第3章 智能建筑内的计算机网络

本章导读

智能建筑内的计算机网络是高速的数据通信网，可以实现数字设备之间的高速数据通信，也可以实现语音和视频信号的数字化传输，或者说，可以实现多媒体通信。它是智能建筑系统集成的平台，是信息传输网的核心。

智能建筑内的计算机网络技术是局域网，传输速率已达 10Gbps，目前的技术可保证到端点的传输速率为 1000Mbps，因此，智能建筑内的计算机网络是一个高速的 IP 网络。通过局域网上的网关/路由器就可以实现与互联网和各种广域计算机网的联接。

在一个智能建筑内实际上构建了多个局域网，每一个局域网完成一类通信服务，如控制专网、安防专网、涉密办公网、公用信息网等。这样做的原因是：隔离带来了安全，降低了网络通信流量。局域网和局域网之间可以有目的地互联起来，使网络的安全性受到控制。计算机网络系统为管理与维护提供相应的网络管理系统，并提供高密度的网络端口，可满足用户容量分批增加的需求。

随着网络技术的飞速发展，从数据和信号的角度来看，目前的各种模拟传输业务均可能经过数字化后在计算机网络上传输。例如，VoIP 可以支持传统的电话通信业务，IPTV 可以支持有线电视业务。也就是说，将来只需要建一个高速 IP 网络，就能实现多种业务的传输。

本章主要介绍当前主流局域网技术以及局域网互联、宽带接入技术，然后介绍计算机网络平台及构建方案，最后对网络管理和安全进行简介。

本章的重点和难点是在所学的网络技术基础上进行智能建筑内的计算机网络方案设计和集成。

3.1 智能建筑内的计算机局域网技术

在智能建筑内构建计算机网络主要是应用局域网以及局域网互联技术。局域网是一组由计算机和其他网络设备互联在一起而形成的系统，其覆盖区域限于建筑物内或建筑群内，允许网络内部的用户之间相互高速通

信,并共享计算机的软硬件资源。局域网通常由网络接口卡、电缆(光缆)系统、交换机、服务器以及网络操作系统等部分组成。决定局域网特性的技术要素包括网络拓扑结构、传输介质类型、介质的访问控制以及安全管理等。当前的技术主流是以太网。

3.1.1 局域网标准

1. 局域网体系结构

IEEE 802是局域网的技术标准。局域网在通信方面有自己的特点:第一,其数据是以帧为单位传输的。第二,局域网内部一般不需中间转接,所以也不要求路由选择。因此,局域网的参考模型对应于OSI参考模型中的最低两层,如图3-1所示,实现了OSI模型最低两层的功能。其中,物理层用来建立物理连接,数据链路层把数据构成帧进行传输,并实现帧顺序控制、错误控制及流控制功能,使不可靠的链路变为可靠的链路。

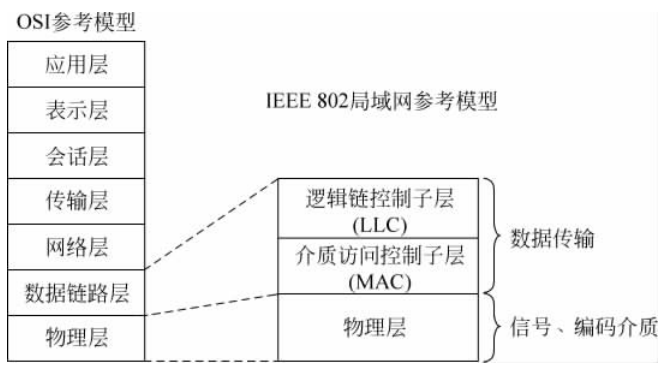

图3-1 IEEE 802局域网参考模型与OSI参考模型

(1) 物理层。负责在物理层实体间发送和接收位流,提供发送和接收信号的能力、对宽带的频道分配和对基带信号的调制等。

(2) 数据链路层。该层又细分为两个功能子层:逻辑链控制(Logical Link Control,LLC)子层和介质访问控制(Media Access Control,MAC)子层。这种功能分解主要是为了使数据链功能中与硬件有关的部分和与硬件无关的部分分开。

MAC子层与物理层相邻,为物理层访问提供接口。MAC子层负责对介质的访问控制,为用户分配信道使用权,具有管理多个源和目的链路的功能。IEEE 802制定了几种介质访问控制方法,同一个LLC子层能与其中任一种访问方法接口,目前这些介质访问控制方法包括载波监听冲突检测多重访问(CSMA/CD)、令牌总线(token-bus)及令牌环(token-ring)等访问方法。

LLC子层在MAC子层的支持下向网络层提供服务。LLC子层与具体的传输介质无关,这种独立于介质的访问控制方法屏蔽了各种IEEE 802网络连接之间的

差别，向网络层提供一个统一的格式和接口。LLC 子层的功能包括数据帧的组装与拆卸、帧的收发、差错控制、数据流控制和发送顺序控制等，并为网络层提供两种类型的服务——面向连接服务和无连接服务。

2. IEEE 802 标准

IEEE 802 是一个标准系列，包含多个协议，其组成如图 3-2 所示。

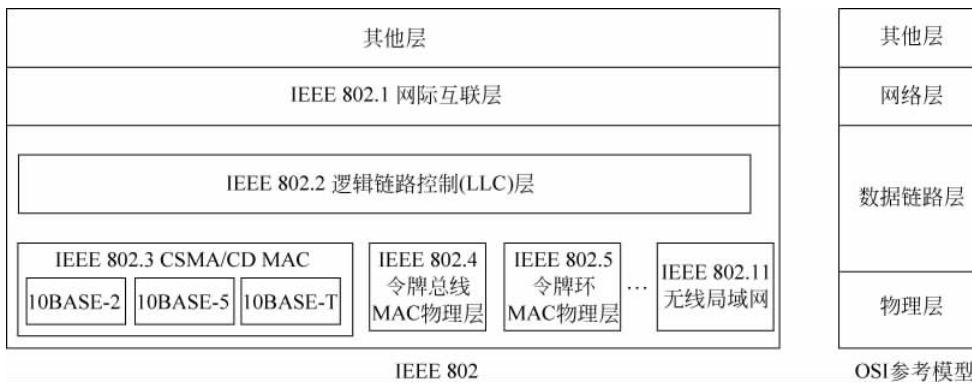

图 3-2　IEEE 802 协议栈

3.1.2　以太网和快速以太网

1. 以太网

以太网(Ethernet)是当今最流行的局域网，采用 CSMA/CD 介质访问方式进行通信访问，网络的速率是 10Mbps。虽然现在构建的局域网几乎已不再应用 10Mbps 以太网技术，但是考虑到与以前所建系统的兼容性，我们仍有必要了解 10Mbps 以太网技术 10BASE-T。

10BASE-T 以太网所采用的传输介质为 3 类、4 类和 5 类 UTP，其相关标准见表 3-1。网络结构为以集线器(hub，现在采用交换机)为节点的星形拓扑结构。

表 3-1　以太网(IEEE 802.3)UTP 介质标准

标准要求	10BASE-T	100BASE-TX	100BASE-T4	100BASE-T2	1000BASE-T
数据速率	10Mbps	100Mbps	100Mbps	100Mbps	1000Mbps
介质要求	3 类 100m 4 类 140m 5 类 150m	5 类 100m	3 类 100m 4 类 100m 5 类 100m	3 类 100m 4 类 100m 5 类 100m	5 类 100m
使用电缆对数	2	2	4	2	4
插座接线模式	1.2 和 3.6	1.2 和 3.6	全部线对	1.2 和 3.6	全部线对

10BASE-T要求每台计算机都有一块网络接口卡与一条从网卡到集线器的直接连接。图3-3表明了10BASE-T布线方案。尽管所有集线器都能容纳多台计算机,但集线器还是有许多种尺寸。一个典型的小型集线器有24个端口,每个提供一条连接。这样,一个集线器能在一个小组中连接所有计算机(如在一个部门中)。较大的集线器能容纳几百条连接。

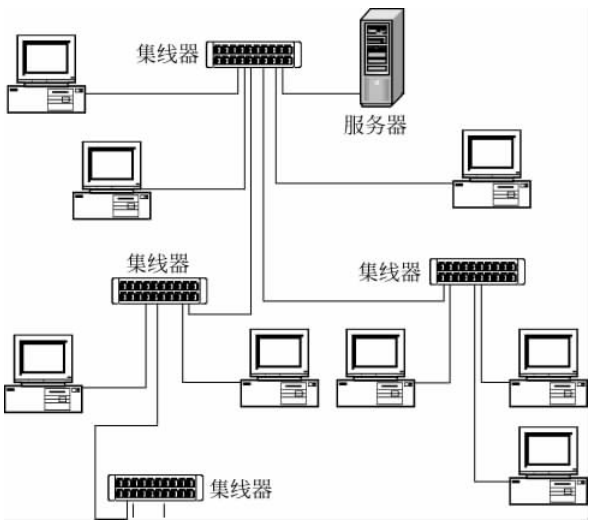

图3-3 10BASE-T以太网

2. 100BASE-T快速型以太网

可以说,100BASE-T是双绞线以太网的100Mbps速率版,它的标准为IEEE 802.3u,它是现行IEEE 802.3标准的补充。有3个不同的100BASE-T物理层规范,其相关标准见表3-2,其中两个物理层规范支持长度为100m的无屏蔽双绞线,第三个规范支持单模或多模光缆。与10BASE-T和10BASE-F一样,100BASE-T要求有中央集线器的星形布线结构。

表3-2 不同100Mbps快速以太网介质标准

标准要求	100BASE-TX	100BASE-T4	100BASE-FX
距离/m	100	100	2000
拓扑结构	星形	星形	星形
介质	5类UTP或STP	3/4/5类UTP	多模或单模光缆
要求线对数	2	4	2
编码方法	4B/5B	8B/6T	4B/5B
信号频率/MHz	125	25	125

100BASE-T的MAC(介质访问方式)与10Mbps“经典”以太网MAC几乎完全一样,正如前面所述,IEEE 802.3 CSMA/CD MAC具有固有的可缩放性,即它可以

以不同速度运行，并能与不同物理层连接。

100BASE-TX 物理层支持快速以太网运行在 5 类 2 对 UTP 或 1 类 STP 上。100BASE-T4 物理层支持快速以太网运行在 3 类、4 类或 5 类的 4 对 UTP 上。100BASE-FX 支持多模或单模光缆布线，这样快速以太网就能在 2km 的距离内传输信息。

100BASE-T4 是为完全迎合庞大的 3 类音频级布线安装需要而设计的。100BASE-T4 使用 4 对音频级或数据级无屏蔽 3 类、4 类或 5 类电缆。由于信号频率只有 25MHz，也可使用音频级 3 类线缆。100BASE-T4 使用所有的 4 对无屏蔽双绞线，3 对线用来同时传送数据，而第 4 对线用来作为冲突检测时的接收信道。与 10BASE-T 和 100BASE-TX 不同，它没有单独专用的发送和接收线，所以不可能进行全双工操作。

100BASE-T4 为目前大量的 10Mbps 以太网向 100Mbps 快速以太网过渡提供了极大方便，大多数情况下只需要更换网卡和集线器，而不需要重铺电缆线。

3.1.3　千兆以太网

1. 千兆以太网标准

千兆以太网是建立在以太网标准基础之上的技术，它与快速以太网和标准以太网完全兼容，并利用原以太网标准所规定的全部技术规范，其中包括 CSMA/CD 协议、帧格式、流量控制以及 IEEE 802.3 标准中所定义的管理对象等。为了实现高速传输，千兆以太网定义了千兆介质专用接口(GMII)，从而将介质子层和物理层分开，使得当物理层的传输介质和编码方式变化时不会影响到介质子层。千兆以太网技术有两个标准——IEEE 802.3z 和 IEEE 802.3ab。IEEE 802.3z 为光纤和同轴电缆的全双工链路方案的标准，IEEE 802.3ab 为非屏蔽双绞线的半双工链路标准。

2. 千兆以太网介质

千兆以太网可采用 4 类介质：1000BASE-SX(短波长光纤)、1000BASE-LX(长波长光纤)、1000BASE-CX(短距离铜缆)、1000BASE-T(100m 4 对 6 类 UTP)，其介质标准如表 3-3 所示。

表 3-3　千兆以太网介质标准

标准要求	1000BASE-SX	1000BASE-LX		1000BASE-CX	1000BASE-T
介质	多模光纤(62.5μm 或 50μm)	多模光纤(62.5μm 或 50μm)	单模光纤(9μm 或 10μm)	150Ω STP	5 类 UTP，4 对
工作波长/nm	770～860	1270～1355	1270～13 550		
距离/m	220～550	550	5000	25	100

其中,1000BASE-SX使用短波长(850nm)激光的多模光纤,1000BASE-LX使用长波长(1300nm)激光的单模和多模光纤。使用长波长和短波长的主要区别是传输距离和费用。不同波长传输时信号衰减程度不同。短波长传输衰减大,距离短,但节省费用;长波长可传输更长的距离,但费用高。1000BASE-CX为150Ω平衡屏蔽的特殊电缆集合,线速为1.25Gbps,使用8B/10B编码方式。

3. 1000BASE-T

1000BASE-T是100BASE-T的自然扩展,与10BASE-T、100BASE-T完全兼容。1000BASE-T规定可以在5类4对平衡双绞线上传送数据,传输距离最远可达100m。1000BASE-T的重要性在于:可以直接在100BASE-TX快速以太网中通过升级交换机和网卡实现千兆到桌面,而不需要重铺电缆线。

1000BASE-T是专门为在5类双绞线上传送数据而设计的。1000BASE-T与100BASE-T采用相同的传送时钟频率(125MHz),但是利用了一种更加复杂的信号传输和编/解码机制——PAM-5码,每个符号(5级脉冲幅度调制,取+2,+1,0,-1,-2之一)对应两位二进制信息(其中4级表示两位,一级用于前向纠错码)。1Gbps的传送速率可以等效地看作分布在4对双绞线上(4×125Mbps×2=1Gbps)。

4. 千兆以太网应用

千兆以太网的光纤连接方式解决了楼层干线的高速连接,1000BASE-T千兆以太网技术用来解决桌面之间的高速连接。

千兆以太网可用于高速服务器之间的连接、建筑物的高速主干网、内部交换机的高速链路以及高速工作组网络。

由于千兆以太网采用大家熟悉的技术,是一种从目前普遍采用的以太网技术平滑过渡到千兆以太网的技术,是10Mbps和100Mbps以太网技术的自然扩展,因此有很好的应用前景。图3-4所示是某高校图书馆计算机网络系统集成方案。

3.1.4 万兆以太网

1. 万兆以太网的标准

2002年,IEEE 802委员会通过了万兆以太网(10Gigabit Ethernet)标准IEEE 802.3ae,定义了3种物理层标准:10GBASE-X、10GBASE-R、10GBASE-W。

1) 万兆物理层标准

10GBASE-X为并行的局域网物理层标准,采用8B/10B编码技术,只包含一个规范:10GBASE-LX4。为了达到10Gbps的传输速率,使用稀疏波分复用(CWDM)技术,在1310nm波长附近以25nm为间隔,并列配置了4对激光发送器/接收器组成的4条通道,每条通道的10B码的码元速率为3.125Gbaud。10GBASE-LX4使用

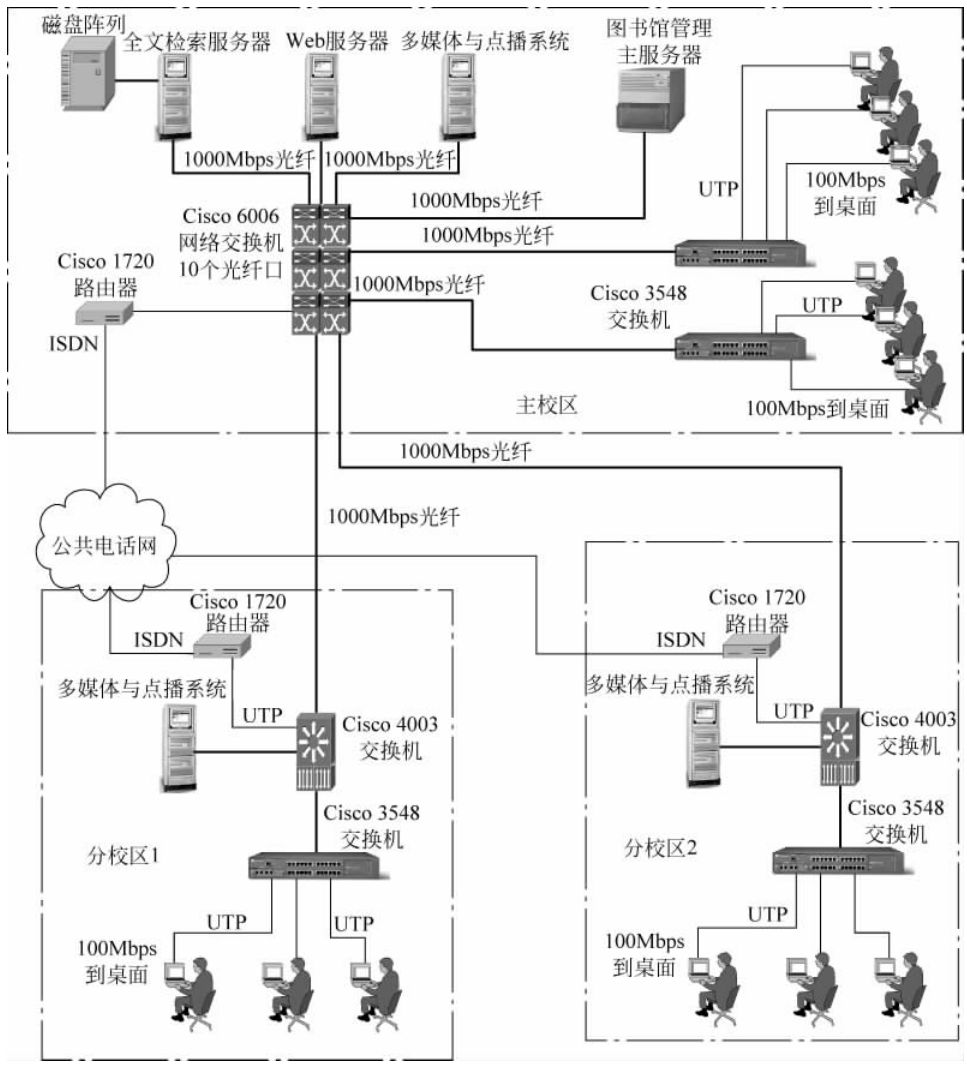

图 3-4　千兆以太网应用案例

多模光纤和单模光纤的传输距离分别为 300m 和 10km。

10GBASE-R 为串行的 LAN 类型的物理层标准，使用 64B/66B 编码格式，包含 3 个规范：10GBASE-SR、10GBASE-LR、10GBASE-ER，分别使用 850nm 短波长、1310nm 长波长和 1550nm 超长波长。10GBASE-SR 使用多模光纤，传输距离一般为几十米；10GBASE-LR 和 10GBASE-ER 使用单模光纤，传输距离分别为 10km 和 40km。

10GBASE-W 为串行的 WAN 类型的物理层，采用 64B/66B 编码格式，包含 3 个规范：10GBASE-SW、10GBASE-LW 和 10GBASE-EW，分别使用 850nm 短波长、1310nm 长波长和 1550nm 超长波长。10GBASE-SW 使用多模光纤，传输距离一般为几十米；10GBASE-LW 和 10GBASE-EW 使用单模光纤，传输距离分别为 10km 和 40km。

除上述3种物理层标准外,IEEE还制定了一项使用铜缆的称为10GBASE-CX4的万兆以太网标准IEEE 802.3ak,可以在双芯同轴电缆上实现10Gbps的信息传输速率,提供数据中心的以太网交换机和服务器群的短距离(15m之内)10Gbps连接的经济方式。10GBASE-T是另一种万兆以太网物理层,通过6/7类双绞线提供100m内的10Gbps的以太网传输链路。

万兆以太网的介质接口标准如表3-4所示。

表3-4 万兆以太网介质标准

接口类型	应用范围	传送距离	波长	介质类型
10GBASE-LX4	局域网	300m	1310nm	多模光纤
10GBASE-LX4	局域网	10km	WDM	单模光纤
10GBASE-SR	局域网	300m	850nm	多模光纤
10GBASE-LR	局域网	10km	1310nm	单模光纤
10GBASE-ER	局域网	40km	1550nm	单模光纤
10GBASE-SW	广域网	300m	850nm	多模光纤
10GBASE-LW	广域网	10km	1310nm	单模光纤
10GBASE-EW	广域网	40km	1550nm	单模光纤
10GBASE-CX4	局域网	15m	—	4根Twinax线缆
10GBASE-T	局域网	25～100m	—	双绞铜线

2) MAC子层标准

万兆以太网仍采用IEEE 802.3数据帧格式,维持其最大、最小帧长度。

由于万兆以太网只定义了全双工方式,所以不再支持半双工的CSMA/CD的介质访问控制方式,也意味着万兆位以太网的传输不受CSMA/CD冲突域的限制,从而突破了局域网的概念,进入广域网范畴。

2. 万兆以太网优势

与千兆以太网相比,万兆以太网有哪些优势?过去有时候需采用数个千兆以太网捆绑以满足交换机互连所需的高带宽,因而浪费了更多的光纤资源,现在可以采用万兆以太网互连,甚至4个万兆以太网捆绑互连,达到40Gbps的宽带水平。

在愈来愈多的服务器改采用千兆以太网作为上连技术后,数据中心或群组网络的骨干带宽相应增加,以千兆以太网或千兆以太网捆绑作为平台已不能满足需求,升级到万兆以太网在服务质量及成本上都将占有相对的优势。万兆以太网也可以在其他多媒体应用,如VOD视频点播或多媒体制作领域寻找更多的应用空间。

万兆以太网在技术上基本承续过去的以太网、快速以太网及千兆以太网的技术,因此在用户的普及率、使用的方便性、网络的互操作性及简易性上皆占有极大的优势,在升级到万兆以太网解决方案时,用户不需担心既有的程序或服务受到影响,因此升级的风险是非常低的,这可以从过去以太网一路升级到千兆以太网中得到证

明，同时在未来升级到万兆以太网，甚至四万兆以太网(40G)、十万兆以太网(100G)，这都将是一个很明显的优势。

以太网采用 CSMA/CD 机制，即带碰撞检测的载波监听多重访问。千兆以太网接口基本应用在点到点线路，不再共享带宽。碰撞检测、载波监听和多重访问已不再重要。千兆以太网与传统低速以太网最大的相似之处在于采用相同的以太网帧结构。万兆以太网与千兆以太网类似，仍然保留了以太网帧结构。通过不同的编码方式或波分复用提供 10Gbps 传输速度。所以就其本质而言，万兆以太网仍是以太网的一种类型。万兆以太网与千兆以太网的比较如表 3-5 所示。

表 3-5　万兆以太网与千兆以太网的比较

对比项目	千兆以太网	万兆以太网
应用方面	汇聚、接入层	核心层，具有 SDH 接口
工作模式	CSMA/CD＋全双工	只支持全双工
编码方式	8B/10B	新的 64B/66B
传输媒介	光纤/铜线	只支持光纤(将来支持铜线)
传输距离/km	5	40

3. 40G/100G 以太网标准

40G/100G 以太网标准是 IEEE 802.3ba，将包含这两个速度的规范。每种速度将提供一组物理接口：40Gbps 将有 1m 交换机背板链路、10m 铜缆链路和 100m 多模光纤链路标准；100Gbps 将有 10m 铜缆链路、100m 多模光纤链路和 10km、40km 单模光纤链路标准。

4. 400Gbps 带宽的下一代以太网传输标准

2013 年 4 月 2 日，IEEE 宣布组建新的 IEEE 802.3 Standard for Ethernet 工作组，探讨制定 400Gbps 带宽的下一代以太网传输标准，400Gbps 以太网标准是 IEEE P802.3bs，尚未获批发布。工作组近期主要工作是制定 100m 多模光纤、500m 单模光纤、2km 单模光纤、10km 单模光纤的相关标准。

5. 万兆以太网应用

图 3-5 是某大学城校园计算机网络系统集成方案，采用万兆以太网作为建筑群网络主干，实现接入层(楼层)与网络中心的高速数据交换。还可通过链路汇聚技术实现主干交换机之间、主干交换机和接入层交换机之间更高的网络带宽，以满足不同的应用系统要求。楼层内可通过快速以太网技术实现 100Mbps 交换到桌面，完全满足当前及将来的计算机应用需求。

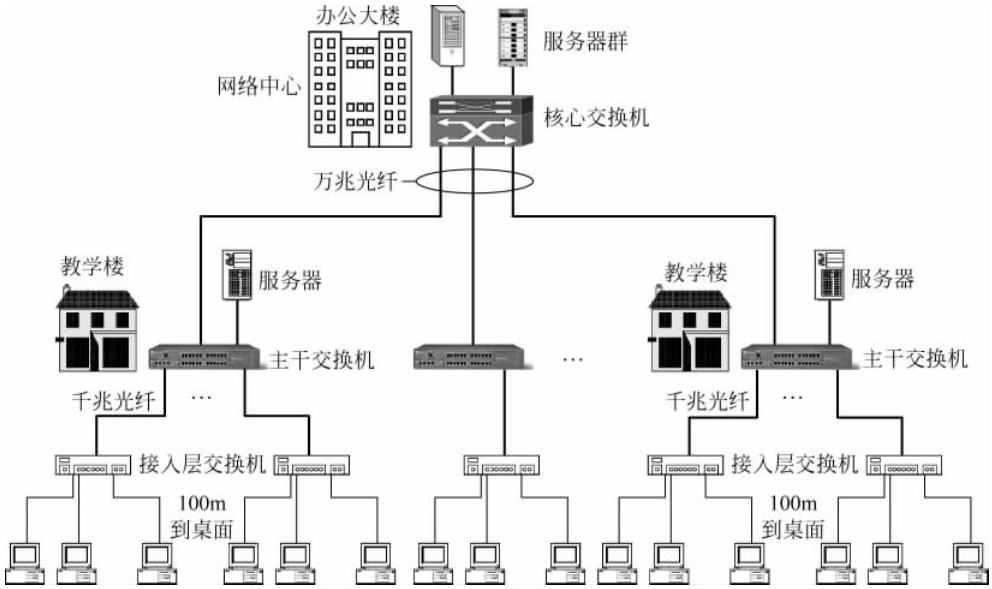

图 3-5 万兆校园计算机网络系统方案

3.1.5 交换式局域网及三层交换技术

1. 交换式局域网的特点和工作原理

交换式局域网以不同于传统共享式局域网所采用的竞争方式来使用信道,而是采用了交换机制,以网络交换机为中心,每一个站点都与交换机相连,站点间可以并行地实现一对一通信的局域网。交换机为数据帧从一个端口到另一个任意端口的转发提供了低时延、低开销的通路。由于交换式局域网中的节点在进行通信时,数据信息是点对点传递的,这些数据并不向其他站点进行广播,所以网络的安全性较高,同时各节点可以独享带宽,如图 3-6 所示。

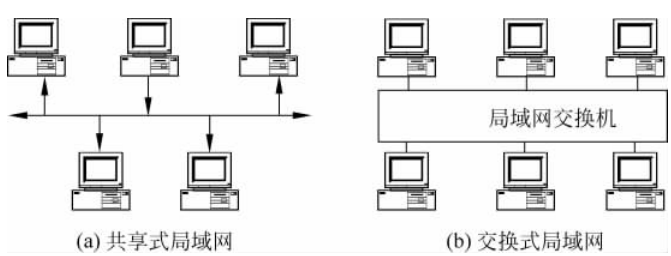

图 3-6 共享式局域网与交换式局域网参考模型

传统共享式局域网上的所有节点(如主机、工作站)共享同一带宽,当网上两个任意节点交换数据时,其他节点只能等待。而交换式局域网利用网络交换机在不同网段之间建立多个独享连接(就像电话交换机可同时为众多的用户建立对话通道一

样),采用按目的地址的定向传输,为每个单独的网段提供专用的频带(即带宽独享),增大了网络的传输吞吐量,提高了传输速率,其主干网上无碰撞问题。交换式局域网克服了共享式局域网的缺点,并借助于 IP 技术的新发展,如 IP Multicast、IP QoS 等技术的推出,使得交换式局域网可以支持多媒体技术等多种业务服务。

交换式局域网的核心是局域网交换机,目前普遍使用的局域网交换设备是以太网交换机(switch),也称为交换式集线器。以太网交换机可以看作是一种改进了的多端口网桥,除了提供存储转发(store-and-forward)功能外,还提供了如直通(cut through)方式等其他桥接技术。以太网交换机的工作原理如下:首先检测节点计算机送至端口的数据帧中的源和目的 MAC 地址,然后与交换机内部动态维护的 MAC 地址对照表进行比较,将数据发送至与目的地址对应的目的端口,将新发现的 MAC 地址及其端口的对应关系记录到地址对照表中。

使用局域网交换机,可以实现高速与低速网络间的转换和不同网络的协同。许多以太网交换机提供 10Mbps 和 100Mbps 的自适应端口,使得配备不同网络通信速率网卡的计算机可以在同一个网络中协同工作。交换式局域网允许不同入网计算机间同时进行传送,如一个 24 端口的以太网交换机最多允许 24 个节点计算机在 12 条链路间同时通信,且每个节点的计算机可以独享所连接交换机端口提供的全部带宽。

2. 三层交换技术

三层交换技术(也称多层交换技术,或 IP 交换技术)是相对于传统交换概念而提出的。传统的交换技术是在 OSI 参考模型中的第二层——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数据包的高速转发。简单地说,三层交换技术就是二层交换技术加三层转发技术。三层交换技术的出现,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问题,突破了传统路由器低速、复杂所造成的网络瓶颈。

一个具有三层交换功能的设备并不是路由器和第二层交换机的简单堆叠,而是把三层路由模块直接叠加在二层交换的高速背板总线上,突破了传统路由器的接口速率限制,能够实现数据的高速转发。下面简单描述三层交换机的技术原理和工作过程。

假设两个使用 IP 协议的站点 A、B 通过第三层交换机进行通信,发送站点 A 在开始发送时把自己的 IP 地址与 B 站的 IP 地址比较,判断 B 站是否与自己在同一子网内。若目的站 B 与发送站 A 在同一子网内,则进行二层的转发。若两个站点不在同一子网内,如发送站 A 要与目的站 B 通信,发送站 A 要向“默认网关”发出 ARP(地址解析)封包,而“默认网关”的 IP 地址其实是三层交换机的三层交换模块。当发送站 A 对“默认网关”的 IP 地址广播一个 ARP 请求时,如果三层交换模块在以前的通信过程中已经知道 B 站的 MAC 地址,则向发送站 A 回复 B 的 MAC 地址。否则三层交换模块根据路由信息向 B 站广播一个 ARP 请求,B 站得到此 ARP 请求后向

三层交换模块回复其MAC地址,三层交换模块保存此地址并回复给发送站A,同时将B站的MAC地址发送到二层交换引擎的MAC地址表中。从这以后,当A向B发送的数据包便全部交给二层交换机处理,信息得以高速交换。由于仅仅在路由过程中才需要三层交换机处理,绝大部分数据都通过二层交换机转发,因此三层交换机的速度很快,接近二层交换机的速度,同时比相同路由器的价格低很多。

三层交换机并不等于路由器,同时也不可能取代路由器。三层交换机与路由器之间还是存在着非常大的本质区别的。第三层交换机无法适应网络拓扑各异、传输协议不同的广域网络系统。第三层交换机主要用于局域网环境,而路由器主要用于广域网环境。

3. 第三层交换在虚拟局域网规划中的应用

在第三层交换机面世之前,交换机所提供的虚拟局域网(VLAN)划分方式只有两种:基于端口划分方式和基于MAC地址划分方式。基于端口的VLAN提供了把某个或某几个端口上的机器划分为一个VLAN的方法,缺点在于无法实现位置无关的虚拟网配置;基于MAC地址的VLAN将子网以MAC地址来划分,可实现位置无关的虚拟网,缺点在于子网中节点的增删不方便。第三层交换技术提供了一种全新的VLAN划分法:基于IP及策略的VLAN,即不管节点处于哪一个物理网段,都可以以它们的IP地址为基础或根据报文协议不同来划分子网,这使得网络管理和应用变得更加方便。

例如,在某校园网VLAN的划分中,利用第三层交换技术,使得校园网的VLAN划分很容易和校内各部门一致起来,尽管校内某一部门站点分布在不同物理位置,但基于IP地址划分子网,能使得同一部门在不同物理网段的节点可被设为同一逻辑子网,实现与物理位置无关的特性;对于网络中心、财务部门等要害部门可采用基于传统的MAC地址的VLAN划分技术,以防止非授权节点在该子网中出现;对于学生宿舍等比较分散,物理子网比较多,难以有效管理的地方可采用混合策略,如在同一端口细分不同的逻辑虚拟子网或基于MAC地址划分子网,以尽量减少IP地址盗用和其他安全问题。

3.1.6 无线局域网

无线局域网(Wireless LAN,WLAN)是利用无线通信技术在一定的局部范围内建立的网络,是计算机网络与无线通信技术相结合的产物,它以无线多址信道作为传输媒介,提供传统有线局域网的功能,能够使用户真正实现随时、随地、随意的宽带网络接入。WLAN作为有线局域网络的延伸,提供了局部范围内高速移动计算的条件。随着应用的进一步发展,WLAN正逐渐从传统意义上的局域网技术发展成为“公共无线局域网”,成为国际互联网宽带接入手段。WLAN具有易安装、易扩展、易管理、易维护、高移动性、保密性强、抗干扰等特点。

1. 无线局域网标准

无线局域网标准是 IEEE 802.11X 系列(IEEE 802.11a、IEEE 802.11b、IEEE 802.11g、IEEE 802.11n)、HIPERLAN、HomeRF、IrDA 和蓝牙等标准。表 3-6 是 IEEE 802.11 无线局域网标准,也是当前常用的 WLAN 标准。

表 3-6　IEEE 802.11 无线局域网标准

标 准 要 求	IEEE 802.11b	IEEE 802.11a	IEEE 802.11g	IEEE 802.11n
每子频道最大的数据速率	11Mbps	54Mbps	54Mbps	300Mbps
调制方式	CCK	OFDM	OFDM 和 CCK	MIMO-OFDM
每子频道的数据速率	1,2,5.5,11Mbps	6,9,12,18,24,36,48,54Mbps	CCK:1,2,5.5,11Mbps OFDM:6,9,12,18,24,36,48,54Mbps	
工作频段	2.4～2.4835GHz	5.15～5.35GHz 5.725～5.875GHz	2.4～2.4835GHz	2.4/5GHz
可用频宽	83.5MHz	300MHz	83.5MHz	
不重叠的子频道	3	12	3	13

1) IEEE 802.11b

IEEE 802.11b 工作在 2.4～2.4835GHz,采用 CCK(Complementary Code Keying,补码键控)技术提供高达 11Mbps 的数据通信带宽,最多可提供 3 个互不重叠的子频道。WiFi 认证保证不同厂家产品之间的兼容。由于 IEEE 802.11b 工作的 2.4GHz 频带是免费的,因此一经推出便得到了用户的认可。

2) IEEE 802.11a

IEEE 802.11a 工作在 5GHz,采用 OFDM(Orthogonal Frequency Division Multiplexing,正交频分复用)技术提供 54Mbps 的数据通信带宽,最多可提供 12 个互不重叠的子频道。由于 IEEE 802.11a 标准工作在更高的频段,具有更多不重叠的子频道和更高的数据通信带宽,因此也得到了较为广泛的应用。

IEEE 802.11a 和 IEEE 802.11b 工作在两个完全不同的频带,采用完全不同的调制技术,因此两者是完全不兼容的。但两者可以共存于同一区域当中而互不干扰。

3) IEEE 802.11g

IEEE 802.11g 有两个最为主要的特征:高传输速率和兼容 IEEE 802.11b。高速率是由于其采用 OFDM 调制技术可得到 54Mbps 的数据通信带宽。兼容 IEEE 802.11b 是由于其仍然工作在 2.4GHz 并且保留了 IEEE 802.11b 所采用的 CCK 技术,因此可与 IEEE 802.11b 的产品保持兼容。也就是说,基于 IEEE 802.11g 的无线接入点(AP)可与基于 IEEE 802.11b 的无线网卡相连接,而基于 IEEE 802.11g 的无线网卡也可与基于 IEEE 802.11b 的无线接入点(AP)相连接。IEEE 802.11g

标准是主流的无线局域网标准。它提供了高速的数据通信带宽,并以较为经济的成本提供了对原有主流无线局域网标准的兼容。

4) IEEE 802.11n

使用2.4GHz频段和5GHz频段,传输速度为300Mbps,最高可达600Mbps。IEEE 802.11n采用智能天线技术,其传播范围更广,且能够以不低于108Mbps的传输速率保持通信。它可以作为蜂窝移动通信的宽带接入部分,与无线广域网更紧密地结合。一方面,IEEE 802.11n可以为用户提供高数据率的通信服务(比如视频点播VOD,在线观看HDTV)。另一方面,无线广域网为用户提供了更好的移动性。和以往的IEEE 802.11标准不同,IEEE 802.11n协议为双频工作模式(包含2.4GHz和5.8GHz两个工作频段)。这样IEEE 802.11n保证了与以往的IEEE 802.11a/b/g标准兼容。

5) IEEE 802.11ac

IEEE 802.11ac是IEEE 802.11n的继承者。它采用并扩展了源自IEEE 802.11n的空中接口(air interface)概念,其特性包括更宽的RF带宽(提升至160MHz)、更多的MIMO空间流(增加到8),多用户的MIMO以及更高阶的调制(达到256QAM)。理论上,IEEE 802.11ac可以为多个站点服务提供1Gbps的带宽,或是为单一连接提供500Mbps的传输带宽。

2. 无线局域网拓扑结构

根据无线接入点(Access Point,AP)的功用不同,WLAN可以实现不同的组网方式。目前有基础架构模式、点对点模式、多AP模式、无线网桥模式和无线中继器模式5种组网方式。

1) 点对点模式(Ad-hoc)

点对点模式由无线工作站组成,用于一台无线工作站和另一台或多台其他无线工作站的直接通信,该网络无法接入到有线网络中,只能独立使用。无需AP,安全由各个客户端自行维护。因此对等网络只能用于少数用户的组网环境。点对点模式的组网如图3-7所示。

2) 基础架构模式

这种方式以星形拓扑为基础,以访问点AP为中心,所有的无线工作站通信要通过AP接转。AP主要完成MAC控制及信道的分配等功能。AP通常能够覆盖几十至几百用户,覆盖半径达百米。覆盖的区域称基本服务区(Basic Service Set,BSS)。

由于AP有以太网接口,这样,既能以AP为中心独立组建一个无线局域网,当然也能将AP作为一个有线网的扩展部分,用于在无线工作站和有线网络之间接收、缓存和转发数据。由于对信道资源分配、MAC控制采用集中控制的方式,这样使信道利用率大大提高,网络的吞吐性能优于分布式对等方式。基础架构模式的组网如图3-8所示。

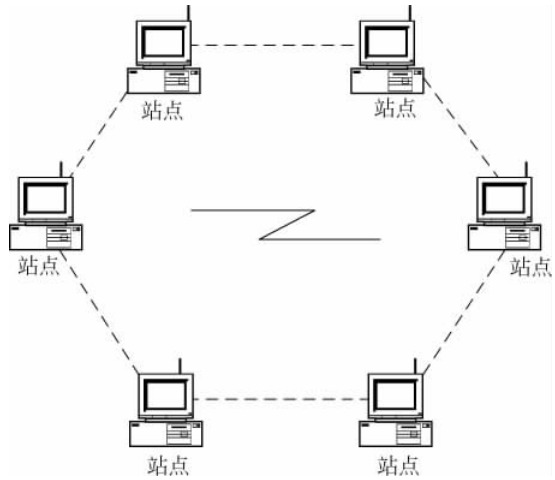

图 3-7　点对点模式

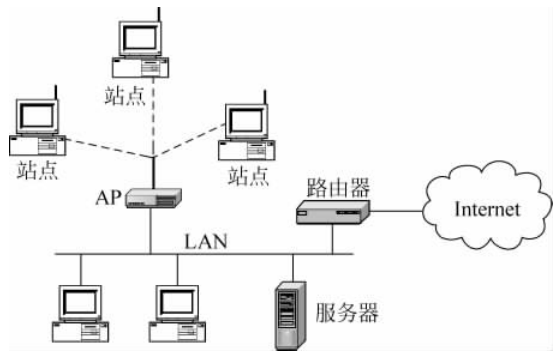

图 3-8　基础架构模式

3）多 AP 模式

多 AP 模式是指由多个 AP 以及连接它们的分布式系统(有线的骨干 LAN)组成的基础架构模式网络，也称为扩展服务区(Extend Service Set，ESS)。扩展服务区内的每个 AP 都是一个独立的无线网络基本服务区(BSS)，所有 AP 共享同一个扩展服务区标示符(ESSID)。分布式系统在 IEEE 802.11 标准中并没有定义，但是目前大多是指以太网。可以在相同 ESSID 的无线网络间进行漫游，不同 ESSID 的无线网络形成逻辑子网。多 AP 模式的组网如图 3-9 所示。

4）无线网桥模式

无线网桥模式利用一对 AP 连接两个有线或者无线局域网网段。无线网桥模式的组网如图 3-10 所示。

5）无线中继器模式

无线中继器用来在通信路径的中间转发数据，从而延伸系统的覆盖范围。无线中继器模式的组网如图 3-11 所示。

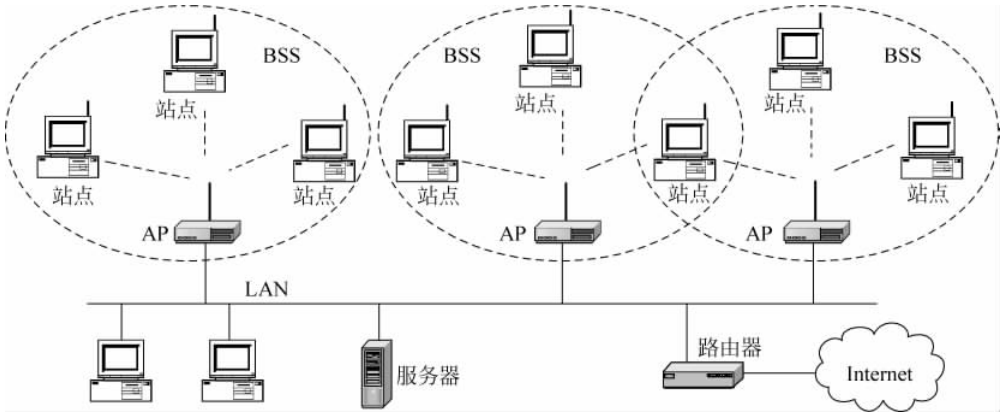

图 3-9 扩展服务区 ESS

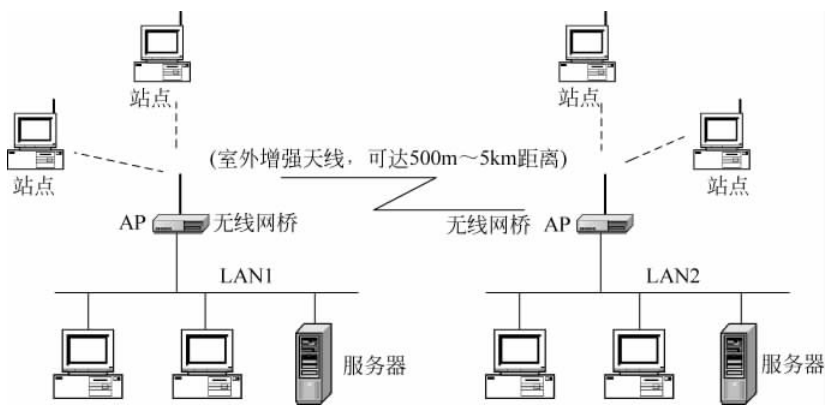

图 3-10 无线网桥模式

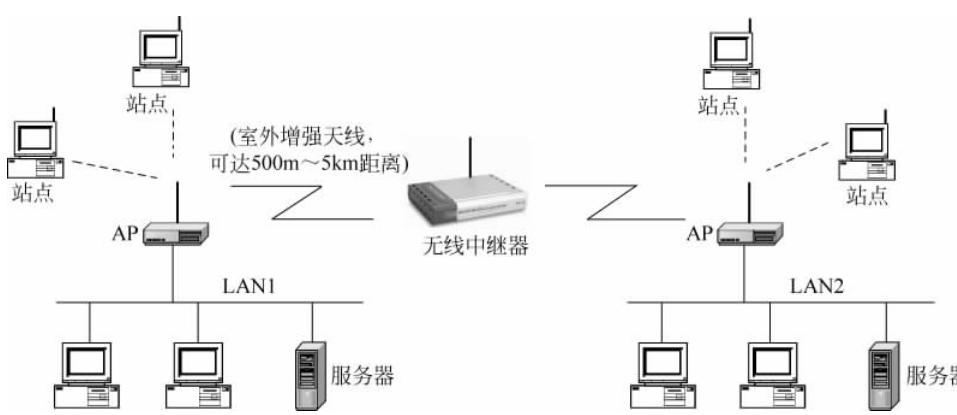

图 3-11 无线中继器模式

应用上述 5 种不同的工作模式，可以灵活方便地组建各种无线网络结构以满足各种需求。

3. 无线局域网安全技术

由于无线局域网采用公共的电磁波作为载体，电磁波能够穿过天花板、玻璃、楼层、砖、墙等物体，因此，在一个无线访问点所服务的区域中任何一个无线客户端都可以接收到网络中传输的数据，包括并不希望其接收数据的客户端。因此在无线局域网中，只要有和无线局域网设备工作在同一个频段的设备，任何人都有条件窃听或干扰信息，为了阻止非授权用户访问无线网络，以及防止对无线局域网数据流的非法侦听，在无线局域网的应用当中引入了相应的安全技术。

通常网络的安全性主要体现在访问控制和数据加密两个方面。访问控制保证敏感数据只能由授权用户进行访问，而数据加密则保证发送的数据只能被所期望的用户接收和理解。无线局域网采用如下安全技术。

1）物理地址（MAC）过滤

每个无线工作站网卡都由唯一的物理地址标示，该物理地址编码方式类似于 48 位以太网物理地址。可在无线访问点（AP）中手工维护一组允许访问的 MAC 地址列表，实现物理地址过滤。

2）服务区标识符（SSID）匹配

无线工作站必须出示正确的 SSID，与无线访问点（AP）的 SSID 相同，才能访问 AP。如果出示的 SSID 与 AP 的 SSID 不同，那么 AP 将拒绝该站通过本服务区上网。因此可以认为 SSID 是一个简单的口令，从而通过口令认证机制实现一定的安全。

3）有线等效保密（WEP）

有线等效保密（WEP）协议是由 IEEE 802.11 标准定义的，用于在无线局域网中保护链路层数据。WEP 使用 40 位密钥、采用 RSA 开发的 RC4 对称加密算法在链路层加密数据。

WEP 加密采用静态的保密密钥，各 WLAN 终端使用相同的密钥访问无线网络。WEP 也提供认证功能，当加密机制功能启用，客户端要尝试连接上 AP 时，AP 会发出一个 Challenge Packet 给客户端，客户端再利用共享密钥将此值加密后送回 AP 以进行认证比对，如果正确无误，才能获准存取网络的资源。40 位 WEP 具有很好的互操作性，所有通过 WiFi 组织认证的产品都可以实现 WEP 互操作。现在的 WEP 也一般支持 128 位的密钥，提供更高等级的安全加密。

4）端口访问控制技术（IEEE 802.1x）和可扩展认证协议（EAP）

该技术也是用于无线局域网的一种增强性网络安全解决方案。当无线工作站与无线访问点（AP）关联后，是否可以使用 AP 的服务要取决于 IEEE 802.1x 的认证结果。如果认证通过，则 AP 为无线工作站打开这个逻辑端口，否则不允许用户上网。

IEEE 802.1x要求无线工作站安装IEEE 802.1x客户端软件,无线访问点要内嵌IEEE 802.1x认证代理,同时它还作为RADIUS客户端,将用户的认证信息转发给RADIUS服务器。

5) VPN Over Wireless技术

目前已广泛应用于局域网及远程接入等领域的VPN(Virtual Private Networking,虚拟专网)安全技术也可用于无线局域网,与IEEE 802.11b标准所采用的安全技术不同,VPN主要采用DES、3DES等技术来保障数据传输的安全。对于安全性要求更高的用户,将现有的VPN安全技术与IEEE 802.11b安全技术结合起来,这是目前较为理想的无线局域网的安全解决方案。

6) IEEE 802.11i

为了进一步加强无线网络的安全性和保证不同厂家之间无线安全技术的兼容,IEEE 802.11工作组开发作为新的安全标准的IEEE 802.11i,致力于从长远角度考虑解决IEEE 802.11无线局域网的安全问题。IEEE 802.11i标准主要包含加密技术TKIP(Temporal Key Integrity Protocol)和AES(Advanced Encryption Standard)以及认证协议IEEE 802.1x。

WLAN应用中,对于家庭用户、公共场景安全性要求不高的用户,使用VLAN隔离、MAC地址过滤、服务区域认证ID(ESSID)、密码访问控制和Wi-Fi保护访问(Wi-Fi Protected Access,WPA)可以满足其安全性需求。但对于公共场景中安全性要求较高的用户,WLAN仍然存在着安全隐患,需要将有线网络中的一些安全机制引进到WLAN中,在无线接入点(AP)实现复杂的IEEE 802.11i标准加密解密算法,通过无线接入控制器(AC),利用PPPoE或者DHCP+WEP认证方式对用户进行第二次合法认证,对用户的业务流实行实时监控。

4. HomeRF

HomeRF是专门为家庭用户设计的一种无线局域网技术标准,利用跳频扩频方式,既可以通过时分复用支持语音通信,又能通过CSMA/CA协议提供数据通信服务。HomeRF还提供了与TCP/IP协议良好的集成,支持广播、多播和IP地址。目前,HomeRF标准工作在2.4GHz的频段上,跳频带宽为1MHz,最大传输速率为2Mbps,传输范围超过100m。

美国联邦通信委员会(FCC)已经允许下一代HomeRF无线通信网络传送的最高速度提升到10Mbps。这个速度是目前该网络速度的5倍,将使HomeRF的带宽与IEEE 802.11b标准所能达到的11Mbps的带宽相差无几,并使HomeRF更加适合在无线网络上传输音乐和视频信息。美国联邦通信委员会还接受了HomeRF工作组的要求,将HomeRF/SWAP(Shared Wireless Access Protocol,共享无线访问协议)使用的2.4GHz频段中的跳频带宽增加到5MHz。

5. IrDA技术

IrDA是红外数据标准协会(Infrared Data Association)的简称,成立于1993年,

是非营利性组织，致力于建立无线传播连接的国际标准，目前其来自全世界的 160 个会员中包括计算机与通信设备厂商、软件公司及电信公司机构。

IrDA 是一种利用红外线进行点对点通信的技术，软件和硬件技术比较成熟，主要优点是体积小、功率低，适合设备移动的需要；传输速率高，可达 16Mbps；成本低，应用普遍。目前全世界 95％的笔记本电脑安装了 IrDA 接口，最近市场上还出现了可以通过 USB 接口与 PC 相连接的 USB-IrDA 设备。使用 IrDA 技术组建无线局域网被认为是一种很有发展潜力的领域。

但是 IrDA 技术也有局限性。首先它是一种视线传输技术，两个具有 IrDA 端口的设备在传输数据时，中间不能有阻挡物。这对于两个设备不难实现，但对于多个设备组网通信，就必须彼此调整位置和角度（传统的 IrDA 接收角度只有 30°，现在扩展到 120°）。这是 IrDA 技术组网的致命弱点。其次，IrDA 设备使用红外线 LED 器件作为核心部件，不十分耐用。如果经常用 IrDA 端口联网，可能不堪重负。

6. 蓝牙技术

蓝牙（Bluetooth）技术是一种近距离无线通信连接技术，用于各种固定与移动的数字化硬件设备之间通信，具有连接稳定、无缝和低成本的优点。蓝牙技术将通信驱动软件固化在微型芯片上，可以方便地嵌入设备之中，使得它能够被广泛应用于日常生活中。

蓝牙技术同样采用了跳频技术，但与其他工作在 2.4GHz 频段上的系统相比，蓝牙跳频更快，数据包更短，这使蓝牙比其他系统都更稳定。蓝牙技术理想的连接范围为 0.1～10m，但是通过增大发射功率可以将距离延长至 100m。

蓝牙基带协议是电路交换与分组交换的结合。在被保留的时隙中可以传输同步数据包，每个数据包以不同的频率发送。一个数据包名义上占用一个时隙，但实际上可以被扩展到占用 5 个时隙。蓝牙可以支持异步数据通道、多达 3 个同步话音信道，还可以用一个信道同时传送异步数据和同步话音。异步信道可以支持一端最大速率为 721kbps 而另一端速率为 57.6kbps 的不对称连接，也可以支持 43.2kbps 的对称连接。

蓝牙技术面向的是移动设备间的小范围连接，本质上说，它是一种代替线缆的技术，可以应用于任何可以用无线方式替代线缆的场合，适合用在手机、掌上型电脑等简易数据传递中。

7. 某酒店会议中心无线局域网设计方案

某酒店会议中心为四层楼，一楼为大厅，二至四层各有两个会议室和若干客房。构建一个能覆盖整个酒店的无线局域网络，系统结构如图 3-12 所示。

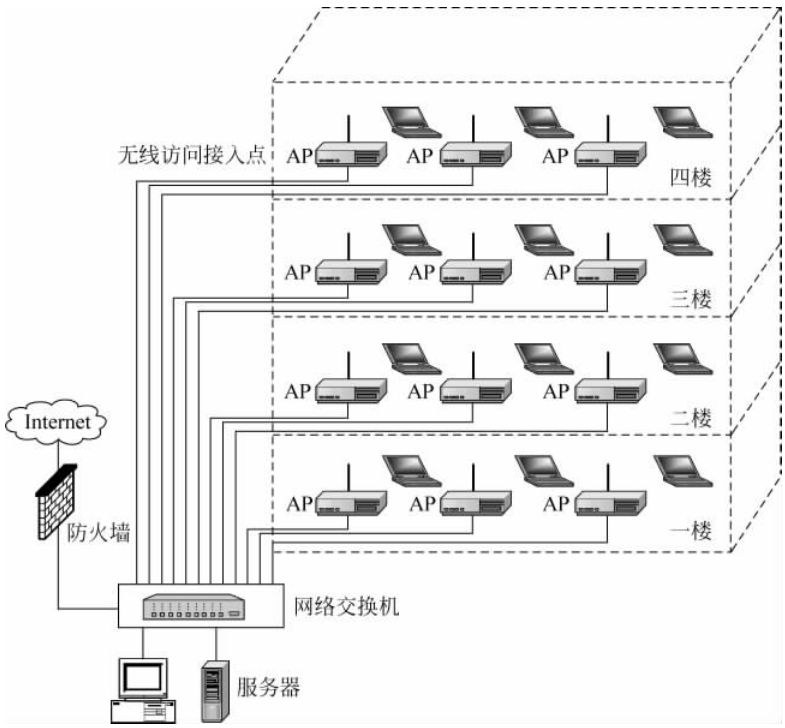

图 3-12 某酒店会议中心无线局域网结构图

3.2 局域网扩展与网络互联

3.2.1 局域网扩展

扩展局域网常用的方法包括光纤扩展、中继器扩展和网桥扩展等。

最简单的局域网扩展是光纤扩展,如图 3-13 所示,在外围计算机和局域网之间使用光纤和一对光纤收发器(例如 10/100Mbps 以太网光纤收发器)。因为光纤的延迟短、带宽大,使得计算机能和远处的网络连接。当然,必须提供双向通信功能以使计算机能收发帧。实际使用中用一对光纤,使之能双向同时传送数据。光纤收发器的主要优点是能连接远处的局域网,而不改变原来的局域网和计算机。一般用它来把一幢大楼内的计算机连接到另一幢大楼内的局域网中。

中继器是扩展共享介质本身的硬件设备。每个中继器连接两个网段。中继器能侦听一个网段的所有信号并转发到另外一个网段,反之亦然。中继器的缺点是既传播有效信号也传播电子干扰。

网桥能连接几个局域网从而扩大局域网的规模。每个网桥连接两个网段,并能转发一个网段的帧到另外一个网段,反之亦然。网桥像计算机一样连到局域网上。

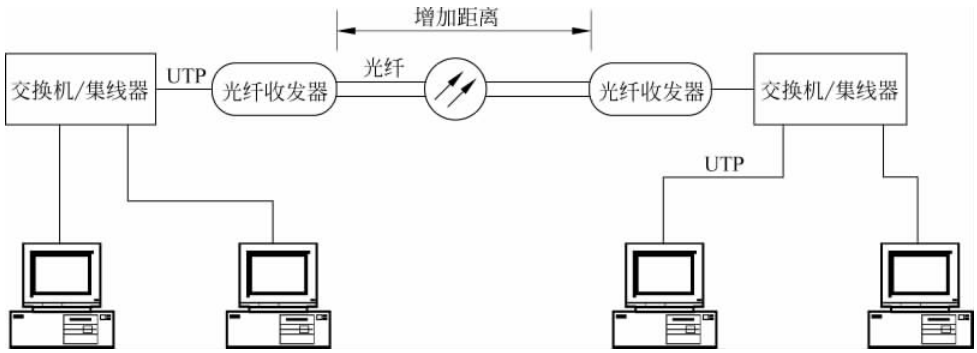

图 3-13　使用光纤扩展

网桥以混合模式侦听每个网段，这样可以保证网桥能收到每个穿越网段的帧。然后网桥发送帧副本到另外一个网段上。网桥系统可用铜缆、光纤、租用串行线路或租用卫星频道来连接近距离或远距离的局域网网段。网桥检查所收到每个帧的帧头中的物理地址。网桥用源地址来判断计算机连到哪个网段上，并用目标地址来判断是否要转发该帧。由于网桥在不需要时就不转发帧，所有桥接网允许各自网段中的计算机间的通信可以同时进行。因此，桥接局域网的性能要优于简单的共享型局域网。

3.2.2　局域网互联

如果几个计算机网络只是在物理上连接在一起，它们之间并不能进行通信，这种“互联”并没有什么实际意义。因此通常在谈到“互联”时，是指这些相互连接的计算机是可以进行通信的，也就是说，从功能上和逻辑上看，这些计算机网络已经组成了一个大型的计算机网络，或称为互联网络。将网络互联起来要使用一些中间设备（或中间系统），称为中继（relay）系统。根据中继系统所在的层次，可以有以下 5 种中继系统：

（1）物理层（第一层）中继系统，即转发器（repeater）。

（2）数据链路层（第二层）中继系统，即网桥或桥接器（bridge）。

（3）网络层（第三层）中继系统，即路由器（router）。

（4）网桥和路由器的混合物——桥路器（brouter），兼有网桥和路由器的功能。

（5）在网络层以上的中继系统，即网关（gateway）。

当中继系统是转发器时，一般不称之为网络互联，因为这仅仅是把一个网络扩大了，而其仍然是一个网络。高层网关由于比较复杂，目前使用得较少。因此一般讨论网络互联时都是指用交换机和路由器进行互联的网络。

1. 网桥

网桥（bridge）工作在数据链路层的 MAC 子层，其基本功能是在不同局域网段之

间转发帧。网桥从端口接收该接口所连接网段上的所有数据帧,每收到一个帧,就存在缓存区并进行差错效验。如果该帧没有出现传输错误而且目的站属于其他网段,则根据目的地址通过查找存有端口-MAC地址映射的桥接表,找到对应的转发端口,将该帧从该端口上转发出去,如果该帧有错误则丢弃该帧。如果数据帧的源站和目的站在同一个网段内,网桥不进行转发。其工作原理如图3-14所示,网络初始化时,网桥接收来自网段1的数据帧(对应接收端口为1),检查其源物理地址,并将此物理地址和对应的端口号写入工作表中,将目的站的物理地址广播到连接网段上,然后将响应者的物理地址和接收端口号写入桥接表中,工作一段时间后,网段上的所有站都和端口号形成了映射关系。桥接表建立好以后,网桥就根据表中对应关系判断数据帧是否需要转发。

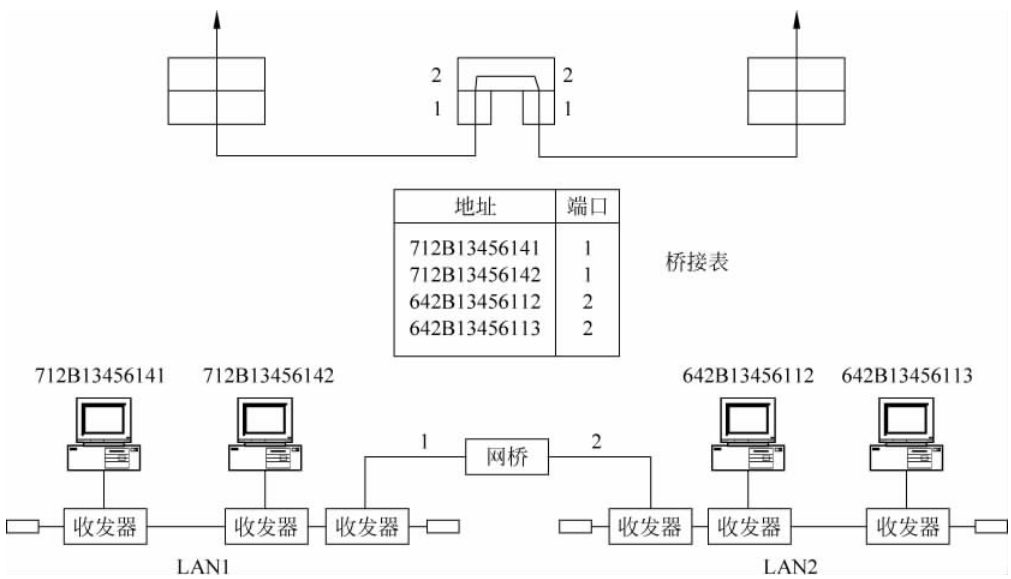

图3-14 网桥工作原理图

2. 二层交换机

二层交换机是具备桥接功能的网络设备。可以这样理解:它等同于网络交换机上堆叠了网桥,但是,转发速度要比网桥快很多。二层交换机是数据链路层的设备,它能够读取数据包中的MAC地址信息并根据MAC地址来进行交换。交换机内部有一个地址表,这个地址表标明了MAC地址和交换机端口的对应关系。当交换机从某个端口收到一个数据包,它首先读取包头中的源MAC地址,这样它就知道源MAC地址的机器是连在哪个端口上的,它再去读取包头中的目的MAC地址,并在地址表中查找相应的端口,如果表中有与该目的MAC地址对应的端口,则把数据包直接复制到这端口上,如果在表中找不到相应的端口,则把数据包广播到所有端口上,当目的机器对源机器回应时,交换机又可以学习到目的MAC地址与哪个端口对

应，在下次传送数据时就不再需要对所有端口进行广播了。二层交换机就是这样建立和维护它自己的地址表。由于二层交换机一般具有很宽的交换总线带宽，所以可以同时为很多端口进行数据交换。如果二层交换机有 N 个端口，每个端口的带宽是 M，而它的交换机总线带宽超过 $N \times M$，那么这个交换机就可以实现线速交换。二层交换机对广播包是不做限制的，把广播包复制到所有端口上。二层交换机一般都含有专门用于处理数据包转发的 ASIC（Application Specific Integrated Circuit）芯片，因此转发速度可以做到非常快。

3. 路由器

路由器是在第三层的分组交换设备（或网络层中继设备），路由器的基本功能是把数据（IP 报文）传送到正确的网络，包括以下功能：IP 数据报的寻径和传送；子网隔离，抑制广播风暴；维护路由表，并与其他路由器交换路由信息；IP 数据报的差错处理及简单的拥塞控制；实现对 IP 数据报的过滤和日志。

对于不同规模的网络，路由器的侧重点有所不同。在主干网上，路由器的主要作用是路由选择。在地区网中，路由器的主要作用是网络连接和路由选择，同时负责下层网络之间的数据转发。在园区网内部，路由器的主要作用是子网间的报文转发和广播隔离。路由器每一接口连接一个子网，广播报文不能经过路由器广播出去，连接在路由器不同接口的子网属于不同子网，子网范围由路由器物理划分。

4. 三层交换机与路由器的区别

三层交换机也具有路由功能，能够执行传统路由器的大多数功能。虽然如此，三层交换机与路由器还是存在着相当大的本质区别。

（1）适用的环境不一样。

三层交换机的路由功能通常比较简单，路由路径远没有路由器那么复杂。它主要用在局域网中子网间的连接，提供快速数据交换功能，满足局域网不同子网数据交换频繁的应用特点。

而路由器则不同，它主要是为了满足不同类型的网络互联。虽然也适用于局域网子网之间的互联，但它的路由功能更多地体现在不同类型网络之间的互联上，如局域网与广域网之间的互联、不同协议的网络之间的互联（如以太网和令牌环网的互联）等。解决好各种复杂路由路径网络的互联就是路由器的最终目的，所以路由器的路由功能通常非常强大。为了与各种类型的网络互联，路由器的接口类型非常丰富，而三层交换机则一般仅有同类型的局域网接口，非常简单。

（2）性能体现不一样。

路由器和三层交换机在数据包交换操作上存在着明显区别。路由器一般由基于微处理器的软件路由引擎执行数据包交换，而三层交换机通过硬件执行数据包交换。三层交换机在对第一个数据流进行路由后，它将会产生一个 MAC 地址与 IP 地址的映射表，当同样的数据流再次通过时，将根据此表直接从二层通过而不是再次

路由,从而消除了路由器进行路由选择而造成网络的延迟,提高了数据包转发的效率。同时,三层交换机的路由查找是针对数据流的,它利用缓存技术,很容易利用ASIC技术来实现,因此,可以大大节约成本,并实现快速转发。而路由器的转发采用最长匹配的方式,实现复杂,通常使用软件来实现,转发效率较低。

从整体性能上比较,三层交换机的数据包转发性能要远优于路由器,非常适用于数据交换频繁的局域网中。而路由器虽然路由功能非常强大,但它的数据包转发效率远低于三层交换机,更适合于数据交换不是很频繁的不同类型网络的互联。所以,如果把路由器,特别是高档路由器用于局域网中,则在相当大程度上是一种浪费(就其强大的路由功能而言),而且还不能很好地满足局域网通信性能需求,影响子网间的正常通信。

三层交换机具有以下优势:

(1) 子网间传输带宽可任意分配。传统路由器每个接口连接一个子网,子网通过路由器进行传输的速率被接口的带宽所限制。而三层交换机则不同,它可以把多个端口定义成一个虚拟网(VLAN),把多个端口组成的虚拟网作为虚拟网接口,该虚拟网内信息可通过组成虚拟网的端口送给三层交换机,由于端口数可任意指定,子网间传输带宽没有限制。

(2) 合理配置信息资源。由于访问子网内资源速率和访问全局网(子网外的跨网段网络)中资源速率没有区别,子网设置单独服务器的意义不大,通过在全局网中设置服务器群不仅节省费用,更可以合理配置信息资源。

(3) 降低成本。通常的网络设计用交换机构成子网,用路由器进行子网间互联。目前采用三层交换机进行网络设计,既可以进行任意虚拟子网划分,又可以通过交换机三层路由功能完成子网间通信,为此节省了价格昂贵的路由器。

(4) 交换机之间连接灵活。在计算机网络通信设备中,作为交换机,它们之间是不允许存在任何回路的,而作为路由器,又可以采用多条通路(如主、备路由)来提高网络的可靠性和平衡负载。为了解决这类矛盾,在三层交换机中,一方面采用生成树算法来阻塞造成回路的端口,在进行路由选择时,又能依然把阻塞的通路作为可以选择的路径来参与路由选择,从而极大地提高了交换机连接的灵活性。

综上所述,三层交换机与路由器之间存在着非常大的本质区别。无论从哪方面来说,在局域网中进行多子网连接,最佳方案是选用三层交换机。在智能建筑的计算机网络设计中,通常用三层交换机来组建建筑内计算机网络,再用路由器与各种广域网相连。

5. 网关

网关工作在OSI参考模型的最高层——应用层。从一个网络向另一个网络发送信息,必须经过网关。网关实质上是一个网络通向其他网络的IP地址。如图3-15所示,有网络A和网络B,网络A的IP地址范围为192.168.1.1～192.168.1.254,子网掩码为255.255.255.0;网络B的IP地址范围为192.168.2.1～192.168.2.254,

子网掩码为 255.255.255.0。在没有路由器的情况下，两个网络之间是不能进行 TCP/IP 通信的，即使是两个网络连接在同一台交换机（或集线器）上，TCP/IP 协议也会根据子网掩码（255.255.255.0）判定两个网络中的主机处在不同的网络里。而要实现这两个网络之间的通信，则必须通过网关。如果网络 A 中的主机发现数据包的目的主机不在本地网络中，就把数据包转发给它自己的网关，再由网关转发给网络 B 的网关，网络 B 的网关再转发给网络 B 的某个主机。网络 B 向网络 A 转发数据包的过程也是如此。

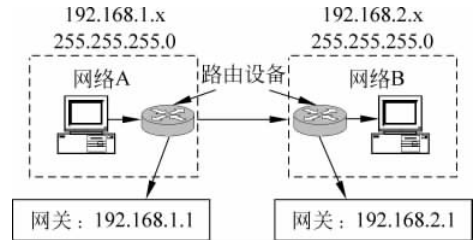

图 3-15　网关工作原理

6. 远程网络互联

通过电信网可实现远程局域网互联，如图 3-16 所示。

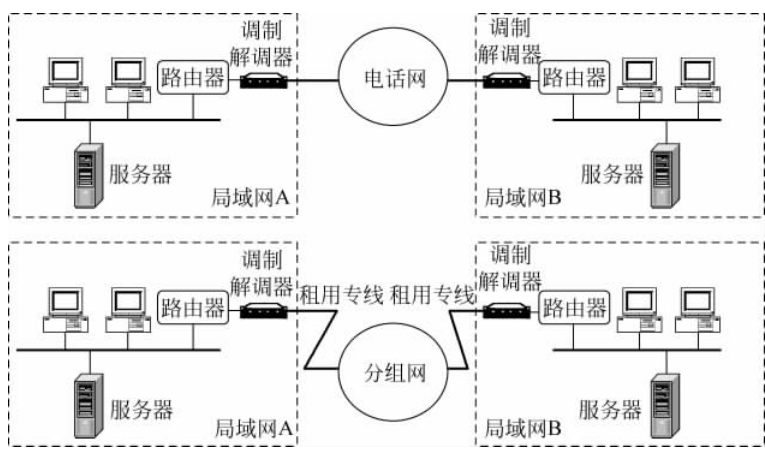

图 3-16　远程局域网互联

3.2.3　校园网、园区网设计

1. 校园网的特点

校园网实际上是特大型建筑群的计算机网络系统，是大规模的局域网，其特点如下：校园都是占地面积很大的建筑楼群，少则几座，多则几十座建筑分布在很大的区域内。从地域范围来论，校园网已经远远超出传统的局域网的范畴。所以说，校园网是一个大局域网。其次，校园网的站点数量非常大，可达上万个计算机终端，涉及的部门和人员众多，因此存在大量的子网。

校园网负担着整个校园的所有数据通信业务，几乎涵盖了 Internet 所有的应用

类型。因此,校园网应具有极高性能和带宽、面向应用的网络服务、极大的灵活性、极高的可靠性、高度可管理性和极强的安全性。

综上所述,校园网一个高速的、大范围的、大规模的局域网。

2. 校园网设计原则

校园网是一个以IP应用为基础的多业务综合平台,在这一网络平台上集成的应用包括数据传输、数据库查询、Web应用、视频会议、视频点播和VoIP等多媒体应用。其应用的复杂性要求网络的规划设计和建设在总体上应该满足以下原则:

(1) 先进性。采用国际先进并代表发展方向的技术和设备,满足目前及可预见的将来的业务需求。

(2) 高可靠性/可用性。作为承载学校内部多种业务的网络系统,要求具有极高的可靠性,同时也要求具有很高的可用性。需要充分考虑冗余、备份和负载均衡等技术的应用。

(3) 开放性。系统必须具有良好的开放性,必须支持国际标准,能够实施网络内部及与其他外部网络系统的互联互通,资源共享。

(4) 高安全性。应充分考虑到网络安全性,不仅要考虑来自网络外部的安全威胁,也要考虑网络内部的安全威胁。在采用安全策略的情况下,不应给网络带来瓶颈。

(5) 可管理性和可维护性。网络系统具有可管理的工具和界面,网络管理工具应具有很全面的管理功能,能够方便地进行各种性能监测、数据分析、故障排除和日常维护。

(6) 高性能及QoS。网络应具备足够的容量和处理性能,支持大容量的数据传输与交换。同时因应用的不同,如有时延敏感型应用VOD、VoIP、视频会议和非时延敏感型应用FTP等,网络必须能够对不同的应用提供不同的服务优先级,这种保证措施不仅要在带宽充裕的局域网上可以实施,而且要在带宽资源较少的广域网上也可以实施。

(7) 可扩展性和可升级性。由于网络应用总是不断在增长的,必须保证网络具有很强的可扩展能力,包括带宽、容量和规模的扩展,网络的升级和扩展不应对现有业务造成影响,即必须保证升级扩展是平滑的。同时,网络的升级和扩展要能够保护现有投资。

3. 万兆校园网解决方案

万兆校园网结构如图3-17所示。

该方案采用当今主流的层次化结构——星形的网络拓扑。系统分为三层:核心层、汇聚层和接入层。核心层是网络中心,主要是进行高速的数据交换和服务器组的高速接入。汇聚层的主要目的是进行高速的数据交换,同时还进行安全策略的实施。接入层用于用户终端的接入。网络结构采用完全的星形结构,即以主机房核心

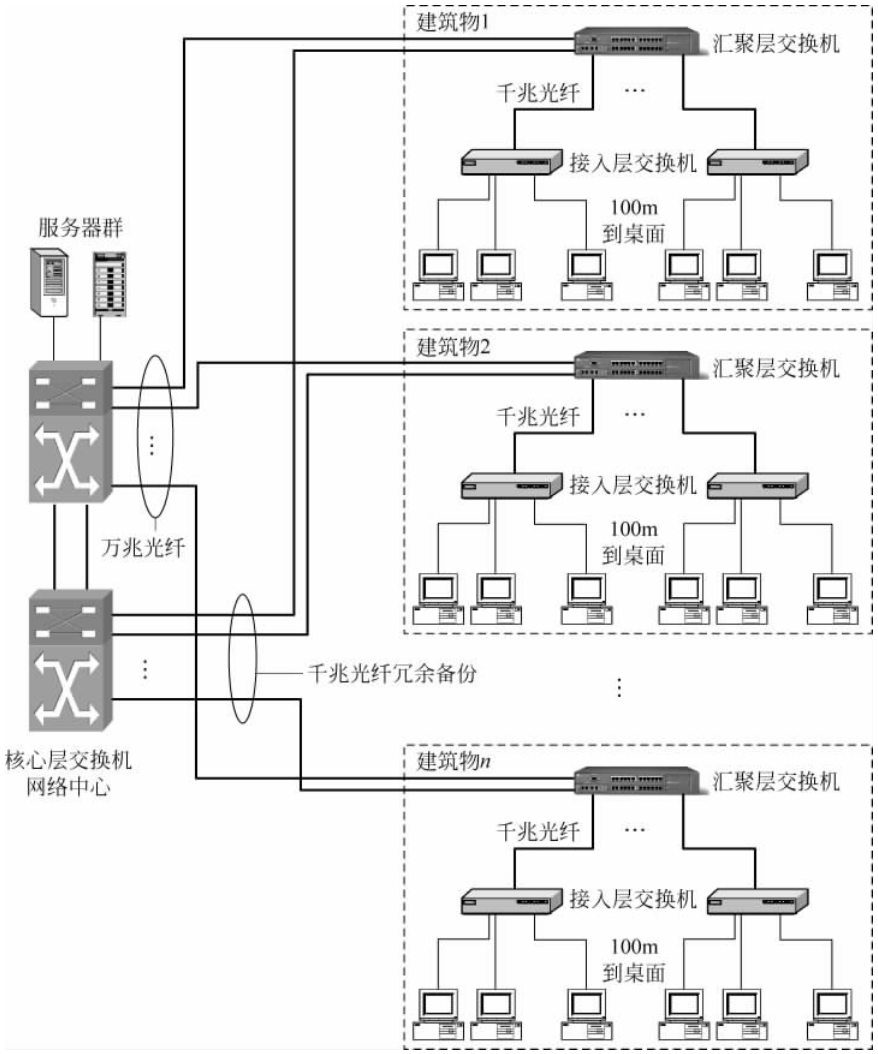

图 3-17　万兆校园网解决方案

交换机为中心，各座建筑设备间的汇聚层交换机直接以光纤通路与核心交换机进行连接，各楼层的接入层交换机可通过光纤或 UTP 与汇聚层交换机相接，形成三级的星形网络结构。这种系统结构具有相当高的灵活性，当网络规模扩展时，不会影响原有网络的正常运行。

核心层由两台万兆交换机组成，交换机之间由两条万兆线路连接，通过 IEEE 802.3ad 进行链路捆绑，从而把整个网络提升到万兆骨干，同时具有充分的扩展能力。汇聚层通过万兆线路分别连接到两台核心交换机上，然后采用千兆线路进行冗余备份，以防万兆线路万一失效，千兆线路立刻可以启用，达到 100％的线路安全和可靠性。

通过双核心技术，不但可以让设备进行冗余备份，而且可以进行中心数据通信

负载均衡,从而让中心设备减轻负荷,保证核心层的稳定性和可靠性。同时,运用两台核心交换机通过 IEEE 802.3ad 进行链路聚合,达到了 40Gbps 带宽。

核心层、汇聚层和接入层都需要采用三层交换机。

对于稳定性和安全性要求特别高的场合,可以采用如图 3-18 所示的三层冗余结构,汇聚层和核心层交换机冗余配置,接入层、汇聚层和核心层交换机之间采用冗余链路连接。

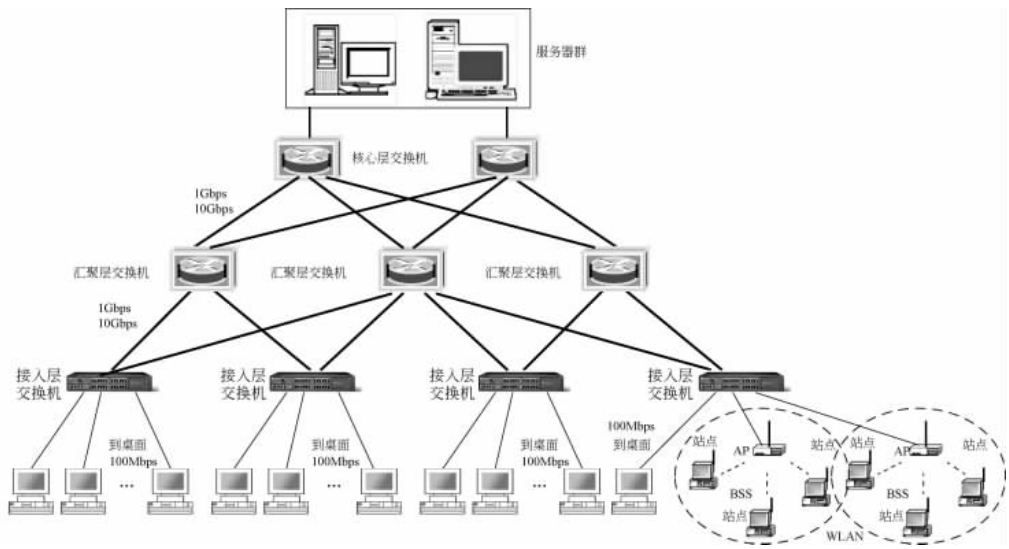

图 3-18 以太网的三层冗余网络结构图

4. 以太网的全连接拓扑网络结构

数据中心(IDC 或云数据中心)容纳了数千至数十万台服务器主机,支持多种云计算应用,是当今息信社会的基础设施。主机一般采用所谓刀片式结构(包括 CPU、内存和磁盘存储的主机)堆叠在机架上,每个机架一般堆放 20～40 台刀片。在机架顶部有一台交换机,又称机架顶部交换机(Top of Rack,TOR),它们与机架上的主机互联,并与数据中心的其他交换机互联。

数据中心网络需要支持外部客户与内部主机之间的高速数据流量,也要支持内部主机之间互联的高速数据流量,因此,对数据中心网络结构需要进行全新的思考。传统的分层结构体系存在不同机架内主机到主机流量受限的问题,一种解决方案是采用全连接拓扑网络结构,如图 3-19 所示。在这种方案中,每台第一层交换机都与所有第二层交换机相连,因此主机到主机的流量不会超过第一层交换机层次。

图 3-19 所示的网络结构可以支持内部任意主机之间互联的 1Gbps 数据流量,网络主干为 10Gbps 以太网,机架交换机到主机终端速率为 1Gbps。

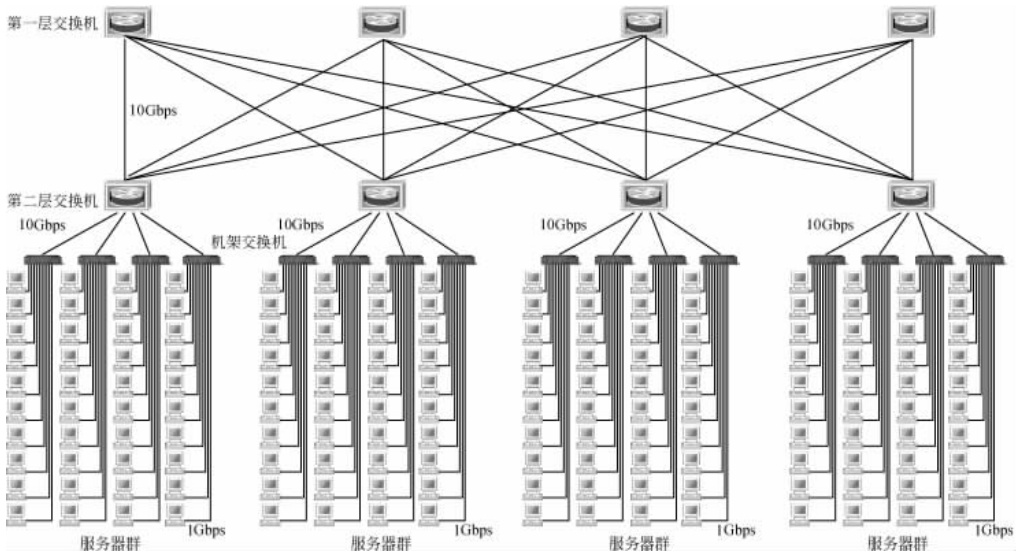

图 3-19　以太网的全连接拓扑网络结构

5. 某大学校园网设计案例

某大学的校园网始建于 1999 年，随着学校的扩展，网络业务种类和用户接入数量呈几何级数增长，原有校园网在带宽、稳定性、覆盖率、管理手段和业务提供上存在不足。新校区包括教学行政区和学生公寓的网络建设，新校区和两处老校区之间距离为 8km，各校区需要通过校园网高速互联，实现统一的教学和办公系统。根据新校园网的整体需求，结合学校的发展，建立一个以先进的多层交换机与多条万兆以太网构成核心体系的高性能、高可靠的三校区互联网络成为校园网的整体目标。校园网系统方案如图 3-20 所示。

核心设备采用两台万兆核心路由交换机 ProCurve 9408sl 和一台万兆核心路由交换机 ProCurve 9308m。

汇聚层设备采用 3 台万兆汇聚三层交换机 ProCurve 3400cl；9308m 和 3400cl 通过万兆线路分别接到两台 9408sl，然后采用千兆线路进行冗余备份。而中心的两台 9408sl 通过一条万兆线路和一条千兆线路互相连接，使用 VRRP 和生成树协议。其余汇聚交换机 5308xl 和 2824 采用冗余千兆线路接入到核心设备。

接入交换机使用 2626 和 2650，采用冗余千兆线路接入到汇聚交换机，实现百兆到桌面。

采用 ProCurve 的 IDM 解决方案，实现中心控制，边缘交换机支持 IEEE 802.1x 或基于 MAC 地址、基于 Web 的用户认证。

通过这种组网方案，保持全面的网络控制，并将控制和智能推至连接用户的网络边缘，使得网络基础设施架构将以网络为中心转变到以用户为中心成为可能。交换机提供智能化的边缘控制，如 IEEE 802.1x 接入认证，解决了全网用户的安全认

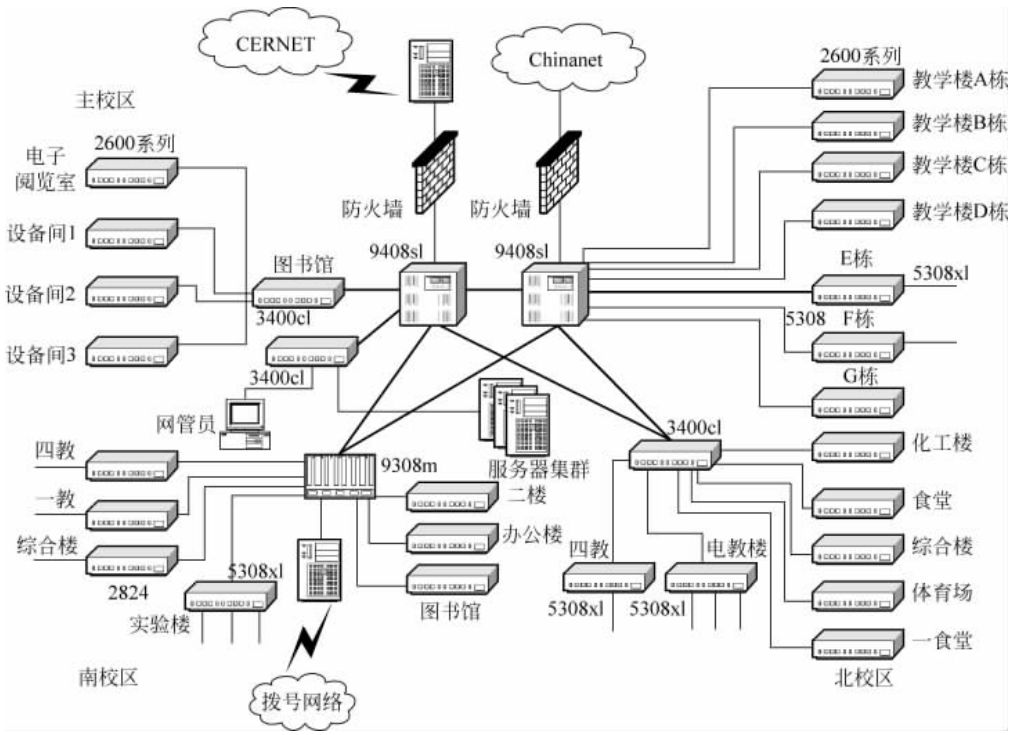

图 3-20 某大学校园网系统方案

证要求,能根据用户的特征由网络管理人员给予个性化的服务,实施针对用户的安全策略,而且不用考虑用户处在校园网中的哪个位置,接入到哪个交换机的端口上。对于教学机房的网络接入,可将非智能化的交换机接入到 5308xl,5308xl 每个端口支持并发的多个 IEEE 802.1x 用户认证。5308xl 系列交换机中集成 IPS(入侵保护系统)技术组件,具有病毒抑制功能,这种技术并不是依靠病毒特征码进行病毒的识别,它无须外置 IPS 模块,而是根据类似蠕虫病毒的特性来进行病毒的划分,识别可路由 VLAN 上的数据特性,可智能地进行病毒的抑制、阻断、防御。

核心交换机具备高密度的万兆端口,汇聚交换机有万兆上联端口,交换机满配置也能实现线速转发,硬件实现 ACL、QoS 以及组播等功能;核心、汇聚、接入都采用冗余连接,确保物理层、链路层、网络层运营稳定、可靠。

3.3 宽带接入技术

3.3.1 接入网和接入技术

接入网是用来将本地的用户端数据设备(通常就是计算机)连接到公用电信网(PSTN、DDN、PSPDN、帧中继网等)的传输线路。类似于传统电话网的用户线路,如图 3-21 所示。从应用的角度理解,接入网是将用户主机连接到 ISP(Internet

Service Provider，互联网服务提供商）/ ICP（Internet Content Provider，互联网内容提供商）的通信链路。

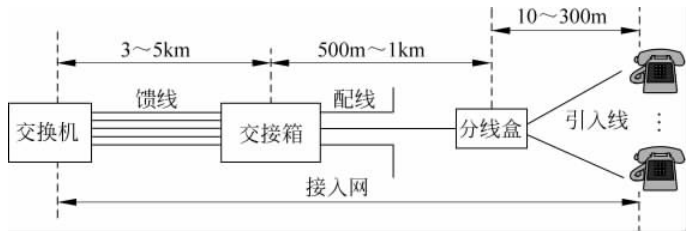

图 3-21　典型的电话用户接入网结构图

用户端数据设备只有接入公用电信网才能够与全球的用户进行信息传输交换，就好像一部电话机只有连接入 PSTN 才可能与全球的电话用户通信，否则只能是局部范围的内部通话。

从计算机网络技术的角度看，接入网要解决的是网络间互联的一段传输介质（信道）问题，在这里的互联是指全球范围的互联，必须借用公用数据传输网而不是自行构建的专线，如图 3-22 所示。

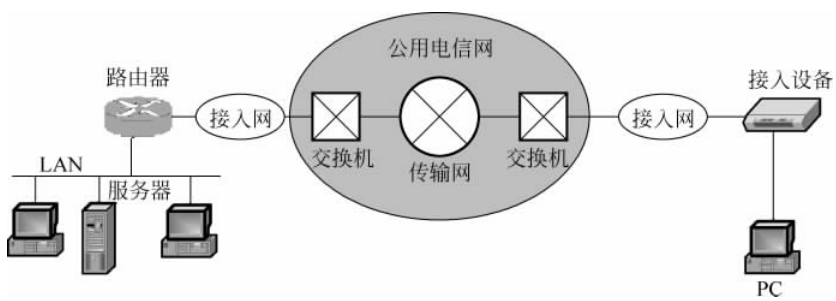

图 3-22　接入网是网络间互联的一段传输介质

从应用的角度，接入网广义是指将 LAN 或单台计算机连接到各种广域网的传输线路，狭义是指将 LAN 或单台计算机连接到 Internet 的传输线路。

国际电联（ITU-T）定义接入网为（公用数据传输网的）本地交换机与用户端设备之间的实施系统。接入网可使用各种传输媒体（如金属双绞线、光纤、同轴电缆、无线系统等），可支持不同的接入类型和业务。

所谓的接入技术就是指各种接入网的构建技术。其中又有宽带接入技术之说。楼宇智能化工程中常用的接入技术如表 3-7 所示。

表 3-7　常用的接入技术应用特性

连接类型	传输速率	使用价格	特性描述
PSTN	最高为 45kbps	最便宜	使用电话线通过调制解调器拨号连接
ISDN	基本速率（BRI）：128 kbps，群速率（PRI）：2Mbps	BRI 比 ADSL 贵，比帧中继便宜	使用电话线通过 ISDN 终端适配器拨号连接，拨号后始终处于连接状态。同时提供语音和数据的可靠数字通信。是一种临时性连接，按需使用带宽，按时、按实际使用带宽付费

续表

连接类型	传输速率	使用价格	特性描述
ADSL	下行：1.544～8.448Mbps，上行：640kbps～1.544Mbps	便宜	使用电话线通过ADSL调制解调器拨号连接。始终处于连接状态。语音和数据可以通过同一根线路同时传输，只能在有限的地方(离ISP约5km距离内)获得接入服务。上行速率慢，不适合上传密集型任务，传输速率不能得到保证
CE1	64kbps	较便宜	是CE1的单个信道。CE1就是把E1(2M)的传输分成30个64kbps的时隙，一般写成$N\times64$
DDN	2.048Mbps	是ADSL的10～20倍，比ISDN贵，比帧中继便宜	在用户端使用信道服务设备(CSU)/数据服务设备(DSU)通过铜缆或光缆与ISP线路连接，是专用的数字电路，通过点对点连接提供高速数据、语音、音频、视频通信。可获得保证的带宽(比ADSL贵的原因)
帧中继	56kbps～44.736Mbps	较贵	使用帧中继访问设备(FRAD)，通过T1线路动态连接。是比较新的快速分组技术，是X.25技术的变体和改良，是最流行的WAN技术之一。实现使用永久虚拟线路(PVC)或交换型虚拟线路(SVC)提供始终在线的连接。可获得保证的带宽，并在信息突发(burst)超过租用带宽时，不需承担额外的费用
光纤	25.6Mbps～2.46Gbps	昂贵	使用ATM交换机，通过租用线路与ISP的ATM交换机进行信元交换。点对点通信，支持使用SVC高速传输语音和视频、图像等多媒体信息，是最完美的WAN技术。网络上所有的硬件都必须支持ATM，造价昂贵
以太网接入	10Mbps～10Gbps	较贵	使用网络交换机，通过租用线路与ISP相连，有时使用协议转换器。依照用户需要可提供不同的带宽，以满足多种需要。网络设备的额外投资不太大，线路费用稍高

3.3.2 宽带接入技术

当前的网络技术飞速发展，电信公用数据传输网已经是光纤的高速网，核心网通道带宽达到百Gbps，节点交换机(或路由器)吞吐量达几十Gbps。LAN的带宽主干达到几十Gbps，到端点可达到100～1000Mbps。但是，接入网的带宽相比之下就过低了，比如，家庭计算机用调制解调器上网速率只有56kbps。因此，接入网已成为网络的瓶颈。宽带接入的目标就是为了突破这个瓶颈，实现用户接入网的数字化、宽带化，提高用户上网速度。从业务需求来看，单一业务越来越少，语音、数据、图像

等综合的多媒体业务需求在增长。宽带接入网按传输介质不同可分为铜线接入技术(xDSL)、光纤接入网技术(FTTx)、无线接入技术、光纤/同轴混合接入网技术。

3.3.3　铜线接入技术

铜线接入技术即数字用户线(Digital Subscriber Line，DSL)技术。它以普通电话线和 3 类/5 类线等铜质双绞线作为传输媒质。由于它采用了全新的数字调制解调技术，所以传输速率比采用音频调制技术、电话拨号的方式快得多。DSL 技术有一个庞大的家族，统称 xDSL，主要有 HDSL、SDSL、ADSL 等，其技术特性如表 3-8 所示。这些方案都是通过一对调制解调器来实现的，其中一个调制解调器放置在电信局，另一个调制解调器放置在用户侧。它们主要的区别就是体现在信号传输速度和距离的不同以及上行速率和下行速率对称性的不同这两个方面。

表 3-8　xDSL 技术特性比较

DSL 类别	下行速率	上行速率	可用距离	应用范围	双绞线数量	语音数据分离器
HDSL	2Mbps	2Mbps	最大 5km，增加中继设备可达 12km	蜂窝通信，T1/E1 连接	2	无
HDSL2	2Mbps	2Mbps	最大 5km	类似 HDSL，互联网接入，远程视频会议，网间连接	1	无
ADSL	最大 8Mbps	最大 768kbps	最高速度下最大距离 3.6km	互联网接入，远程视频会议，交互多媒体，视频点播，网间连接	1	有
RADSL	最大 8Mbps	最大 768kbps	最大 6km	互联网接入，远程视频会议，交互多媒体，视频点播，网间连接	1	有
IDSL	最大 2Mbps	最大 2Mbps	最大 5km	互联网接入，远程视频会议，交互多媒体，视频点播，网间连接	1	有
SDSL	768kbps	768kbps	最大 4km	互联网接入，远程视频会议，交互多媒体，视频点播，网间连接	1	有
VDSL	13/26/52Mbps	6/13Mbps	最大 1.5km	互联网接入、远程视频会议、交互多媒体、视频点播、网间连接、HDTV 高清电视传送	1	有

3.3.4 光纤接入网技术

光纤接入网(FTTx)是指用光纤作为主要传输介质来实现信息传输的接入网。它具有可用带宽宽、传输质量高、传输距离长、抗干扰能力强、网络可靠性高、节约管道资源等优点。光纤接入网从技术上可分为两大类：有源光网络(Active Optical Network，AON)和无源光网络(Passive Optical Network，PON)。FTTx技术代表FTTB(Fiber To The Building，光纤到大楼)、FTTH(Fiber To The Home，光纤到户)、FTTC(Fiber To The Curb，光纤到配线盒/路边)等。除了FTTH外，其他方式都需通过铜芯线作接入转换，组成混合接入网络。

1. 有源光网络

有源光网络(AON)比无源光网络(PON)容易实现，AON的传输距离和容量均大于PON，传输带宽易于扩展。图3-23是用AON实现智能建筑计算机网络高速接入的原理图。AON的缺点是需要进行光电、电光转换，要使用专门的场地和机房，远端供电问题不易解决，日常维护工作量较大。AON包括基于ATM、SDH、PDH和LAN的有源光网络，目前AON主要采用SDH环形网络结构和ATM技术，因而具有环形网络结构的自愈功能。ATM信元在SDH环形网络中传输，其带宽由环形网络上的所有节点所共享。针对接入网中用户数量多、带宽需求不确定等情况，AON能够根据环形网络上各节点所需的业务质量级别(QoS)和需要传输的实际业务量，动态地按需分配带宽到各节点和各用户，所以AON既能够适应高QoS业务的传输，也能够适应突发性业务的传输。

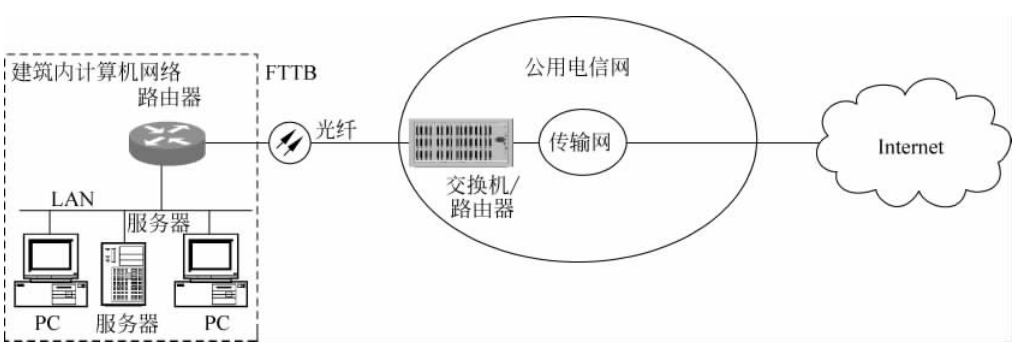

图3-23 FTTB智能建筑计算机网络高速接入

2. 无源光网络

无源光网络(PON)不需要在外部站点安装有源电子设备，如图3-24所示。PON由局端的OLT(Optical Line Terminal，光线路终端)、用户端的ONT/ONU(Optical Network Terminal/Optical Network Unit，光网络终端/光网络单元)、连接

前两种设备的光纤和无源分光器(splitter)组成的 ODN(Optical Distribution Network,光分配网络)以及网管系统组成。PON 的“无源”是指 ODN 全部由分光器等无源器件组成,不含有任何电子器件及电源。PON 包括 ATM-PON(APON,即基于 ATM 的无源光网络)和 Ethernet-PON(EPON,即基于以太网的无源光网络)两种。

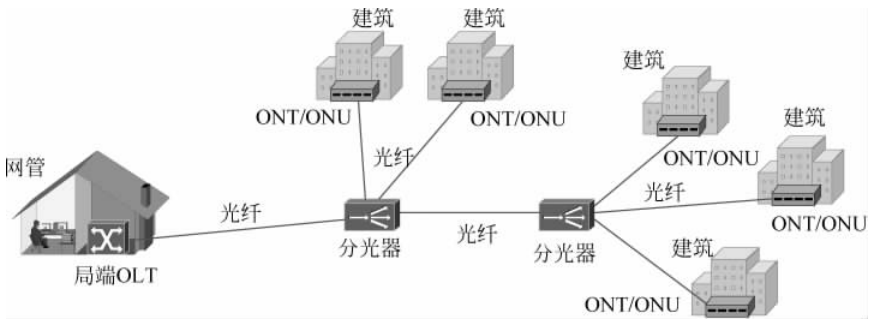

图 3-24　无源光网络(PON)的组成结构

3. EPON 以太网无源光网络

EPON 的结构如图 3-25 所示。局端 OLT 与用户 ONT/ONU 之间仅有光纤、分光器等光无源器件,无须租用机房,无须配备电源,无须有源设备维护人员,因此,可有效节省建设和运营维护成本。

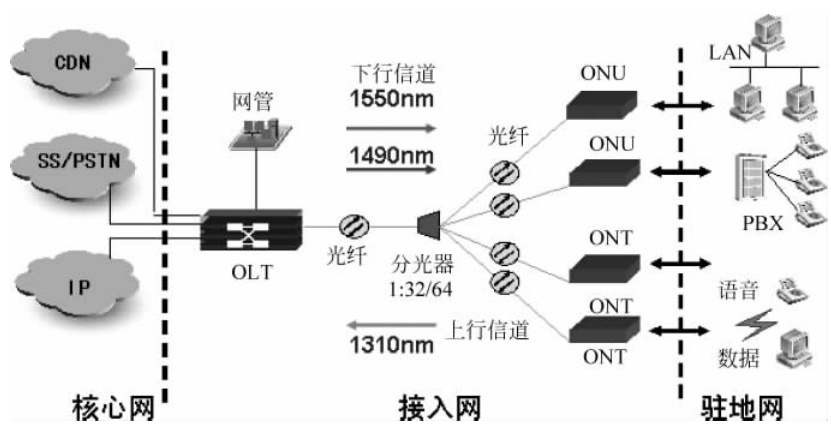

图 3-25　EPON 以太网无源光网络结构

EPON 采用单纤波分复用技术(下行 1490nm,上行 1310nm),仅需一根主干光纤和一个 OLT,传输距离可达 20km。在 ONU 侧通过光分路器分送给最多 32 个用户,因此可大大降低成本压力。每个节点可提供 1～1000Mbps 的接入带宽,真正实现“千兆到桌面”的带宽接入。

TDM 数据(语音业务)和 IP 数据采用 IEEE 802.3 以太网的格式进行传输,辅

以电信级的网管系统,足以保证传输质量。通过扩展第三个波长(通常为1550nm)即可实现视频业务广播传输。

4. GPON千兆无源光网络

GPON(Gigabit PON)是最新一代宽带无源光综合接入标准,对于其他的PON标准而言,GPON标准提供了前所未有的高带宽,下行速率高达2.5Gbps,其非对称特性更能适应宽带数据业务市场(如数字广播业务、VOD、IPTV、文件下载等)。GPON的传输机制和EPON完全相同,都是采用单纤双向传输机制,在同一根光纤上,使用WDM技术,用不同波长传输上下行数据,实现信号的双向传输。一根光纤可以被中心站20km范围内的所有用户共享,典型的支持速率是上行1.244 16Gbps、下行2.488 32Gbps。

在GPON标准中,明确规定需要支持的业务类型包括数据业务(Ethernet业务,包括IP业务和MPEG视频流)、PSTN业务(POTS,ISDN业务)、专用线(T1、E1、DS3、E3和ATM业务)和视频业务(数字视频)。GPON中的多业务映射到ATM信元或GEM帧中进行传送,对各种业务类型都能提供相应的QoS保证。

GPON承载有QoS保证的多业务和强大的OAM能力等优势很大程度上是以技术和设备的复杂性为代价换来的,从而使得相关设备成本较高。GPON比EPON带宽更大,它的业务承载更高效,分光能力更强,可以传输更大带宽的业务,实现更多用户接入,更注重多业务和QoS保证,但实现更复杂,这也导致其成本相对EPON较高。随着GPON技术的大规模部署,GPON和EPON成本差异在逐步缩小。

光纤接入是接入网的发展方向,当前应用中,FTTB已经成为智能建筑计算机网高速接入的主流。FTTH是家庭用户网今后发展的必然方向。

3.3.5 以太网接入

以太网接入是指将以太网技术与综合布线相结合,作为公用电信网的接入网,直接向用户提供基于IP的多种业务的传送通道。以太网技术的实质是一种两层的介质访问控制技术,可以在UTP铜缆/光纤上传送,是LAN的技术推广至城域网的结果,也可以与其他接入介质相结合,形成多种宽带接入技术。以太网与电话铜缆上的VDSL相结合,形成EoVDSL技术;与无源光网络相结合,产生EPON技术;在无线环境中,发展为WLAN技术。

3.3.6 无线接入

只要在交换节点到用户终端部分地或全部地采用了无线传输方式,就称为无线接入。有两种应用方式:固定无线接入方式和移动无线接入方式。固定无线接入方式是指固定用户以无线的方式接入到固定电信网的交换机,又称为无线本地环路

(WLL)。移动无线接入方式是指移动的用户以无线的方式接入到固定电信网的交换机。

无线接入可以理解为公用数据网应用 WLAN 技术,将服务区覆盖到本地固定用户,如图 3-26 所示。无线接入不是在现有的移动通信网平台上,而是应用 WLAN 技术,构建的是一个高速无线数据传输网,传输速率达到 54Mbps,将来会达到 300Mbps 的速率。无线接入技术是继 FTTH 之后又一个值得期待的接入技术,由于它无须布线,又支持移动计算,因此有巨大的应用前景。

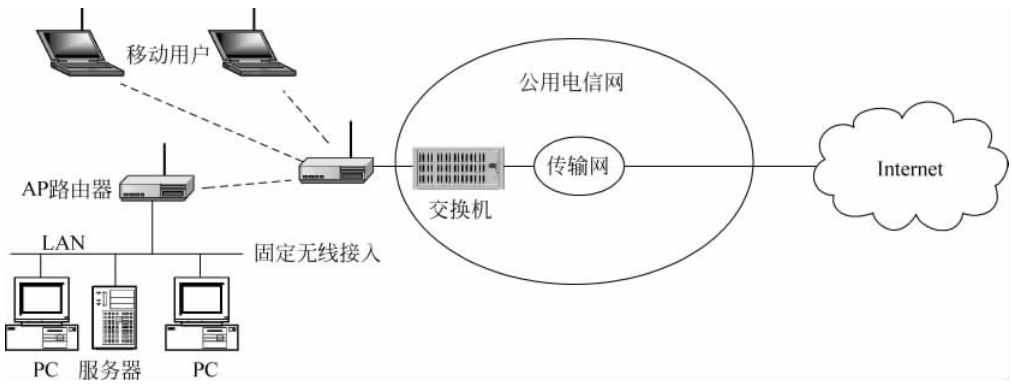

图 3-26　无线网高速接入

3.4　建筑内的 Intranet

3.4.1　Internet 网络技术

从一般的意义而言,Internet 这个词可指由多个不同的网络通过网络互联设备连接而成的大网络,人们常把这类网络称为网际网。本书所讨论的 Internet 是指开始在美国建立,现在已连接到世界各国的一个特定的大网络,尽管它也是一种网际网,但人们都称之为 Internet(因特网),从而 Internet 成了这个特定网际网的名字。

1. Internet 的概念

从网络的角度,Internet 就是一个分布式的全球性的计算机网络,如图 3-27 所示。这个网络的互联基础就是 TCP/IP,各个子网有一个唯一的地址(IP 地址),相互之间通过路由器连接,数据的传输和交换都是在 IP 数据包中遵守 TCP 协议进行的。

图 3-27 中的主机 A 可能是在中国大学的一台计算机,主机 B 可能是在英国大学的一台计算机,它们都接入 Internet,相互之间就可以进行数据通信。如果仅此而已,则 Internet 好似国际电话网,主机 A 和主机 B 好似两部电话机一般,Internet 可以为两台计算机提供通信信道。实际上,Internet 的作用远不是这些,它的价值不在于为两台计算机提供通信信道,而是开创了所谓“信息服务”的时代。

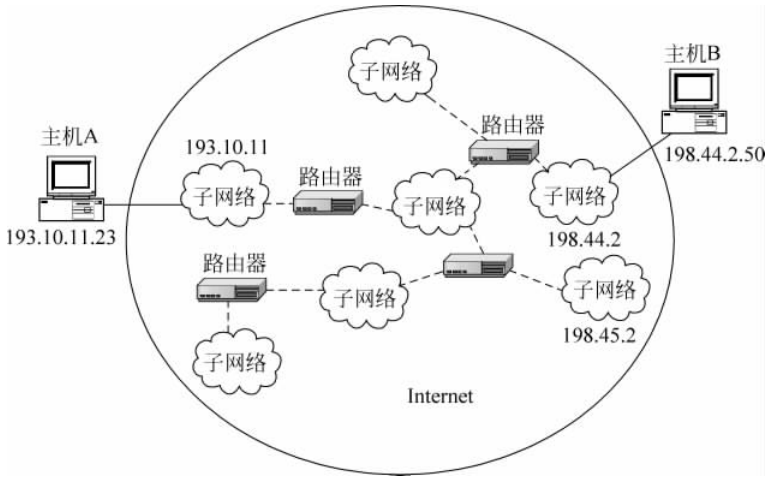

图 3-27 Internet 是一个分布式的全球性的计算机网络

所以,我们在理解 Internet 的时候必须换一个角度。从信息服务功能角度来看,Internet 是这样的一个信息系统及平台:Internet 是由许多提供各类服务的主机(服务器)所组成的集合,用户向它们提出请求(访问),它们就会响应请求而提供服务,这一切对用户而言是透明的,如图 3-28 所示。

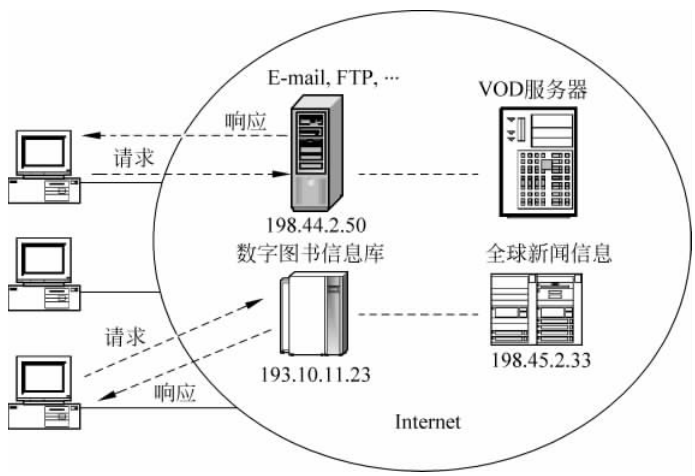

图 3-28 Internet 是信息系统及平台

所谓的透明,是指用户在向某个主机提出服务请求时,并不关心该主机在何地,它是如何连接到 Internet 的,它的硬件是什么,它运行何种 NOS 等等,只需要知道该主机的 IP 地址(或域名)。

Internet 用 C/S 和 B/S 方式来提供信息服务,向所有用户提供标准的请求响应。只要一台主机愿意提供某种服务,在遵守这一规则的前提下,就可以融入 Internet 的信息系统中,所以,Internet 也为所有用户提供了一个信息服务的平台。

Internet 所提供的信息服务绝大多数是免费的，只要支付一定数量的通信费用，用户就可以获得巨大的信息。这是 Internet 成功的根本保证。

Internet 是由分散在世界各国的大量网络互联而成的网络集合，这些网络的规模各异，有各国的国家级网络，有各部门的专业网络、校园网、企业网等，它们归属于不同的组织和部门，由各单位和部门负责使用和管理。因此，严格意义上，Internet 是一个松散的大集体，没有统一的管理机构。这也是 Internet 取得成功的重要原因。

经过二十多年的发展，Internet 获得了巨大的成功。Internet 是目前世界上规模最大、用户最多、资源最丰富的网络互联系统，是全球信息高速公路的雏形和未来信息社会的蓝图。

2. Internet 提供的主要服务

当前的 Internet 所能提供服务实在是太多了，并且，每一时刻都有新的服务出现。这里只能介绍一些常见服务类型，目的是帮助读者进一步理解 Internet 的技术内涵。

Internet 的资源涉及人们从事的各个领域、行业以及社会公共服务等方面，包括自然科学、社会科学、技术科学、农业、气象、医学、军事等。Internet 的信息资源是分布在整个网络中的，没有统一的组织和管理，也没有统一的目录。但对于用户来说，Internet 提供了以下一些基本信息服务。

1）远程登录服务（Telnet）

远程登录（remote login）是 Internet 提供的最基本的信息服务之一。Internet 用户的远程登录是在网络通信协议 Telnet 的支持下，使自己的计算机暂时成为远程计算机仿真终端的过程。要在远程计算机上登录，首先应给出远程计算机的域名或 IP 地址。登录成功的用户可以实时使用远程计算机对外开放的功能和资源。许多大学图书馆都通过 Telnet 对外提供联机检索服务，一些政府部门、研究机构也将它们的数据库对外开放，便于用户通过 Telnet 进行查询。

2）文件传输服务（FTP）

FTP 与 Telnet 类似，也是一种实时的联机服务。在进行工作时，用户首先要登录到对方的计算机上，登录后用户只能进行与文件搜索和文件传送等有关的操作。使用 FTP 几乎可以传送任何类型的文件，如文本文件、二进制文件、图像文件、声音文件、数据压缩文件等。

3）电子邮件服务（E-mail）

电子邮件是 Internet 上使用最广泛、最受欢迎的服务之一。它是网络用户之间进行快速、简便、可靠且低成本联络的现代通信手段。电子邮件使网络用户能够发送或接收文字、图像和语音等多种形式的信息。

4）网上浏览服务（万维网服务 WWW）

网上浏览服务通常是指 WWW（World Wide Web）服务，它是 Internet 信息服务的核心，也是目前 Internet 上使用最广泛的信息服务。WWW 是一种基于超文本文

件的交互式多媒体信息检索工具。WWW 服务采用 B/S(浏览器/服务器)工作模式,由 WWW 客户端软件(浏览器)、Web 服务器和 WWW 协议组成。WWW 的信息资源以页面(也称网页、Web 页)的形式存储在 Web 服务器中,用户通过客户端的浏览器向 Web 服务器(通常也称为 WWW 站点或 Web 站点)发出请求,服务器将用户请求的网页返回给客户端,浏览器接收到网页后对其进行解释,最终将一个文字、图片、声音、动画、影视并茂的画面呈现给用户。

5) 搜索引擎服务

搜索引擎是目前最好的信息查询服务,它帮助用户利用某些关键词在 Internet 上查找自己所需要的资料。在搜索引擎出现以前,常见的信息查询工具有 Archie、WAIS、Gopher 和 WWW 等。常见的搜索引擎网站有 www. baidu. com, www. google. com 等。

除了上述服务外,Internet 上还提供诸如新闻组(Usenet)、电子公告板(BBS)、网上聊天、网上寻呼、网络会议、网上购物、网上教学和娱乐等功能。这些功能很多都可以通过网络应用软件来实现,例如,Microsoft Chat 可以实现网上聊天; Internet Explorer 可以实现网上购物; Microsoft NetMeeting 可以实现网络会议; Microsoft NetShow 可以实现网上教学和娱乐功能等。

3.4.2 Intranet 网络技术

1. Intranet 的概念与模型

Intranet 又称为企业内部网,是 Internet 技术在企业 LAN 或 WAN 上的应用。它的基本思想是:在内部网络上采用 TCP/IP 作为通信协议,利用 Internet 的 Web 模型作为标准平台,同时建立防火墙把内部网和 Internet 隔开。当然,Intranet 并非一定要和 Internet 连接在一起,它完全可以自成一体为一个独立的网络。

Intranet 基于 Internet 的 Web 模型,这一模型称为 B/S 模型(Browser/Server,浏览器/服务器模型)。Web 平台是一种先进的计算平台。Web 的 B/S 计算模式是一种三层结构的 C/S 计算,它把传统 C/S 模型中的服务器分解为一个应用服务器(Web 服务器)和一个或多个数据服务器。在服务器端集中了所有应用逻辑。所有的开发与维护工作都可集中在服务器端。在客户机上通过直观、易于使用的浏览器来从 Web 服务器上获取信息。Web 服务器通过 HTTP 建立了内部页面和各相关后端数据库的超文本链接,所以最终可以用浏览器查询所有网络服务器上的信息。

2. Intranet 的系统结构

Intranet 的一般系统结构如图 3-29 所示。如果 Intranet 只是一个单纯的企业 LAN,就不需要和 Internet 连接起来,建立这样的 Intranet 相对简单,只需配置 Intranet 服务器,并在工作站上安装 Intranet 客户端软件即可。如果 Intranet 需要和 Internet 连接,为了保证 Intranet 的安全,需要在 Intranet 内部数据区与外部

Internet 之间构筑一道防火墙，Intranet 主机可以拥有 IP 地址以便外部 Internet 访问。和 Internet 相连的 Intranet 一般都有一个 Internet 服务器作为公共 Web 服务器和 E-mail 服务器。Web 服务器可作为企业 Intranet 对外发布信息的窗口，允许任何 Internet 用户自由地访问。Intranet 服务器包括一个内部 Web 服务器和一个或多个数据库服务器。

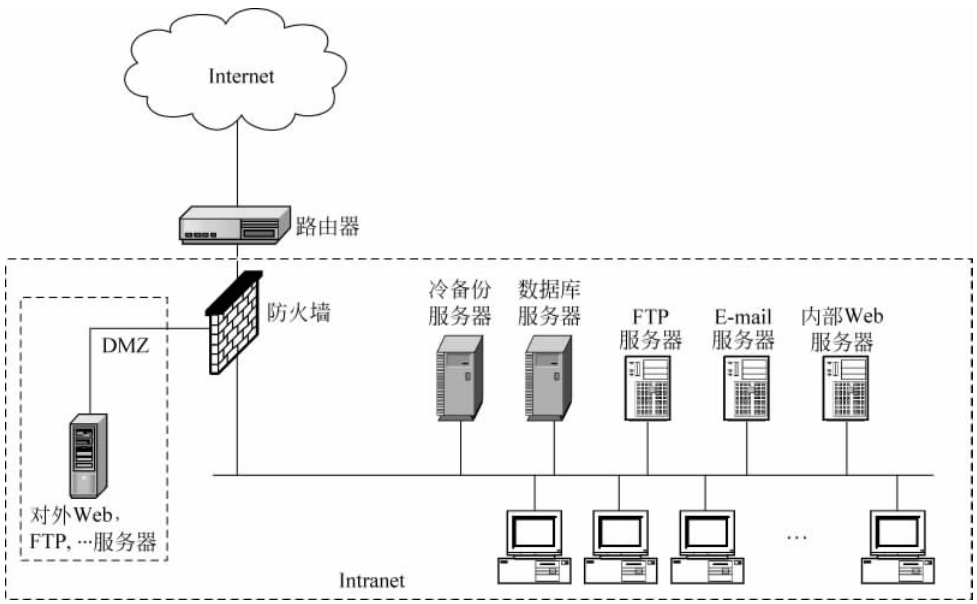

图 3-29　Intranet 的一般系统结构

3. Intranet 的特点

与过去的企业网相比较，Intranet 虽然还是企业内部的局域网（或多个局域网局部相连的广域网），但它与传统局域网 C/S（客户机/服务器）模式又有不同。简单地说，在网络拓扑结构上采用传统的构网理论，但在技术上，以 Internet 协议和 Web 技术为基础。可实现任意的点对点通信。而且依赖 Web 服务和其他 Internet 网络服务完成以往无法实现的功能。Intranet 具有以下特点：

（1）Intranet 归企业的内部使用，因此对用户有严格的权限控制，并设置防火墙等安全机制。外部用户只能访问企业的 Web 站点，未经授权无法进入 Intranet 获取企业其他内部资源。

（2）Intranet 的动态页面能实时反映数据库的内容，用户可以查询数据，还可以增加、修改和删除数据库的数据。

（3）采用 TCP/IP 作为网络的传输协议。基于 TCP/IP 协议，它可以跨越当前几乎所有的平台。任何平台上只要安装一个浏览器，就可以访问 Web 服务器。用 HTML、Java 开发的应用系统可以简单地移植到任何平台上。克服了传统企业的网络因平台的不同而必须改变已开发的应用系统的缺点。

4. Intranet 的功能

Intranet 除了能提供 Internet 上提供的基本服务(例如 E-mail、WWW、FTP 等)外,Intranet 最重要的特点是网络安全功能和企业多种应用信息系统的功能。

Intranet 的服务类型可分为基本服务、可选服务和特殊服务。Intranet 提供的基本服务包括 DNS、E-mail 和 WWW 服务;提供的可选服务包括 FTP、Telnet 等,用于网络文件的传输、网络的远程管理操作;某些企业构建的 Intranet 还提供一些为本企业服务的特殊服务,如数据库、事务处理、CIS、CAD、视频会议、网络电话、网络 Fax、远程教育等。

5. Intranet 安全管理

企业内部网在经过几年的发展后,逐渐从封闭走向开放,各单位纷纷加入 Intranet。为保护内部网络的安全性,在规划网络时,应统一考虑和建立网络安全措施。与 Internet 相比,Intranet 网络的最大优势也是其安全性。

网络安全措施可分为加密技术和防火墙技术。加密技术对于网络中传输的数据进行加密处理,在达到目的地址后,解密还原为原始数据,以此防止非法用户对信息的截取和盗用。

防火墙技术通过对网络的隔离和限制访问的方法来控制网络的访问权限,从而保护网络资源。防火墙技术是一种访问控制技术,它用于加强两个或多个网络间的边界防卫能力。其工作方法是:在公共网络和专用网络之间设立隔离墙,在此检查进出专用网络的信息是否被允许通过,或用户的服务请求是否被允许,从而防止对信息资源的非法访问和非法用户的进入,它属于一种被动型防卫技术。由于防火墙只能对跨越网络边界的信息进行监测、控制,而对网络内部人员的攻击不具备防范能力,因此单纯依靠防火墙保护网络的安全性是不够的,还必须与其他安全措施综合使用,才能达到目的。

3.4.3 Web 服务器

Web 是传送文档,包括文件、图形甚至是语音和视频图像给远程访问者的平台。Web 采用 B/S 模式进行信息的传输:客户 Web 浏览器通过 HTTP 协议将特定的 URL(Uniform Resource Location,统一资源定位符)发送到 Web 服务器来请求页面,Web 服务器使用 URL 中的信息来定位和返回页面内容。与传统的 C/S 模式不同的是,这里 Web 服务器不需要保留与客户端浏览器连接的信息,当客户通过 HTTP 协议连接到 Web 服务器并提出文档请求,Web 服务器响应请求,将文档提交给客户便立即关闭连接。

Web 服务器中除提供它自身的独特信息服务之外,还“指引”着存放在其他服务器上的信息,而那些服务器又“指引”着更多的服务器。这样,全球范围的信息服务

器互相指引而形成信息网络。这也是将其称之为 World Wide Web 的原因。

Web 服务器应能支持和响应多种请求。从 Web 服务器返回的页面可以是 3 种类型：静态 HTML 页面、动态 HTML 页面或目录列表页面。

1. 基于 Web 的信息管理模式

当前流行的企业信息管理模式是一种分布式的基于 Web 的管理模式，如图 3-30 所示。在这种信息管理模式下，企业中可有多台 Web 服务器和数据库服务器，用户可在浏览器上通过 Web 服务器实现对各数据库的访问。其中客户机端只需要安装相应的浏览器软件，而 Web 服务器上需要开发对各数据库的访问接口。

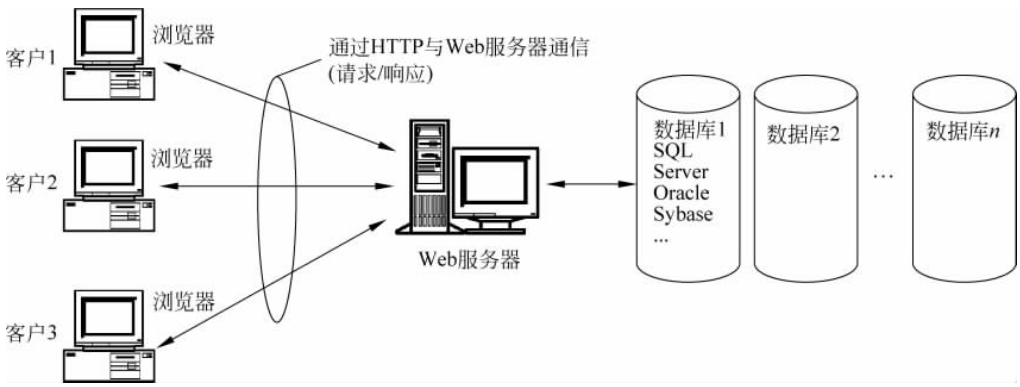

图 3-30　基于 Web 的管理模式

与传统的 C/S 方案相比，基于 Web 的信息系统可以给应用开发者和管理者带来以下好处：用户只需在一种界面上（浏览器）就可访问所有类型的信息，而不用操作多种多样的、经常不相容的传统应用和数据库界面。同时具有传统的 C/S 系统的可用性和灵活性，用户访问权力和限制的集中管理，使得基于 Web 的 B/S 应用更易于扩充，更易于管理。

现在，XML Web Services 已经使应用程序服务器和 Web 服务器的界线混淆了。通过传送一个 XML 有效载荷（payload）给服务器，Web 服务器现在可以处理数据和响应（response）的能力与以前的应用程序服务器同样多了。

2. 组建 Web 服务器平台

虽然从客户端的浏览器来看，所有的 Web 服务器都是透明的，但是 Web 服务器平台实际上是有多种构建方案和选择的。B/S 方式将开发工作全部转移到 Web 服务器端，因此，在组建 Web 服务器平台时的就应考虑开发环境及工具。

1）操作系统

任何 Web 服务器都是运行在网络操作系统上的，如图 3-31 所示。实际上 Web 服务器就是网络操作系统的一个应用。相类似的还有数据库服务等。

目前，网络操作系统可分为两大类：UNIX 系统和 Windows 系统。对应这两大

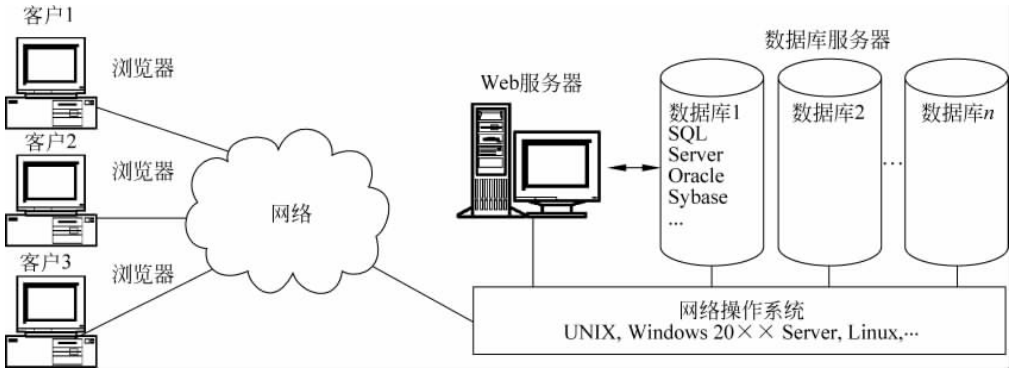

图 3-31 Web 服务器建在网络操作系统之上

类操作系统,Web 的开发平台构架分别是 J2EE 和 ASP. NET。

运行在 Windows 操作系统上的 Web 服务器主要是 IIS,IIS 是 Internet Information Services 的缩写,是 Microsoft 公司的 Web 服务器,Gopher 服务器和 FTP 服务器全部包容在里面。

Apache 是世界使用排名第一的 Web 服务器软件。它可以运行在几乎所有广泛使用的计算机平台上,由于其跨平台和安全性而被广泛使用,是最流行的 Web 服务器端软件之一。

Nginx 是一款轻量级的 Web 服务器/反向代理服务器及电子邮件(IMAP/POP3)代理服务器,其特点是占用内存少,并发能力强。

2) ASP. NET 开发平台

ASP. NET 的前身是 ASP 技术,ASP(Active Server Pages)是早先 Windows 系统上开发 Web 应用的技术。ASP. NET 不能只被看作是 ASP 的下一个版本,它是一种建立在通用语言上的优秀程序架构,而且可以运行于多种平台的 Web 服务器之上。ASP . NET 在 2. 0 版时功能已大致确定,成为 Web 应用程序的基础架构,Microsoft 公司开始在 ASP. NET 2. 0 上开发扩充的功能,包括 AJAX 的支持、MVC 架构的支持以及更容易开发出数据库应用的架构。目前的 ASP. NET 4. 0 版与 Visual Studio 2010 一起发布,配合. NET Framework 4. 0 让 Web 应用程序具有如并行运算库(parallel library)等新功能。

因为 ASP. NET 是基于通用语言的编译运行的程序,其实现完全依赖于虚拟机,所以它拥有跨平台性,ASP. NET 构建的应用程序可以运行在几乎全部的平台上。ASP. NET 开发的首选语言是 C# 及 VB. NET,同时也支持多种语言的开发,例如 Java/J#、Python、JScript 等。

IIS 是 Microsoft 公司的 Web 服务器,包含了对 ASP. NET、JSP 和 PHP 的支持。ADO. NET 是一种能够让用户采用 SQL 语言与数据库进行交互的编程模型。是一组用于和数据源进行交互的面向对象类库。通常情况下,数据源是数据库,但它同样也可以是文本文件、Excel 表格或者 XML 文件。Windows 系统上的 ASP.

NET 开发平台如图 3-32 所示。

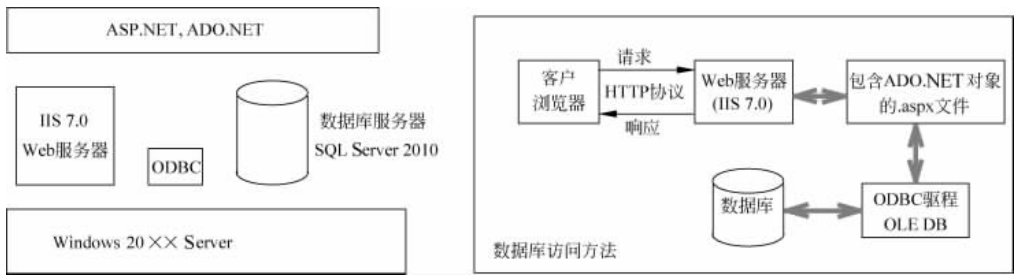

图 3-32　Windows 系统上的 ASP. NET 开发平台

3）J2EE 开发平台

J2EE(Java 2 Platform Enterprise Edition)是建立在 Java 2 平台上的企业级应用的解决方案。Java 本身的跨平台性使得 J2EE 有许多优点，例如“编写一次、随处运行”的特性、方便存取数据库的 JDBC API、CORBA 技术以及能够在 Internet 应用中保护数据的安全模式等，同时还提供了对 EJB(Enterprise JavaBeans)、Java Servlets API、JSP(Java Server Pages)以及 XML 技术的全面支持。其最终目标是成为一个支持企业级应用开发的体系结构，简化企业解决方案的开发、部署和管理等复杂问题。J2EE Web Services 开发模型如图 3-33 所示。

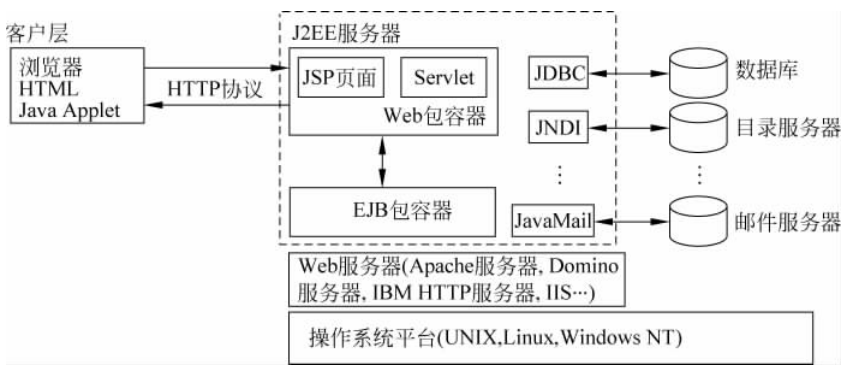

图 3-33　J2EE Web Services 开发模型

3.4.4　建立楼宇内的 Intranet 网

建立智能楼宇的 Intranet 网，实质就是在智能楼宇内的计算机局域网络环境下构建 B/S 方式的运行和开发平台。在实现 Intranet 方案时，要考虑到系统的可靠性、安全性和扩展性。客户端的方案首选是 Windows＋IE，也可以采用 Linux＋Netscape。对 Web 服务器端，目前的技术提供了多个可选方案，但是，根据所采用的主机操作系统大致可分为三类：低端的 Linux 架构、性价比优良的 Windows 20xx Server 架构和高端的 UNIX 架构。

1. Linux 架构

Linux 是免费的操作系统,在其上构建 Web 服务器平台是廉价的解决方案。在 Linux 系统下,Apache 是最好、最普及的 Web 服务器,后台数据库可根据实际情况选择 Oracle、Sybase、DB2 或 Informax、MySQL 等。图 3-34 所示的是一种 Linux 架构解决方案——Linux+Apache+Tomcat+MySQL,该方案支持 JSP 技术。

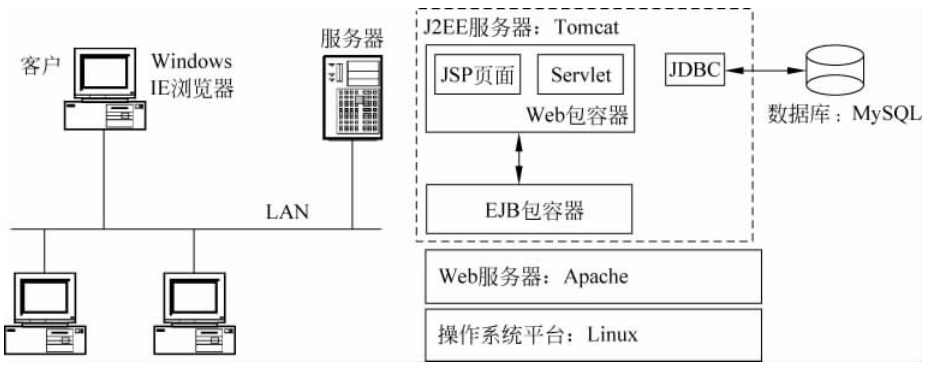

图 3-34 一种 Linux 架构解决方案：Linux+Apache+Tomcat+MySQL

Apache 和 Tomcat 都可以作为独立的 Web 服务器来用,Apache 功能强大、高效,但并不能支持 JSP 及 Servlet。Tomcat 能支持 JSP,但是当处理静态页面时 Tomcat 不如 Apache 迅速,又不如 Apache 一样强壮。基于以上原因,使用一个 Apache 作为 Web 服务器,为网站的静态页面请求提供服务。使用 Tomcat 服务器作为一个 Servlet/JSP 插件,显示网站的动态页面。Apache+Tomcat 结构具有更好的可扩展性和安全性。

2. Windows 20×× Server 架构

这是当前应用最广泛的 Intranet 方案架构:Windows 20×× Server+IIS+SQL Server+ASP.NET,如图 3-35 所示。实际上,Windows 20×× Server 已经将一整套的 Web 服务器应用集成到操作系统中,其中就包括了服务功能强大的 Web 服务器 IIS(Internet Information Server)。

3. UNIX 构架

对于大型企业而言,选用 UNIX 系统构建 Intranet 更为合适。UNIX 本身具备丰富的网络功能,易于配置成为企业内部的 Web 服务器,利用客户端的浏览器软件就可实现 WWW 的各项功能。同时 UNIX 良好的稳定性和安全性对企业网也是至关重要的。

Apache 仍然是 UNIX 系统下最好的 Web 服务器之一,对于支持 J2EE 的 Web 服务器,大型的企业级网站可采用 IBM WebSphere Application Server、BEA

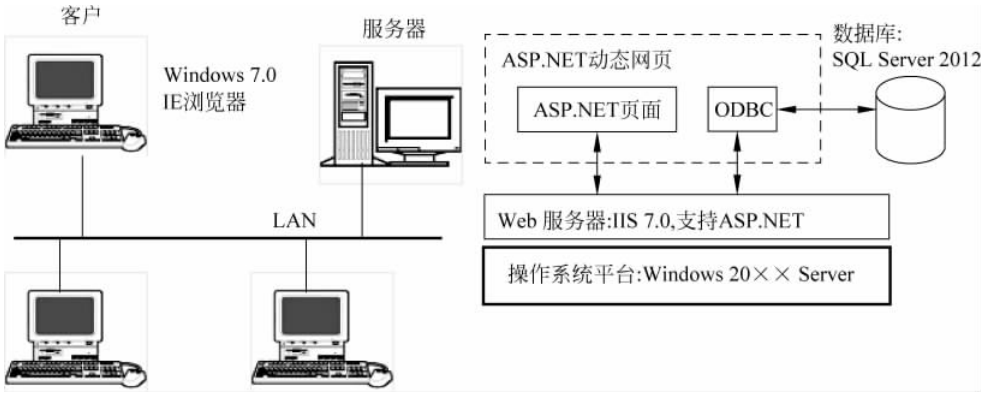

图 3-35　Intranet 的 Windows 20×× Server 构架方案

Weblogic Application Server 和 SUN iPlanet Enterprise Web Server 等作为 Web 服务器。图 3-36 是 UNIX 架构的一种方案：UNIX＋Apache＋WebSphere＋J2SDK＋Oracle。

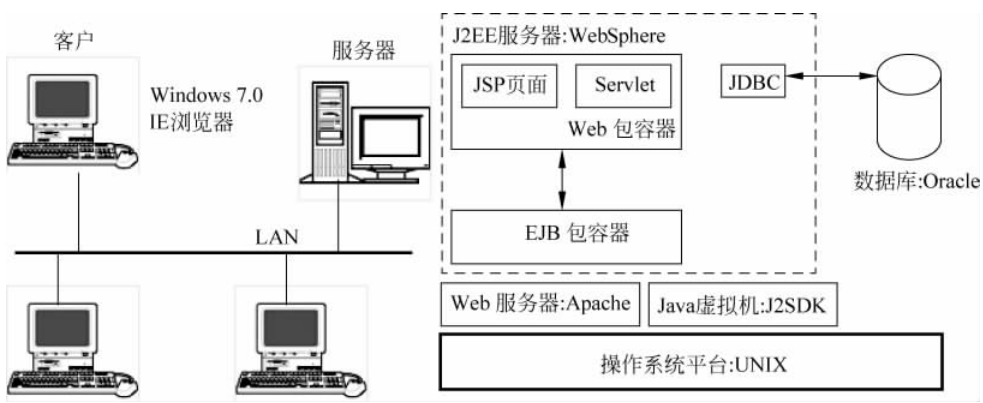

图 3-36　UNIX 构架的一种方案

4. Internet/Intranet 的互联

图 3-37 是一个 Internet/Intranet 互联方案。Intranet 到 Internet 的连接之间应设置防火墙进行安全控制。同时根据不同服务器的安全级别不同，把它们安装在不同的位置。其中的对外 Web 服务器和 DNS/E-mail 服务器安装在 DMZ 区（防火墙的中立区），网管工作站等安装在网络内部。所有对数据库的访问都必须经过二级防火墙，确保数据库服务器的安全。使用一台路由器通过宽带接入 Internet。

一级防火墙为隔离 Internet 与 Intranet 的第一道屏障。

DMZ 是英文 Demilitarized Zone 的缩写，中文名称为“隔离区”，也称“非军事化区”。它是为了解决安装防火墙后外部网络不能访问内部网络服务器的问题而设立的一个非安全系统与安全系统之间的缓冲区，这个缓冲区位于企业内部网络和外部

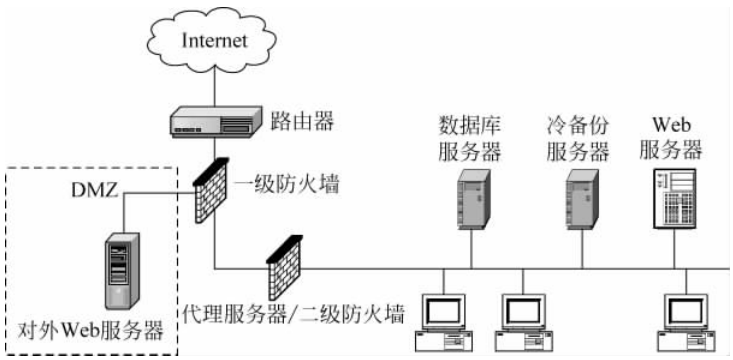

图 3-37 一个 Internet/Intranet 互联方案

网络之间的小网络区域内,在这个小网络区域内可以放置一些必须公开的服务器设施,如企业 Web 服务器、FTP 服务器和论坛等。另一方面,通过这样一个 DMZ 区域,更加有效地保护了内部网络,对攻击者来说,因为这种网络部署比一般的防火墙方案又多了一道关卡。

二级防火墙是网络的第二道安全防线,在一级防火墙被攻破时,它还可以保护中心数据库的安全不受影响。而 Intranet 内部对于 Internet 的访问由代理服务器控制。

对于系统可靠性要求很高的场合,建议在系统中再配置一台冷备份服务器。这台服务器中同时存有数据库系统和 Web 系统的备份。此服务器定期从数据库服务器和 Web 服务器上备份新的资料与数据。平时这台服务器处于关机状态,使它完全没有被攻击的可能。当第二道防火墙被攻破,数据库系统也被破坏时,可以用这台服务器及时恢复数据库服务器和 Web 服务器中的内容。冷备份服务器是本系统最后的保障。

3.5 网络的管理与安全运行

一个安全的计算机网络应该具有可靠性、可用性、完整性、保密性和真实性等特点。不仅要保护计算机网络设备安全和计算机网络系统安全,还要保护数据安全等。因此针对计算机网络本身可能存在的安全问题,必须实施网络安全保护方案以确保计算机网络自身的安全性。

1. 网络安全隐患

计算机网络面临的安全威胁大体可分为两种:一是对网络本身的威胁,包括对网络设备和网络软件系统平台的威胁;二是对网络中信息的威胁,其中包括对网络中数据的威胁,还包括对处理这些数据的信息系统及应用软件的威胁。对网络安全的威胁主要来自人为的管理失误、恶意攻击、网络软件系统的漏洞和“后门”。

(1) 技术性缺陷导致的安全隐患。计算机网络中总会存在一些安全缺陷,如路

由器配置错误、保留匿名 FTP 服务、开放 Telnet 访问及口令文件缺乏安全保护等。技术性的网络安全隐患主要表现在 3 个方面：一是以传统宏病毒、蠕虫等为代表的入侵性病毒传播；二是以间谍软件(spyware)、广告软件(adware)、网络钓鱼软件(phishing)、木马程序(trojan)为代表的恶意代码威胁；三是以黑客为首的有目标的专门攻击或无目标的随意攻击为代表的网络侵害。

(2) 安全管理漏洞导致的安全隐患。除技术性缺陷外，发生最频繁的网络安全威胁实际上来自安全管理漏洞，只有把安全管理制度与安全管理技术手段相结合，整个网络系统的安全性才有保证。

网络攻击经常能够得逞，主要有以下几个方面的原因：一是现有的网络系统具有内在的安全脆弱性；二是管理者思想麻痹，对网络入侵造成的严重后果重视不够，舍不得投入必要的人力、财力、物力来加强网络的安全；三是没有采取正确的安全策略和安全机制。

2. 网络安全应对方法

网络的安全策略应是针对各种不同的威胁和脆弱性提出的全方位解决方案，这样才能确保网络和信息的机密性、完整性、可用性、可控性和不可否认性。计算机网络的安全策略可以分为物理安全策略、访问控制策略、攻击防范策略、加密认证策略和安全管理策略等。

(1) 物理安全策略。其目的是保护计算机网络通信系统和网络服务器等硬件基础设施免受自然灾害、人为破坏和搭线攻击，确保网络系统有良好的工作环境。抑制和防止电磁泄露是物理安全策略要解决的一个主要问题。

(2) 访问控制策略。是网络安全防范和保护的核心策略之一，其任务是保证网络资源不被非法使用和非法访问。访问控制策略包括入网访问控制策略、操作权限控制策略、目录安全控制策略、属性安全控制策略、网络服务器安全控制策略、网络监测和锁定控制策略以及防火墙控制策略。

(3) 攻击防范策略。是为了对来自外部网络的攻击进行积极的防御。积极防御有两种情况：及时发现外部对网络的攻击并且进行抵御；努力寻找网络自身的安全漏洞进行弥补。

(4) 加密认证策略。信息加密是保障网络安全的有效策略之一。一个加密的网络不但可以防止非授权用户的搭线窃听和入网，而且也是对付恶意软件的有效方法之一。网络加密常用的方法有链路加密、端到端加密和节点加密 3 种。链路加密的目的是保护链路两端网络设备间的通信安全，节点加密的目的是对源节点计算机到目的节点计算机之间的信息传输提供保护，端到端加密的目的是对源端用户到目的端用户的应用系统通信提供保护。用户可以根据需求酌情选择上述加密方式。

(5) 安全管理策略。在网络安全中，除了诸如访问控制、攻击防范、加密认证等技术措施之外，加强网络的安全管理，制定有关规章制度，对于确保网络安全、可靠地运行将起到十分有效的作用。

从安全技术保障手段上来讲,应当采用先进的网络安全技术、工具、手段和产品,同时采取先进的备份手段。这样,一旦防护手段失效时,可以迅速进行系统和数据的恢复。

3.5.1 网络管理

网络管理就是对网络进行规划、配置、监视及控制,以便更好地利用网络资源,确保网络高效、可靠和安全地运行。实现的管理功能为故障管理、性能管理、配置管理、安全管理和计费管理。网络管理的通俗理解就是对网络的设备运行进行监控。但是,能否对网络设备进行管理还要看它是否提供管理接口,是否内嵌符合国际标准的代理(agent)程序。目前,主要有两个网络管理协议:SNMP 和 CMIP。SNMP 是基于 TCP/IP 的,几乎所有路由器和交换机厂商都提供基于 SNMP 的网络管理功能。

1. SNMP 协议

SNMP(Simple Network Management Protocol,简单网络管理协议)是由一系列协议和规范组成的,它包含 4 个组成部分。

(1) SNMP NMS (SNMP 管理站):利用 SNMP 协议对网络设备进行管理和监控的系统。

(2) SNMP Agent (SNMP 代理):是运行在被管设备上的软件模块,用于维护被管设备的信息数据(即 MIB),还负责接收、处理、响应来自 NMS 的请求报文,也可以主动发送一些通知报文给 NMS。

(3) SNMP 协议:规定 NMS 和 Agent 之间是如何交换管理信息的应用层协议,以 GET、SET 方式替代了复杂的命令集,实现网管需求。

(4) MIB (管理信息库):每个 Agent 都有自己的 MIB 库。MIB 是一种对象数据库,由设备所维护的被管理对象组成。它们提供了一种从网络上的设备中收集网络管理信息的方法。从被管理设备中收集数据有两种方法:一种是轮询(polling-only)方法,另一种是基于中断(interrupt-based)的方法。

SNMP 使用嵌入到网络设备中的代理(agent)软件来收集网络的通信信息和有关网络设备的统计数据。代理软件不断地收集统计数据,并把这些数据记录到 MIB 中。网管中心通过向代理的 MIB 发出查询信号可以得到这些信息,这个过程就称为轮询(polling),如图 3-38 所示。网管员可以使用 SNMP 来评价网络的运行状况,并揭示出通信的趋势,例如,哪一个网段接近通信负载的最大能力或通信出错等。

轮询方法的缺陷在于无法保证信息的实时性,尤其是错误的实时性,因为不合适的轮询间隔和顺序将影响轮询结果。与之相比,当有异常事件发生时,基于中断的方法可以立即通知网络管理工作站,其优点在于实时性很强,缺点在于产生错误或自陷需要系统资源,从而影响网管功能。

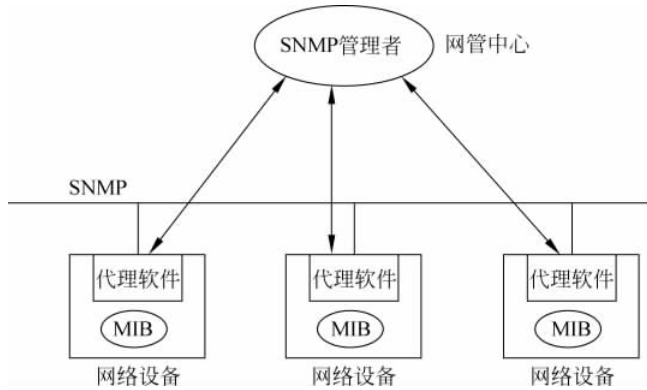

图 3-38　SNMP 网络管理工作方式

面向自陷的轮询方法(trap-directed polling)是上述两种方法的结合：网络管理工作站轮询在被管理设备中的代理来收集数据，并且在控制台上用数字或图形的表示方法来显示这些数据。被管理设备中的代理可以在任何时候向网络管理工作站报告错误情况，而并不需要等到管理工作站为获得这些错误情况而轮询它的时候才会报告。

2. CMIP 协议

CMIP(Common Management Information Protocol，公共管理信息协议)是由 ISO 制定的国际标准。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。

CMIP 采用面向对象的方法来描述被管资源，用事件驱动的方法管理被管对象。在网络管理过程中，CMIP 通过事件报告进行工作，由网络中的各个设备监测设施在发现被检测设备的状态和参数发生变化后及时向管理进程进行事件报告。管理进程一般都对事件进行分类，根据事件发生时对网络服务影响的大小来划分事件的严重等级，网络管理进程很快就会收到事件报告，具有及时性的特点。

CMIP 和 SNMP 这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 是由国际标准化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。

3.5.2　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。下面简单介绍网络管理技术的一些新趋势。

1. 远程网络监控

网络管理技术的一个新的趋势是使用RMON(Remote Monitor,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、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,是对SNMP框架的重要补充,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给RMON客户应用程序。RMON的强大之处在于它完全与SNMP框架兼容。

2. 基于Web的网络管理技术

基于Web的网络管理模式(Web-Based Management,WBM)就是通过Web浏览器进行网络管理,有两种实现方式。第一种方式是代理方式,即在一个内部工作站上运行Web服务器(代理)。这个工作站轮流与端点设备通信,浏览器用户与代理通信,同时代理与端点设备之间通信。在这种方式下,网络管理软件成为操作系统上的一个应用。它介于浏览器和网络设备之间。在管理过程中,网络管理软件负责将收集到的网络信息传送到浏览器(Web服务器代理),并将传统管理协议(如SNMP)转换成Web协议(如HTTP)。第二种实现方式是嵌入式。它将Web功能嵌入到网络设备中,每个设备有自己的Web地址,管理员可通过浏览器直接访问并管理该设备。在这种方式下,网络管理软件与网络设备集成在一起。网络管理软件无须完成协议转换。所有的管理信息都是通过HTTP协议传送。

3. 面向业务的网络管理

新一代的网络管理系统,已开始从面向网络设备的管理向面向网络业务的管理过渡。这种网管思想把网络服务、业务作为网管对象,通过实时监测与网络业务相关的设备、应用,通过模拟客户实时测量网络业务的服务质量,通过收集网络业务的业务数据,实现全方位、多视角监测网络业务运行情况的目的,从而实现网络业务的故障管理、性能管理和配置管理。

网络管理本身是一项极其复杂的工作,无论网络管理技术进步到何种程度,我们都不能奢望出现让网管人员一劳永逸的网管工具。即使有了带有人工智能的网

管工具，它也仅仅让网络管理变得容易一些，而不会全部代替人的工作。

3.5.3　VLAN 管理

VLAN(Virtual LAN，虚拟局域网)是通过路由器和交换设备在局域网的基础上建立的一个或多个逻辑结构。每个逻辑网络可看成是一个虚拟工作组，它也是一组网段和站点的集合。它们可以不受物理位置的限制，而好像处于同一局域网那样，能方便地进行通信和资源共享。

1. VLAN 的作用

VLAN 基于交换技术，通过不同的划分方法把原来一个大的广播区的局域网从逻辑上划分为若干个“子广播区”，一个子广播区的广播包只能在该子广播区传送，而不会送到其他广播区中。处于不同 VLAN 上的主机不能进行直接通信，不同 VLAN 之间的通信要引入第三层交换技术才可以解决。网络设备通过 VTP 协议以及 ISL 或 IEEE 802.1q 协议允许一个 VLAN 跨越多个交换机，从而提高 VLAN 划分的灵活性。以太网交换机上通过引入 VLAN，具有以下优点：

(1) 限制了局部的网络流量，在一定程度上可以提高整个网络的处理能力。

(2) 通过灵活的 VLAN 设置，把不同的用户划分到虚拟的工作组内。

(3) 一个 VLAN 内的用户和其他 VLAN 内的用户不能互访，提高了安全性。

2. VLAN 的管理方法

VLAN 的管理主要涉及 VLAN 的划分和 VLAN 的配置。VLAN 的划分即确定 VLAN 成员(站点和服务器)的方法。VLAN 的划分方式大致划分为 5 类。

1) 基于端口划分的 VLAN

这是常用的 VLAN 划分方法，这种划分方法比较简单，通过交换机配置命令将交换机端口划分到一个指定的 VLAN 中，所有连接到这个端口的工作站和服务器(包括通过这个端口级联)都属于这个 VLAN。这种方式的特点就是管理比较简单，但是灵活性不高。

2) 基于 MAC 地址划分 VLAN

这种划分 VLAN 的方法是根据每个主机的 MAC 地址来划分，即对每个 MAC 地址的主机都配置为属于某个组，它实现的机制就是每一块网卡都对应唯一的 MAC 地址，VLAN 交换机跟踪属于 VLAN MAC 的地址。这种方式的 VLAN 允许网络用户从一个物理位置移动到另一个物理位置时自动保留其所属 VLAN 的成员身份。这种方式特点在于灵活性很高，桌面工作站的移动变化都不需要对交换机重新配置。缺点在于其管理比较复杂，需要做出每个 MAC 地址与 VLAN 的对应表。

3) 基于网络层协议划分 VLAN

VLAN 按网络层协议来划分，可分为 IP、IPX、DECnet、AppleTalk、Banyan 等

VLAN网络。这种按网络层协议组成的VLAN可使广播域跨越多个VLAN交换机。这对于希望针对具体应用和服务来组织用户的网络管理员来说是非常具有吸引力的。而且,用户可以在网络内部自由移动,但其VLAN成员身份仍然保留不变。

4) 根据IP多播划分VLAN

IP多播实际上也是一种VLAN的定义,即认为一个IP多播组就是一个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,主要适合于不在同一地理范围的局域网用户组成一个VLAN,但不适合局域网,主要是效率不高。

5) 基于用户的VLAN划分方式

在这种方式中,VLAN的划分根据用户登录到NT域的用户名来动态划分交换机端口的VLAN,这种方式对客户机的要求是用户端必须要登录到NT域上,并且其IP地址设置为动态分配方式。同时,需要配置基于Windows NT的管理软件实现。这种方式可管理性和灵活性非常高,用户可在任何地方获得其特有的权限。缺点就是需要额外投资。

3.5.4 防火墙技术

防火墙技术是建立在现代通信网络技术和信息安全技术基础之上的一种安全技术,用于抵御黑客对计算机网络的侵扰,常用于专用网络与公用网络的互联环境之中。以防火墙为代表的被动防卫型安全保障技术已被证明是一种较有效的防止外部入侵的措施。

1. 什么是防火墙

防火墙形象地讲与建筑物中的防火墙类似,它可以防止外部网络(例如Internet)上的危险(黑客)在内部网络上的蔓延。如图3-39所示,用专业语言来说,所谓防火墙就是一个或一组网络设备(计算机或路由器等),可用来在两个或多个网络间加强相互的访问控制。内部网上设立防火墙的主要目的是保护自己不受来自另外一个网络的攻击,要保护的是内部网络,而要防备的则是外部网络。对网络的保护包括拒绝未授权的用户访问,同时允许合法用户不受妨碍地访问网络资源。防火墙的职责就是根据本单元的安全策略,对外部网络与内部网络交流的数据进行检查,符合安全规定的通过,不符合安全规定的拒绝。

2. 防火墙的组成与基本结构

防火墙一般由以下两部分组成:包过滤路由器(packet filtering router)和应用网关(application gateway)。

防火墙能根据一定的安全规定检查、过滤网络之间传送的报文分组,以确定它们的合法性。这项功能一般是通过具有分组过滤功能的路由器来实现的,通常把这

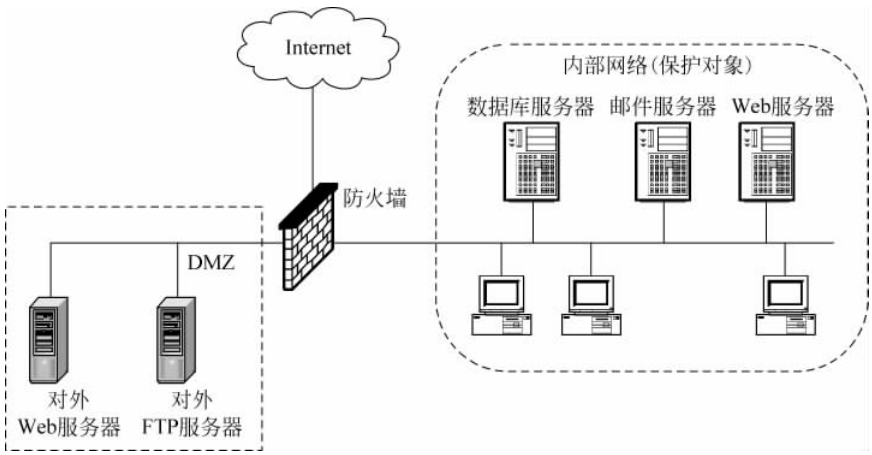

图 3-39　防火墙示意图

种路由器称为分组过滤路由器，也称为筛选路由器(screening router)。

分组过滤路由器一般是作为系统的第一级保护，它与普通的路由器在工作机理上有较大的不同。普通的路由器工作在网络层，可以根据网络层分组的 IP 地址决定分组的路由；而分组过滤路由器要对 IP 地址、TCP 或 UDP 分组头进行检查与过滤。通过分组过滤路由器检查过的报文，还要进一步接受应用网关的检查。因此，从协议层次模型的角度看，防火墙应覆盖网络层、传输层与应用层。

根据物理特性，防火墙分为两大类，软件防火墙和硬件防火墙。

软件防火墙是一种安装在负责内外网络转换的网关服务器或者独立的个人计算机上的特殊程序。软件防火墙工作于系统接口与 NDIS(Network Driver Interface Specification，网络驱动接口规范)之间，用于检查过滤由 NDIS 发送过来的数据，在无须改动硬件的前提下便能实现一定强度的安全保障，但是由于软件防火墙自身属于运行于系统上的程序，不可避免地需要占用一部分 CPU 资源维持工作，而且由于数据判断处理需要一定的时间，在一些数据流量大的网络里，软件防火墙会使整个系统工作效率和数据吞吐速度下降，甚至有些软件防火墙会存在漏洞，导致有害数据可以绕过它的防御体系，给数据安全带来损失，因此，许多企业并不会考虑用软件防火墙方案作为公司网络的防御措施，而是使用看得见摸得着的硬件防火墙。

硬件防火墙是一种以物理形式存在的专用设备，通常架设于两个网络的驳接处，直接从网络设备上检查并过滤有害的数据报文。硬件防火墙一般是通过网线连接于外部网络接口与内部服务器或企业网络之间的设备，它可分为两种结构。一种是普通硬件级别防火墙，此类防火墙拥有标准计算机的硬件平台和一些功能经过简化处理的 UNIX 系列操作系统和防火墙软件，这种防火墙措施相当于专门拿出一台计算机安装了软件防火墙，除了不需要处理其他事务以外，它毕竟还是一般的操作系统，因此有可能会存在漏洞和不稳定因素，安全性并不能达到最好。另一种是所谓的“芯片”级硬件防火墙，它采用专门设计的硬件平台，在上面搭建的软件也是专

门开发的,因而可以达到较好的安全性能保障。但无论是哪种硬件防火墙,管理员都可以通过计算机连接上去设置工作参数。由于硬件防火墙的主要作用是把传入的数据报文进行过滤处理后转发到位于防火墙后面的网络中,因此它自身的硬件规格也是分档次的,尽管硬件防火墙已经足以实现比较高的信息处理效率,但是在一些对数据吞吐量要求很高的网络里,档次低的防火墙仍然会形成瓶颈,所以对于一些大企业而言,芯片级的硬件防火墙才是他们的首选。

企业内部网通过将防火墙技术与用户授权、操作系统安全机制、数据加密等多种方法结合,来保护网络资源不被非法使用与网络系统不被破坏,全面地执行网络安全策略,增强系统安全性。

习题与思考题

1. 简述局域网体系结构。
2. 什么是快速以太网? 它有哪几种介质标准?
3. 什么是千兆以太网? 它有哪几种介质标准?
4. 什么是万兆以太网? 它有哪几种介质标准?
5. 什么是100BASE-T? 什么是1000BASE-T?
6. 与千兆以太网相比,万兆以太网有哪些优势?
7. 名词解释: LAN,CSMA/CD,ADSL,HDSL,FTTB。
8. 简述交换式局域网的特点和工作原理。
9. 什么是三层交换技术? 它有何特点?
10. 什么是无线局域网? 它有哪些介质标准?
11. 什么是IEEE 802.11g? 什么是IEEE 802.11b?
12. 无线局域网有哪些组网方式? 有何特点?
13. 什么是HomeRF? 什么是IrDA?
14. 扩展局域网有哪些常用的方法?
15. 局域网互联有哪些常用的方法?
16. 三层交换机与路由器有哪些区别?
17. 计算机网络系统设计有哪些原则?
18. 简述万兆校园网解决方案。
19. 什么是宽带接入网? 有哪些宽带接入技术?
20. 什么是xDSL? 有哪些DSL技术?
21. 什么是FTTx? 它有何特点?
22. 有哪些网络操作系统? 它们各有何特点?
23. 什么是Internet? 它有哪些信息服务?
24. 什么是Intranet? 它有何特点?
25. 在计算机网络中,网络协议的作用是什么?

26. 简述中继器、网桥、交换机、路由器和网关的功能及特点。
27. 基于电话线的接入技术主要有哪几种？各自的特点是什么？
28. 采用光纤的接入技术主要有哪几种？各自有何特点？
29. 什么是 Web？Web 服务器有何功能？
30. 有哪些 Web 服务器平台？如何组建？
31. 建立智能建筑的 Intranet 有哪些方案？
32. 什么是网络管理？它有哪些功能？
33. 什么是 SNMP？什么是 CMIP？
34. 什么是 RMON？什么是 WBM？
35. 什么是 VLAN？它有哪些功能？
36. VLAN 有哪些划分方式？各自有何特点？
37. 什么是防火墙？防火墙的组成与基本结构是什么？