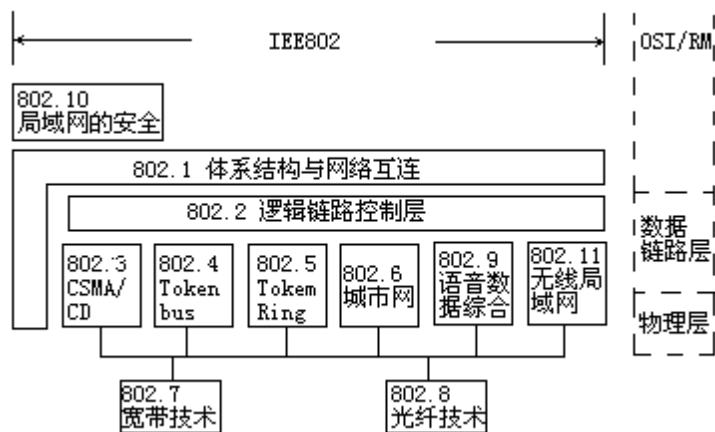


图 4-3 局域网组成示意图

- (6) IEEE802.6，定义城市网介质访问控制方法与物理层规范；
- (7) IEEE802.7，定义了宽带技术；
- (8) IEEE802.8，定义了光纤技术；
- (9) IEEE802.9，定义了语音与数据综合局域网技术；
- (10) IEEE802.10，定义了局域网的安全机制；
- (11) IEEE802.11，定义了无线局域网技术；
- (12) IEEE802.12，定义了按需优先的介质访问方法，用于快速以太网。

## 4.6 典型局域网

按照网络的拓扑结构和传输介质，局域网通常可划分为以太网（Ethernet）、令牌环网（Token Ring）、光纤分布式数据接口（FDDI）、异步传输模式（ATM）等，其中最常用的是以太网。我们简要介绍一下其它局域网使用。

令牌环网采用环型拓扑进行令牌单向传送，数据传输率低。

光纤分布式数据接口是使用光纤连接的双向环型网络，带宽利用率低，数据传输慢。

这两种局域网远不如以太网的应用，它已逐步被替代。

### 4.6.1 以太网工作原理

以太网是局域网里使用最多的一种网络模型。它的结构很简单，用一条无源总线将局域网的所有用户连接起来实现通信，所以也称为总线局域网。在 IEEE802.3 标准中规定了总线网的 CSMA/CD 访问方法和物理层技术规范。

CSMA/CD (Carrier Sense Multiple Access/Collision Detect) 即载波监听多路访问/冲突检测协议。该协议规定在以太网中每站在发送数据前，先监听信道是否空闲：若信道空闲，则发送数据，并继续监听下去；一旦监听到冲突，便立即停止发送，并在短时间内坚持连续向总线上发送一串阻塞信号(JAM)强化冲突，通知总线上各站有冲突发生，以便及早空出信道，提高信道的利用率；如果信道忙，则暂不发送，退避一段时间后再尝试。(CSMA/CD 协议与电话会议非常类似，许多人可以同时在线路上进行对话，但如果每一个人都在同时讲话，则你将听到一片噪声；如果每个人等别人讲完后再讲，则你可以理解各人所说的话)，如图 4-4 所示。

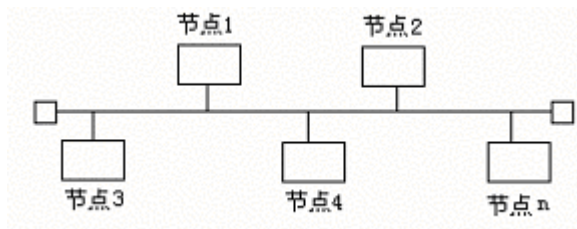


图 4-4 总线结构

### 4.6.2 传统的以太网系统

传统的以太网如图 4-5 所示。这种网络是 1975 年由美国 Xerox(施乐)公司研制成功的、

采用无源电缆作为总线传输信息的以太网(Ethernet)。以太网采用的媒体访问控制方法就是后来成为 IEEE802.3 标准的载波监听多路访问/冲突检测(CSMA/CD)技术。

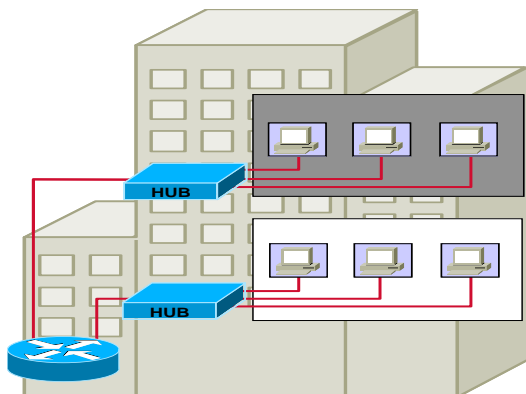


图 4-5 传统的以太网

从 80 年代后期到 90 年代初,越来越多的被加入局域网工作站,并且不同的局域网之间可以通过转发器进行互连。这些条件满足不了网络用户不断增长的应用需要和对共享资源进行访问的要求。虽然有流量控制机制,但对于一个以太网来说,冲突的发生是不可避免的。并且,随着冲突次数的增加,可用带宽的降低,应用程序更加繁忙,最终导致用户服务的响应时间变长,用户面临更长的等待时间。如图 4-6 所示。

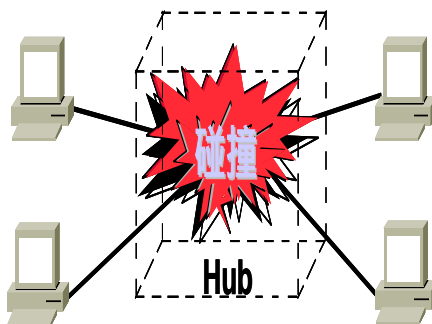


图 4-6 以太网冲突的产生

另一种削弱网络性能的因素是广播。大多数网络协议都利用广播来提供服务信息,而广播包到达所有的计算机,计算机必须处理这些广播包,大大降低了处理器的性能,另外,在共享式网络中,安全问题得不到保障,由于所有数据包到达中继器后往所有端口广播,这样信息很容易被窃取。

### 4.6.3 以太网分段

随着技术的更新,网络的不断发展,出现了更多的智能型台式机和工作站,音频信号和视频信号也被在数据网中进行传输,网络不再仅仅用于发送电子邮件、声音、图象,此时对

网络带宽的需求也越来越高，对网络分段便是获得高带宽的一种有效途径。通过网络分段，可以使每个用户获得更多的带宽，同时使在同一网段中的节点拥有更多的网络流量。

目前主要用路由器、交换机、网桥来完成以太网分段。在图 4-7 中，三个区域被创建，在每个区域内部是一个冲突域，这样在本网段内部发生的信息交换不会传到其它的网段上，也就是说把流量只限定在本区域内。只要用户的通讯只在本网段内进行，每个用户就会比所有用户在同一个大共享局域网下拥有较多的带宽。

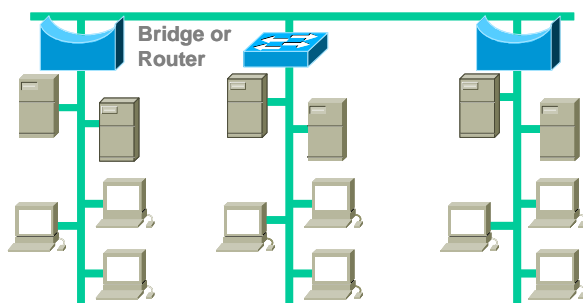


图 4-7 采用交换机/路由器分段

#### （一）采用网桥进行分段

网桥曾被广泛地应用于局域网的分段，以便为用户提供更多的带宽，如图 4-8 所示。

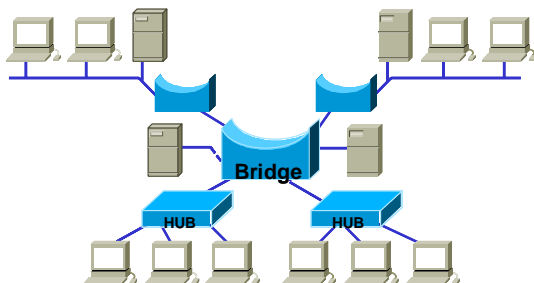


图 4-8 网桥分段

特点：

- 分段可以使在同一个网段中拥有相对较少数量的用户
- 网桥存储、转发所有的帧
- 独立于协议，即插即用
- 网桥的市场已经被交换机所取代

#### （二）采用路由器进行分段

路由器作用在 OSI 协议的网络层。路由器可以扩展网络，在互连的网络中寻找从源站点到目的站点间的路径。如图 4-9 所示。



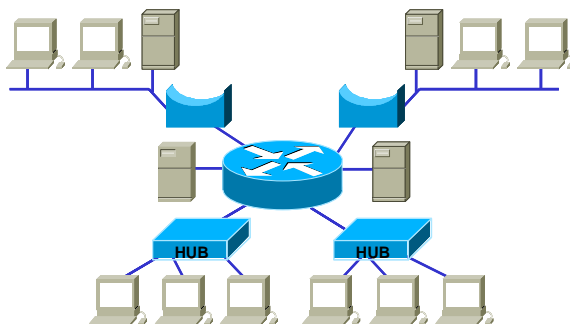


图 4-9 使用路由器进行分段

特点：

- 更好的管理性，更强的功能性，同时存在多条可用的路径
- 更复杂

### （三）采用交换机进行分段

特点：如图 4-10 所示

- 可以建立多条高速数据交换通道
- 具有较低的延迟和较高的帧转发率
- 增加了可用的网络带宽

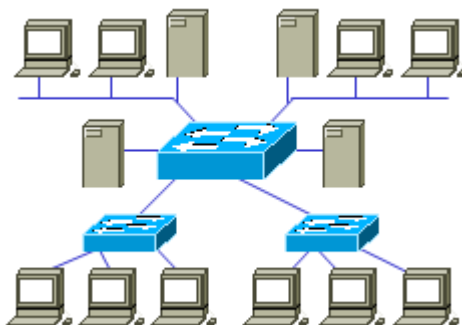


图 4-10 采用交换机进行分段

## 4.6.4 以太网电缆使用标准

以太网根据不同的媒体可分为：10BASE-2、10BASE-5、10BASE-T 及 10BASE-FL。下图表

4.1 为几种媒体的比较：

名称	电缆	最大区间长度	节点数/段	优点
10Base5	粗同轴电缆	500m	100	用于主干很好
10Base2	细同轴电缆	200m	30	最便宜的系统
10Base-T	双绞线	100m	1024	易于维护

10Base-F	光纤	2000m	1024	最适于在楼间使用
----------	----	-------	------	----------

表 4.1 媒体比较

## 4.7 快速以太网

快速以太网（Fast Ethernet）是一类新型的局域网，其名称中的“快速”是指数据速率可以达到 100Mbps，是标准以太网的数据速率的十倍。IEEE802 委员会为快速以太网制定了标准：IEEE802.3u。快速以太网的电缆标准为 100Base-T。

100Base-TX：是 IEEE 制定的执行 100Mbps 速率的双绞线的标准。它的最大网段长度为 100 米。

100 Base-FX：是 IEEE 制定的执行 100Mbps 速率的多模或单模光纤。主要是用作高速主干网，从节点到集线器的距离可以达到 450m。

## 4.8 千兆以太网

千兆以太网是 IEEE802.3 以太网标准的扩展。千兆以太网建立在以太网协议之上，但比快速以太网（FAST Ethernet）快 10 倍，其数据速率可达到 1000Mbps。采用千兆以太网的好处在于：千兆以太网将提供 10 倍于快速以太网的性能并与现有的 10/100 以太网标准兼容。

千兆以太网技术有两个标准：IEEE802.3z 和 IEEE802.3ab。

千兆以太网的电缆标准为：

1000BASE-SX：面向低成本的多模光线，用在水平或短距离主干应用。

1000BASE-LX：面向更长距离的多模建筑物光纤主干以及单模校园主干。

1000BASE-CX：基于铜缆的标准。适用于交换机之间的短距离连接，尤其适合千兆主干交换机和主服务器之间的短距离连接。

## 4.9 万兆以太网

万兆以太网可以满足新的容量需求，解决低带宽接入、高带宽传输的瓶颈问题，能扩大应用范围，并涵盖和兼容以前的几类以太网技术，其速率可达到 10Gbps。万兆以太网具有统一的标准，覆盖范围也大大增加。在现有的网络市场上，尤其是带宽需求颇为迫切的几个

市场上将会有较大的发展空间，这包括以下几个应用领域：

- 宽带交换机之间互连
- 数据中心或服务器群组网络中作为宽带汇聚
- 城域网宽带汇聚与骨干更新
- 新兴的宽带广域网

万兆以太网的标准为：802.3ae.

## 4.10 以太网标准

以下为以太网的标准：

IEEE 802.3 非屏蔽双绞线(UTP)上的 10BASE-T 以太网.

IEEE 802.3u UTP 或光线电缆上的 100BASE-T 快速以太网.

IEEE 802.3ab 5 类 UTP 电缆上的 1000BASE-TX 千兆以太网.

IEEE 802.3z 多模或单模光纤上 1000BASE-SX 的千兆以太网.

IEEE 802.3ae 万兆以太网

## 4.11 ATM

随着人们对集语音、图像和数据为一体的多媒体通信需求的日益增加，特别是为了适应今后信息高速公路建设的需要，人们又提出了的宽带综合业务数字网（B-ISDN）这种全新的通信网络，而 B-ISDN 的实现需要一种全新的传输模式，此即异步传输模式（ATM）。

ATM 是目前网络发展的最新技术，它能把实时的语音、图像和非实时的文本、数据等业务综合在一起，并在同一网络上传输。ATM 参考模型的二维简化模型如下图 4-11 示。

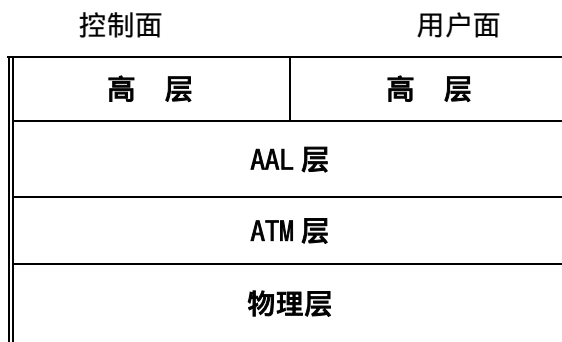


图 4-11 ATM 的简化参考模型

物理层主要负责系统和通信线路的连接。ATM 层主要负责信元的形成和交换。AAL

( ATM Adaptation Layer )层主要负责高层数据与 ATM 信元的适配和差错控制、流量控制等。高层分两部分，一部分属于控制面，用于传输各种控制指令，另一部分属于用户面，用于运行各种应用软件。

ATM 技术具有如下特点：

- 1、实现网络传输有连接服务，实现服务质量保证(QoS)。
- 2、交换吞吐量大、带宽利用率高。
- 3、具有灵活的组网拓扑结构、伸缩性、可靠性极高。
- 4、ATM 是现今唯一可同时应用于局域网、广域网两种网络应用领域的网络技术，它将局域网与广域网技术统一。

## 第五章 广域网技术

### 5.1 广域网的定义

广域网(WAN, wide area network), 有时也称为远程网, 是覆盖地理范围相对较广的数据通信网络. 它常利用公共网络系统(如电话公司)提供的便利条件进行传输, 可以分布在一个城市、国家, 甚至跨过许多国家分布到各洲。如图 5-1 所示。国内的如中国公用分组交换网 (CHINAPAC)、中国公用数字数据网 (CHINADDDA), 以及建议中的国家教育和科研网 (CERNET) 等都属于广域网。

区别广域网和局域网的关键所在是其规模。广域网可以不断扩展, 以满足跨越广阔地域的多个地点, 每个地点都有多个计算机之间连网的需要。不仅如此, 广域网还应有足够的能力, 使得联网的多个计算机能同时通信。另外, 几个不同地域的局域网经公共网络相互连接也可构成一个广域网。

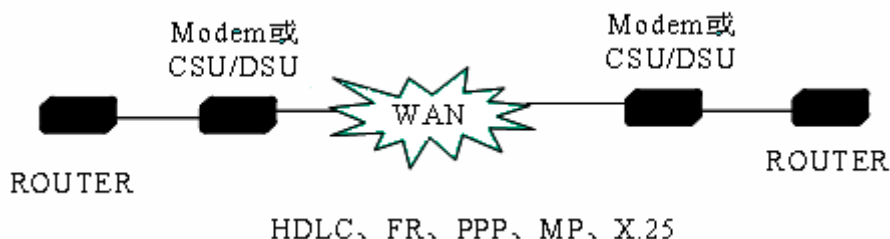


图 5-1 WAN 构成

与覆盖范围较小的局域网相比、广域网具有以下优点：

- 1) 覆盖范围广, 可达数千、甚至数万公里。
- 2) 数据传输速率较低, 通常为几千位每秒至几兆位每秒。
- 3) 可使用多种传输介质, 例如光纤、双绞线、同轴电缆等, 无线有微波、卫星、红外线、激光等。
- 4) 数据传输延时大, 例如卫星通信的延时可达几秒钟。
- 5) 数据传输质量不高, 例如误码率高, 信号误差大等。
- 6) 广域网管理、维护困难。

### 5.2 广域网中常用设备

广域网中常用设备：Modem、路由器、广域网交换机、接入服务器、CSU/DSU 等。

- 广域网交换机：广域网交换机工作在 OSI 参考模型的数据链路层，可以对帧中继，X.25 等数据流量进行操作。下图是广域网两端的两台路由器通过广域网交换机进行连接的示意图。

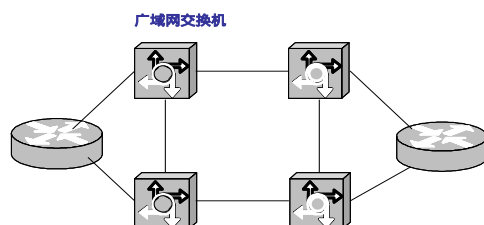


图 5-2 广域网交换机

- Modem：调制解调器主要用于数字和模拟信号之间的转换，从而能够通过话音线路传送数据信息。下图 5-3 是跨越广域网的调制解调器之间的简单连接形式。



图 5-3 Modem 连接方式

- 接入服务器：接入服务器是广域网中拨入和拨出连接的会聚点。图 5-4 说明了接入服务器如何将多条拨出连接集合在一起接入广域网。

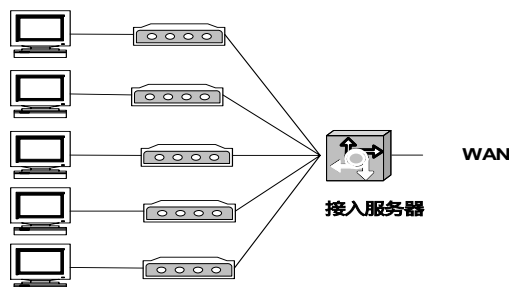


图 5-4 接入服务器

- CSU/DSU：信道服务单元（CSU）/数据服务单元（DSU）可以提供以下功能：信号再生，线路调节，误码纠正，信号管理等。下图 5-5 显示 CSU/DSU 在广域网下的实现方式。

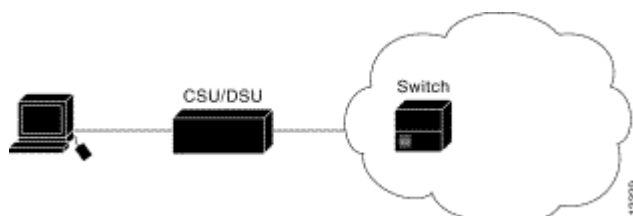


图 5-5 CSU/DSU 在广域网下的实现方式

## 5.3 广域网的体系结构

对照 OSI 参考模型，广域网技术位于底层的 3 个层次，分别是物理层、数据链路层和网络层。如图 5-6 所示。

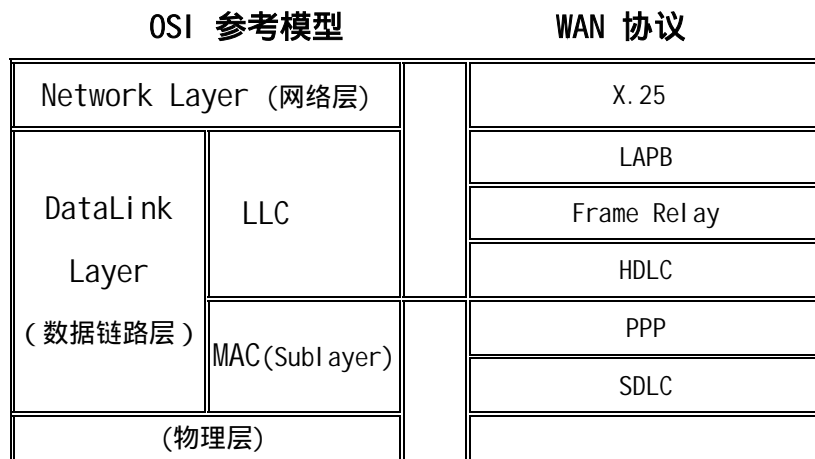


图 5-6 广域网体系结构

## 5.4 广域网协议

常用的广域网协议：

- HDLC：高级数据链路控制，ISO 标准的链路层协议；
- LAPB：平衡型链路访问规程，增强了错误检验和更正；
- PPP：点到点协议，有丰富功能的同异步链路层协议；
- X.25：分组交换协议，定义了终端和分组交换网络的连接规程；
- FR：帧中继，在 X.25 的基础上发展起来的简洁高效的分组交换协议。

## 5.5 典型广域网

广域网分为宽带广域网和窄带广域网，两者区别：

- 宽带是指 2M bps 以上的带宽，宽带采用了基于 ATM、IP、光纤以太网、MPLS 等分组技术；而窄带是基于电路交换技术；
- 宽带 IP 城域网一般具有层次结构，可以分为骨干层、汇聚层、接入层、用户层等。
- 拨号上网、ISDN、DDN 提供了基于窄带网络接入的数据应用；
- 宽带接入通过 ADSL/VDSL、LAN、HFC、无线接入等方式接入宽带网络；

目前，常见的窄带广域网有：公用电话交换网（PSTN）、公用分组交换网（X.25）、公用数

字数据网(DDN)、综合业务数字网(ISDN)、帧中继网(Frame-Relay)、宽带广域网有 ATM、SONET/SDH 等。

### 5.5.1 公用电话交换网 PSTN

所谓公用电话交换网(PSTN——Public Switch Telephone Network)，即我们日常生活中常用的电话网。

PSTN 技术是利用 PSTN 通过调制解调器拨号实现用户接入的方式。这种接入方式是大家非常熟悉的一种接入方式，目前最高的速率为 56kbps，这种速率远远不能够满足宽带多媒体信息的传输需求；但由于电话网非常普及，用户终端设备 Modem 很便宜，大约在 100 ~ 500 元之间，而且不用申请就可开户，只要家里有电脑，把电话线接入 Modem 就可以直接上网。因此，PSTN 拨号接入方式比较经济，至今仍是网络接入的主要手段。

PSTN 接入方式如图 5-7 所示。随着宽带的发展和普及，这种接入方式将被淘汰。

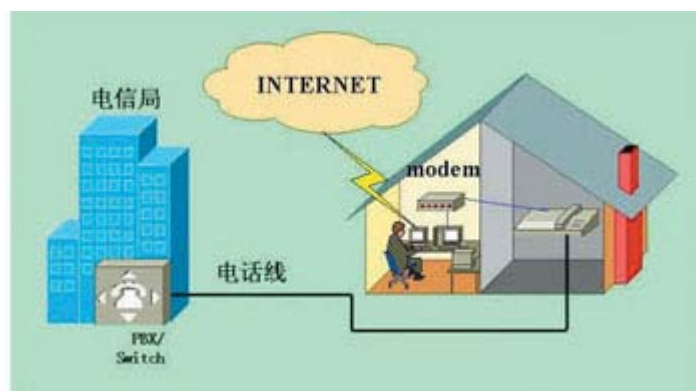


图 5-7 PSTN 接入技术

### 5.5.2 数字数据网 DDN

DDN 是英文 Digital Data Network 的缩写，这是随着数据通信业务发展而迅速发展起来的一种新型网络。DDN 的主干网传输媒介有光纤、数字微波、卫星信道等，用户端多使用普通电缆和双绞线。DDN 将数字通信技术、计算机技术、光纤通信技术以及数字交叉连接技术有机地结合在一起，提供了高速度、高质量的通信环境，可以向用户提供点对点、点对多点透明传输的数据专线出租电路，为用户传输数据、图像、声音等信息。如图 5-9 所示。

DDN 具有传输质量高、速度快、带宽利用率高等一系列优点。



用户租用 DDN 业务需要申请开户。DDN 的租用费较贵,普通个人用户负担不起,DDN 主要面向集团公司等需要综合运用的单位。

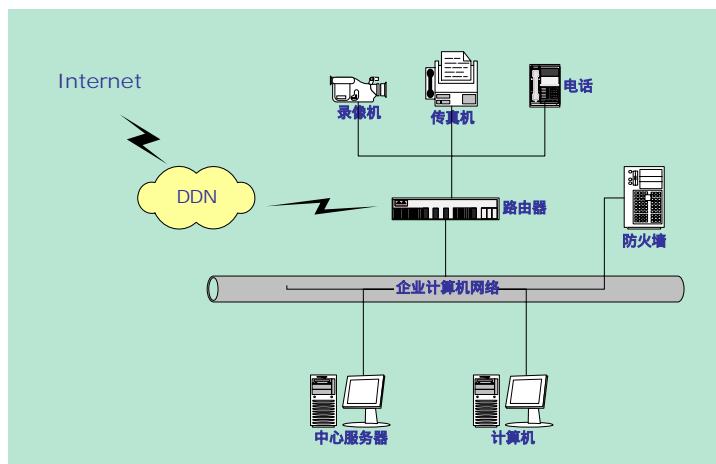


图 5-8 DDN 接入技术

### 5.5.3 分组交换网 X.25

X.25 常用于公共载波分组交换网,可以满足不同设备及系统间的网络通信。其主要特点是在一条电路上可以同时开放多条虚电路,网络具有动态路由及先进的差错检验功能,网络性能稳定,但速度较慢。

X.25 提供两种虚电路服务。

- 交换虚电路 (SVC)

交换虚电路类似于电话交换,即双方通信前要临时建立一条虚电路供数据传输,通信完毕后要拆除该虚电路,供其他用户使用。

- 永久虚电路 (PVC)

永久虚电路可在两个用户之间建立永久的虚连接,用户间需要通信时无需建立连接,可直接进行数据传输,如使用专线一样。

### 5.5.4 帧中继 Frame-Relay

帧中继 (Frame Relay) 是在分组交换网的基础上,结合数字专线技术而产生的数据业务网络。在某种程度上它可被认为是一种“快速分组交换网”。用户信息以帧为单位进行传输,并对用户信息进行统计复用。同分组交换网相比,它简化了相关协议,提高了传输速度。

它主要有 4 个特征:高传输速率、低网络延迟、连通性、高效带宽利用。如图 5-10 所

示。

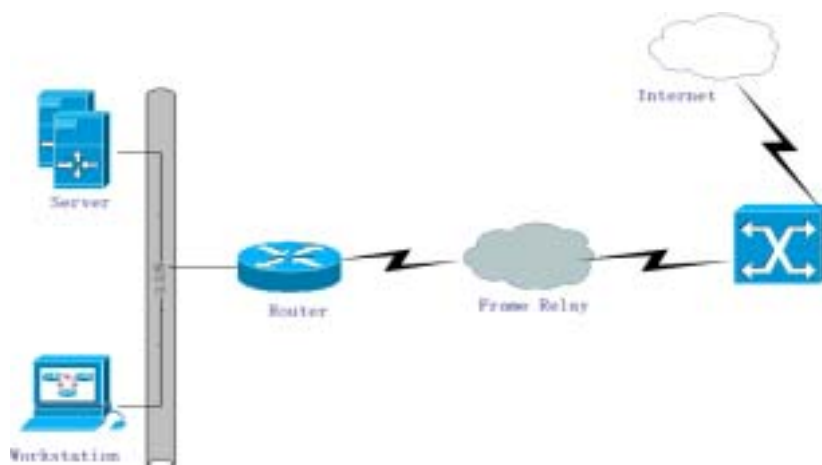


图 5-9 FR 接入技术

它只完成 OSI 七层协议中物理层和数据链路层的功能，而将流量控制、纠错等功能留给智能终端完成。

帧中继适合于突发性较强、速率较高、时延较短且要求经济性较好的数据传输业务，如公司间进行网络互联、开放远程医疗等多媒体业务、进行电子商务以及 VPN 组网等。

### 5.5.5 综合业务数字网 ISDN

ISDN(Integrated Service Digital Network，综合业务数字网)接入技术俗称“一线通”，它利用公众电话网向用户提供了端对端的数字信道连接，用来承载包括话音和非话音在内的各种电信业务。用户利用一条 ISDN 用户线路，可以在上网的同时拨打电话、收发传真，就像两条电话线一样。

就像普通拨号上网要使用 Modem 一样，用户使用 ISDN 也需要专用的终端设备，主要由网络终端 NT1 和 ISDN 适配器组成。

同 DDN 和帧中继相比，它主要优势如下：

- 业务实现方便，提供的业务种类丰富。凡是普通电话覆盖到的地方，只要电话交换机有 ISDN 功能模块，即可为用户提供 ISDN 业务。
- 用户使用非常灵活便捷。可以在上网的同时拨打电话。
- 适宜的性价比。

ISDN 适合于个人家庭用户或 SOHO 用户接入因特网、中小企事业单位 LAN 联网、连锁店的销售联网以及在公网开放可视电话、会议电视等增值业务，或被各中小企事业单位用于 DDN、帧中继等专线电路的备用方式。

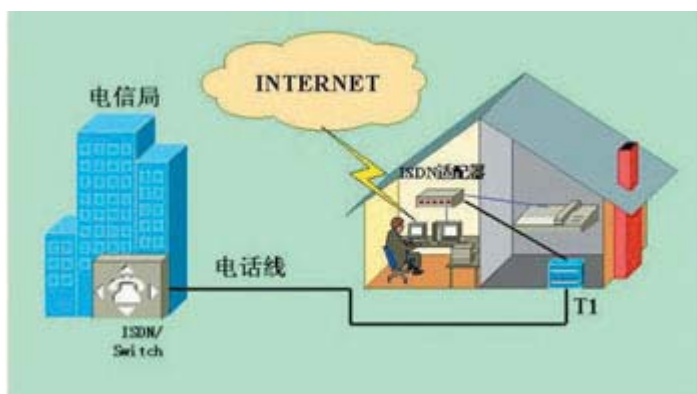


图 5-10 ISDN 接入技术

## 5.6 ADSL

ADSL(Asymmetrical Digital Subscriber Line，非对称数字用户环路)是一种能够通过普通电话线提供宽带数据业务的技术，也是目前极具发展前景的一种接入技术。ADSL 素有“网络快车”之美誉，因其下行速率高、频带宽、性能优、安装方便、不需交纳电话费等特点而深受广大用户喜爱，成为继 Modem、ISDN 之后的又一种全新的高效接入方式。

ADSL 接入技术示意如图 5-11 所示。ADSL 方案的最大特点是不需要改造信号传输线路，完全可以利用普通铜质电话线作为传输介质，配上专用的 Modem 即可实现数据高速传输。在一对双绞线上可为用户提供高达 8Mbps 的下行速率，1Mbps 的上行速率。其有效的传输距离在 3~5 公里范围以内。在 ADSL 接入方案中，每个用户都有单独的一条线路与 ADSL 局端相连，它的结构可以看作是星形结构，数据传输带宽是由每一个用户独享的。

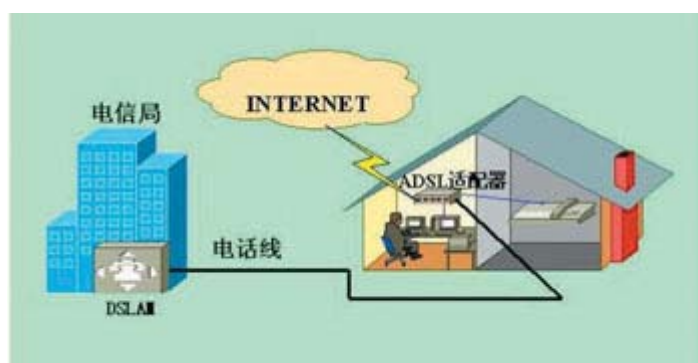


图 5-11 ASDL 接入方式

## 5.7 VDSL

VDSL 比 ADSL 还要快。使用 VDSL，短距离内的最大下载速率可达 55Mbps，上传速率可达 2.3Mbps（将来可达 19.2Mbps，甚至更高）。VDSL 使用的介质是普通电话线，有效传输距离可超过 1000 米。但 VDSL 技术仍处于发展初期，长距离应用仍需测试，端点设备的普及也需要时间。

目前有一种基于以太网方式的 VDSL，它的传输介质也是普通电话线，在 1.5 公里的范围之内能够达到双向对称的 10Mbps 传输，即达到以太网的速率。如果这种技术用于宽带运营商社区的接入，可以大大降低成本。基于以太网的 VDSL 接入方式示意图见图 5-12，方案是在机房端增加 VDSL 交换机，在用户端放置用户端 CPE，二者之间通过室外五类线连接，每栋楼只放置一个 CPE。

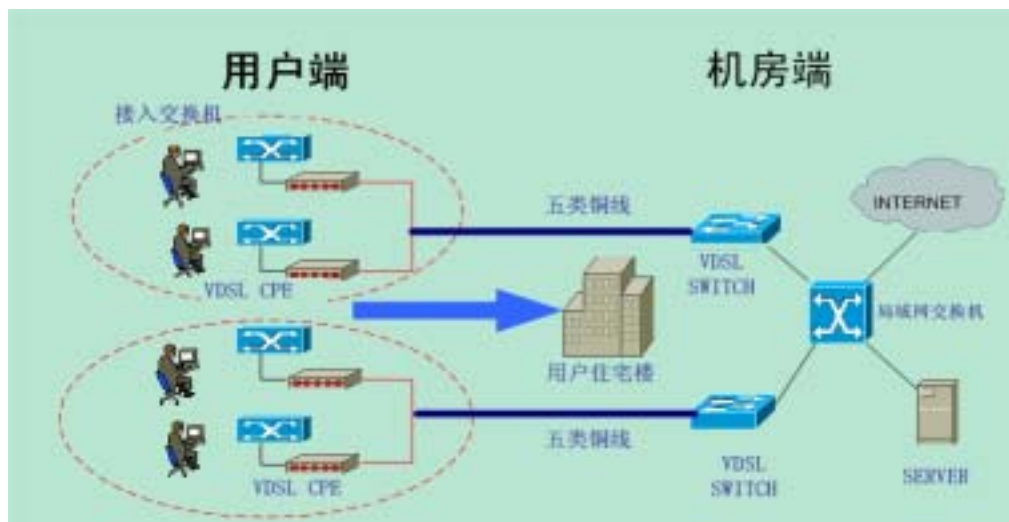


图 5-12 VDSL 接入技术

## 5.8 HFC 方式

HFC（Hybrid Fiber/Coax），即网络传输主干为光纤，到用户端为同轴电缆的用户网络接入方式。我国各城市的有线电视网按照电信网络的要求进行一定的升级改造，即可为用户提供 HFC 接入，实现普通电话、VOD、远程医疗等窄带和宽带业务。

利用这种技术实现宽带接入，有线网的优势主要表现为：

- 其信号的通频带宽为 750 MHz，为市话双绞线所无法比拟。

- 能充分适应信息网络的发展，易于过渡为最终的 FTTH/O 方式。
- 同利用 ADSL 等电信网络实现宽带接入的成本相比，它的成本费用很低。

但同时，现有的有线网同 ADSL 相比，也存在一些劣势：

- 有线电视网的带宽为所有用户所共享。

即每一用户所占的带宽并不固定，它取决于某一时刻对带宽进行共享的用户数。随着用户的增加，每个用户分得的实际带宽将明显降低，甚至低于用户独享的 ADSL 带宽。

- 由于其现为共享型网络，数据传送基于广播机制，通信的安全性不够高。

它主要敷设在住宅小区，显然不及市话双绞线覆盖的范围广泛。

## 5.9 VPN 技术

### 5.9.1 VPN 概述

VPN--虚拟专用网（Virtual Private Network）是专用网络在公共网络如Internet上的扩展。有了VPN，用户在家里或在路途中也可以利用Internet或其他公共网络对企业服务器进行远程访问。从用户的角度来看，VPN就是在用户计算机即VPN客户机和企业服务器即VPN服务器之间点到点的连接，由于数据通过一条仿真专线传输，用户感觉不到公共网络的实际存在，能够像在专线上一样处理企业内部信息。换言之，虚拟专用网不是真正的专用网络，但却能够实现专用网络的功能。

针对不同的用户要求，VPN 有三种解决方案：远程访问虚拟网（Access VPN）、企业内部虚拟网（Intranet VPN）和企业扩展虚拟网（Extranet VPN）。

### 5.9.2 远程访问虚拟网（AccessVPN）

AccessVPN通过一个拥有与专用网络相同策略的共享基础设施，提供对企业内部网或外部网的远程访问。AccessVPN能使用户随时、随地以其所需的方式访问企业资源。AccessVPN包括模拟、拨号、ISDN、数字用户线路(xDSL)、移动IP和电缆技术，能够安全地连接移动用户、远程工作者或分支机构。如图5-13所示。

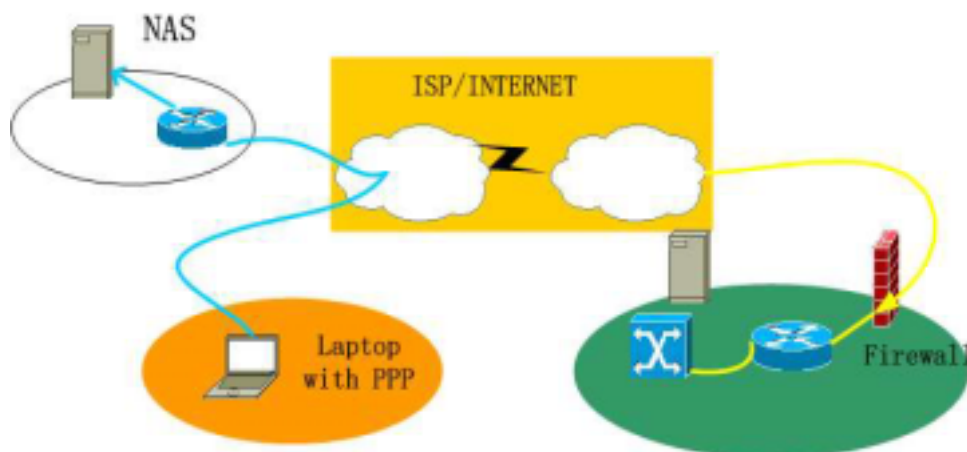


图5-13 AccessVPN结构图

AccessVPN最适用于公司内部经常有流动人员远程办公的情况。出差员工利用当地ISP提供的VPN服务，就可以和公司的VPN网关建立私有的连接。RADIUS服务器可对员工进行验证和授权，保证连接的安全，同时负担的电话费用大大降低。

### 5.9.3 企业内部虚拟网（IntranetVPN）

越来越多的企业需要在全国乃至世界范围内建立各种办事机构、分公司、研究所等，各个分公司之间传统的网络连接方式一般是租用专线。显然，在分公司增多、业务开展越来越广泛时，网络结构趋于复杂，费用昂贵。利用VPN特性可以在Internet上组建世界范围内的IntranetVPN。利用Internet的线路保证网络的互联性，保证信息在整个IntranetVPN上安全传输。IntranetVPN通过一个使用专用连接的共享基础设施，连接企业总部、远程办事处和分支机构。企业拥有与专用网络的相同政策，包括安全、服务质量(QoS)、可管理性和可靠性。如图5-14所示。



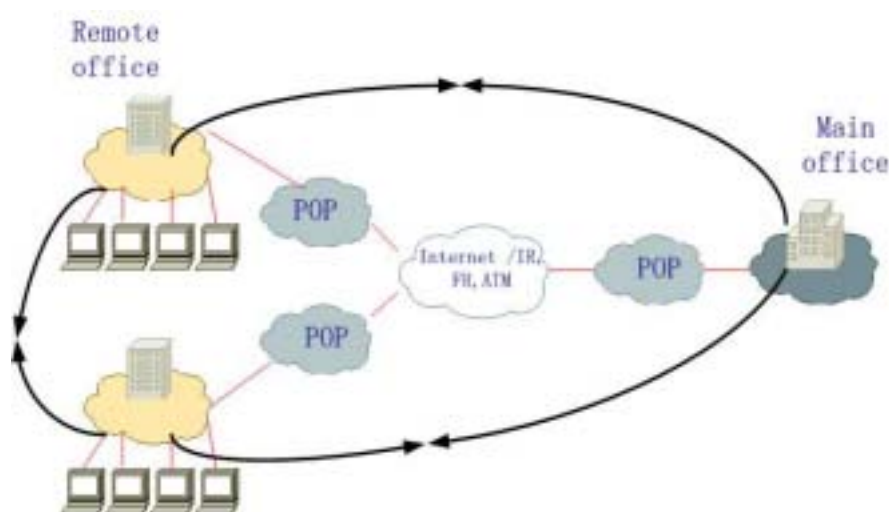


图5-14 IntranetVPN结构图

### 5.9.4 企业扩展虚拟网（ExtranetVPN）

各个企业越来越重视各种信息的处理。希望可以提供给客户最快捷方便的信息服务，通过各种方式了解客户的需要，同时各个企业之间的合作关系也越来越多，信息交换日益频繁。Internet为这样的一种发展趋势提供了良好的基础，而如何利用Internet进行有效的信息管理，是企业发展中不可避免的一个关键问题。利用VPN技术可以组建安全的Extranet，既可以向客户、合作伙伴提供有效的信息服务，又可以保证自身的内部网络的安全。

ExtranetVPN通过一个使用专用连接的共享基础设施，将客户、供应商、合作伙伴或兴趣群体连接到企业内部网。企业拥有与专用网络的相同政策，包括安全、服务质量(QoS)、可管理性和可靠性。如图5-15所示。

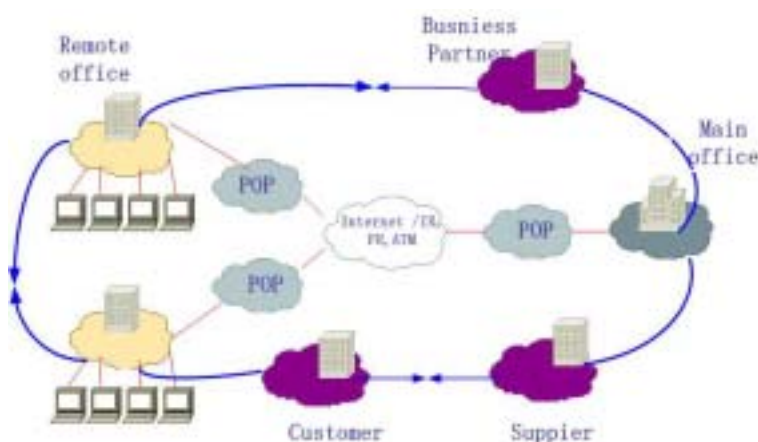


图5-15 ExtranetVPN结构图

ExtranetVPN对用户的吸引力在于：能容易地对外部网进行部署和管理，外部网的连接可以使用与部署内部网和远端访问VPN相同的架构和协议进行部署。主要的不同是接入许可，外部网的用户被许可只有一次机会连接到其合作人的网络。

## 第六章 路由技术

### 6.1 路由器工作原理

#### 6.1.1 路由器的概念

路由器是用于网络互连的网络设备，它工作在 OSI 参考模型第三层（即网络层），连接多个独立的网络或子网，同时为不同的网络之间报文寻径并存储转发。它在 OSI 参考模型中的位置如图 6-1 所示。路由器利用 IP 地址来区别不同的网络(如图 6-2 所示)，实现网络的互连和隔离，保持各个网络的独立性。路由器不转发广播消息，而把广播消息限制在各自的网络内部。

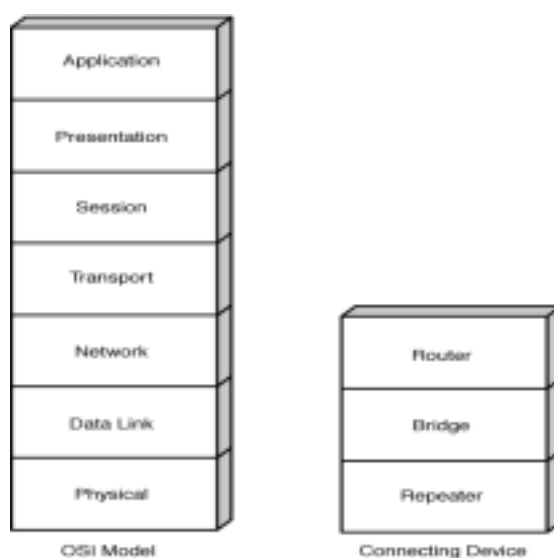


图 6-1 路由器在 OSI 结构中的位置

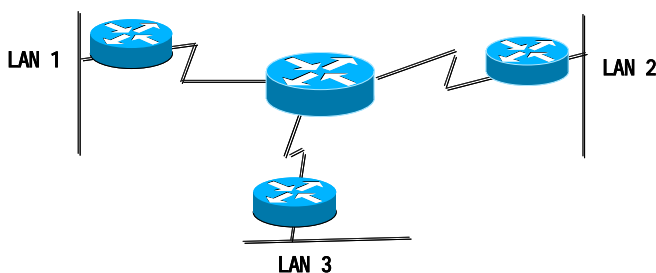




图 6-2 路由器功能

作为路由器，必须具备：

- 两个或两个以上的接口：用于连接不同的协议；
- 协议至少实现到网络层：只有理解网络层协议才能与网络层通讯；
- 至少支持两种以上的子网协议：异种子网互连；
- 具有存储、转发、寻径功能：实现速率匹配与路由寻径；
- 一组路由协议：包括域内路由协议和域间路由协议。

### 6.1.2 路由器作用

- 异种网络互连：主要是具有异种子网协议的网络的互连。
- 子网协议转换：不同子网间包括局域网和广域网间协议转换。
- 路由寻径：路由表建立、刷新、查找。
- 速率适配：不同接口具有不同的速率，路由器可以利用自己缓存及流控协议适配。
- 隔离网络：防止网络风暴，网络安全。
- 备份、流量流控：主备线路的切换及复杂的流量控制。

### 6.1.3 路由器的优缺点

- 优点：

适用于大规模的网络；

复杂的网络拓扑结构和最优路径；

能更好地处理多媒体；

安全性高；

隔离不需要的通信量；

节省局域网的频宽；

减少主机负担。

- 缺点：

它不支持非路由协议；

数据包需要软件处理，容易成为瓶颈；

安装和调试比较复杂；

价格高。

### 6.1.4 路由器的工作原理

当一台主机发送信息给同一子网的另一台主机时，对方可直接接收到，如果送给不同子网的主机时，则选择一个能到达目的子网上的路由器进行转发，同主机一样，路由器也要判定端口所接的是否是目的子网，如果是，就直接把分组通过端口送到网络上，否则，也要选择下一个路由器来传送分组。这样一级级地传送，IP 分组最终将送到目的地，送不到目的地的 IP 分组则被网络丢弃了。

如图 6-3 所示，主机 A 要发送信息给主机 B，A 和 B 属于不同网络，则 A 通过路由器 1 转发寻找 B 主机的 IP 地址，如果未找到，再通过路由器 2 转发，依次类推。

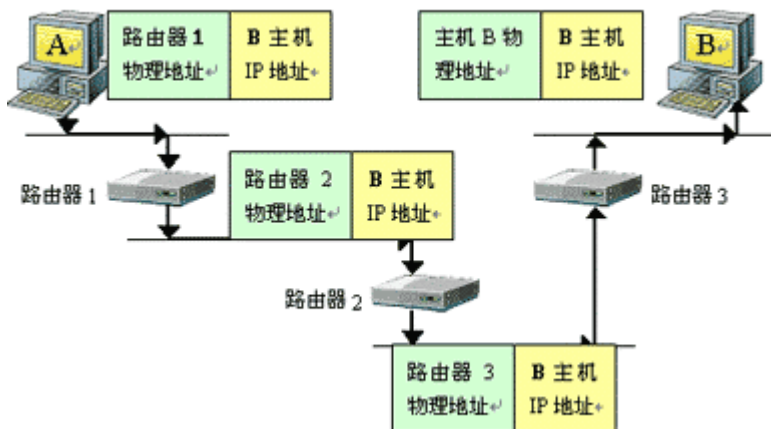


图 6-3 路由寻址过程

### 6.1.5 路由选择方式

典型的路由选择方式有两种：静态路由和动态路由。

静态路由是在路由器中设置的固定的路由表。除非网络管理员干预，否则静态路由不会发生变化。静态路由一般用于网络规模不大、拓扑结构固定的网络中。静态路由的优点是简单、高效、可靠。当动态路由与静态路由发生冲突时，以静态路由为准。

动态路由是网络中的路由器之间相互通信，传递路由信息，利用收到的路由信息更新路由器表的过程。动态路由适用于网络规模大、网络拓扑复杂的网络。

## 6.1.6 路由算法

路由算法在路由协议中起着至关重要的作用，采用何种算法往往决定了最终的寻径结果。常用的路由算法有：

- 距离向量算法：每一台路由器向外发送全部或绝大部分的路由表信息，不过该信息只能发送给临近的路由器。
- 链路状态算法：也称为最短路径优先算法，可以把路由信息传递到网络上的所有节点。不过每一台路由器只是向外界发送描述自己链路状态的那一小部分路由表信息。

两者的区别就是链路状态算法可以向整个网络范围发送数据量较小的更新信息，而距离向量算法则是只能向临近的路由器发送大批量的更新信息。

## 6.2 路由协议

大型网络如因特网，会被分解成为多个自治系统（Autonomous System）。每个自治系统被看做是一个进行自我管理的网络，一个自治系统只负责管理自己内部的路由。对于因特网来说，两个自治系统内部的路由选择信息是互不共享的。

路由协议分为两种：

- 内部网关协议 IGP（Interior Gateway Protocol）

内部网关协议是指运行在一个自治系统内部的，一般适用由单个组织（ISP）管理的网络，常见协议有 RIP/RIP2，OSPF。

- 外部网关协议 EGP（Exterior Gateway Protocol）

外部网关协议是指自治系统之间的路由选择协议，主要用于多个 ISP 共同管理的网络，如 BGP。

### 6.2.1 RIP 路由协议

RIP 是 Routing Information Protocol（即路由信息协议）的简称，是 Internet 中常用的路由协议。它是一种内部路由协议。RIP 采用距离向量算法，即路由器根据距离选择路由，所以也称为距离向量协议。RIP 运行简单，适用于小型网络。

## 6.2.2 OSPF 路由协议

OSPF 是 Open Shortest Path First (即“开放最短路由优先协议”)的缩写。它是 IETF 组织开发的一个基于链路状态的自治系统内部路由协议,在 IP 网络上,它通过收集和传递自治系统的链路状态来动态地发现并传播路由; OSPF 协议使用 IP Multicasting 方式发送和接收报文。OSPF 是一种相对复杂的路由协议。

## 6.2.3 BGP 协议

BGP 协议是 Border gateway protocol 的缩写,即边界网关协议, BGP 是为 TCP / IP 互联网设计的外部网关协议,用于多个自治域之间。它既不是基于纯粹的链路状态算法,也不是基于纯粹的距离向量算法。它的主要功能是与其它自治域的 BGP 交换网络可达信息。各个自治域可以运行不同的内部网关协议。

## 6.2.4 多播路由协议

为适应 Internet 网络一对多的多点传送应用如天气预报、网络会议等,出现了一种新的传输模式——多播 (multicast)。多播适合于一到多的传输环境,同时也可适用多到多、多到一的情况。

## 第七章 网络交换技术

### 7.1 共享式以太网

早期的局域网一般工作在共享方式下。在使用共享式以太网时，会有这样的感觉：有时候网络快得如行云流水，有时候却慢似蜗牛爬行。为什么会有这样的现象呢？这就得从共享式以太网的工作机制谈起了。

共享式以太网（即使用集线器或共用一条总线的以太网）采用了载波检测多路侦听（Carries Sense Multiple Access with Collision Detection，简称 CSMA/CD）机制来进行传输控制。如图 7-1 所示。

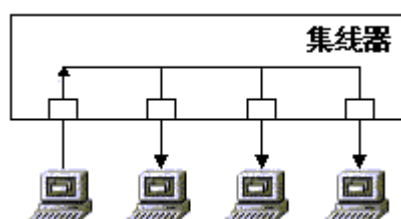


图 7-1 共享式以太网

在局域网中，数据都是以“帧”的形式传输的。共享式以太网是基于广播的方式来发送数据的，这样网络上所有的主机都可以收到这些帧，如图 7-1 所示。这就造成了只要网络上有一台主机在发送帧，网络上所有其他的主机都只能处于接收状态，无法发送数据。也就是说，在任何一时刻，所有的带宽只分配给了正在传送数据的那台主机。举例来说，虽然一台 100Mbps 的集线器连接了 20 台主机，表面上看起来这 20 台主机平均分配 5Mbps 带宽。但是实际上在任何一时刻只能有一台主机在发送数据，所以带宽都分配给它了，其他主机只能处于等待状态。图 7-2 显示了共享式以太网的碰撞冲突。



图 7-2 共享式以太网

## 7.2 交换式以太网

交换式以太网技术是作为对共享式局域网提供有效的网段划分的解决方案而出现的,它可以使每个用户尽可能地分享到最大带宽。

### 7.2.1 交换式以太网工作原理

交换式以太网技术在传统以太网技术的基础上,用交换技术替代原来的 CSMA/CD 技术,从而避免了由于多个站点共享并竞争信道导致发生的碰撞,减少了信道带宽的浪费,同时还可以实现全双工通信,极大的提高了信道的利用率,如图 7-3 所示。因此,交换式以太网技术已经越来越广泛的成为当今局域网实现的技术。

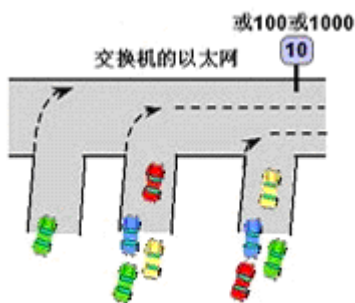


图 7-3 交换式以太网

以太网交换机的原理很简单,它检测从以太网端口来的数据包的源和目的地的 MAC (介质访问层) 地址,然后与系统内部的动态查找表进行比较,若数据包的 MAC 层地址不在查找表中,则将该地址加入查找表中,并将数据包发送给相应的目的端口。这就是以太网交换机的帧转发和学习机制。如图 7-4 所示,终端 A 向 C 发出一组数据帧,交换机通过从 E0 端口进来的数据帧学到了终端 A 的 MAC 地址,并将其地址与交换机端口的对应关系存入其 MAC 地址表。交换机将终端 A 所发出的数据帧向交换机的所有端口 (除了 E0) 发送。

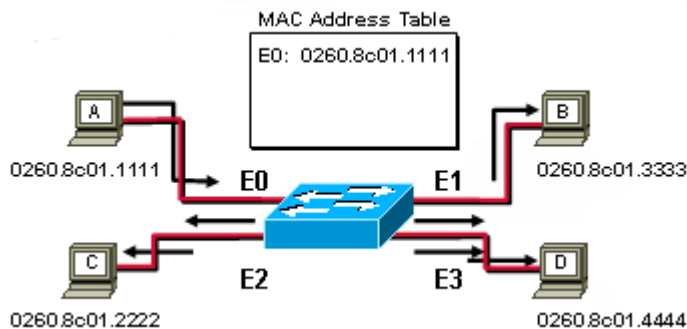


图 7-4 交换机的学习机制

## 7.2.2 交换式以太网的基本结构

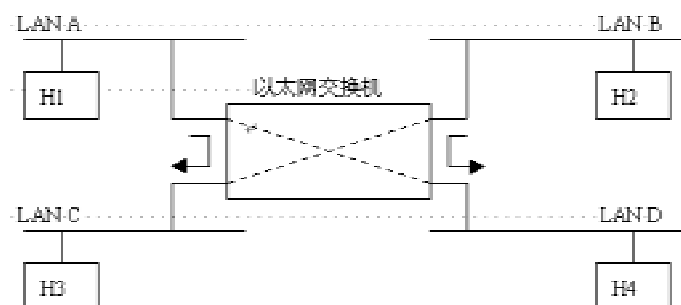


图 7-5 交换式以太网的基本结构

在如上的组网结构中，以太网交换机所连接的四个 LAN 中的任意两个 LAN（如 LAN A 与 LAN C）在通信的同时，另外两个 LAN（LAN B 与 LAN D）也可以同时通过交换机通信，这对于共享式集线器是无法实现的。从而可以把这四个 LAN 看作是一个大的新 LAN，但是它的冲突域却没有扩大，仍然保持在原来各自的冲突域（LAN A-D）。而同样规模的共享式以太网的冲突域是整个 LAN 范围内，因此交换式以太网的性能要优于共享式以太网。

## 7.2.3 交换机数据转发方式

它有两种帧交换方式，如图 7-6 所示：

- 直通交换(Cut-through)：只需读取帧的目的 MAC 地址，就可以把帧转发到相应的端口中去。这种方法的交换速度非常快，但缺乏对网络帧进行更高级的控制，缺乏智能性和安全性，同时也无法支持具有不同速率的端口的交换。
- 存储转发方式(store-and-forward)：在转发之前，交换机必须收到完整的数据帧，读取目的和源地址，进行 CRC 校验，在作相应的过滤。这样加长了数据延迟，但保证了数据的准确性。



图 7-6 直通交换与存储转发交换

## 7.2.4 交换式以太网技术的优点

交换式以太网不需要改变网络其它硬件，包括电缆和用户的网卡，仅需要用交换式交换机改变共享式 HUB，节省用户网络升级的费用。

可在高速与低速网络间转换，实现不同网络的协同。目前大多数交换式以太网都具有 100Mbps 的端口，通过与之相对应的 100Mbps 的网卡接入到服务器上，暂时解决了 10Mbps 的瓶颈，成为网络局域网升级时首选的方案。

它同时提供多个通道，比传统的共享式集线器提供更多的带宽，传统的共享式 10/100Mbps 以太网采用广播式通信方式，每次只能在一对用户间进行通信，如果发生碰撞还得重试，而交换式以太网允许不同用户间进行传送。

## 7.2.5 共享式以太网和交换式以太网比较

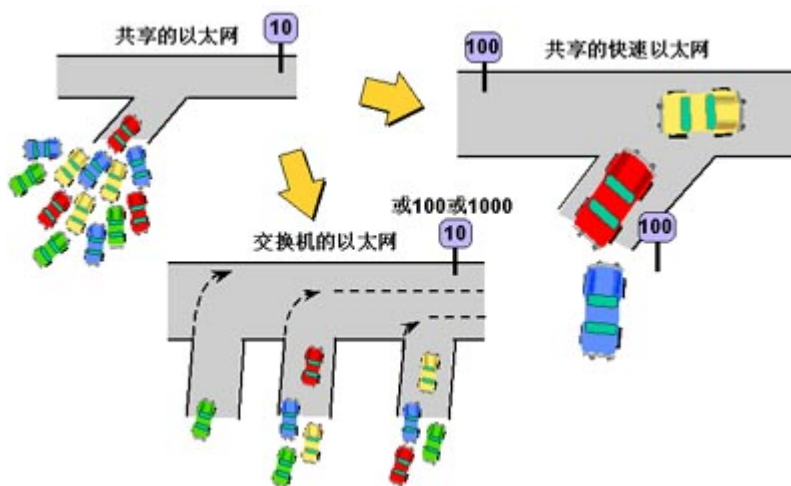


图 7-7 共享式以太网和交换式以太网

## 7.2.6 半双工以太网

常规的共享介质以太网采用 CSMA/CD 介质访问机制，以半双工模式工作，网络在同一时间要么发送数据，要么接收数据，而不能同时发送和接收数据。它可以同时连接多条线路，对所有的用户，共享以太网都依赖单条共享介质，如图 7-8 所示。



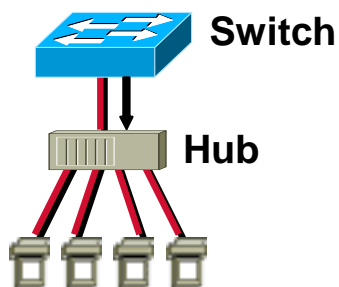


图 7-8 半双工方式

半双工以太网的特点:

- 单向的数据传输
- 容易产生碰撞
- 主要实现于 Hub 等设备上

## 7.2.7 全双工以太网

全双工操作简单，而且全双工链路两端的设备均可同时收发数据。由此而来的一个好处就是在理论上全双工的理论带宽是传统以太网(半双工)的二倍。全双工操作模式要求链路上的每一端都只连接一个设备，如一个工作站与一个交换机端口相连。如图 7-9 所示。

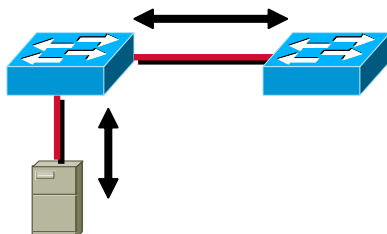


图 7-9 全双工方式

全双工以太网特点:

- 只能用于点到点的传输方式
- 实现于交换机等设备上
- 需要另一端也支持全双工的传输方式
- 产生碰撞的几率很小

## 7.2.8 生成树

为了解决大型交换式以太网的广播风暴问题，就引入了生成树.那么,什么是广播风暴呢?

如图 7-10 所示. 主机 X 发送一个广播数据包, 广播帧在网络循环多次, 产生了越来越多的广播帧, 最后形成广播风暴 (如图 7-11)。

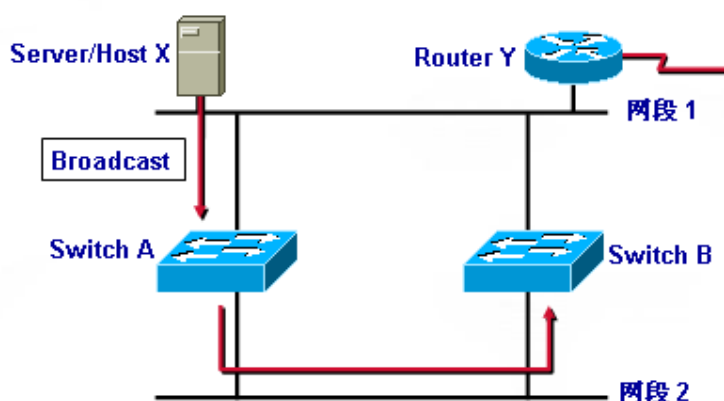


图 7-10 发送广播数据包

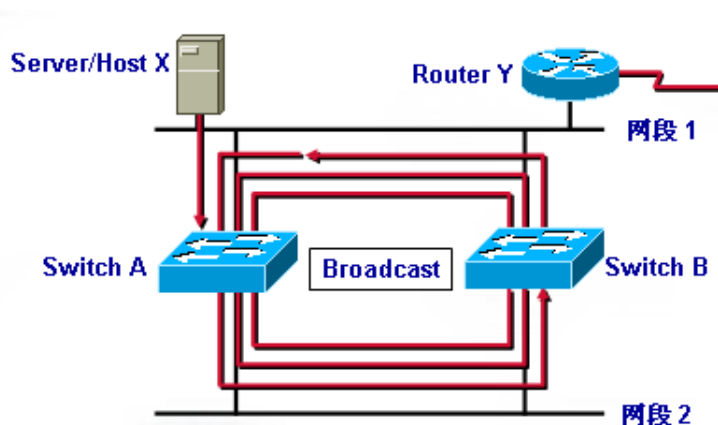


图 7-11 网络风暴的产生

生成树协议又称 STP(Spanning Tree Protocol)。标准的生成树可以解决因网络循环连接造成的网络风暴、同时也为网络备份提供可能。

STP 是一个防止环路, 同时提供冗余线路的第二层的管理协议。为了使交换网络正常运行, STP 网络上的任何两个终端之间只有一条有效路径。STP 使用生成树算法计算没有环路的最佳路径, 使一些备用路径处于阻塞状态。如图 7-12 所示。

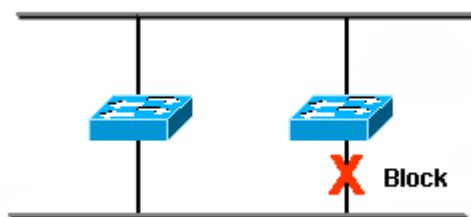


图 7-12 STP 生成树

## 7.3 虚拟局域网 VLAN

### 7.3.1 VLAN 的工作原理

VLAN ( Visual local area network ) 称为虚拟局域网，它将区域分散的组织在逻辑上成为一个新的工作组，而且同一工作组的成员能够改变其物理地址而不必重新配置节点，这就是所谓的虚拟局域网技术。如图 7-13 所示。

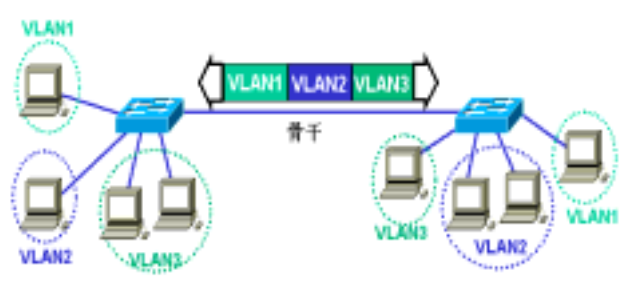


图 7-13 虚拟局域网

用交换机建立虚拟网就是使原来的一个大广播域(交换机的所有端口)逻辑的分为若干个"子广播域"，在子广播域里的广播只会在该广播域内传送，其它的广播域是收不到的。VLAN 通过交换技术将通信量进行有效分离，从而更好地利用带宽，并可从逻辑的角度出发将实际的 LAN 基础设施分割成多个子网，它允许各个局域网运行不同的应用协议和拓扑结构。VLAN 的标准是 IEEE802.1Q。下图 7-14 所示就是基于端口划分的基本的 VLAN 结构：

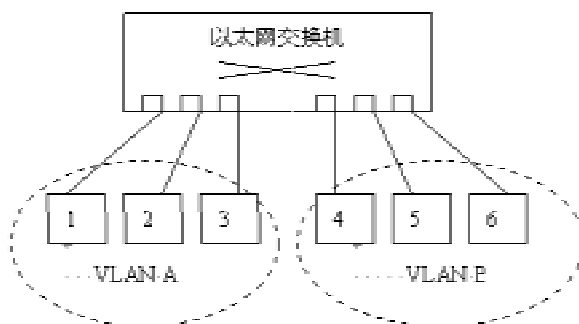


图 7-14 基于端口的 VLAN 结构

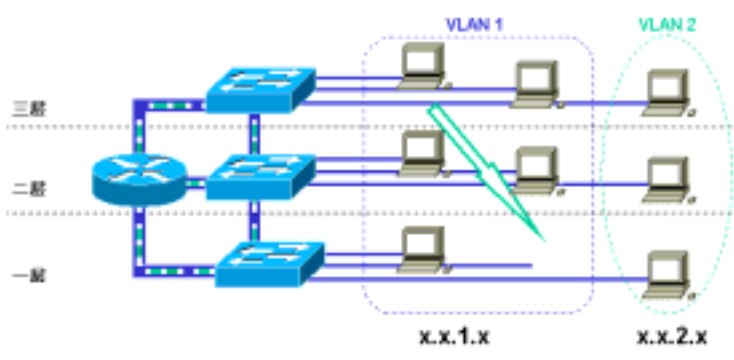
在上图中，原来的广播域 1~6 端口被划分成了两个子广播域，VLAN A 包括了原来的 1~3 端口，VLAN B 包括了原来的 4~6 端口，因此 1~3 端口收到的广播数据帧就不会转发到 VLAN B 中的端口上，同样 4~6 端口上收到的广播报文也不会转发到 VLAN A 中的端口上。这就减少了整个交换式以太网中广播报文的数量。

### 7.3.2 虚拟局域网的优点

那么为什么引入虚拟局域网呢？它的优势在哪里？下面我们将介绍它的优势所在。

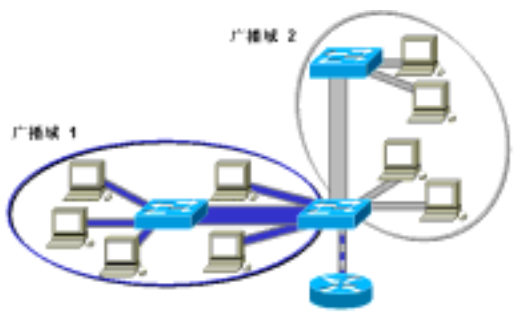
#### 1. 降低管理费用，简化移动、添加和改变。

每年大约有 20 %到 40%的员工发生物理位置的改变，在同一 VLAN 中移动的节点不必改变它的网络地址，同时路由器的配置不发生改变。如图 7-15 所示。



7-15 VLAN 中位置移动

#### 2. 广播域控制，阻止广播风暴，将信息有效隔离。如图 7-16。



7-16 控制网络风暴

3. 加强网络安全。通过路由访问列表和 MAC 地址分配等 VLAN 划分原则，可以控制用户访问权限和逻辑网段大小，将不同用户群划分在不同 VLAN，从而提高交换式网络的整体性能和安全性。

### 7.3.3 VLAN 的分类

VLAN 在交换机上的实现方法，可以大致划分为 4 类：

#### （1）基于端口划分的 VLAN

这种划分方法是根据以太网交换机的端口来划分，属于同一 VLAN 的端口可以不连续，如何配置则由管理员决定。如果有多个交换机，例如：可以指定交换机 1 的 1-6 端口和交换机 2 的 1-4 端口为同一 VLAN，即同一 VLAN 可以跨越数个以太网交换机，这种根据端口来划分 VLAN 的方式仍然是最常用的一种方式。

这种划分的方法的优点是定义 VLAN 成员时非常简单，只要将所有的端口都指定一下就可以了。它的缺点是如果 VLAN 的用户离开了原来的端口，到了一个新的交换机的某个端口，那么就必须重新定义。

#### （2）基于 MAC 地址划分 VLAN

这种划分方法是根据每个主机的 MAC 地址来划分，即对每个 MAC 地址的主机都配置他属于哪个组。MAC 地址其实就是指网卡的标识符，每一块网卡的 MAC 地址都是唯一且固化在网卡上的。这种划分方法的最大优点就是当用户物理位置移动时，即从一个交换机换到其他的交换机时，VLAN 不用重新配置，这种方法的缺点是在站点入网时，所有的用户都必须进行配置，如果有几百个甚至上千个用户的话，配置将非常的繁琐。

#### （3）基于网络层划分 VLAN

这种划分方法是根据每个主机的网络层地址或协议类型(如果支持多协议)划分的，这种方法的优点是用户的物理位置改变了，不需要重新配置所属的 VLAN，而且可以根据协议类型来划分 VLAN，这对网络管理者来说很重要。这种方法的缺点是效率低，因为检查每一个数据包的网络层地址是需要消耗处理时间的(相对于前面两种方法)。例如办公用的电脑用 TCP/IP，看行情的电脑使用 IPX，他们将处于不同的网络。

#### （4）根据 IP 组播划分 VLAN

IP 组播实际上也是一种 VLAN 的定义，即认为一个组播组就是一个 VLAN，这种划分的方法将 VLAN 扩大到了广域网，因此这种方法具有更大的灵活性，而且也很容易通过路由器进行扩展，当然这种方法不适合局域网，主要是效率不高。

### 7.3.4 以端口为中心的 VLAN 的实施

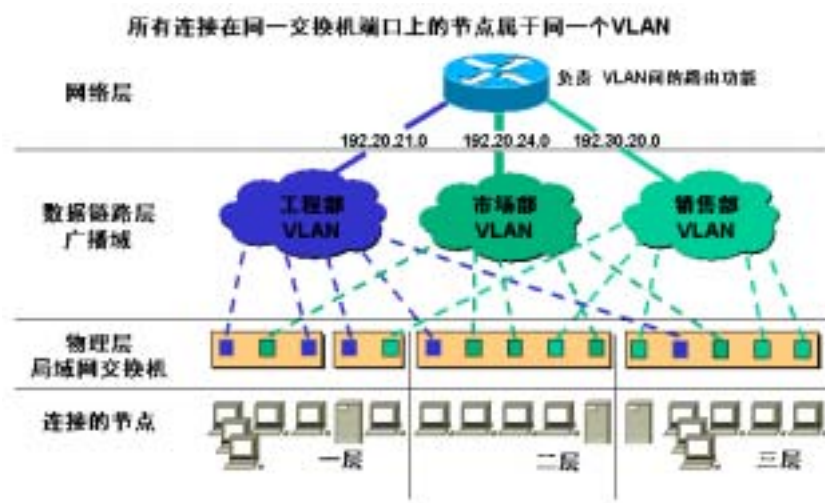


图 7-17 VLAN 的实施

## 7.4 组播

### 7.4.1 组播定义

当代社会已经进入信息时代，网络技术在飞速发展。由于视频会议、推送技术、大规模协作计算、为用户群进行软件升级、用于培训和企业报告的共享白板式的多媒体应用、网络代理、镜像和高速缓存站点等等应用，都依赖于从一个主机向多个主机或者从多个主机向多个主机发送同一信息的能力，而在 Internet 上分发的数目可能达数十万台，这些都需要更高的带宽，并且大大超出了单播的能力。一种能最大限度地利用现有带宽的有力武器是 IP 组播技术，这项技术已获得了包括 AT & T、HP、IBM、Intel、Microsoft、Cisco 和 3Com 等业界有影响的众多厂商的支持。

组播技术可形象的描述如下：

假设一个企业分布于各地的子公司（两个以上）之间需要通过 Internet 进行实时的交换信息（数据，声音，图像），他们的计算机可能不属于同一物理网络，甚至不属于同一自治系统，这种通信的特点是“多点”式的。子公司发出的数据希望其他子公司都能收到，而总部发出的指示全体子公司都应收到。这种多点通信方式为组内广播，即组播技术，也称多播技术，多目网关技术。如图 7-18 所示。

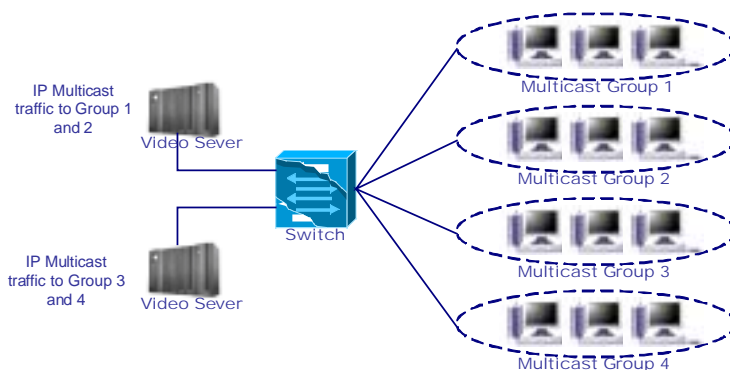


图 7-18 组播技术

组播在企业中的应用：

通常人们想到 IP 组播就会想到视频会议和视频点播。尽管第一个使用的 IP 组播网络常常是视频网络，但视频只是许多 IP 组播应用之一。IP 组播在其他领域应用的也很广泛。

#### 1．多媒体应用

一些出色的 IP 组播多媒体应用程序已经被开发出来，允许通过 IP 组播实现多对多的音频或音频 / 视频会议。

#### 2．数据分发

数据分发是 IP 组播应用的另一个领域。通过使用 IP 组播，公司可以采用“推”的模式进行文件和数据库更新。企业可使用软件通过卫星链路向所属分公司分发软件升级和数据更新消息。一次性向所有的分公司传送一种数据，而不是依次向每个分公司重发，节省了时间和通信费用。

#### 3．实时数据组播

实时数据传送是使 IP 组播深受欢迎的又一应用领域。一个好的例子是将股票信息发送到交易大厅的工作站。通过指定不同的财务分类（债券、运输、药品等等）给不同的组播组，交易员能使用他们的工作站来接收他们感兴趣的实时金融数据。

#### 4．游戏和仿真

IP 组播非常适合于网络游戏或者仿真应用的使用。虽然很多的游戏和仿真支持联机的方式进行游戏，事实上所有这些应用使用单播，是点对点的连接。IP 组播可用于有大量参与者的游戏和仿真。参与的计算机只需进入 IP 组播组就开始发送和接受游戏及仿真数据。

## 7.4.2 组播技术的原理

组播是一种允许一个或多个发送者（组播源）发送单一的数据包到多个接收者（一次的，同时的）的网络技术。组播源把数据包发送到特定组播组，而只有属于该组播组的地址才能接收到数据包。组播可以大大的节省网络带宽，因为无论有多少个目标地址，在整个网络的任何一条链路上只传送单一的数据包。它提高了数据传送效率。减少了主干网出现拥塞的可能性。组播组中的主机可以是在同一个物理网络，也可以来自不同的物理网络（如果有组播路由器的支持）。

其网络模型如下图所示：

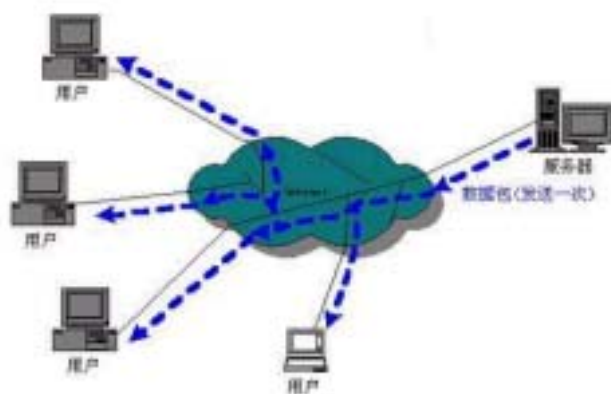


图 7-19 组播模型

## 7.4.3 组管理协议

IGMP 组播成员管理机制是针对第三层设计的，在第三层，路由器可以对组播报文的转发进行控制。

IGMP 协议运行于主机与和主机直接相连的组播路由器之间，主机通过此协议告诉本地路由器希望加入并接受某个特定组播组的信息，同时路由器通过此协议周期性地查询局域网内某个已知组的成员是否处于活动状态（即该网段是否仍有属于某个组播组的成员），实现所连网络组成员关系的收集与维护。

## 7.4.4 IGMP SNOOPING 协议（IGMP 监听）

在很多情况下，组播报文要不可避免地经过一些第二层交换设备，尤其是在局域网环境里。如果不对第二层设备进行相应的配置，则组播报文就会转发给第二层交换设备的所有端



口，显然这会浪费大量的资源。IGMP Snooping可以解决这个问题。

IGMP监听的工作原理如下：

- 主机发出IGMP成员报告消息，这个消息是给路由器的，在IGMP成员报告经过交换机时，交换机对这个消息进行监听并记录下来，形成组成员和端口的对应关系；
- 交换机在收到组播数据报文时，根据组成员和端口的对应关系，仅向具有组成员的端口转发组播报文。

## 7.5 三层交换技术

简单地说，三层交换技术就是：二层交换技术 + 三层转发技术。是相对于传统交换概念而提出的。众所周知，传统的交换技术是在 OSI 网络标准模型中的第二层——数据链路层进行操作的，而三层交换技术是在网络模型中的第三层实现了数据包的高速转发。

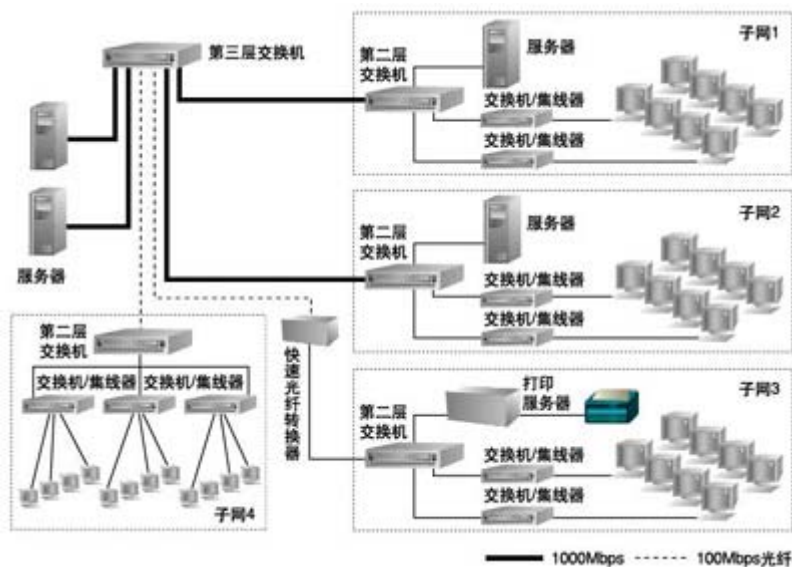
它解决了局域网中网段划分之后，网段中子网必须依赖路由器进行管理的局面，解决了传统路由器低速、复杂所造成的网络瓶颈问题。

传统路由器是基于纯 CPU 和软件的，而交换机则减少了对 CPU 处理能力的依赖，直接在每个端口的硬件中缓存大多数 IP 地址信息。

### 7.5.1 三层交换机的特点

- 以交换机的速度实现了路由功能。
- 拥有基于三层的数据包转发能力。
- 内部建立了路由表。
- 可以在各个子网间进行路由并转发数据包。
- 也可以进行基于二层 MAC 地址的数据帧交换。

## 7.5.2 三层交换机的应用



7-20 三层交换机应用

## 7.6 交换机的基本性能参数

### 7.6.1 交换机分类

交换机从设计理念上讲只有两种：

- 机箱式交换机（也称为模块化交换机）

机箱式交换机最大的特色就是具有很强的可扩展性，它能提供一系列扩展模块，诸如千兆以太网模块、FDDI 模块、ATM 模块、快速以太网模块、令牌环模块等等，所以能够将具有不同协议、不同拓扑结构的网络连接起来。它最大的缺点就是价格昂贵。机箱式交换机一般作为骨干交换机或者需要高密度端口接入的配线间来使用。

- 独立式固定配置交换机。

一般具有固定端口的配置。固定配置交换机的可扩充性不如机箱式交换机，但是成本却要低得多。

交换机其它分类方式：

交换机按工作所在层次分：一层、二层、三层、多层

交换机按端口速率分：十兆、百兆、千兆、万兆

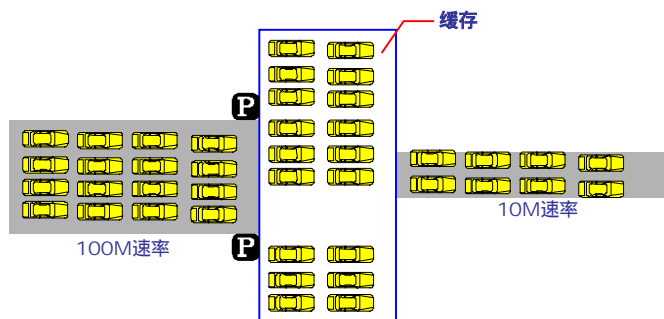
按功能性能要求分：电信级、企业级

按网络层次：核心、边缘（汇聚）、工作组接入

按管理性分：Dump、Smart、Managed

## 7.6.2 交换机性能参数

- 机架插槽数：是指机架式交换机所能安插的最大模块数。
- 扩展槽数：是指固定配置式带扩展槽交换机所能安插的最大模块数。
- 最大可堆叠数：是指一个堆叠单元中所能堆叠的最大交换机数目。此参数说明了一个堆叠单元中所能提供的最大端口密度。
- 最小/最大 10M 以太网端口数：是指一台交换机所支持的最小/最大 10M 以太网端口数量。
- 最小/最大 100M 以太网端口数  
是指一台交换机所支持的最小/最大 100M 以太网端口数量。
- 最小/最大 1000M 以太网端口数  
是指一台交换机所能连接的最小/最大 1000M 以太网端口数量。
- 背板吞吐量（bps）  
也称背板带宽，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。一台交换机的背板带宽越高，所能处理数据的能力就越强，但同时设计成本也会比较高。
- 包转发率：交换机每秒转发的数据包的数量。
- 缓存  
缓存也叫缓冲区，是一种应用于存储器上的队列结构。交换机用缓冲区来协调不同网络设备之间传输速度的不同。如图 7-21 所示。



7-21 队列结构

- MAC 地址表  
连接到局域网上的每个端口或设备都需要一个 MAC 地址，其它设备要用到此地址来定位

特定的端口及更新路由表和数据结构。MAC 地址有 6 字节长，由 IEEE 来分配，又叫物理地址。一个设备的 MAC 地址表（如图 7-22）大小反映了连接到该设备能支持的最大节点数。

MAC Address Table	
E0:	0260.8c01.1111
E1:	0260.8c01.3333
E2:	0260.8c01.2222
E3:	0260.8c01.4444
⋮	
E24:	0260.8c01.4423

7-22 MAC 地址表

- 最大电源数

一般地，核心设备都提供有冗余电源供应，在一个电源失效后，其它电源仍可继续供电，不影响设备的正常运转。在接多个电源时，要注意用多路市电供应，这样，在一路线路失效时，其它线路仍可供电。

- QoS

服务质量（Quality of Service）是传输系统的性能度量，反映了其传输质量以及服务的可获得性。它主要靠 RSVP（资源预留协议）及 802.1P 来保证。

## 7.7 联想网络交换机产品线介绍

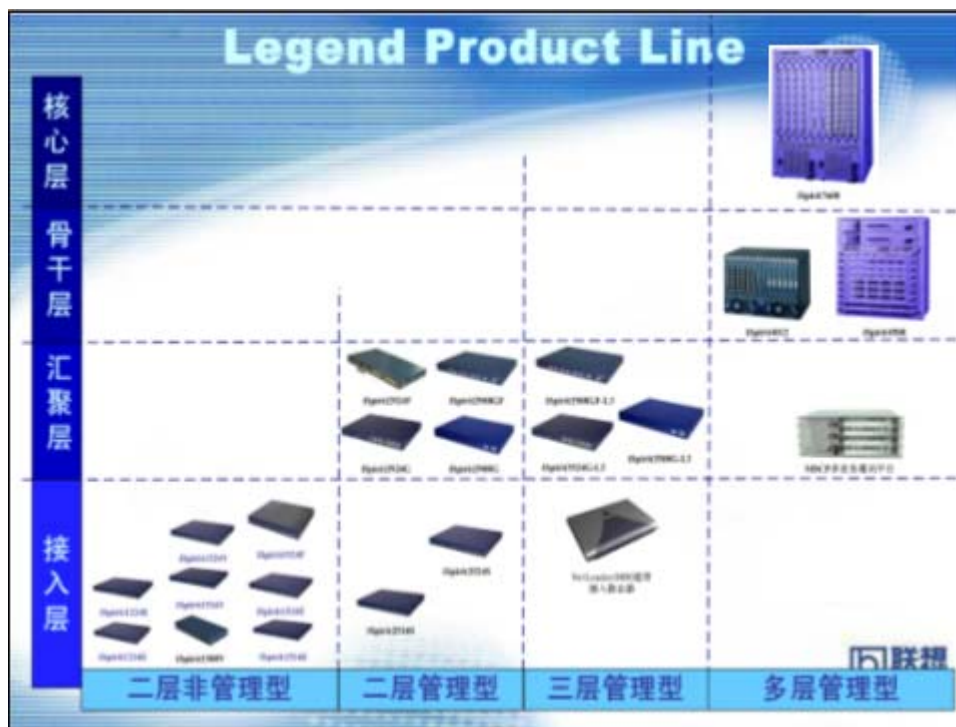


图 7-23 联想交换机产品线

### 7.7.1 机架式交换机

- 联想 iSpirit6808 骨干交换机
- 联想 iSpirit4808 中心交换机
- 联想 iSpirit4012 中心交换机

### 7.7.2 固定配置式交换机

- 联想 iSpirit35xxG/GF-L3 系列
- 联想 iSpirit29xxG/F/GF 系列
- 联想 iSpirit25xxS 系列
- 联想 iSpirit15xxV 系列
- 联想 iSpirit12xxE 系列

## 第八章 网络管理

网络是新经济时代的基础设施，信息传递、办公、营销、服务、交流、娱乐等各种活动都可以通过网络完成，网络的质量直接决定了社会生活和经济生活的质量。在计算机网络的质量体系中，网络管理是其中一个关键环节，正如一个管家对于大家庭生活的重要，网络管理的质量也会直接影响网络的运行质量。

### 8.1 网络管理的发展

网络管理并不是一个什么新概念。从广义上讲，任何一个系统都需要管理，只是根据系统的大小、复杂性的不同，管理在整个系统中的重要性也就有重有轻。追溯到 19 世纪末的电信网络，就已经有了自己相应的管理“系统”，这就是整个电话网络系统的管理员，尽管他能管理的内容非常有限。而计算机网络的管理可以说伴随着 1969 年世界上第一个计算机网络——ARPANET 的产生便产生了，当时，ARPANET 就有一个相应的管理系统。不过，虽然网络管理很早就有，却一直没有得到应有的重视。这是因为当时的网络一是规模较小，二来复杂性不高，一个简单的网络管理系统就可以满足网络正常管理的需要，因而对其研究较少。但随着网络的发展，规模逐渐增大，复杂性增加，以前的网络管理技术已不能适应网络的迅速发展。

网络系统规模的日益扩大和网络应用水平的不断提高，一方面使得网络的维护成为网络管理的重要问题之一，例如排除网络故障更加困难、维护成本上升等；另一方面，如何提高网络性能也成为网络系统应用的主要问题。

### 8.2 网络管理功能

一般说来，网络管理就是通过某种方式对网络状态进行调整，使网络能正常、高效地运行。其目的很明确，就是使网络中的各种资源得到更加高效的利用，当网络出现故障时，能及时作出报告和处理，并协调、保持网络的高效运行等。

网络管理功能主要包括以下几方面：

- (1) 配置管理：自动发现网络拓扑结构，构造和维护网络系统的配置。监测网络被管对象的状态，完成网络关键设备配置的语法检查，配置自动生成和自动配置备份系统，对于配置的一致性进行严格的检验。

- (2) 故障管理：过滤、归并网络事件，有效地发现、定位网络故障，给出排错建议与排错工具，形成整套的故障发现、告警与处理机制。
- (3) 性能管理：采集、分析网络对象的性能数据，监测网络对象的性能，对网络线路质量进行分析。同时，统计网络运行状态信息，对网络的使用发展作出评测、估计，为网络进一步规划与调整提供依据。
- (4) 安全管理：结合使用用户认证、访问控制、数据传输、存储的保密与完整性机制，以保障网络管理系统本身的安全。维护系统日志，使系统的使用和网络对象的修改有据可查。控制对网络资源的访问。
- (5) 计费管理：对网际互联设备按 IP 地址的双向流量统计，产生多种信息统计报告及流量对比，并提供网络计费工具，以使用户根据自定义的要求实施网络计费。

### 8.2.1 配置管理

#### (1) 配置信息的自动获取

一个先进的网络管理系统应该具有配置信息自动获取功能。即使在管理人员不是很熟悉网络结构和配置状况的情况下，也能通过有关的技术手段来完成对网络的配置和管理。

#### (2) 自动配置、自动备份

配置信息自动获取功能相当于从网络设备中“读”信息，相应的，在网络管理应用中还有大量“写”信息的需求。

#### (3) 配置一致性检查

在一个大型网络中，由于网络设备众多，这些设备很可能不是由同一个管理人员进行配置的。实际上即使是同一个管理员对设备进行的配置，也会由于各种原因导致配置一致性问题。因此，对整个网络的配置情况进行一致性检查是必需的。

#### (4) 用户操作记录功能

在配置管理中，需要对用户操作进行记录，并保存下来。管理人员可以随时查看特定用户在特定时间内进行的特定配置操作。



## 8.2.2 性能管理

(1)性能监控：由用户定义被管对象及其属性。被管对象类型包括线路和路由器；被管对象属性包括流量、延迟、丢包率、CPU 利用率、温度、内存余量。对于每个被管对象，定时采集性能数据，自动生成性能报告。

(2)阈值控制：可对每一个被管对象的每一条属性设置阈值，对于特定被管对象的特定属性，可以针对不同的时间段和性能指标进行阈值设置。可通过设置阈值检查开关控制阈值检查和告警，提供相应的阈值管理和溢出告警机制。

(3)性能分析：对历史数据进行分析，统计和整理，计算性能指标，对性能状况作出判断，为网络规划提供参考。

(4)可视化的性能报告：对数据进行扫描和处理，生成性能趋势曲线，以直观的图形反映性能分析的结果。

(5)实时性能监控：提供了一系列实时数据采集；分析和可视化工具，用以对流量、负载、丢包、温度、内存、延迟等网络设备和线路的性能指标进行实时检测，可任意设置数据采集间隔。

(6)网络对象性能查询：可通过列表或按关键字检索被管网络对象及其属性的性能记录。

## 8.2.3 故障管理

(1)故障监测：主动探测或被动接收网络上的各种事件信息，并识别出其中与网络和系统故障相关的内容，对其中的关键部分保持跟踪，生成网络故障事件记录。

(2)故障报警：接收故障监测模块传来的报警信息，以报警窗口 / 振铃(通知一线网络管理人员)或电子邮件(通知决策管理人员)发出网络严重故障警报。

(3)故障信息管理：依靠对事件记录的分析，定义网络故障并生成故障卡片，记录排除故障的步骤和与故障相关的值班员日志，构造排错行动记录。

(4)排错支持工具：向管理人员提供一系列的实时检测工具，对被管设备的状况进行测试并记录下测试结果以供技术人员分析和排错。

## 8.2.4 安全管理

安全管理的功能分为两部分，首先是网络管理本身的安全，其次是被管网络对象的安全。



网络管理过程中,存储和传输的管理和控制信息对网络的运行和管理至关重要,一旦泄密、被篡改和伪造,将给网络造成灾难性的破坏。网络管理本身的安全由以下机制来保证:

(1)管理员身份认证,为提高系统效率,对于信任域内(如局域网)的用户,可以使用简单口令认证。

(2)管理信息存储和传输的加密与完整性,对管理信息加密传输并保证其完整性;内部存储的机密信息,如登录口令等,也是经过加密的。

(3)网络管理用户分组管理与访问控制,网络管理系统的用户(即管理员)按任务的不同分成若干用户组,不同的用户组中有不同的权限范围,保证用户不能越权使用网络管理系统。

(4)系统日志分析,记录用户所有的操作,使系统的操作和对网络对象的修改有据可查,同时也有助于故障的跟踪与恢复。

## 8.3 网络管理系统组成

现代计算机网络管理系统主要由四个要素组成:

- 若干被管的代理 ( Managed Agents )
- 至少一个网络管理器 ( Network Manager )
- 一种公共网络管理协议 ( Network Management Protocol )
- 一种或多种管理信息库 ( MIB,Management Information Base )

其中网络管理协议是最重要的部分,它定义了网络管理器与被管代理间的通信方法。目前有影响的网络管理协议是 SNMP ( Simple Network Management Protocol ) 和 CMIS/CMIP ( the Common Management Information Service/Protocol )。它们代表了目前两大网络管理解决方案。其中,SNMP 流传最广,应用最多,获得支持也最广泛,已经成为事实上的工业标准。

## 8.4 网络管理协议

### 8.4.1 SNMP 协议

简单网络管理协议(SNMP)是最早提出的网络管理协议之一,它一推出就得到了广泛的应用和支持,特别是很快得到了数百家厂商的支持,其中包括 IBM, HP, SUN 等大公司 and 厂商。目前大多数网络管理系统和平台都是基于 SNMP 的。

简单网络管理协议 (SNMP : Simple Network Management Protocol ) 是由互联网工程任务组 ( IETF : Internet Engineering Task Force ) 定义的一套网络管理协议。该协议基于简单网关监视协议,利用 SNMP , 一个管理工作站可以远程管理所有支持这种协议的网络设备,包括监视网络状态、修改网络设备配置、接收网络事件警告等。

SNMP 特点 :

- 简单性, 容易实现且成本低;
- 可伸缩性: SNMP 可管理绝大部分符合 Internet 标准的设备;
- 扩展性: 通过定义新的“被管理对象”, 可以非常方便地扩展管理能力;
- 健壮性: 即使在被管理设备发生严重错误时, 也不会影响管理者的正常工作。

## 8.4.2 CMIP 协议

作为国际标准, 由 ISO 制定的公共管理信息协议 ( CMIP ) 着重于普适性 ( Generality )。CMIP 主要针对 OSI 七层协议模型的传输环境而设计, 采用报告机制, 具有许多特殊的设施和能力, 需要能力强的处理机和大容量的存储器, 因此目前支持它的产品较少。但由于它是国际标准, 因此发展前景很广阔。

与 SNMP 相比, 两种管理协议各有所长。SNMP 是 Internet 组织用来管理 TCP/IP 互联网和以太网的, 由于实现、理解和排错很简单, 所以受到很多产品的广泛支持, 但是安全性较差。CMIP 是一个更为有效的网络管理协议, 把更多的工作交给管理者去做, 减轻了终端用户的工作负担。此外, CMIP 建立了安全管理机制, 提供授权、访问控制、安全日志等功能。但由于 CMIP 是由国际标准组织指定的国际标准, 因此涉及面很广, 实施起来比较复杂且花费较高。

## 8.5 网络管理新技术

在过去的十几年中, 通信技术快速发展, 网络正在向智能化、综合化、标准化发展, 先进的计算机技术、ATM 交换技术、神经网络技术正在不断应用到网络中来, 给网络管理提出了新的挑战。与之相适应, 网络管理也在逐渐成熟并日臻完善。下面对网络管理技术的一些新趋势做一个简单的介绍。

## 8.5.1 基于命令行管理技术

通过终端和 TELNET 对单个设备进行管理，它和基于 SNMP 的网络管理不同，命令行着重于对设备的管理。

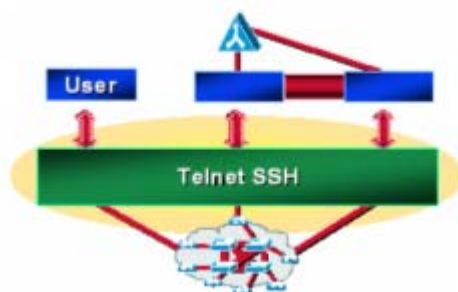


图 8-1 命令行管理

## 8.5.2 基于 Web 的网络管理技术

随着 Web 的流行和技术的发展，可考虑将网络管理和 Web 结合起来。基于 Web 网络管理系统的根本点就是允许通过 Web 浏览器进行网络管理。

这种管理技术的特点如下：

- 通过 WEB Client 和网管系统连接
- 直接在 BROWSER 中完成管理工作
- 可以摆脱网管站的限制
- 由于 WEB 的安全性不够，所以通常只允许读操作，不允许写操作

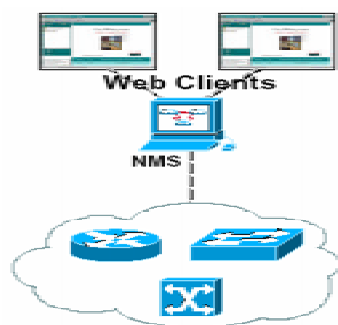
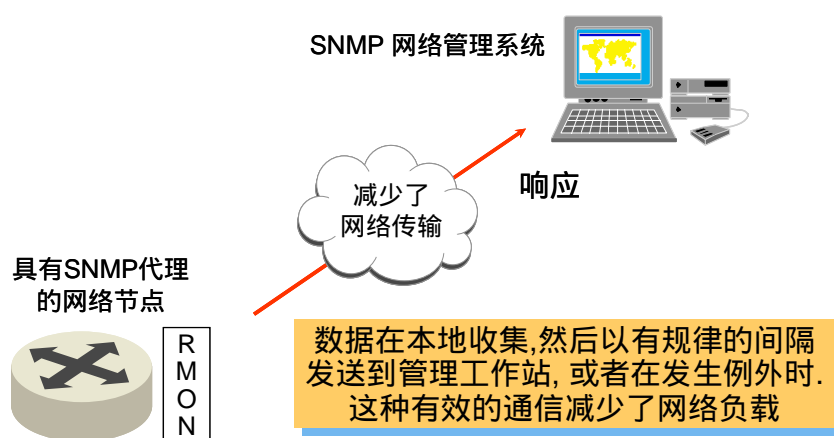


图 8-2 基于 WEB 管理

## 8.5.3 RMON 技术

网络管理技术的一个新的趋势是使用 RMON（远程网络监控）。RMON 的目标是为了扩

展 SNMP 的 MIB - II ( 管理信息库 ), 使 SNMP 更为有效、更为积极主动地监控远程设备。RMON MIB 由一组统计数据、分析数据和诊断数据构成, 利用许多供应商生产的标准工具都可以显示出这些数据, 因而它具有独立于供应商的远程网络分析功能。RMON 探测器和 RMON 客户机软件结合在一起在网络环境中实施 RMON。RMON 的监控功能是否有效, 关键在于其探测器要具有存储统计数据历史的能力, 这样就不需要不停地轮询才能生成一个有关网络运行状况趋势的视图。当一个探测器发现一个网段处于一种不正常状态时, 它会主动与网络管理控制台的 RMON 客户应用程序联系, 并将描述不正常状况的捕获信息转发。如图 8-3 所示。



8-3 RMON 技术

## 8.6 联想 Hyper-manager 网管软件

Hyper-manager 网络管理系统是按照国际规范开发的一套全面面向计算机网络系统的综合管理软件, 适用于园区网络 ( 政府、校园、企业等 ) 和宽带城域网的管理。系统采用 TCP/IP 和 SNMP 协议标准, 以及面向对象的 CORBA / RMI 技术规范。系统将 XML、Java 等先进技术融入其中, 采用业内领先, 具有自主知识产权的技术, 针对各种规模的计算机网络环境, 提供了一整套的网络管理解决方案, 实现网络主干到桌面的端到端的管理。

### 8.6.1 Hyper-manger 特点

- 全中文的操作界面, 简单、易懂;
- 平台级网管软件, 不需要第三方网管即可管理网络;;
- 管理各种厂家 ( 品牌 ) 的设备, 并通过独创的模板技术可迅速识别新的设备;

- 可管理、监视服务器和工作站；
- 完善的地域等级管理以及多种配置工具；
- 应用程序接口，具有强大的二次开发能力；
- 开放性强，用户可以根据自身需要自己开发一些功能；
- 可广泛用于各类电信网、广域网、城域网、局域网等。

## 8.6.2 Hyper-manger 功能

### (1) 自动拓扑

- 能够对单个设备或多个设备进行网络拓扑；如图 8-2 所示。
- 自动以不同的图标表示不同的设备；
- 系统可根据发现的数据自动生成整个网络的拓扑图，如图 8-3。



图 8-2 拓扑单个设备



图 8-3 生成拓扑图

### (2) 配置管理

- 设置 VLAN：利用虚拟网络技术，将工作组组成逻辑子网，大大降低网络维护费用；如图 8-4。
- 端口设置，查看端口。如图 8-5。

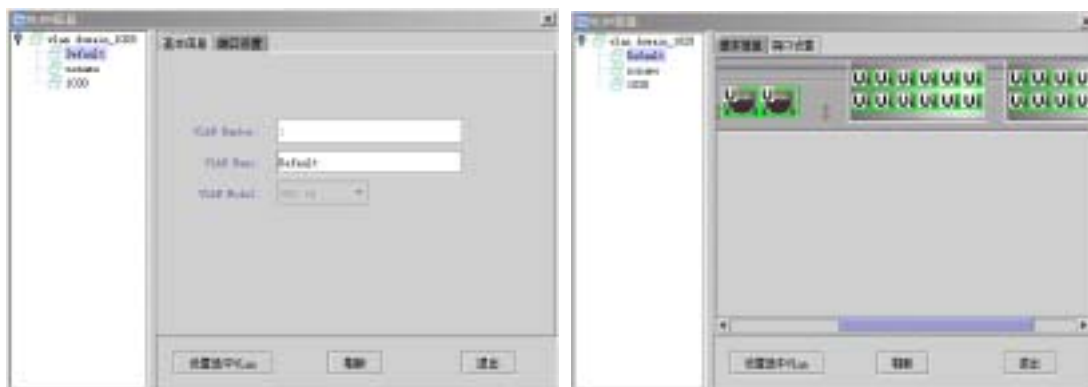


图 8-4 设置 VLAN

图 8-5 端口设置

### (3) 性能管理

通过设备运行情况收集和实时监测网络设备的性能指标实现网络性能管理,包括网络流量、设备吞吐情况,设备 IP 包差错情况,子网或网段丢包情况等,可以实时报警,并以数据表和实时图形曲线方式显示出来,并且可以拓展性能管理的种类。如图 8-6 所示。

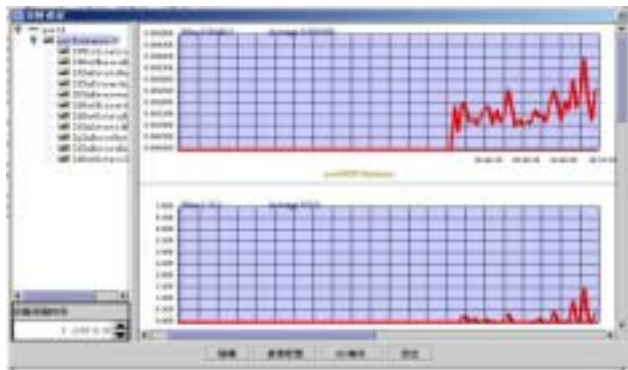


图 8-6 端口流量图

### (4) 故障管理

Hypermanager 通过用户设定的阈值对网络进行轮询或请求/应答方式对整个网络的设备进行监控,当设备有问题时,在拓扑图上以红色表示。如图 8-7 所示。



图 8-7 故障管理

### (5) 地域管理

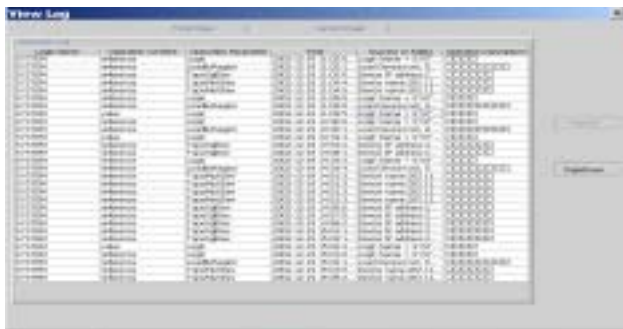
通过该功能能对网络进行分地域设备管理,使整个网络结构更加清晰,有利于系统的维护和故障定位。如图 8-8 所示。



图 8-8 地域管理

### (6) 安全与日志查询

Hypermanager 网络管理系统提供了严格的等级和权限管理，每个管理员只能在其等级和权限范围内操作可分为：用户等级、功能权限、管理权限。系统记录了每个登录进来的管理员的名字及其所作的各种操作，便于日后查询以及出错恢复。



8-9 查询日志

## 8.7 联想 HyperView 网管软件

### 8.7.1 Hyperview 系统特点

- 全中文的操作界面，简单、易懂
- 软件安装简单，不需要过高的设备要求
- 可管理、监视服务器和工作站
- 只要接入网络网络就可以管理、监控网络，实现移动管理
- 适合用于各类大中小型局域网等
- 专门针对联想的交换机使用



## 8.7.2 Hyperview 系统功能

### (1) 多种方式实现网络拓扑图

建立网络拓扑图有三种方法：

- 自动拓扑设备：它可自动发现网络中的可以连通的设备。
- 按 IP 地址段拓扑设备如图 8-10。



图 8-10 IP 地址段拓扑

- 按 IP 地址拓扑设备。如图 8-11。



图 8-11 拓扑单个设备

### (2) 故障报警

### (3) 网络配置管理

可以通过设置端口速度，端口优先级，端口与 MAC 地址绑定来进行网络配置。



图 8-12 设置端口优先级



图 8-13 端口与 MAC 地址绑定

### (4) 性能监控



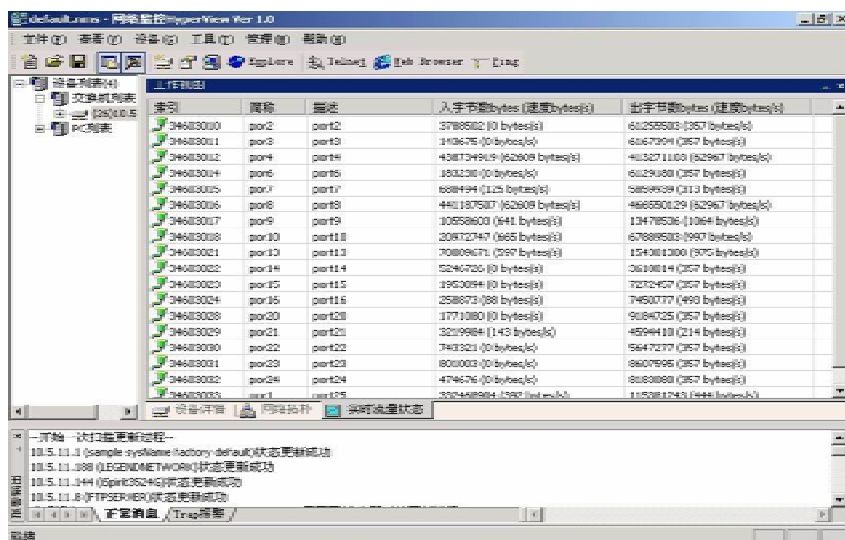


图 8-14 性能监控

## 8.7.3 HyperManager 与 HyperView 区别

### 1、软件运行环境不一样

HyperManager 对服务器的要求比较高，需要后台的 SQL 数据库支持，而 HyperView 对系统要求低，不需要数据库支持；

### 2、适用的范围不一样

HyperManager 一般适合用在管理大型的网络，包括城域网等等，而 HyperView 一般适合与一些园区网络中；

### 3、功能上的区别

HyperManager 比 HyperView 相比较功能上能更强大更全面。

## 第九章 网络安全

随着 Internet 的发展，网络系统安全问题越来越引起世界各国、各行各业的人们的关注，它所涉及的范围非常广泛，小到个人的 PC 机，大到各种网络应用系统（如：政府网络、Internet ISP、ICP、企业 OA 系统、E-business 等）都曾经不同程度地受到攻击和破坏。下面我们将介绍网络安全有关的关键技术。

### 9.1 访问控制技术 ACL

访问控制是网络安全防范和保护的主要策略，它的主要任务是保证网络资源不被非法使用和访问。它是保证网络安全最重要的核心策略之一。访问控制涉及的技术也比较广，包括入网访问控制、网络权限控制、目录级控制以及属性控制等多种手段。

#### （1）入网访问控制

入网访问控制为网络访问提供了第一层访问控制。它控制哪些用户能够登录到服务器并获取网络资源，控制准许用户入网的时间和准许他们在哪台工作站入网。用户的入网访问控制可分为三个步骤：用户名的识别与验证、用户口令的识别与验证、用户账号的缺省限制检查。三道关卡中只要任何一关未过，该用户便不能进入该网络。

#### （2）权限控制

网络的权限控制是针对网络非法操作所提出的一种安全保护措施。用户和用户组被赋予一定的权限。

#### （3）目录级安全控制

网络应允许控制用户对目录、文件、设备的访问。用户在目录一级指定的权限对所有文件和子目录有效，用户还可进一步指定对目录下的子目录和文件的权限。

#### （4）属性安全控制

当用文件、目录和网络设备时，网络系统管理员应给文件、目录等指定访问属性。属性安全在权限安全的基础上提供更进一步的安全性。属性往往能控制以下几个方面的权限：向某个文件写数据、拷贝一个文件、删除目录或文件、查看目录和文件、执行文件、隐含文件、共享、系统属性等。

#### （5）服务器安全控制

网络允许在服务器控制台上执行一系列操作。用户使用控制台可以装载和卸载模块，可

以安装和删除软件等操作。网络服务器的安全控制包括可以设置口令锁定服务器控制台，以防止非法用户修改、删除重要信息或破坏数据；可以设定服务器登录时间限制、非法访问者检测和关闭的时间间隔。

## 9.2 防火墙

防火墙就是一个位于计算机和它所连接的网络之间的软件。该计算机流入流出的所有网络通信均要经过此防火墙。它作为对网络访问进行有效控制的信息安全设备，在对用户的网络访问进行控制的时候，要使用有效的用户认证技术来区分不同的用户身份，以适应不同访问级别的用户对网络访问的不同权限。

### 9.2.1 防火墙功能

防火墙是一类防范措施的总称，它使得内部网络与 Internet 之间或与其它外部网络之间相互隔离，限制网络互访用来保护内部网络，防火墙简单的可以只用路由器实现，复杂的可以用主机甚至一个子网来实现，设置防火墙的目的都是为了在内部网和外部网之间设立唯一通道，简化网络的安全管理。如图 9-1 所示。

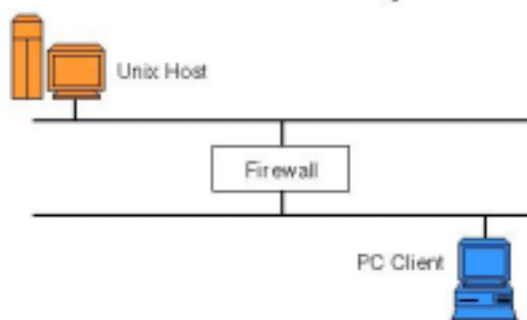


图 9-1 防火墙

防火墙的功能：

- 认证功能

用户通过定制的客户端软件，可以使用电子钥匙自动认证方式或用户手动认证方式，向服务器防火墙证明自己的身份。只有当登录用户成功证明自己的身份，该用户才可以成为防火墙系统的认可的认证用户。

- 支持本地认证或 RADIUS 认证

可以使用本地认证服务器或者第三方的标准 RADIUS 认证服务器。使用 RADIUS 时,支持 RADIUS 的审计功能。

- 用户管理功能

用户可以通过客户端软件修改自己的密码。

- 系统管理员管理功能

系统管理员可以通过 WEB 浏览器管理认证服务器,包括:认证服务器参数的设置,增加/删除/修改本地组和用户;锁定/解除锁定特定的组或用户;设置用户可使用的总的时间和总的流量,时间和流量控制和统计。

- 防火墙系统在线检测

防火墙系统对认证通过的用户且正在使用网络服务的用户还要进行在线检测,当发现在线用户不是刚才的认证用户时,系统会自动断开网络服务的连接。

## 9.2.2 防火墙类型

现有的防火墙主要有:包过滤型、代理服务器型、复合型以及其他类型(双宿主主机、主机过滤以及加密路由器)防火墙。

- 包过滤型防火墙通常安装在路由器上,而且大多数商用路由器都提供了包过滤的功能。

包过滤规则以 IP 包信息为基础,对 IP 源地址、目标地址、封装协议、端口号等进行筛选。包过滤在网络层进行。

- 代理服务器型防火墙通常由两部分构成,服务器端程序和客户端程序。客户端程序与中间节点连接,中间节点再与提供服务的服务器实际连接。与包过滤防火墙不同的是,内外网间不存在直接连接,而且代理服务器提供日志和审计服务。

- 复合型防火墙将包过滤和代理服务两种方法结合起来,形成新的防火墙,由堡垒主机提供代理服务。

## 9.3 以太网运营

以太网运营的主要问题是(如图 9-2 所示):

- 合适的计费方案
- 安全问题
- 维护问题



图 9-2 以太网运营问题

自网络诞生以来，认证（Authentication）、授权（Authorization）以及计费（Accounting）体制（AAA）就成为其运营的基础如图 9-3 所示。网络中各类资源的使用，需要由认证、授权和计费进行管理。而 AAA 的发展与变迁自始至终都吸引着营运商的目光。

认证(Authentication) 用户在使用网络系统中的资源时对用户身份的确认。这一过程，通过与用户的交互获得身份信息（诸如用户名 - 口令组合），然后提交给认证服务器；后者对身份信息与存储在数据库里的用户信息进行核对处理，然后根据处理结果确认用户身份是否正确。例如，GSM 移动通信系统能够识别其网络内网络终端设备的标志和用户标志。

授权(Authorization) 网络系统授权用户以特定的方式使用其资源，这一过程指定了被认证的用户在接入网络后能够使用的业务和拥有的权限，如授予的 IP 地址等。仍以 GSM 移动通信系统为例，认证通过的合法用户，其业务权限（是否开通国际电话主叫业务等）则是用户和运营商在事前已经协议确立的。

计费(Accounting) 网络系统收集、记录用户对网络资源的使用，以便向用户收取资源使用费用，或者用于审计等目的。以互联网接入业务供应商 ISP 为例，用户的网络接入使用情况可以按流量或者时间被准确记录下。



9-3 以太网运营构件

## 9.4 认证技术

当前普遍应用的三种主流认证技术：PPPoE 认证、VLAN+Web 认证和 802.1x 认证。

### 9.4.1 PPPoE 认证

PPPoE 是基于帐号、密码的认证方式，它是从基于 ATM 的窄带网引入到宽带以太网的，在 PPPoE 认证中，认证系统必须将每个包进行拆解才能判断和识别用户是否合法，一旦用户增多或者数据包增大，封装速度必然跟不上，成为了网络瓶颈。其次这样大量的拆包解包过程必须由一个功能强劲同时价格昂贵的设备来完成，这个设备就是我们传统的宽带接入服务器 BAS，为了解决瓶颈问题，厂商想出了提高 BAS 性能，或者采用大量分布式 BAS 等方式来解决问题，但是 BAS 的功能就决定了它是一个昂贵的设备，这样一来建设成本就会越来越高。

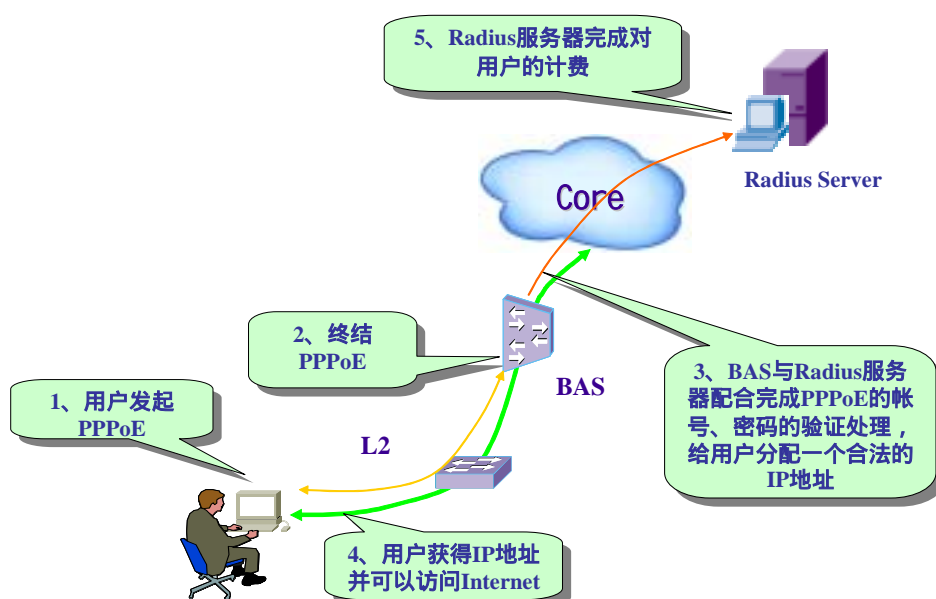


图 9-4 PPPoE 认证

图 9-4 所示为 PPPoE 的认证过程。用户通过 PPPoE 拨号软件输入帐号和密码，宽带接入服务器与 Radius 配合完成用户认证过程，并为用户分配一个合法的 IP 地址。用户即可访问网络，Radius 服务器完成对用户的计费。

## 9.4.2 VLAN+Web 认证

VLAN+Web 认证方式可提供多种增值业务，引起了普遍关注，特点如下：

- 采用帐号和物理位置结合的认证方式；
- 利用 VLAN 隔离和加密保障 Web 认证的安全性；
- 效率高于 PPPoE；
- 通过自动下载的 JAVA 程序替代 PPPoE 虚拟拨号软件，降低维护成本；
- 与业务相关，可作为实现 Portal（门户业务）的基础。

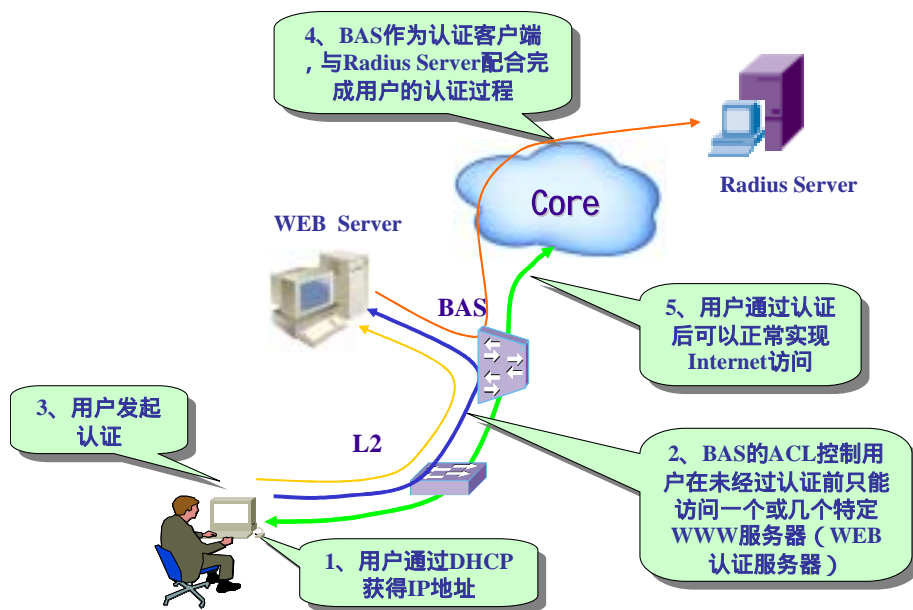


图 9-5 VLAN+Web 认证

图 9-5 为其工作过程。用户开机即通过 DHCP 过程获取 IP 地址，用户通过 Web 认证页面输入用户名和密码，点击“登录”按钮，Web Server 通过 HTTP 协议获取用户输入的用户名和密码信息，然后将用户名和密码通过 Portal 协议发送到接入设备 BAS，接入设备通过 Radius 协议将用户名和密码传送到 Radius Server 进行验证，验证通过后，接入设备将认证通过的信息转发给 Web Server，Web Server 将认证通过的页面下推给用户。



### 9.4.3 802.1X 认证

802.1X 认证是基于端口的访问控制协议，它在 LAN 设备的物理接入级对接入设备进行认证和控制。仅适用于接入设备与接入端口间点到点的连接方式。如图 9-6 所示。

802.1x 协议的体系结构包括三个重要的部分：客户端、认证系统、认证服务器。

- 客户端系统：一般为一个用户终端系统，该终端系统通常要安装一个客户端软件，用户通过启动这个客户端软件发起 802.1x 协议的认证过程。
- 认证系统：通常为支持 802.1x 协议的网络设备（如以太网交换机）。该设备对应于不同用户的端口（可以是物理端口，也可以是用户设备的 MAC 地址、VLAN、IP 等）有两个逻辑端口：受控（controlled Port）端口和不受控端口（uncontrolled Port）。不受控端口始终处于双向连通状态，可保证客户端始终可以发出或接受认证。受控端口只有在认证通过的状态下才打开，用于传递网络资源和服务。
- 认证服务器：通常为 RADIUS 服务器，该服务器可以存储有关用户的信息，比如用户所属的 VLAN、CAR 参数、优先级、用户的访问控制列表等等。当用户通过认证后，认证服务器会把用户的相关信息传递给认证系统，由认证系统构建动态的访问控制列表，用户的后续流量就将接受上述参数的监管。

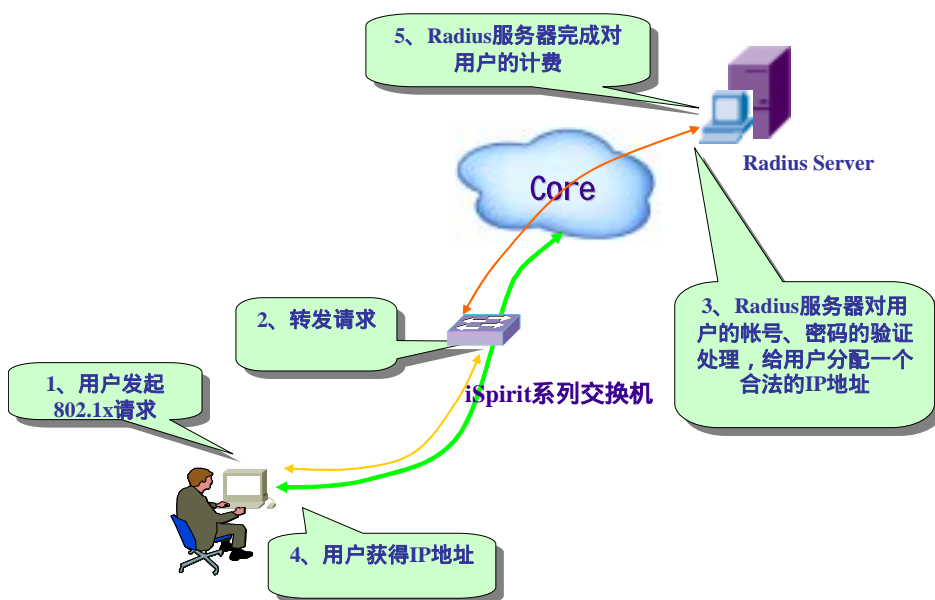


图 9-6 802.1X 认证

802.1X 特点如下：

- 简洁高效：纯以太网技术内核，保持 IP 网络无连接特性，去除冗余昂贵的多业务网关设备，消除网络认证计费瓶颈和单点故障，易于支持多业务。



- 容易实现：可在普通 L3、L2、IP DSLAM 上实现，网络综合造价成本低。
- 安全可靠：在二层网络上实现用户认证，结合 MAC、端口、账户和密码等；绑定技术具有很高的安全性。
- 行业标准：IEEE 标准，微软操作系统内置支持。
- 易于运营：控制流和业务流完全分离，易于实现多业务运营，少量改造传统包月制等单一收费制网络即可升级成运营级网络。

## 9.5 计费系统概述

基于宽带网的接入和各种增值服务，正在全球范围内兴起。联想网络针对宽带网运营商当前与今后中长期的需求，开发了“宽带网运维平台软件联想网络 HYPER BOSS”软件系统。

计费管理系统主要解决运营商在网络运营中对计费、业务、用户，公司机构、职员、网络配置、网络资源管理的需求。

### 9.5.1 为什么进行计费管理

- 用户开户/销户、欠费停止上网业务没有办法实现
- 没有办法实施有区别的资费标准，不利于发展用户
- 不能实施卡号业务、帐号业务
- 维护困难，没有用户位置信息表
- 用户彼此可见，存在安全隐患
- 同一终端无法区分多个用户，不适合学校、酒店.....
- IP 地址、MAC 等资源被终端控制

### 9.5.2 联想 Hyper-boss 的特色

- 差别计费，提高初装率增加运营收入
- 用户管理维护、基于位置、帐号的用户数据库
- 网络安全性
- 用户之间访问的控制

- 网络服务，地址冲突、网络资源盗用、服务器资源的安全性
- 带宽管理，差别服务

9.5.3 Hyper-boss 的功能

(1) 普通受理

对普通客户开展业务是普通受理的主要内容，在这一部分包含了付费、开户、销户、变更、暂停、恢复、客户密码重置，以及客户服务管理。如图 9-7 所示。

客户信息	
客户号	1001
证件类型	A710
开户证件类型	SVST690
真实姓名	陈雅
当前地址	湖北孝感
联系电话	027076022094
注册地址	南湖康乐苑
邮编	430079
工作单位	武汉光谷软件园
证件类型	身份证
证件号码	43062580011010102
性别	男
出生日期	1980-01-01
电子邮箱	2504902140@hotmail.com
电子邮箱	高申是高中以下
MAC地址	08:00:4c:73:32:0f
IP地址	202.114.33.88
SLA等级	3

已办业务	
业务号	internet
业务名称	包月
计费标准	活动状态

图 9-7 普通受理

(2) 卡业务管理

有关卡的业务管理包括：卡套餐管理，卡类型管理和卡配置管理，管理卡，查询卡信息。如图9-8所示。

计费套餐	
名称	包月卡
描述	
所属地区	湖北
套餐类型	卡用户套餐
计费方式	只计算月租费
基本月租费	200

图 9-8 卡业务管理

(3) 查询功能

该模块是为客户提供了对客户、客户、职员、帐务等进行查询的功能，以及对设备、属地、职员进行浏览。界面情况如图 9-9 所示。

查询客户

账号	<input type="text"/>
客户号	<input type="text"/>
真实姓名	<input type="text"/>
证件类型	<input type="text"/>
证件号码	<input type="text"/>
属 地	<input type="text"/>
创建职员账号	<input type="text"/>
联系电话	<input type="text"/>
备 注	<input type="text"/>
创建时间	从 <input type="text"/> 到 <input type="text"/>
最后更新	从 <input type="text"/> 到 <input type="text"/>

开始查询

重置填写

（本系统一次查询记录条数不能超过10000行）

图 9-9 查询功能

（4） 帐务管理

此模块提供了帐务方面的各种管理功能。可以进行明细、综合帐单的查询，修改帐户，反销帐，托收处理，查看帐户关系图等，如图9-10。

账号(选):

查 询

明细帐单查询

<input checked="" type="checkbox"/>	当前记录周期的上月费用明细帐单
<input type="checkbox"/>	上月费用明细帐单(最近一个记录周期的记录)
<input type="checkbox"/>	最近 <input type="text"/> 个记录周期的上月费用明细帐单
<input type="checkbox"/>	2002 <input type="text"/> 月的上月费用明细帐单

确定

图9-10 帐务管理

（5） 报表管理

报表管理系统提供了尽可能多的手段及时、准确的反映宽带网的运营状况。可对运营数据进行分类统计：各个属地，各职员下的客户数情况统计、Internet 业务情况分析统计、计费套餐使用情况分析统计、帐户分析统计。如图 9-11。

制定各属地普通客户报表

所在属地*	<input type="text" value="ROOT"/>
执行时间*	<input type="text" value="1"/> 日 <input type="text" value="1"/> 时 <input type="text" value="0"/> 分

增加

重新填写

图 9-11 报表管理

（6） 系统管理

系统管理主要包括与计费系统运行有关的一些重要信息的配置，由属地管理、职员管

理、计费套餐管理、日志管理，系统制定,安全管理以及服务管理组成。可以进行对属地，职员，套餐，日志的增加，删除，修改等操作。

## 9.5.4 业务管理

计费管理系统主要用于：

- 卡业务
- 酒店业务小区业务
- 专线业务
- 代理商业务

图 9-12 为酒店管理模式

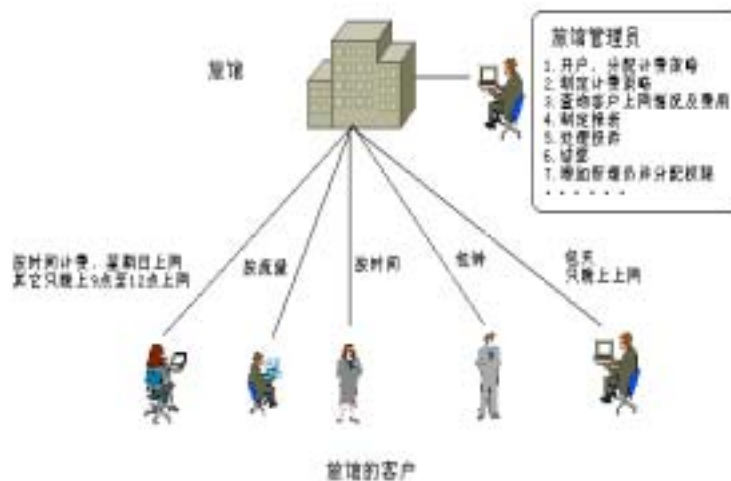


图 9-12 酒店管理模式

## 第十章 企业网络解决方案

### 10.1 网络的设计思想

要建设大型的、性能优良的、具有很强扩展能力和升级能力的综合网络，在设计中就必須采用层次化的网络设计原则。

在网络设计中，采用网络层次化的优点：

- 可扩展性：使网络可模块化增长而不会遇到问题；
- 简单性：通过将网络分成许多小单元，降低了网络的整体复杂性，使故障排除更容易；
- 设计的灵活性：使网络容易升级到最新的技术，升级任意层次的网络不会对其他层次造成影响，无需改变整个环境；
- 可管理性：层次结构使单个网络设备的配置的复杂性大大降低，更易管理。

### 10.2 网络层次结构

从逻辑上分，网络可分为核心层、分布层和接入层，每层都有其特点。一些小型的网络可能就把其中的相邻两层功能合而为一。

下图 10-1 为网络的三层结构示意图。

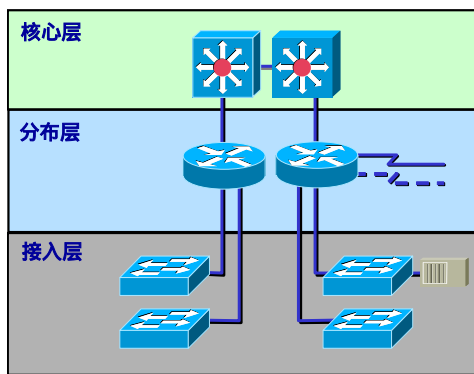


图 10-1 网络结构图

#### 10.2.1 核心层的功能及设计

核心层为下两层提供优化的数据输运功能，它是一个高速的交换骨干，其作用是尽可能快地交换数据包而不卷入到具体的数据包的运算中，否则会降低数据包的交换速度。

- 核心层作用：把多个边缘汇聚层连接起来，为汇聚层网络提供数据的高速转发，成为整个网络的核心。
- 设计考虑因素：  
可靠性（中心故障，网络全部瘫痪）；  
可扩展性（今后可以平滑的升级）；  
开放性（可以和采用不同技术的骨干网络互联）。
- 特点：大容量交换，快速路由转发，高背板，可冗余。

### 10.2.2 汇聚层的功能及设计

汇聚层又称分布层，它是核心层和访问层的分界点，对数据包进行复杂的运算。在园区网络环境中，分布层主要提供如下功能：地址的聚集，部门和工作组的接入，广播域/多目传输域的定义，VLAN 路由，任何介质的转换，安全控制，QoS。

- 汇聚层作用：  
完成本地业务的区域汇接；  
进行带宽和业务汇聚、收敛及分发；  
进行用户管理，通过识别定位用户实现；  
基于用户的访问控制和带宽许可；  
提供安全保证和灵活的计费方式；  
可网管。
- 特点：智能，大容量汇聚，端口密度大。

### 10.2.3 接入层的功能及设计

接入层的主要功能是为最终用户提供对园区网络访问的途径。本层也可以提供进一步的调整，如访问列表过滤等。在园区网络环境中，接入层主要提供如下功能：带宽共享，交换带宽，MAC 层过滤，网段微分。

- 接入层作用：直接连接用户，实现用户对网络的接入。
- 设计考虑因素：易管理、维护，可以实现简单的端口聚合，端口隔离，简单的网络管理或者仅仅具有接入功能。

## 10.3 方案设计

主要考虑以下因素：

- 用户的投资
- 用户的需求分析，在网络中开展的业务
- 综合布线的情况

## 10.4 联想网络解决方案

### 10.4.1 校园网典型方案

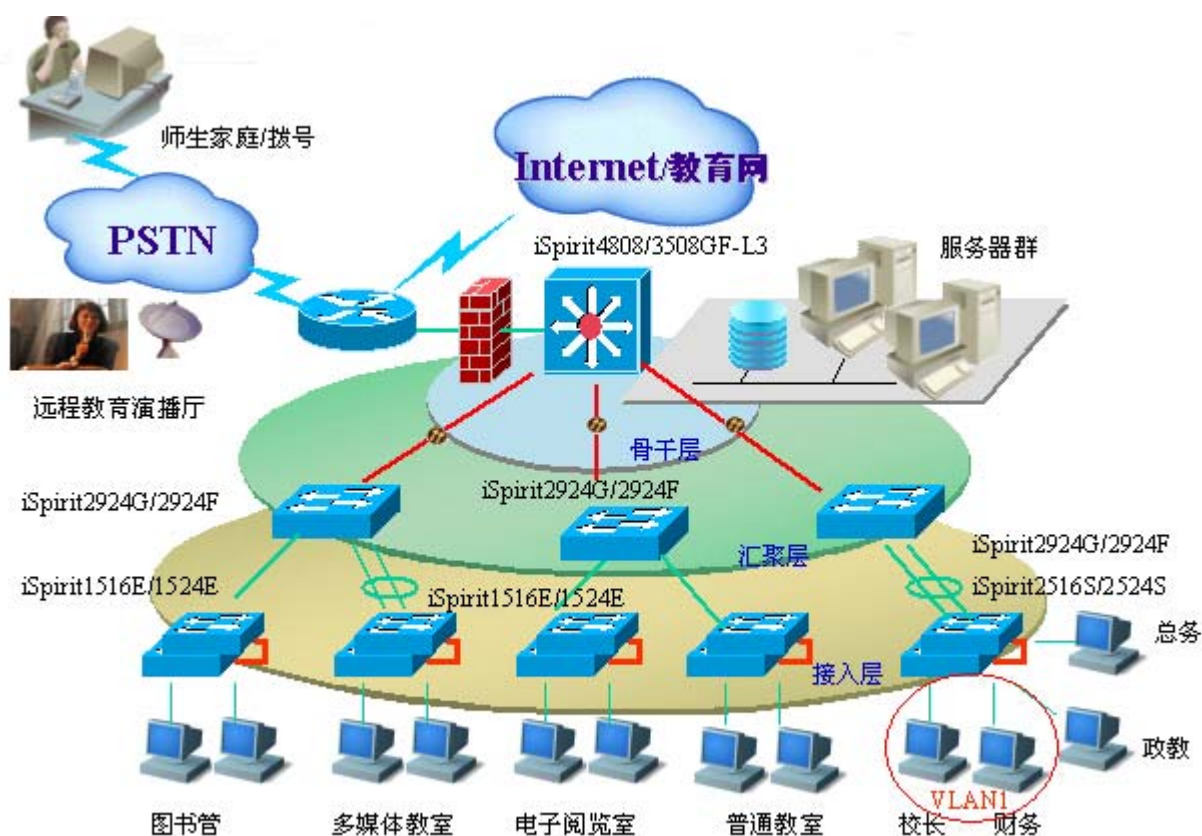


图 10-2 校园网方案

该方案主干采用基于第三层交换的千兆以太网，百兆到桌面的建设思想。中心交换机采用根据学校的网络规模选择相应的核心交换设备，多层高性能 iSpirit t4808 适合大中型校园网络，iSpirit t3508GF-L3 适合中小型千兆校园网络主干，分布层的节点交换机采用



i spirit 2924G, 距离较远的节点交换机和主干交换机之间采用千兆光纤连接, 这样网络在设计上既达到性能上的要求, 又节省了资金。各个楼层的办公交换机使用 i spirit 的 2500 系列快速交换机, 可以基于学校的职能部门进行安全 VLAN 划分。在多媒体教室、电子阅览室采用 15 系列的快速桌面交换机。

## 10.4.2 企业网方案

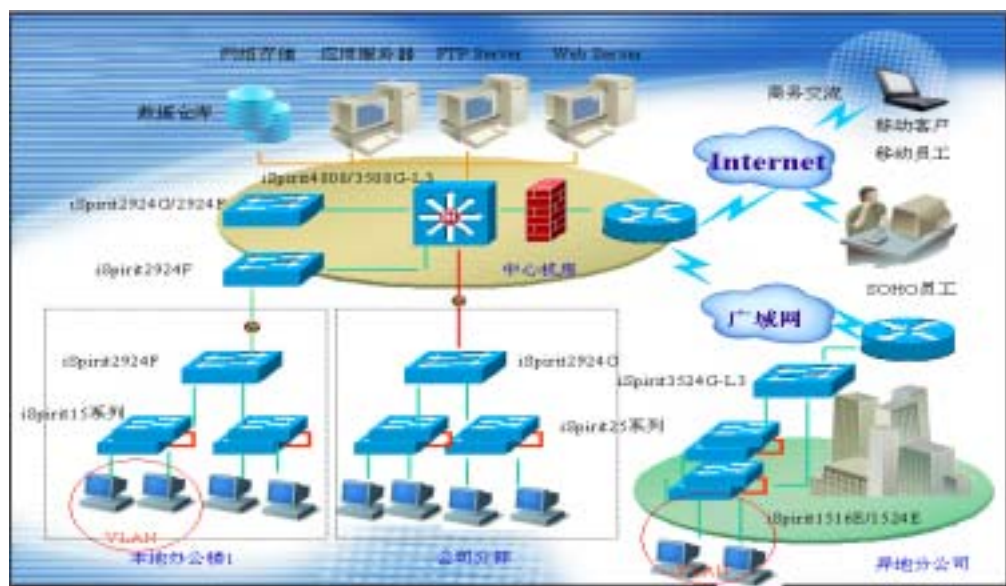


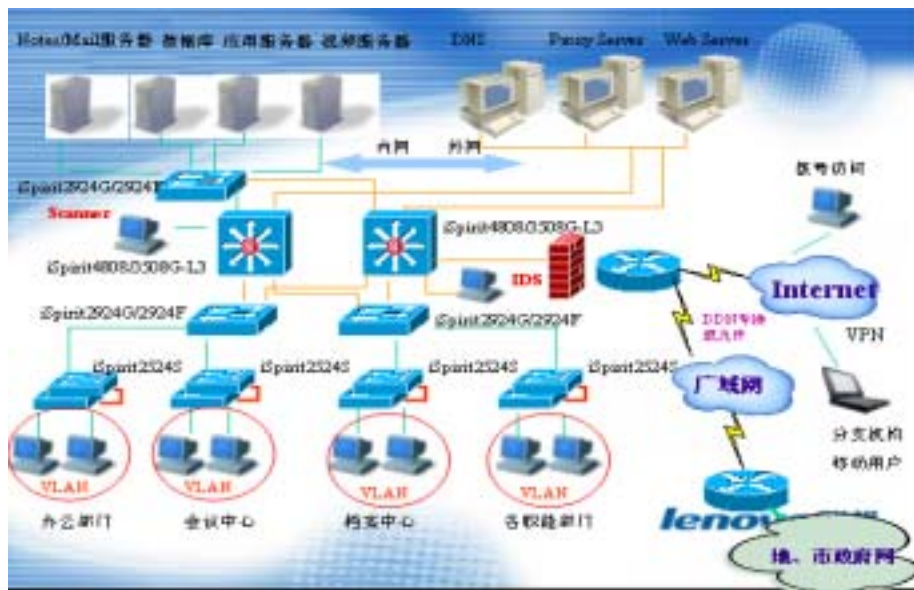
图 10-3 企业网方案

企业网络的建设关系到网络时代企业发展的未来,它是今后电子商务的基石,电子商务是中小企业计算机网络的未来,它能使企业降低运作成本,提高竞争力,实现利益最大化。

企业网主干采用基于第三层交换的千兆以太网,根据企业网络规模选择相应的核心交换设备,由于这个企业的数据库及各种资源、网站全部放在中心机房,所以高性能的主干交换首当其冲,多层高性能 i spirit 4808 适合大型企业网络, i spirit 3508GF-L3 适合中小型千兆企业网络主干。距离较近的办公楼日常办公网络数据流量不大的可以采用 i spirit 2924F 百兆光纤上联到中心机房,距离较远的流量较大的本地公司分部采用 i spirit 2924G 千兆多模光纤链接到公司中心机房。接入级交换机可以采用 25 系列和 15 系列的快速以太网交换机。对于异地的公司机构以及移动的员工和 SOHO 员工可以有 PSTN、ISDN、ASDL、数字专线等远程接入方式。



### 10.4.3 政务网方案



10-4 政务网方案

电子政务的实现，首先要在各级的政府机构内建立内部的物理网络体系结构，建立基于网络的以数据库为核心的电子化信息发布、信息搜集、信息反馈系统，同时将信息发布系统与政府机构的内部办公自动化系统融为一体，提供决策支持。

整个核心层采用联想网络的高性能多层交换机 i spirit t6808 或者三层全千兆骨干交换机 i spirit t4808，采用星型连接拓扑结构，保证网络的可靠运行。汇聚层主要任务是将接入层大量的工作组交换机，桌面交换机汇聚在一起，通过多条千兆以太网上联到网络中心。I spirit t2924G/2924F 拥有 12Gbps 的交换背板，提供 24 个 RJ-45 的 10/100M 自适应端口和可扩展的千兆上联端口，保障数据的无阻塞传输。接入层主要任务是为接入电子政务网络中心数量极大的网络用户提供大量性价比极高的 10/100 兆网络接口，并与汇聚层通过 100 兆和千兆链路互连为接入的用户提供高速上联。采用 i spirit t25 系列交换机具有支持 VLAN 和 Trunking 的功能，可以为部门提供高速的上联和端口隔离功能，保证网络的使用带宽和安全性。

## 10.5 成功案例

### 10.5.1 重庆网通信息港解决方案

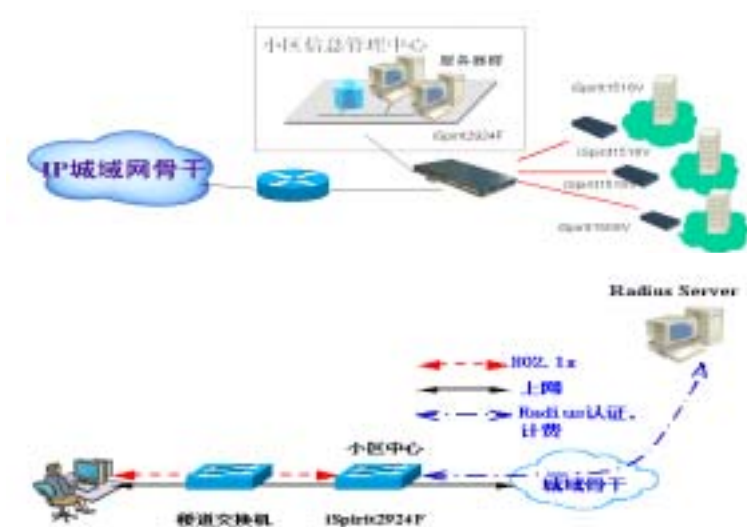


图 10-6 重庆网通信息港小区宽带运营网

小区交换机采用具有流量控制功能的交换机，能根据用户需求灵活配置用户使用带宽，对定制灵活的资费政策提供支持。

接入采用高性能的 Ispirit1508V 交换机或 Ispirit1516V 二层交换机，能真正实现 100M 交换机到桌面，提供对设备完善的管理，避免利用集线器带宽共享的问题，性能稳定，功能完善，结构简单，易管理，同时各设备对环境有很强的适应能力。

接入交换机采用窗口隔离 Ispirit1508V 交换机或 Ispirit1516V 交换机，能有效保证终端用户数据安全。

重庆信息港建设的宽带小区中大量使用了联想网络具有 802.1X 认证功能的 Ispirit2924F，它可为宽带运营商网通提供安全可靠便捷的用户认证机制。802.1X 协议在宽带 L2 上支持，主要用于端口的认证，即通过认证之后才能够使接入端口可用。

## 10.5.2 贵港政务网方案

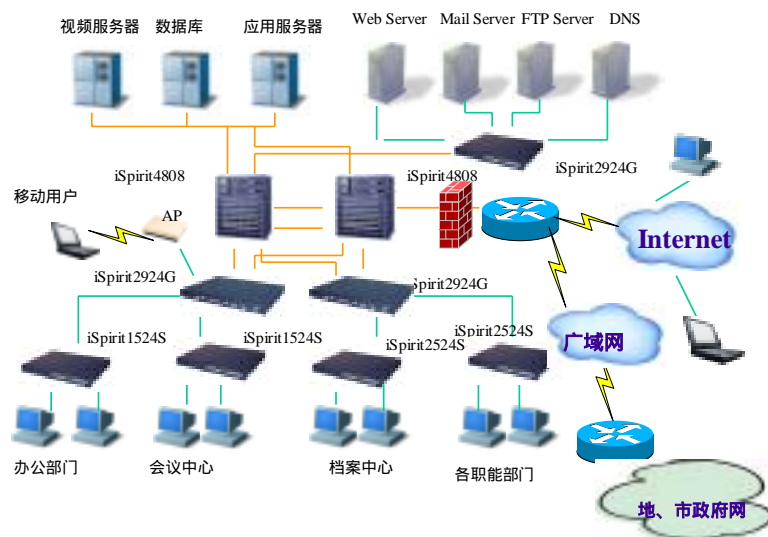


图 10-7 贵港政务网解决方案

“政府上网”将带来政府办公模式与观念上的一次革命。那种为了办成一件事而要到处盖上几十个公章的现象将不复存在，如深圳已经实现了网上交税。在政府内部，各部门之间也可以通过 Internet 联系，各级领导可以在网上相隔部门做出各项批示与指导，从而既提高了办事效率，又节省了政府开支。

采用两级设计方案，第一级为核心汇聚层。采用 1 台多层核心以太网交换机 iSpirit4808 系列构成主干，为政府网络的核心服务器，如文件数据库服务器、电子邮件服务器、VOD 服务器和 Web 服务器等提供 1000M 的网络带宽。为网络主干提供了三层路由、多层应用和强大的吞吐能力。第二级为接入层，则采用超级堆叠技术，由多台 iSpirit 2924G 交换机堆叠在一起的交换机组构成。使每个交换机组具有良好的可扩充性，同时为每个工作站提供 100M 的交换带宽。每个交换机堆叠通过设备提供的千兆上联模块与网络主干交换机形成 1000M 的连接。这样，就形成了主干 1000M、100M 交换到桌面的高性能的政府网络环境。广域网络部分则采用路由器通过光纤与 Internet 公网形成连接。

### 10.5.3 闵行区中小学网络系统

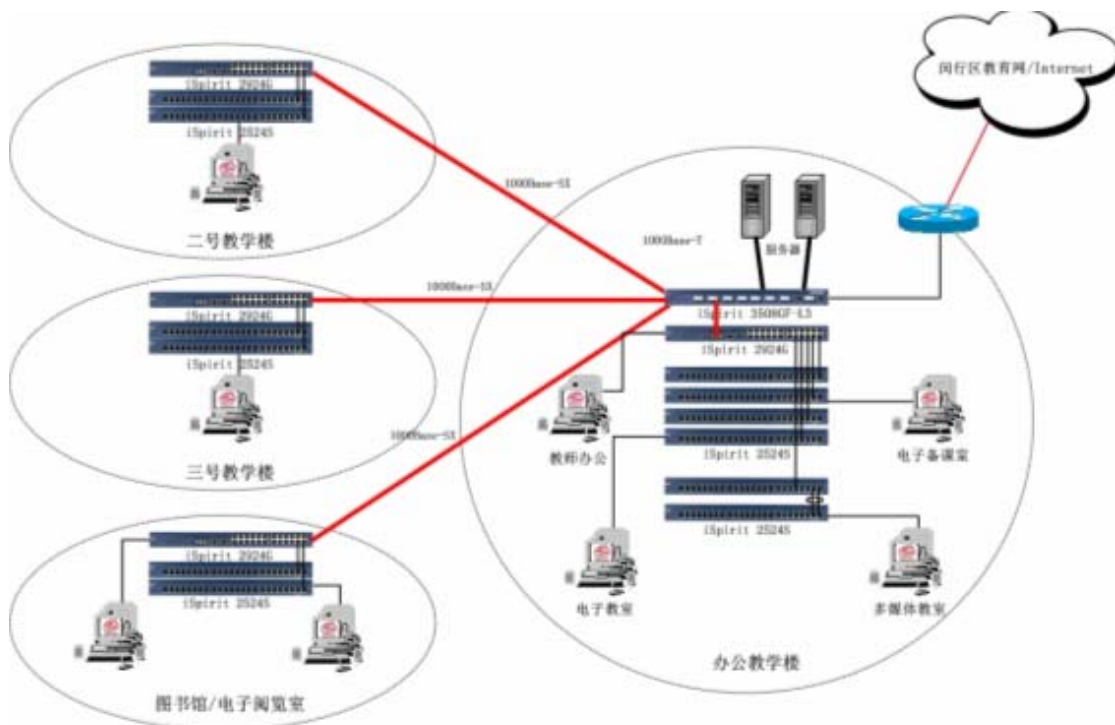


图 10-8 闵行区中小学网络系统（大规模）

闵行区校园网络系统平台满足下列需要：

- 建立 INTRANET（内联网）
- 为多媒体教学提供数据交换服务
- 为电子阅览室提供数据交换服务
- 为电子备课室提供数据交换服务
- 为电子教室提供数据交换服务
- 多服务集成，能够为声音、视像和数据提供集成服务
- 在主干网络可划分虚拟局域网
- 考虑未来扩展能力及多厂商、多协议的支持能力

## 10.5.4 珠海校校通工程

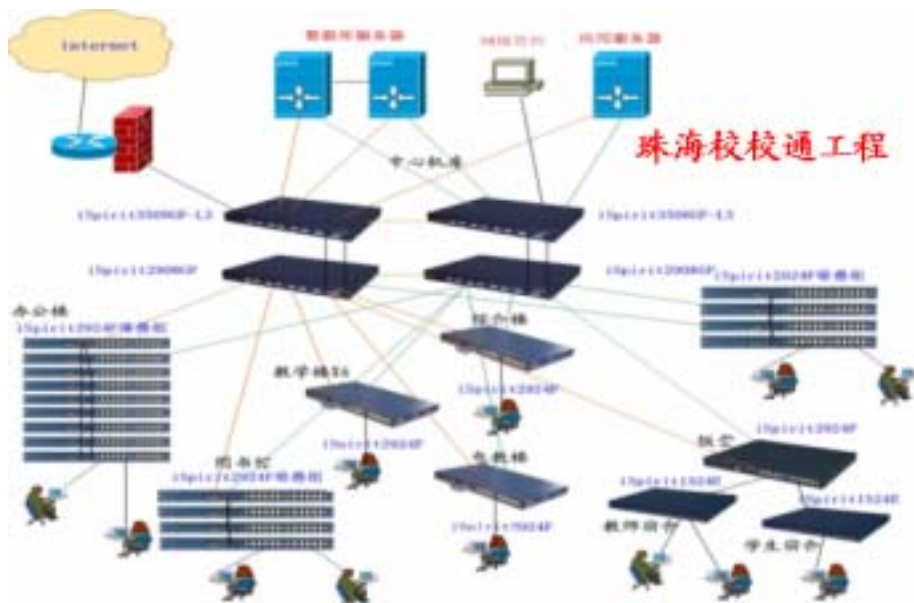


图 10-9 珠海校校通工程

一个校园网络基本上是由网络服务器、教育终端、网络互联设备、网络管理软件以及应用软件等环节组成的。

该方案采用三级设计方案，第一级为核心层。采用 1 台三层千兆以太网交换机 iSpirit 3508GF-L3 和 2 台全千兆以太网交换机 iSpirit 2908GF 构成主干，为校园网络的核心服务器，如文件数据库服务器、电子邮件服务器、VOD 服务器和 Web 服务器等提供 1000M 的网络带宽。为网络主干提供了三层路由和强大的吞吐能力。第二、三级为汇聚接入层，对于教学楼、电教楼则采用外背板级连技术，由 1 台 iSpirit 2924F 交换机和多台以太网交换机 iSpirit 1524E 在一起的交换机组构成。使每个交换机组具有良好的可扩充性，同时为每个工作站提供 100M 的交换带宽。每个交换机堆叠通过设备提供的千兆上联模块与网络主干交换机形成 1000M 的连接。对于这样，就形成了主干 1000M、100M 交换到桌面的高性能的校园网络环境。广域网络部分则采用路由器通过光纤与 Internet 公网形成连接。

### 10.5.5 武汉市武昌区教育城域网

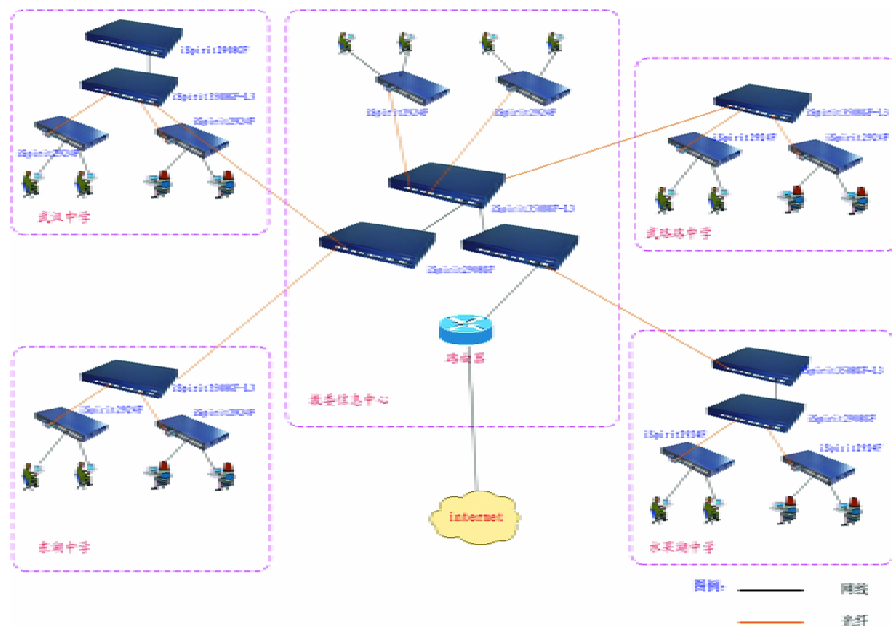


图 10-10 武昌区教育城域网

武昌区教育城域网采用了全套联想的网络产品，整个城域网包括区教委信息中心和武汉中学、水果湖、武珞路、东湖中学四个二级接入节点。信息中心和四个二级接入节点之间采用单模光纤，构成千兆的网络主干。

整个网络采用扩展星型拓扑结构，中心交换机和各个二级接入节点交换机采用联想 iSpirit 3508GF 全千兆三层交换机，配置千兆单模光纤模块，实现信息中心与各二级接入节点之间的千兆连接，由此组成整个网络的千兆交换骨干，实现分布式路由。

通过 802.1x 协议进行用户认证和计费。



## 10.5.6 上海交大 985 工程

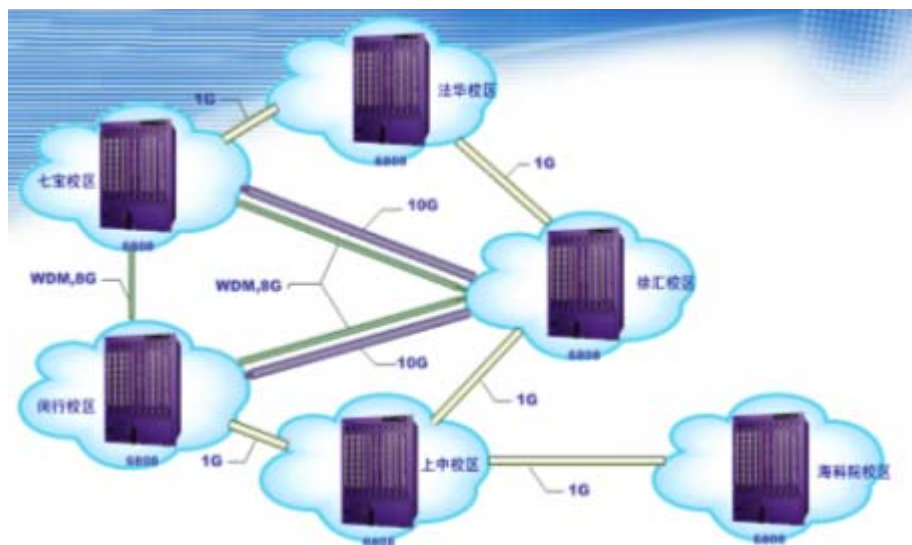


图 10-11 上海交大 985 工程

新方案采用联想 WDM 和万兆以太网技术，共覆盖 6 个校区，校区间最远传输距离为 34 公里，骨干节点校区采用 WDM 技术形成环型网络，其它校区分别与骨干节点采用千兆技术进行冗余连接，保证了整个网络的高可靠性、先进性、高可靠性，可扩展性等，由于整个网络具有很高的连接带宽，加之联想设备无以伦比的处理能力，以及业界领先的 Qos 服务质量保证，使得在整个网络上不仅可以传输传统的数据，同时还可开展视频、语音的应用，真正做到三网融合。

## 10.5.7 山东电信城域网

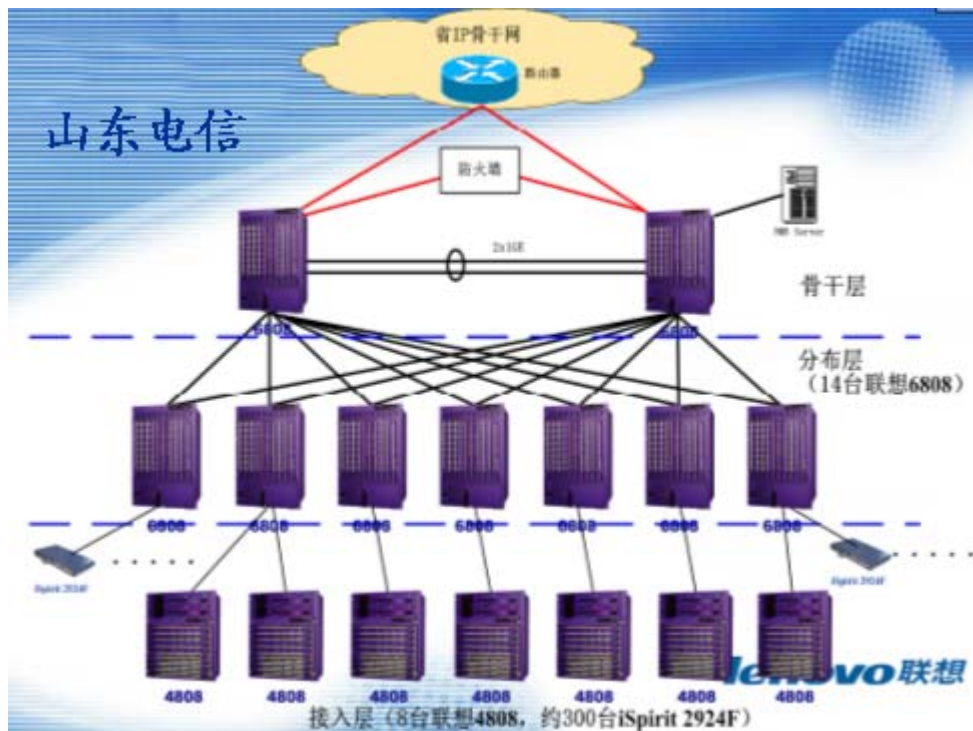


图 10-12 山东电信城域网

该方案采用星型拓扑结构，城域网核心层采用两台联想 iSPIRIT 6808 构成双核心冗余系统，形成带宽为 2G 的核心骨干，在分布层也采用联想 iSPIRIT 6808 作为分布层交换机，通过千兆光纤分别接入双核心交换机，接入层采用 iSPIRIT 4808 交换机，通过千兆端口接入分布层设备，市城域网通过联想路由器连入省骨干网。



## 10.5.8 南京广电城域网

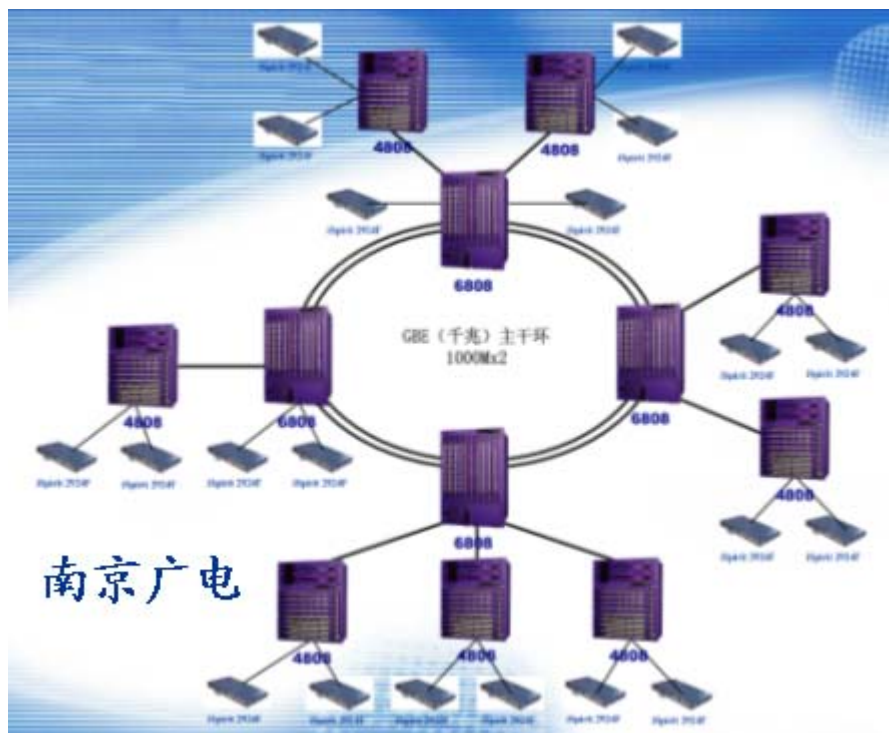


图 10-13 南京广电城域网

宽带 IP 城域网主要提供 IP 为主的数据业务，如超大容量电视节目传送，多点视频、视频广播、电子商务、远程教育等。

按照南京广电城市规划，全市有四个核心站点，骨干层为双环结构，可提供 2G 带宽，该城域网中，远期共覆盖用户 80 万户，每个核心站点覆盖用户 20 万户。每个核心站点下设 4 个二级站点，带宽为 1G，每个二级站点覆盖的用户约为 5 万户左右。

## 第 11 章 专业名词

### 11.1 通信名词

- ADSL (Asymmetric Digital Subscriber Line): 非对称数字用户线  
它是一种通过现有普通电话线为家庭、办公室提供宽带数据传输服务的技术。它能够在现有的普通电话线上提供高达 10Mbps 的下行速率, 远高于 ISDN 速率。
- ARP (Address Resolution Protocol): 地址解析协议  
为已知的 IP 地址确定数据链路层的地址。
- ATM (Asynchronous Transfer Mode): 异步传输模式  
ATM 是一种高性能的数据通信协议, 它既可传输普通数据, 也可传输声音、图象、视频等信息。
- BGP (Border Gateway Protocol): 边界网关协议  
BGP 是为 TCP / IP 互联网设计的外部网关协议, 用于多个自治域之间。
- CSMA/CD (Carrier Sense Multi-Access/Collision Detection): 载波侦听多路访问/冲突检测  
它是一种常用介质访问方法, 采用总线结构进行传输。
- DNS (Domain Name System): 域名系统  
它是一种分布式数据库系统, 广泛用于 INTERNET 和其它 TCP/IP 互连网络中。
- DDN (Digital data network): 数字数据网  
随着数据通信业务发展而迅速发展起来的一种新型网络。可以向用户提供点对点、点对多点透明传输的数据专线出租电路。
- EGP (Exterior Gateway Protocol): 外部网关协议  
外部网关协议是指自治系统之间的路由选择协议, 主要用于多个 ISP 共同管理的网络。
- FDDI (Fiber Distributed Data Interface): 光纤分布式数据接口  
在光纤上传送数据的标准, 速率约为 100Mbps。
- FTP (File Transfer Protocol): 文件传输协议  
在两个 Internet 站点间传递文件的常用方法。
- HDLC (High-Level Data Link Control): 高级数据链路控制协议  
ISO 标准的链路层协议

- HTTP (HyperText Transfer Protocol ): 超文本传输协议  
在 Internet 中传递超文本文件的协议。
- ICMP (Internet Control Message Protocol ): 网际控制信息协议  
它提供了发送差错和控制消息的功能。
- IGMP (Internet Group Management Protocol ): Internet 组管理协议  
允许一个或多个发送者发送单一的数据包到多个接收者（一次的，同时的）的网络技术。
- IGP (Interior Gateway Protocol ): 内部网关协议  
内部网关协议是指运行在一个自治系统内部的，一般适用由单个组织（ISP）管理的网络，常见协议有 RIP/RIP2，OSPF。
- IP (Internet Protocol ): 因特网协议  
定义两个主机之间传送数据的方式，是一种不可靠传输。
- ISDN (Integrated Services Digital Network ): 综合业务数字网  
20 世纪 70 年代出现的通信服务，用户利用一条 ISDN 用户线路，可以在上网的同时拨打电话、收发传真，就像两条电话线一样。
- LAN (Local Area Network ): 局域网
- LLC (Logical Link Control ): 逻辑链路控制
- MAC (Media Access Control ): 介质访问控制
- MAN (Metropolitan Area Network ): 城域网
- OSPF (Open Shortest Path First ): 开放最短路径优先(协议)  
适用于较大规模的路由协议，其路由算法的核算单位基于多种链路特性（包括延迟、带宽、损耗等），这样经过 OSPF 算法得出的最佳路径要比 RIP 算法更完善与更加准确。
- PSTN (Public Switched Telephone Network ): 公用电话交换网  
一个老式的电话系统。
- QoS (Quality of Service ): 服务质量  
服务质量 (Quality of Service) 是传输系统的性能度量，反映了其传输质量以及服务的可获得性。它主要靠 RSVP（资源预留协议）及 802.1P 来保证。
- RARP (Reverse Address Resolution Protocol ): 逆向地址解析协议  
用于数据链路层地址已知时，确定网络地址。
- RIP (Routing Information Protocol ): 路由信息协议

是 Internet 中常用的路由协议。它是一种内部路由协议。

- RMON (Remote Network Monitoring): 远程网络管理

为了扩展 SNMP 的 MIB - II (管理信息库), 使 SNMP 更为有效、更为积极主动地监控远程设备。

- SMTP (Simple Mail Transfer Protocol): 简单邮件传输协议

Internet 发送电子邮件的主要协议, 它定义了一个程序如何发送和接收邮件的规则。

- SNMP (Simple Network Management Protocol): 简单网络管理协议

与连接在 TCP/IP 网络上的设备进行通信的一组标准, 这些设备可以是交换机、路由器、集线器等。

- STP (Spanning Tree Protocol): 生成树协议

解决因网络循环连接造成的网络风暴、同时也为网络备份提供可能。

- TCP (Transmission Control Protocol): 传输控制协议

提供端到端可靠数据传输

- Telnet: 是一段 TCP/IP 终端仿真协议。

- UDP (User Datagram Protocol): 用户数据报协议

它对接收的包不应答, 是传输层使用的一种不可靠的数据通信协议。

- VLAN (Virtual LAN): 虚拟局域网

将区域分散的组织在逻辑上成为一个新的工作组, 而且同一工作组的成员能够改变其物理地址而不必重新配置节点

- VPN (Virtual Private Network): 虚拟专用网络

是专用网络在公共网络如 Internet 上的扩展。有了 VPN, 用户在家里或在路途中也可以利用 Internet 或其他公共网络对企业服务器进行远程访问。

- WAN (Wide Area Network): 广域网

## 11.2 IEEE802 标准

IEEE802.1: 局域网 (LAN) 和城域网 (MAN) 控制

IEEE802.2: LAN 逻辑链路控制

IEEE802.1D: Spanning Tree

IEEE802.1P: Quality of Service

IEEE802.1Q : VLAN Tagging

IEEE802.3 : LAN 和 MAN : CSMA/CD 访问方法和物理层规范

IEEE802.3U : 快速以太网

IEEE802.3Z, 802.3ab : 千兆以太网

IEEE802.3X : 流量控制

IEEE802.11 : 无线局域网标准及物理层和媒体访问控制(MAC)协议的规范

IEEE802.12 : 交换式以太网

## 10.3 交换机常用参数

- 背板吞吐量 ( bps )

也称背板带宽,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。一台交换机的背板带宽越高,所能处理数据的能力就越强,但同时设计成本也会上去。

- 包转发率 : 包转发速率 : 交换机的一项性能参数,指的是交换机每秒所能转发帧或者包的速度。

- MAC 地址表

连接到局域网上的每个端口或设备都需要一个 MAC 地址,其它设备要用到此地址来定位特定的端口及更新路由表和数据结构。MAC 地址有 48 字节长,由 IEEE 来分配,又叫物理地址。一个设备的 MAC 地址表(如图 7-19)大小反映了连接到该设备能支持的最大节点数。

- 缓存

缓存也叫缓冲区,是一种应用于存储器上的队列结构。交换机用缓冲区来协调不同网络设备之间传输速度的不同。

- Uplink(级联)

级联是通过集线器(或交换机)的某个端口与其它集线器或交换机相连的,级联后每台集线器或交换机在逻辑上仍是多个被网管的设备。通过级联端口相连的设备不需要 Cross-over 电缆。

- Stackable(堆叠)

堆叠是通过集线器的背板或是通过专用堆叠线缆连接起来的。堆叠后的数台集线器或交换机在逻辑上是一个被网管的设备。

- Flow Control (流量控制)

为防止计算机网络中信息传输出现拥挤而采取的一种措施。流量控制可在网络的多个层次上实现。

- Full-duplex(全双工)

全双工是在通道中同时双向数据传输的能力。

- Half-duplex(半双工)

在通道中同时只能沿着一个方向传输数据。

- Port Mirror(端口镜像)

Port Mirror 是用于进行网络性能监测。可以这样理解：在端口 A 和端口 B 之间建立镜像关系，这样，通过端口 A 传输的数据将同时复制到端口 B，以便于在端口 B 上连接的分析仪或者分析软件进行性能分析或故障判断。

- Port Trunking(端口干路)

Port Trunking 即将交换机上的多个物理端口，在逻辑上捆绑(bundle)在一起，形成一个拥有较大带宽的端口，组成一个干路。可以均衡负载，并提供冗余连接。

- Multicast(组播)

广播中组播是向选定目标发送信息的处理过程。对于广播信号，所有设备都准备好随时接收，而与广播不同的是组播仅对那些预先设置可以接收组播的网络节点进行有效传送。