

单元一

局域网规划



本单元通过具体的任务讲解局域网规划，具体包括以下几个方面：

- 绘制网络拓扑图
- 局域网规划

模块一 绘制网络拓扑图

本模块通过完成 Microsoft Office Visio 软件的安装和使用，来学习如何绘制网络拓扑图。网络拓扑结构设计是一切网络组建的基础，如果事先不把网络结构确定下来，那么后面的网络设备连接和网络配置也就很难确定，甚至无法进行。即使网络最终连通了，如果连设计者都不清楚整个网络的结构，那么今后的维护和管理就会相当不便，甚至完全不能满足企业的实际应用和未来发展需求。

任务 1 Microsoft Office Visio Professional 2003 软件的安装

【任务描述】

A 公司投标×××大学校园网工程，现招聘员工，要求掌握网络拓扑图的绘制。

【任务目标】

掌握 Microsoft Office Visio 的安装和使用。

【实施过程】

通常使用 Microsoft Office Visio 应用软件绘制网络拓扑图。可以从网上下载 Visio 最新版本 2010 版，但为方便读者下载和注册，本书使用 Microsoft Office Visio Professional 2003 版本，安装步骤如下：

(1) 首先下载 Microsoft Office Visio Professional 2003，单击其中的 setup.exe 安装文件，在如图 1-1 所示的对话框中输入产品密钥，单击“下一步”按钮。



图 1-1 输入产品密钥

(2) 显示“用户信息”对话框，输入用户名，如图 1-2 所示。



图 1-2 输入用户信息

(3) 单击“下一步”按钮，选择“我接受《许可协议》中的条款”，单击“下一步”按钮。显示“安装类型”对话框，选择“典型安装”单选按钮，输入安装位置，然后单击“下一步”按钮，如图 1-3 所示。

(4) 显示安装信息，单击“安装”按钮，提示安装完成后单击“完成”按钮即可。

任务 2 网络拓扑图的绘制

【任务描述】

你应聘进入 A 公司，现公司要求画出一个星型拓扑图。



图 1-3 “安装类型”对话框

【任务目标】

掌握 Microsoft Office Visio 的使用。

【实施过程】

(1) 单击“开始”→Microsoft Office→Microsoft Office Visio 2003 选项，打开 Microsoft Office Visio，其界面如图 1-4 所示。

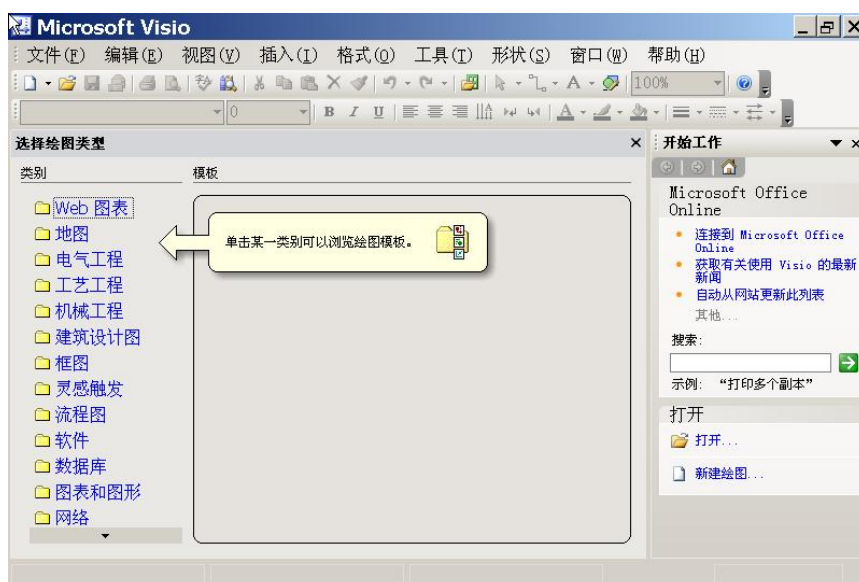


图 1-4 Microsoft Office Visio 界面

(2) 在左侧栏中单击“网络”→“详细网络图”，选择需要的交换机、服务器和 PC 机，拖到工作区，在工具栏上单击“连接线工具”按钮，将它们连接起来即可，如图 1-5 所示。

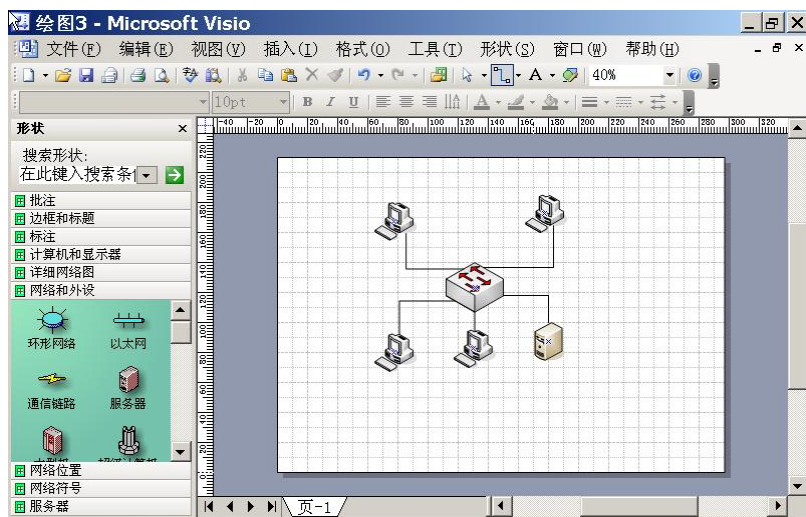


图 1-5 绘制网络拓扑图

【知识链接】

1. 计算机网络的发展历史

过去的 300 年中，每个世纪都有一种主流技术。18 世纪伴随着工业革命而来的是伟大的机械时代；19 世纪则是蒸汽机时代；而在 20 世纪，关键技术是信息收集、处理和发布。我们已经看到了世界范围通信网络的安装，计算机工业的诞生及迅速发展，通信卫星的发射，以及其他种种成就。

由于技术的飞跃发展，这些领域正在迅速地融合。计算机和通信的结合，对计算机系统的组织方式产生深远的影响。“计算机中心”的概念已经完全过时，单台计算机为机构中所有的计算机服务的这一概念很快被大量分散但又互联的计算机共同完成的模式所代替。这样的系统被称为计算机网络（Computer Network），即自主计算机（Autonomous Computers）的互联（Interconnected）集合。

2. 计算机网络的应用

许多机构都有一定数量的计算机在运行，这些机器大都相距甚远。例如，一家公司有许多工厂，可能每个工厂所在地都装配有计算机，用于记录库存，监视生产状况和管理当地的工资发放。最初，每台计算机都独立的工作，但后来管理部门决定把这些独立的计算机连接起来，以获取和核对整个公司的信息。

可以将应用网络的目的归纳为：第一，它试图解除“地理位置的束缚”，实现资源共享；第二个目的就是提高可靠性，例如，可以将所有的文档在两台或多台计算机上留有副本，如果其中一台不能使用，还可以使用其他的副本；第三个目的是节约经费。如果可以用可接受的价格购买到足够大的和功能足够强的主机，大多数公司都会选择把他们所有的数据都放到主机上去，让他们的员工通过终端连接到主机。在 20 世纪 70 年代和 80 年代早期，大多数公司都以这种方式运作。当个人计算机网络提供比主机高得多的性能价格比时，计算机网络才开始流行。

从 20 世纪 90 年代开始，计算机网络开始为居家的个人用户提供服务。第一类应用就是访问远程信息，如在网络上购物、看新闻等。第二类应用就是人际交往，人们可以在网络上聊 QQ，发 E-mail，甚至召开视频会议。第三类应用是娱乐，如在网络上玩游戏，进行视频点播等。网络的信息发布、通信和娱乐的能力将打造一个基于计算机网络的巨大产业。

3. 计算机网络的基本组成

计算机网络主要由四个部分组成，分别为计算机系统、通信线路和通信设备、网络协议和网络软件，它们常被称为计算机网络的四大要素。

(1) 计算机系统。

具有两台以上独立功能的计算机系统是计算机网络的第一个要素，计算机系统是计算机网络的重要组成部分。计算机系统是网络的基本模块，是被连接的对象。它主要负责数据信息的收集、处理、存储和提供共享资源。在网络上可共享的资源包括硬件资源（如巨型机、高性能计算机外围设备、磁盘柜等）、软件资源（如各种软件系统、应用程序、数据库系统等）和信息资源。

(2) 通信线路和通信设备。

计算机网络的硬件除了计算机本身以外，还包括用于连接这些计算机的通信线路和通信设备，即数据通信系统。其中，通信线路是指传输介质连接部件，包括光缆、同轴电缆、双绞线等。通信设备是指网络连接设备、网络互联设备，包括网卡、集线器、交换机、路由器以及调制解调器等。使用通信线路和通信设备将计算机互连起来，在计算机之间建立一条物理通道，以便传输数据。通信线路和通信设备负责控制数据的发出、传送、接收或转发，包括信号转换、路径选择、编码与解码、差错校验、通信控制管理等，确保完成信息交换。通信线路和通信设备是连接计算机系统的桥梁，是数据传输的通道。

(3) 网络协议。

网络协议是指通信双方必须共同遵守的约定和通信规则，如 TCP/IP 协议、NetBEUI 协议、IPX/SPX 协议。它是通信双方对如何进行通信所达成的协议。比如用什么样的格式组织和传输数据，如何校验和纠正信息传输中的错误，以及规定传输信息时的时序组织与控制机制等。现代网络都是层次结构，协议规定了分层原则、层次间的关系、执行信息传递过程的方向和解组与重组等约定。在网络上通信的双方必须遵守相同的协议，才能正确地交流信息，就像人们说话要说同一种语言一样，如果谈话时使用不同的语言，就会造成听不懂对方在说什么，将导致无法进行交流。因此协议在计算机网络中是至关重要的。一般说来，协议的实现是由软件和硬件分别或配合完成的，有的部分由联网设备来承担。

(4) 网络软件。

网络软件是一种在网络环境下使用、运行、控制和管理网络工作的计算机软件。根据软件的功能，计算机网络软件可分为网络系统软件和网络应用软件两大类型。

1) 网络系统软件。网络系统软件是控制和管理网络运行、提供网络通信、分配和管理共享资源的网络软件。它包括网络操作系统、网络协议软件、通信控制软件和管理软件等。

网络操作系统是使网络上的计算机能方便、高效地共享网络资源，为网络用户提供资源访问途径以及其他基本服务的系统软件。

网络协议软件是实现各种网络协议的软件。它是网络软件中最重要的部分，任何网络软件都要通过协议软件才能发生作用。

2) 网络应用软件。网络应用软件是指为某一目的而开发的网络软件。网络应用软件为用户提供访问网络的手段、网络服务、资源共享和信息的传输。

4. 网络分类

(1) 按地理范围分类。

按照网络覆盖的地理范围，可将计算机网络分为局域网、城域网和广域网。

1) 局域网。

局域网是将较小地理区域内的计算机或数据终端设备连接在一起的通信网络。局域网覆盖的地理范围比较小,一般在几十米到几千米。它常用于组建一个办公室、一栋楼、一个楼群、一个校园或一个企业的计算机网络。局域网的主要特点如下:

- ①覆盖的地理区域比较小,仅工作在有限的地理区域内(0.1km~20km)。
- ②传输速率高,能达到1Mb/s~10Gb/s,误码率低。
- ③拓扑结构简单,常用的拓扑结构有总线型、星型、环形等。
- ④局域网通常由单一的组织管理。

2) 广域网。

广域网是在一个广阔的地理区域内进行数据、语言、图像信息传输的通信网。广域网覆盖广阔的地理区域,通信大多借用公用通信网络(如PSTN、DDN、ISDN等)进行,传输速率比较低,这类网络的作用是实现远距离计算机之间的数据传输和信息共享。广域网可以覆盖一个城市、一个国家甚至多个国家。因特网是广域网的一种,但它不是一种具体独立性的网络,它将同类或不同类的物理网络(局域网、广域网和城域网)互联,并通过高层协议实现不同种类网络间的通信。

广域网的主要特点是:

- ①覆盖的地理区域大,网络可跨市、地区、省、国家甚至多个国家。
- ②广域网连接常借用公用网络。
- ③传输速率比较低,一般在64kb/s~2Mb/s。随着广域网技术的发展,其传输速率正在不断提高,目前通过采用光纤介质,传输速率理论上可以达到10Gb/s。
- ④网络拓扑结构复杂。

3) 城域网。

城域网的覆盖范围介于局域网和广域网之间,一般在一个城市内。

(2) 按传输技术分类。

根据使用的传输技术,可以将网络分为广播式和点到点网络。

1) 广播式网络。在广播式网络中,仅使用一条通信信道,该信道由网络上的所有站点共享。在传输信息时,任何一个站点都可以发送数据分组,网络上的其他站点都可以接收。这些站点根据数据包中的目的地址进行判断,如果是发给自己的,就接收,否则丢弃。

2) 点到点网络。在点到点网络中,每对站点之间都有专用的通信信道。当一个站点发送数据分组后,它会根据目的地址,经过一系列中间设备的转发,直接到达目的站点。

(3) 按网络的拓扑结构分类。

按网络的拓扑结构,可以将网络分为总线型网络、环型网络、星型网络、树型网络、网状型网络和混合型网络。拓扑学是几何学的一个分支,它是从图论演变过来的,拓扑学首先把实体抽象成与其大小、形状无关的点,将连接实体的线路抽象成线,进而研究点、线、面之间的关系。计算机网络拓扑通过网络结点与通信线路之间的几何关系,表示网络结构,反映网络中各实体间的结构关系。

1) 总线型结构。

总线型结构采用一条单根的通信线路(总线)作为公共的传输通道,所有的结点都通过相应的接口直接连接到总线上,并通过总线进行数据传输,如图1-6所示。

总线型网络使用广播式传输技术,总线上的所有结点都可以发送数据到总线上,数据沿总线传播。但是,由于所有结点共享同一条公共通道,所以在任何时候只允许一个站点发送数据。当一个

结点发送数据并在总线上传播时,数据可以被总线上的其他结点接收。各结点在接收数据后,分析目的地址再决定是否接收该数据。粗、细同轴电缆以太网就是这种结构的典型代表。

2) 环型结构。

环型结构的各个网络结点通过环接口连在一个首尾相接的闭合环型通信线路中,如图 1-7 所示。环型结构有两种类型,即单环结构和双环结构。令牌环(Toking Ring)是单环结构的典型代表,光纤分布式数据接口(FDDI)是双环结构的代表。

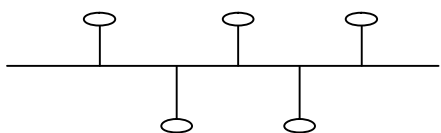


图 1-6 总线型拓扑结构

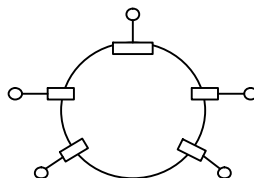


图 1-7 环型拓扑结构

3) 星型结构。

星型结构的每个结点都由一条点到点链路与中心结点(如交换机、HUB 等)相连,如图 1-8 所示。信息的传输是通过中心结点的存储转发技术实现的,并且每个结点只能通过中心结点与其他站点通信。

4) 树型结构。

树型结构是从总线型和星型结构演变而来的,它有两种类型,一种是由总线型拓扑结构派生出来的,它由多条总线连接而成,如图 1-9 (a) 所示;另一种是星型结构的变种,各结点按一定的层次连接起来,形状像一棵倒置的树,顶端有一个根结点,它带有分支,每个分支可以再带子分支,如图 1-9 (b) 所示。

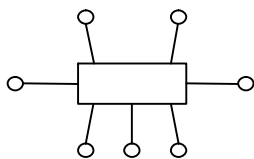
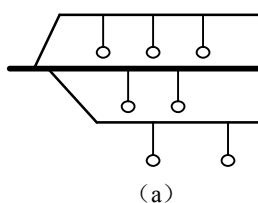
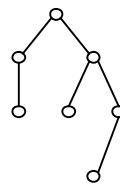


图 1-8 星型拓扑结构



(a)



(b)

图 1-9 树型拓扑结构

5) 网状结构。

网状结构是指将各网络结点与通信线路互连成不规则的形状,每个结点至少与其他两个结点相连的结构。互联网是这种结构的典型代表,如图 1-10 所示。

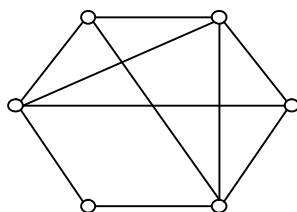


图 1-10 网状拓扑结构

【拓展训练】

读者根据以上知识，独立完成以下任务：

- (1) 在 Windows XP 系统中，安装并配置 Microsoft Office Visio Professional 2003。
- (2) 使用 Microsoft Office Visio Professional 2003 应用软件画出本模块中所有的网络拓扑图。

【分析和讨论】

- (1) 从 Internet 上下载精美绘图模板后如何导入 Microsoft Office Visio 并使用？
- (2) 使用 Microsoft Office Visio 软件画网络拓扑结构图和综合布线系统拓扑图很方便，但在画综合布线管线路由图、楼层信息点平面分布图、机柜配线架信息点分布图时，使用 Microsoft Office Visio 软件却画不精确，怎么办？
- (3) 如何使用 AutoCAD 进行综合布线的图纸设计？

模块二 局域网规划

本模块通过完成小型基本星型网络结构设计、中型扩展星型网络结构设计和校园网网络结构设计，来学习如何进行局域网规划。

任务1 小型基本星型网络结构设计

【任务描述】

A 公司承接×××大学校园网工程，某办公室网络，是由一台具有 24 个 10/100Mb/s、2 个 10/100/1000Mb/s 自适应 RJ-45 端口的以太网交换机进行集中连接的。网络中配置 1 台服务器、1 台用于互联网访问的宽带路由器、1 台网络打印机和 20 个以内的工作站用户。现为这个小型办公室设计出具体的网络拓扑结构。

【任务目标】

掌握小型基本星型网络结构设计。

【实施过程】

星型网络主要以相对廉价的双绞线为传输介质，网线的两端各用一个 RJ-45 水晶头作为网络连接器。这里所指的小型星型网络是指只有一台交换机的星型网络，主要应用于小型独立办公室和 SOHO 用户中。这类星型网络所能连接的用户数一般在 20 个左右，有的连接可以高达 40 多个用户，具体的连接数量根据实际选择的具备相应端口数的交换机而定。

1. 网络要求

具体的网络要求如下：

- (1) 所有网络设备都与同一台交换机连接。
- (2) 整个网络没有性能瓶颈。
- (3) 要有可扩展余地。

2. 设计思路

设计思路要与以上的网络要求紧密结合，主要可按如下几点进行考虑。

(1) 确定网络设备总数。

确定网络设备总数是设计整个网络结构的基础，因为一个网络设备至少需要连接一个端口，这样，设备数一旦确定，所需交换机的端口总数也就确定下来。这里的网络设备包括工作站、服务器、网络打印机、路由器和防火墙等所有需要与交换机连接的设备。任务的设备总数是 20 个以内的工作站用户+1 台服务器+1 台宽带路由器+1 台网络打印机等于 23 台（最多）。根据这个计算结果，交换机的端口数最低需要 24 个。任务中给出的交换机有 24 个 10/100Mb/s 端口和 2 个 10/100/1000Mb/s 端口，共 26 个端口，可以满足该网络的连接需求。

(2) 确定交换机端口类型和端口数。

一般中档交换机都会提供两个或两个以上类型的端口，任务中的 10/100Mb/s 和 10/100/1000Mb/s 口，都采用 RJ-45 端口。有的中档交换机还提供光纤接口。提供这么多不同类型的端口就是为了满足不同类型设备网络连接的带宽需求。

一般来说，在网络中的服务器、边界路由器、下级交换机、网络打印机和特殊用户工作站等所需的网络带宽较高，所以这些设备通常连接在交换机的高带宽端口。任务中服务器所承担的工作负荷是最重的，直接与交换机的其中一个千兆端口连接，另一个保留用于网络扩展。其他设备的带宽需求不是很明显。宽带路由器目前的出口带宽受连接线路限制，一般在 10Mb/s 以内，只需连接在普通的 10/100Mb/s 快速自适应端口即可。

(3) 保留一定的网络扩展所需端口。

交换机的网络扩展端口的功能主要体现在两个方面：一是用于与下级交换机进行连接，二是用于连接后继续添加工作站用户。与下级交换机连接一般是通过高带宽端口进行的，如果交换机提供 Uplink（级联）端口，则可直接用这个端口，但如果没有级联端口，则只能通过普通端口进行连接，这时为了确保下级交换机所连用户的连接性能，最好选择一个带宽较高的端口。任务中可以留下一个千兆端口用于扩展连接，在实际工作中，这个高带宽端口还可以用于其他方面，视具体情况而定。

(4) 确定可连接工作站的总数。

交换机端口总数不等于可连接的工作站用户数，因为交换机中的一些端口还要用来连接那些不是工作站的网络设备，如服务器、下级交换机、网络打印机、路由器、网关、防火墙等。任务中，网络中有 1 台专门的服务器、1 台宽带路由器和 1 台网络打印机，所以网络中可连接的工作站用户总数为 26-3 等于 23 个。如果要保留一个端口用于网络扩展，则实际上可连接的工作站用户数为 22 个。

3. 设计步骤

任务中，网络用户和交换机类型都已确定，根据已知条件，设计一个小型办公室网络方案。

(1) 首先确定关键设备的连接，把需要连接在高带宽端口的设备连接在交换机的可用高带宽端口上。把交换机图示放在设计的平台中心位置，然后把服务器与交换机用一个 10/100/1000Mb/s 端口连接起来，并标注其端口类型，如图 1-11 所示。

(2) 把所有工作站和网络打印机分别与交换机的 10/100 Mb/s 端口连接，如图 1-11 所示。

(3) 如果网络系统需要通过路由器与其他网络连接，则还需要设计 Internet 连接。路由器与外部网络连接是通过广域网端口进行的。虽然路由器广域网端口的类型有很多，但宽带路由器提供的广域网端口都是 RJ-45 端口，一般为 10/100Mb/s，可以直接与 Internet 宽带设备连接。如属于小

区光纤以太网或校园网，则无需宽带设备。

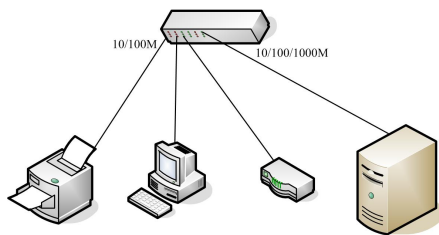


图 1-11 小型基本星型网络

任务 2 中型扩展星型网络结构设计

【任务描述】

A 公司承接×××大学校园网工程，在一个一幢教学楼局域网中，整个网络分布在同一楼层的多间办公室中。整个网络的交换机分 3 层结构。核心交换机是两台提供 1 个 1000 Mb/s SC 光纤接口、4 个 RJ-45 双绞线 10/100/1000 Mb/s 接口和 24 个 10/100 Mb/s 接口的以太网交换机；骨干交换机是三台提供 2 个 10/100/1000 Mb/s 双绞线 RJ-45 接口、48 个 10/100 Mb/s 双绞线 RJ-45 接口的以太网交换机；边缘层还有六台 10/100 Mb/s 双绞线 RJ-45 接口的 24 口以太网交换机。另外，网络边缘通过边界路由器和防火墙与外界网络连接。

【任务目标】

掌握中型扩展星型网络结构设计。

【实施过程】

中型扩展星型网络是指在整个网络中包括多个交换机，而且各交换机是通过级联方式连接的分层结构。在中型扩展星型网络中，一般有边缘层（又称接入层）、骨干层（又称汇聚层）和核心层 3 个层次，在各层中的每一台交换机又各自形成一个相对独立的星型网络结构。中型扩展星型网络结构主要应用于在同一楼层的中小型企业网络中。在这种网络中通常会有一个单独的机房，集中摆放所有的关键设备，如服务器、管理控制台、核心或骨干交换机、路由器、防火墙和 UPS 等。

1. 网络要求

- (1) 核心交换机能提供负载均衡和冗余配置。
- (2) 所有设备都必须连接在网络上，且尽可能均衡负载，整个网络无性能瓶颈。
- (3) 各设备所连交换机要适当，双绞线网段距离不能超过 100m 的限制。
- (4) 通过拓扑结构图可了解各主要设备所连端口的类型和传输介质。

2. 设计思路

设计思路要与以上的网络要求紧密结合，主要可按如下几点进行考虑。

- (1) 采用自上而下的分层结构设计。

首先确定的是核心交换机的连接，然后是骨干交换机的连接，依次类推。

- (2) 把关键设备冗余连接在两台核心交换机上。

要实现核心交换机负载均衡和冗余配置,就必须在核心交换机之间,核心交换机与骨干交换机之间,以及核心交换机与关键设备之间进行负载均衡和冗余连接的配置。

(3) 连接其他网络设备。

把次要重要的多数工作站和网络打印机等设备连接在核心交换机或者骨干交换机的普通端口上,把工作负荷相对较小的普通工作站用户连接在边缘交换机上。

3. 设计步骤

任务中,根据已知条件,设计一个中型扩展星型网络方案。

(1) 首先确定核心交换机的位置及主要设备的连接。

任务中两台核心交换机是通过 SC 光纤接口进行负载均衡和冗余连接的,所以首先把两台交换机的 SC 光纤接口用一条光纤电缆连接起来,然后再把与核心交换机连接的服务器通过两块双绞线千兆网卡与两台核心交换机进行冗余连接,如图 1-12 所示。

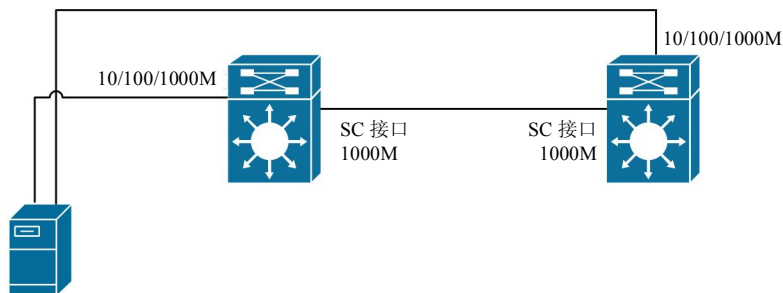


图 1-12 核心交换机及主要设备连接

(2) 级联下级骨干交换机。

通过双绞线,连接核心交换机与骨干交换机的千兆端口,以实现扩展级联。为了实现冗余连接,骨干层的每台交换机都要与每台核心交换机分别连接。任务中核心交换机和骨干交换机都有足够的 RJ-45 千兆接口,可以满足冗余连接要求。然后把其他要与核心交换机连接的网络设备连接起来,如管理控制台、一些特殊应用的工作站和负荷较重的网络打印机等。但要注意每台交换机至少要留有两个备用接口。设备连线图如图 1-13 所示。

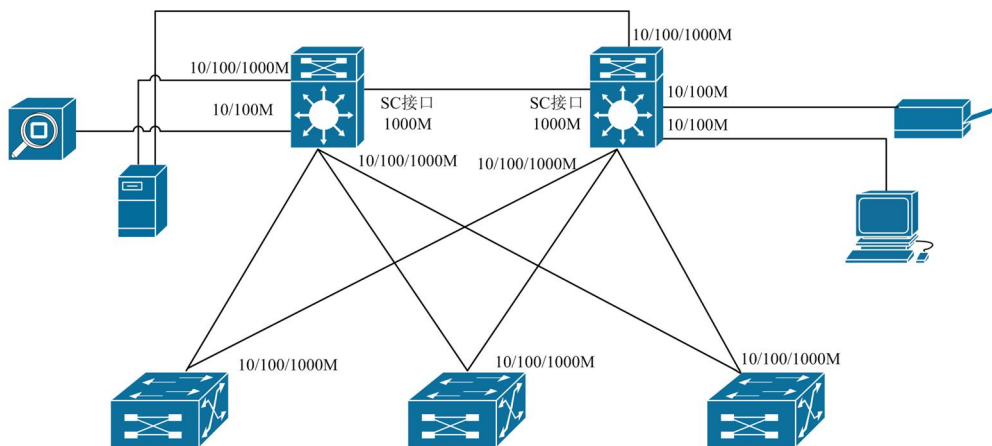


图 1-13 级联下级骨干交换机

(3) 级联边缘交换机。

通过普通的双绞线把边缘交换机与骨干交换机的 10/100Mb/s 接口对应级联起来, 此处不必配置冗余连接。同时要把需要与骨干以及边缘交换机连接的其他网络设备与普通 10/100Mb/s 端口连接起来。同样在骨干层每台交换机上至少要留有两个备用接口。级联边缘交换机的连线图如图 1-14 所示。这样, 整个局域网部分就全部连接成功。

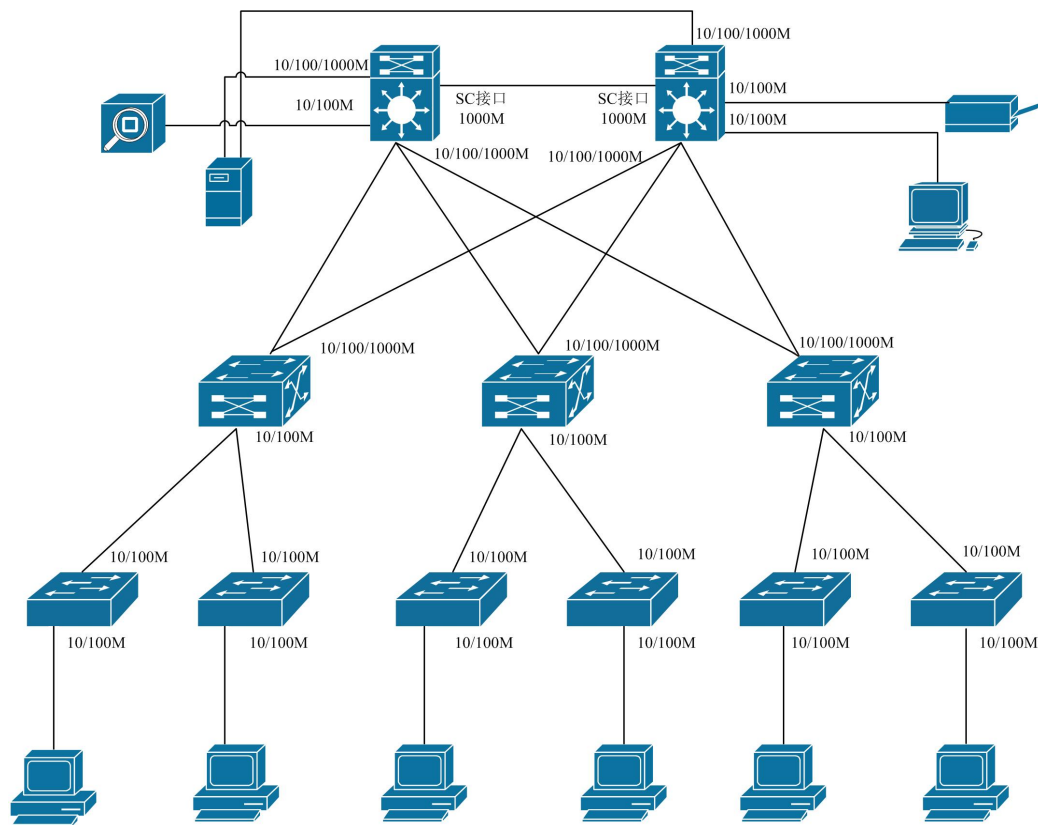


图 1-14 级联边缘交换机

(4) 网络连接。

为了确保与外部网络之间的连接性能, 通常与外部网络连接的防火墙或路由器是直接连接在核心交换机上的。如果同时有路由器和防火墙, 那么防火墙直接与核心交换机连接, 而路由器直接与外部网络连接, 这是因为路由器的广域网接口比较丰富。任务的最终网络结构如图 1-15 所示。

以上的网络结构是一个典型、高效的中型局域网结构, 适合于 200 个用户左右的中型局域网选用。网络中冗余和负载均衡配置也是目前局域网中经常采用的, 但要求核心交换机支持这两方面的技术, 因此在选购时要充分考虑。

任务 3 校园网网络规划设计

【任务描述】

A 公司投标“×××大学”校园网工程, 现进行网络规划设计。

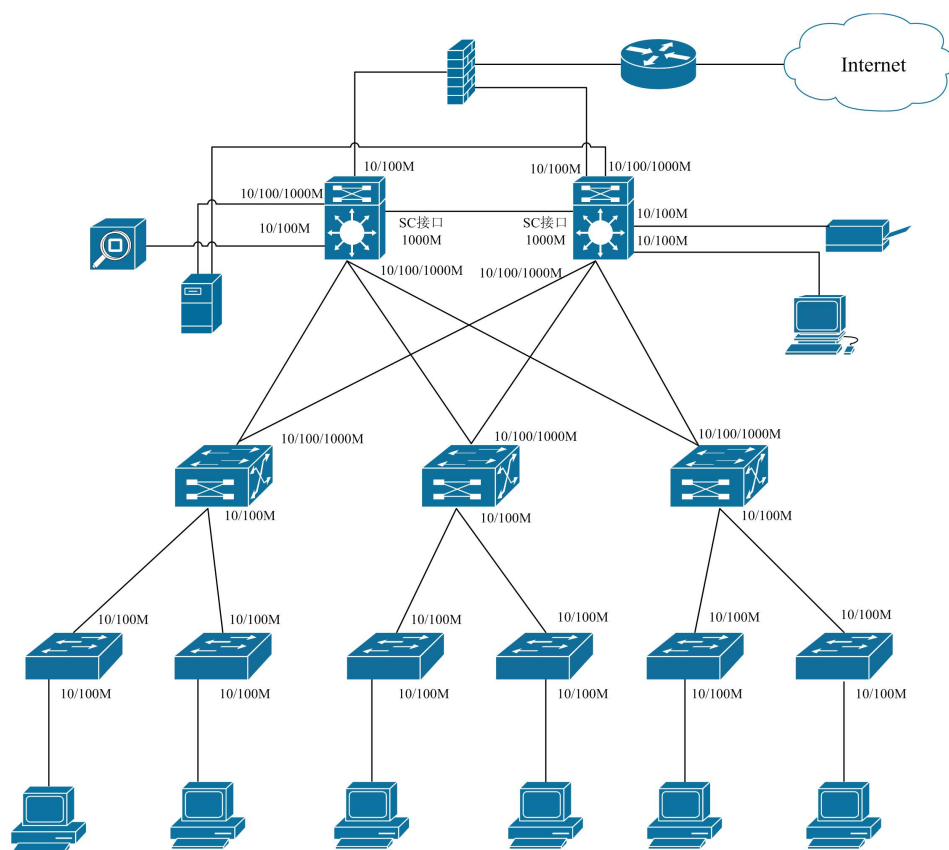


图 1-15 网络连接

【任务目标】

掌握校园网网络结构设计。

【实施过程】

1. 网络要求

(1) 网络建设总体目标。

为满足学校建设与发展的需要，加强校内部门之间的信息交流与合作，增进对外联系，更好地为教学科研服务，有必要在学校内建设校园网。校园网建设应采用先进、成熟的网络技术。连接校内已有的局域网，并通过校园网的网络中心连接中国教育科研网和因特网，为全体师生提供对外科研和学术交流的便捷通道，改善教学科研环境。并且在统一的系统平台上，开发“学校综合管理系统”软件，实现全校的教学、行政管理的计算机化和信息化，以便实现无纸化办公。

(2) 网络建设具体目标。

1) 建立校园网络环境。包括一个网络中心，10个网速为100Mb/s的子网提供多协议、多平台交换式网络系统环境。10个子网，除网络中心的子网，其余子网均通过光缆连接到中心交换机。

2) 建设项目校园主干网。主干网通信速率不低于1000Mb/s，支持多媒体数据通信。设计时应充分考虑将来的发展，以便能够向更快、更先进的网络技术平稳过渡，并且能最大限度地保护前期的投资。

3) 校园网除连接到校内主要建筑外, 还要连接到宿舍区, 包括教职工宿舍和学生的宿舍区, 每个教职工宿舍和每个学生宿舍都应该有一个计算机通信接口。

4) 建立全校的综合网络管理信息系统, 主要涉及教学管理、科研管理、学生管理、财务管理、设备管理、宿舍管理、后勤管理和数字图书馆等。

5) 实现校园网与 CERNET/Internet 的连接, 建立学校的 Web 站点, 编制富有学校特色的 Web 主页, 提供各项标准的 Internet/Intranet 服务, 包括 WWW 浏览、FTP 文件传输、E-mail 电子邮件服务等。

(3) 网络现状。

1) 地理环境。

假定校园内有南北两个校区, 中间为若干城市交通主干线。

2) 现有计算机软硬件设备与通信环境。

校内已有 10 个局域网、500 台 PC 机。校内的 1000 门程控电话机, 连接到各个院部。教工、学生宿舍楼分布在南北两个校区, 有宿舍楼 8 座。教职工现有计算机 100 多台; 已有独立运行的财务管理系统、图书馆管理系统等多个 MIS 系统。预计两年内购买计算机 1000 台, 更换旧计算机 200 台, 届时计算机总数达到 1300 台, 局域网将发展到 20 个。限制: 南北两个校区中间为城市交通主干线。

2. 设计思路

(1) 设计原则。

1) 技术的先进性与成本控制相结合。

2) 技术的先进性与稳定性相结合。

3) 网络的开放性与安全性相结合。

4) 网络建设与技术培训相结合。

5) 确保可管理性和可维护性。

(2) 设计思路要与以上的网络要求和设计原则紧密结合, 主要可按如下几点进行考虑。

1) 采用自上而下的分层结构设计。

首先确定的是核心交换机的连接, 然后是骨干交换机的连接, 依次类推。

2) 把关键设备冗余连接在核心交换机上。

要实现核心交换机负载均衡和冗余配置, 就必须在核心交换机之间, 核心交换机与骨干交换机之间, 以及核心交换机与关键设备之间进行负载均衡和冗余连接的配置。

3) 连接其他网络设备。

把次要重要的多数工作站和网络打印机等设备连接在核心交换机或者骨干交换机的普通端口上, 把工作负荷相对较小的普通工作站用户连接在边缘交换机上。

3. 设计步骤

根据×××大学的需求分析, 该校园网的物理拓扑可以设计为树型网络结构(由三个星型结构组成)。主星型结构位于南校区网络中心, 作为核心层, 另外二个星型结构网络分别位于南校区文学院楼和北校区理学院楼, 作为汇聚层, 其他建筑楼均为接入层。

【知识链接】

一、网络工程目标和设计原则

1. 网络工程目标

一般情况下, 对网络工程目标要进行总体规划, 分步实施。在制定网络工程总目标时应确定采

用的网络技术、工程标准、网络规模、网络系统功能结构、网络应用目的和范围。然后,对总体目标进行分解,明确各个分期工程的具体目标、网络建设内容、所需工程费用、时间和进度计划等。

先根据工程的种类和目标的大小,对网络工程有一个整体规划,然后再确定总体目标,并对目标采用分步实施的策略。

2. 网络工程设计原则

网络信息工程建设目标关系到现在和今后的几年内用户方网络信息化水平和网上应用系统的成败。在工程设计前对主要设计原则进行选择 and 平衡,并排定其在方案设计中的优先级,对网络工程设计和实施将具有指导意义。主要设计原则有:

- (1) 实用、好用与够用性原则。
- (2) 开放性原则。
- (3) 可靠性原则。
- (4) 安全性原则。
- (5) 先进性原则。
- (6) 易用性原则。
- (7) 可扩展性原则。

二、需求分析

1. 用户需求分析的一般方法

(1) 用户需求分析的任务。

对任何一项工程而言,需求分析总是首要的。在为一个中小企业或者学校设计一套局域网方案时,首先要弄清楚客户的具体需求,这对方案的设计和设备的选择起着决定性的作用。在用户找公司对本单位进行网络组建时,需要解决下列问题。

1) 对象分析。

对需要组建的网络进行全面的分析,明确如何完成该工程的设计和制造,这是需求分析中最基本的一条。

2) 局域网系统总体分析。

根据工程设计和制造的需求,初步确定系统硬件和软件应具备的功能和数量,以此确定系统的规模和局域网的拓扑结构。

3) 确定该工程的总目标和阶段目标。

一个中、大型局域网往往需要较强的技术力量和较大的投资。所以,项目一般都是分阶段逐步完善的,并最终实现总目标,即需大致确定工程分几个阶段和每一个阶段的目标。

4) 硬件和软件的选择。

能实现同样功能的硬件和软件可能有很多,但是到底选择哪家公司的硬件和软件最为合适,需要充分的论证。

(2) 用户需求分析的步骤。

需求分析任务书是需求分析的依据。对用户来讲,需求分析就是对多家开发商进行挑选,最终确定一家开发商,签订开发协议后,进行提供具体需求、明确需求的过程,即明确告诉开发商要组建一个什么功能的网络系统。

需求分析的过程。

1) 联系、接触和了解用户方。与用户进行联系并取得对方的人员名单、分工情况、权重、工

作计划、工作时间及节假日安排等。

2) 编写需求分析计划书。根据当前情况,编写需求分析计划书,明确正式开始日期、中间阶段性日期、结束时间、人员名单、分工情况和需要用户提供的帮助等。将计划提交用户确认,在可能的情况下协调用户和开发商的计划,以便共同开展工作。

3) 调研。根据要求调研过程中的进展情况,将需求调研过程分为3个阶段:调研前准备、调研活动管理和调研结束。每个阶段都需要遵循一定的工作流程和注意一些问题。

4) 需求确认。对需求进行最终的确认,需要先由系统开发人员对编写的文档进行内部审核及修订,特别是文字问题。需求确认应真实表达,双方都应明确初步的需求开发工作。

2. 应用概要分析

根据需求的输入,进行第一层次的分析。区分应用分类的特点,在明确项目的应用需求的过程中需要分析以下内容。①带宽、服务需求;②数据吞吐量、存储方案;③网络架构及布局、拓扑结构、容错、负载分配;④Internet/Intranet 网络公共服务、数据库服务、网络基础服务和信息安全平台、网络应用系统。通过应用类型的简要归纳,得出具体的应用需求。

3. 详细需求分析

详细需求分析是局域网需求分析的一部分,它的内容包括以下几个方面。

(1) 网络费用分析。

组建局域网,其本身的费用包括以下几项。

- 1) 网络设备硬件。
- 2) 服务器及客户机设备硬件:服务器群、海量存储设备、网络打印机和客户机等。
- 3) 网络基础设施:UPS 电源、机房装修与综合布线器材等。
- 4) 软件:网管系统、操作系统、数据库、应用系统、安全及定制软件等。
- 5) 远程通信线路或电信租用线路费用。
- 6) 系统集成费用:项目设计、方案和施工等。
- 7) 培训费和网络维护费。

用户都想在经济方面节约,从而获得投资者和单位上级的好评。系统集成费是系统集成商的主要利润的来源,它是一种附加值(一般为外购软硬件的10%~20%)。而品质与费用总是成正比,因此投资规模会影响网络设计、施工和服务水平。

降价是否以网络性能、工程质量和 service 水平的降低为代价呢?事实上,每个网络方案都是在网络性能与用户方所能承受的费用之间进行折中的产物。只有知道用户对网络投资的底细,才能据此确定网络硬件设备和系统集成服务的“档次”,产生与此相配的网络设计方案。随着技术的进步,网络硬件设备性能越来越好,价格却逐步走低,因此工期越长,集成商承担的价格压力就越大。

(2) 网络总体需求分析。

运用应用概要分析结合费用估算的结果和对应用类型及业务密集度的分析,估算出网络数据负载、信息包流量及流向、网络带宽、信息流特征、拓扑结构、网络技术的选择等因素,从而确定网络总体需求框架。

1) 网络数据负载分析。根据当前的应用类型,网络数据主要有3种级别:

- ①MIS/OA/Web 类应用。交换频繁,负载很小。
- ②FTP 文件/CAD/图片文档传输。数据发生不多、负载较大,但无同步要求,允许数据延迟。
- ③流式文件。如 RM/RAM/会议电视/VOD 等,数据随即发生且负载巨大,而且需要图像声音

同步。

数据负载以及这些数据在网络中的传输范围决定着用户要选择多高的网络带宽,选择什么样的传输介质。

2) 信息包流量及流向分析。

信息包流量及流向分析的主要目的是为应用“定界”,即为网络服务器指定地点。分布式存储和协同式网络信息处理是计算机网络的优势之一。把服务器群集中放置在网络管理中心有时并不是明智的作法,明显的缺点有:信息包过分集中在网管中心子网以及为数不多的网卡上,会形成拥塞;若网管中心发生意外,将导致数据损失惨重,不利于容灾。但是服务器系统过于分散也会对管理带来麻烦,且使网络环境复杂化。

通过分析信息包的流向,可以为服务器定位提供重要的依据。例如,对于财务系统服务器来说,信息流主要在财务部,少量流向企业管理子网,因此可以考虑将其放在财务部。

3) 信息流特征分析。主要考虑以下因素。

- ①信息流实时性。
- ②信息最大响应时间和延迟时间的要求。
- ③信息流的批量特性。
- ④信息流交互特性:信息检索/录入不同。
- ⑤信息流的时段性。

4) 拓扑结构分析。可从网络规模、可用性要求、地理分布和房屋结构多种因素来分析。例如,建筑物较多、建筑物内点数过多、交换机端口数不足,就需要增加交换机的个数和连接方式。网络可用性要求高、不允许网络有停顿,需采用双星结构。地理上有空隙的网络要采用特殊拓扑结构,如单位分为两地以上,业务必须一体化,需考虑特殊连接方式的拓扑结构。

5) 网络技术分析选择。尽量选择当前主流的网络技术,如千兆以太网、快速/交换式以太网等技术。一些特别的实时应用(如工业控制、数据采样、音频和视频流)需要采用面向连接的网络技术。面向连接的网络技术能够保证数据的实时传输。传统技术如 IBM Token Bus,现代技术如 ATM 等都可较好地实现面向连接的网络。

(3) 综合布线需求分析。

布线需求分析主要包括以下几方面:

1) 根据造价、建筑物距离和带宽要求确定线缆的类型和光缆的芯数。6类和超5类线较贵,5类线价格稍低。单模光缆传输质量高、距离远,但模块价格昂贵;光缆芯数与价格成正比。

2) 布线路由分析。根据调研中得到的建筑群间距离、马路隔离情况、电线杆、地沟和道路状况对建筑群间光缆布线方式进行分析,为光缆采用架空、直埋还是地下管道的方式铺设找到直接依据。

3) 对各建筑物的规模信息点数和层数进行统计。用以确定室内布线方式和管理间的位置,建筑物楼层较高、规模较大、点数较多时宜采用分布式布线。

(4) 网络可用性/可靠性需求分析。

除采用磁盘双工和磁盘阵列、双机容错、异地容灾和备份减灾措施等,还可采用能力更强的大中小型 UNIX 主机(如 IBM、HP 和 SUN)。

(5) 网络安全需求分析。

安全需求分析具体表现在以下几个方面:

- 1) 分析存在弱点漏洞与不当的系统配置。

- 2) 分析网络系统阻止外部攻击行为和防止内部职工的违规操作行为的策略。
 - 3) 划定网络安全边界,使企业网络系统和外界的网络系统可以安全隔离。
 - 4) 确保租用线路和无线链路的通信安全。
 - 5) 分析如何监控企业的敏感信息,包括技术专利等信息。
 - 6) 分析工作桌面系统安全。安全不单纯是技术问题,而是策略、技术与管理的有机结合。
- (6) 分析结果的交付。

需求分析完成后,应产生明确的《需求分析报告》文档,并与用户交互修改,最终应该经过由用户方组织的评审,评审过后,根据评审意见,形成的最终版本不再更改。之后的需求,按需求变更实施。

三、网络通信平台的设计

1. 网络总体目标和设计原则

(1) 网络总体目标。

- 1) 明确采用的网络技术、标准,满足哪些应用、规模目标。
- 2) 如果分期实施,明确分期工程的目标、建设内容、所需工程费用、时间和进度计划等。
- 3) 不同的网络设计,其目标也大相径庭。除应用外,主要限制因素是投资规模。不仅要考虑实施成本,还要考虑运行成本,有了投资规模,在选择技术时就会有有的放矢。

(2) 总体设计原则。

- 1) 高可用性/可靠性原则。对于像金融、证券、电信、电力、民航和铁路等行业的网络系统应确保高可用性和高可靠性。
- 2) 安全性原则。在企业网、政府行政办公网、国防军工部门内部网、电子商务网等网络方案设计中应重点体现安全性原则,确保网络系统和数据的安全运作;在社区网、校园网中,安全性的考虑相对较弱。
- 3) 实用性原则。即“够用”和“实用”原则。
- 4) 开放性原则。网络系统应采用开放的标准和技术,以利于未来网络系统的扩充和必要时与外部网络的互通。
- 5) 先进性原则。尽可能采用先进而成熟的技术,在一段时期内保证其主流地位。
- 6) 慎用太新的技术。一是不成熟;二是标准还不完备、不统一;三是价格高;四是技术支持力量不足。
- 7) 易用性原则。可管理,满足应用的同时,为升级奠定基础,应具备很高的资源利用率。
- 8) 可扩展性原则。目前网络产品的标准化程度较高,因此可扩展性要求基本可以达到,冗余应适可而止。

2. 网络拓扑结构

网络的拓扑结构主要是指园区网络的物理拓扑结构。

选择拓扑结构时,应该考虑的主要因素有以下几点。

(1) 地理环境。不同的地理环境需要设计不同的物理网络拓扑,不同的物理网络拓扑设计的施工安装的费用也不同。

(2) 传输介质与距离。在设计网络时,考虑到传输介质的不同、距离的远近和可用于网络通信平台的经费投入,网络拓扑结构必须在传输介质、通信距离、可投入经费三者之间进行权衡。

(3) 可靠性。网络设备损坏、光缆被挖断、连接器松动等这类故障是有可能发生的,网络拓

扑结构设计应避免因个别结点损坏而影响到整个网络的正常运行。

网络拓扑结构的规划设计与网络规模息息相关。一个规模较小的星型局域网没有汇聚层、接入层之分。规模较大的网络通常为多星型分层拓扑结构。主干网络称为核心层，用于连接服务器、建筑群到网络中心设备间，或在一个较大型建筑物内连接多个交换机配线间到网络中心设备间。连接信息点的“毛细血管”线路及网络设备称为接入层，根据需要在核心层和接入层中间设置汇聚层。

分层设计有助于分配和规划带宽，有利于信息流量的局部化，比如当全局网络对某个部门的信息访问的需求很少（如财务部门的信息，只能在本部门内授权访问）时，部门业务服务器即可放在汇聚层，这样局部的信息流量传输不会波及到全网。

3. 主干网络（核心层）的设计

主干网技术的选择，要根据以上需求分析中用户方网络规模的大小、网上传输信息的种类和用户方可投入的资金等因素来考虑。

4. 汇聚层和接入层的设计

汇聚层的存在与否，取决于网络规模的大小。

接入层即直接信息点，通过此信息点将网络资源设备（如 PC 等）接入网络。

5. 无线网络的设计

无线网络是为了解决有线网络无法克服的困难而出现的。无线网络首先适用于很难布线的地方（如受保护的建筑物、机场等）或者经常需要变动布线结构的地方（如展览馆等）。学校也是一个很重要的应用领域，一个无线网络系统可以使教师、学生在校园内的任何地方接入网络。

6. 网络通信设备选型

（1）网络通信设备选型原则。

- 1) 品牌选择；
- 2) 扩展性考虑；
- 3) “量体裁衣”策略；
- 4) 性价比高、质量可靠的原则。

（2）核心交换机选型策略。

核心交换机是宽带网的核心，应具备：

- 1) 高性能、高速率；
- 2) 便于升级和扩展；
- 3) 高可靠性；
- 4) 强大的网络控制能力，提供 QoS 和网络安全，支持 RADIUS、TACACS+等认证机制；
- 5) 良好的可管理性，支持通用网管协议。

（3）汇聚层/接入层交换机选型策略。

汇聚层/接入层交换机亦称二级交换机或边缘交换机。在大中型网络中，它用来构成多层次的、结构灵活的用户接入网络。在中小型网络中，它也可以用来构成网络骨干交换设备。它应具备：

- 1) 灵活性；
- 2) 高性能；
- 3) 在满足技术性能要求的基础上，最好价格便宜、使用方便、即插即用、配置简单；
- 4) 具备一定的网络服务质量和控制能力；
- 5) 如果是用于跨地区企业分支部门通过公网进行远程上联的交换机，还应支持虚拟专网 VPN

标准协议；

6) 支持多级别网络管理。

(4) 远程接入与访问设备选型策略。

远程接入与访问设备可以采用路由器。

四、网络资源平台设计

1. 服务器

服务器一般分为两类，一类为全网提供公共信息服务、文件服务和通信服务，为园区网络提供集中统一的数据库服务；另一类是部门业务和网络服务相结合，主要由部门管理维护。其磁盘系统数据吞吐量大，传输速率也高，要求高带宽接入。服务器网络接入方式主要有双网卡冗余接入和单网卡接入两种。

2. 服务器子网连接方案

服务器子网连接的两种方案如图 1-16 所示。如图 1-16 (a) 所示，服务器直接连接核心层交换机，优点是直接利用核心层交换机的高带宽，缺点是需要占用太多的核心层交换机端口，使成本上升。如图 1-16 (b) 所示，两台核心层交换机上连接一台专用服务器子网交换机，服务器通过专用交换机间接与核心层交换机相连，优点是可以分担带宽，减少核心层交换机端口占用，可为服务器组提供充足的端口密度，缺点是容易形成带宽瓶颈，且存在单点故障。

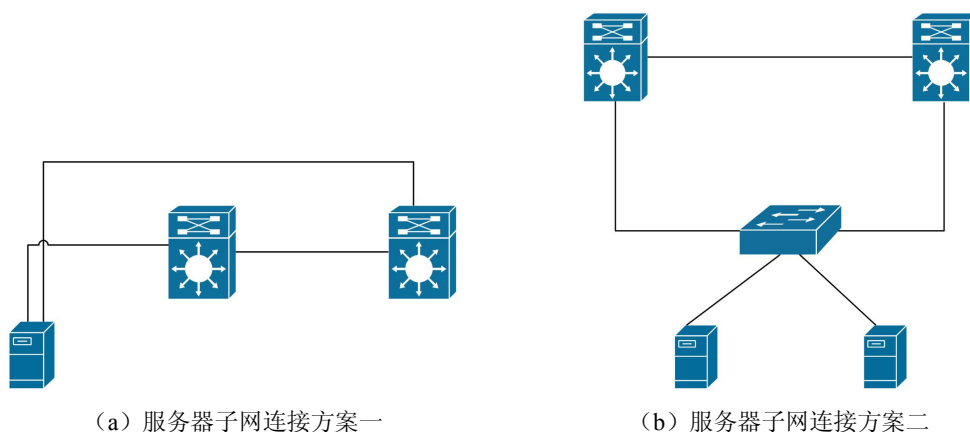


图 1-16 服务器子网连接方案

3. 网络应用系统

在网络方案设计中，服务器的选择配置以及服务器群的均衡技术是非常关键的技术之一，也是衡量网络系统集成商水平的重要指标。很多系统集成商的方案偏重的是网络设备集成而不是应用集成，在应用问题上缺乏高度认识和认真细致的需求分析，待昂贵的服务器设备购进来后发现与应用软件不配套、不够用或造成资源浪费，必然会使预算超支，直接导致网络方案失败。

五、网络操作系统与服务器配置

1. 网络操作系统选型

网络操作系统分为两个大类，即面向 IA 架构 PC 服务器的操作系统族和 UNIX 操作系统家族。UNIX 服务器品质较高、价格昂贵、装机量少而且可选择性也不高，一般根据应用系统平台的实际需求，估计好费用，瞄准某一两个企业的产品去准备即可。与 UNIX 服务器相比，Windows 服务器品牌和产品型号多种多样，一般在中小型网络中普遍采用。

同一个网络中不需要采用同一种网络操作系统,可结合 Windows、Linux 和 UNIX 的特点,在网络中混合使用。通常 WWW、OA 及管理信息系统服务器上可采用 Windows Server 2008 平台,E-mail、DNS、Proxy 等 Internet 应用可使用 Linux/UNIX,这样,既可以享受到 Windows 应用丰富、界面直观、使用方便的优点,又可以享受到 Linux/UNIX 稳定、高效的好处。

2. Windows 服务器配置

(1) 根据需求阶段的调研成果,如网络规模、客户数量流量、数据库规模、所使用的应用软件的特殊要求等,决定 Windows 服务器的档次、配置。

(2) 选择 Windows 服务器时,对服务器上几个关键部分的选取一定要把好关。因为 Windows Server 2008 虽然是兼容性相对不错的操作系统,但并不能保证 100%兼容。

(3) 在升级已有的 Windows 服务器时,则要仔细分析原有网络服务器的瓶颈所在,此时可简单利用 Windows Server 2008 系统中集成的软件工具,根据网络应用系统的实际情况来确定增加服务器处理器的数目。

3. 服务器群的综合配置与均衡

所谓的 PC 服务器、UNIX 服务器、小型机服务器,其概念主要限于物理服务器(硬件)范畴。在网络资源存储、应用系统集成中,通常将服务器硬件上安装各类应用系统的服务器系统冠以相应的应用系统的名字,如数据库服务器、Web 服务器、E-mail 服务器等,其概念属于逻辑服务器(软件)范畴。根据网络规模、用户数量和应用密度的需要,有时一台服务器硬件专门运行一种服务,有时一台服务器硬件需安装两种以上的服务程序,有时两台以上的服务器需安装和运行同一种服务系统。网络规模小到只用 1 至 2 台服务器的局域网,大到使用十几台至数十台服务器的企业网和校园网,如何根据应用需求、费用承受能力、服务器性能和不同服务程序之间对硬件占用的特点合理搭配和规划服务器配置,在最大限度地提高效率 and 性能的基础上降低成本,是系统集成方要考虑的问题。

六、网络安全体系

网络安全体系设计的重点在于根据安全设计的基本原则,制定网络各层次的安全策略和措施,然后确定选用什么样的网络安全系统产品。

1. 网络安全设计原则

尽管没有绝对安全的网络,但是,如果在网络方案设计之初就遵从一些安全原则,那么网络系统的安全就会有保障。设计时如不全面考虑,消极地将安全和保密措施寄托在网络管理阶段,这种事后“打补丁”的思路是相当危险的。从工程技术角度出发,在设计网络方案时,应该遵守以下原则。

(1) 网络安全前期防范。

应强调对信息系统全面地进行安全保护。大家都知道“木桶的最大容积取决于最短的一块木板”,此道理对网络安全来说也是有效的。网络信息系统是一个复杂的计算机系统,它本身在物理上、操作上和管理上的种种漏洞构成了系统的安全脆弱性,尤其是多用户网络系统由于自身的复杂性、资源共享性,使单纯的技术保护防不胜防。攻击者秉承的是“最易渗透性”原则,自然在系统中最薄弱的地方进行攻击。因此,充分、全面、完整地系统的安全漏洞和安全威胁进行分析、评估和检测(包括模拟攻击),是设计网络安全系统的必要前提条件。

(2) 网络安全在线保护。

应强调安全防护、监测和应急恢复。要求在网络发生被攻击、破坏的情况下,必须强调安全防

护、监测和应急恢复。要求在网络发生被攻击、破坏的情况下，必须尽可能快地恢复网络信息系统的服务，减少损失。所以，网络安全系统应该包括3种机制：安全防护机制、安全监测机制、安全恢复机制。安全防护机制是指根据系统具体存在的各种安全漏洞和安全威胁采取的相应防护措施，避免非法攻击的进行；安全监测机制用来监测系统的运行，及时发现和制止对系统进行的各种攻击；安全恢复机制用来在安全防护机制失效的情况下，进行应急处理和及时地恢复信息，减少攻击的破坏程度。

（3）网络安全有效性与实用性。

网络安全应以不影响系统的正常运行和合法用户方的操作活动为前提。网络中的信息安全和信息应用是一对矛盾。一方面，为健全和弥补系统缺陷的漏洞，会采取多种技术手段和管理措施；另一方面，安全措施给系统的运行和用户方的使用造成负担和麻烦，“越安全就意味着使用越不方便”。尤其在网络环境下，实时性要求很高的业务不能容忍安全连接和安全处理造成的时延。网络安全采用分布式监控、集中式管理。

（4）网络安全等级划分与管理。

良好的网络安全系统必然是分为不同级别的，包括对信息保密程度分级（绝密、机密、秘密、普密）、对用户操作权限分级（面向个人及面向组）、对网络安全程度分级（安全子网和安全区域）、对系统结构层分级（应用层、网络层、数据链路层等）的安全策略。针对不同级别的安全对象，提供全面的、可选的安全算法和安全体制，以满足网络中不同层次的各种实际需求。

网络总体设计时要考虑安全系统的设计。避免因考虑不周，造成经济上的巨大损失，避免对国家、集体和个人造成无法挽回的损失。由于安全与保密问题是一个相当复杂的问题。因此必须注重网络安全管理，安全策略部署到具体设备、安全责任分配到个人、安全机制贯穿到整个网络系统，这样才能保证网络的安全性。

（5）网络安全经济实用。

网络系统的设计是受经费限制的。因此在考虑安全问题解决方案时必须考虑性能价格比，而且不同的网络系统所要求的安全侧重点各不相同，网络安全产品实用、好用、够用即可。一般园区网络要具有身份认证、网络行为审计、网络容错、防黑客、防病毒等功能。

2. 网络信息安全设计与实施步骤

（1）确定面临的各种攻击和风险。

（2）确定安全策略。

安全策略是网络安全系统设计的目标和原则，是对应用系统完整的安全解决方案。安全策略的制定要综合以下几方面的情况。

1) 系统整体安全性，由应用环境和用户需求决定，包括各个安全机制子系统的安全目标和性能指标。

2) 对原系统的运行造成的负荷和影响，如网络通信时延、数据扩展等。

3) 方便网络管理人员进行控制、管理和配置。

4) 有可扩展的编程接口，便于更新和升级。

5) 具备界面的友好性和使用方便性。

6) 估算投资总额和工程时间等。

（3）建立安全模型。模型的建立可以使复杂的问题简单化，更好地解决和安全策略有关的问题。安全模型包括网络安全系统的各个子系统。网络安全系统的设计和实现可以分为安全体制、网

络安全连接和网络安全传输三部分。

1) 安全体制：包括安全算法库、安全信息库和用户方接口界面。

2) 网络安全连接：包括安全协议和网络通信接口模块。

3) 网络安全传输：包括网络安全管理系统、网络安全支撑系统和网络安全传输系统。

(4) 选择并实现安全服务。

1) 物理层的安全：物理层信息安全主要防止物理通路的损坏、物理通路的窃听和对物理通路的攻击、干扰等。

2) 链路层的安全：链路层的网络安全需要保证通过网络链路传送的数据不被窃听。主要采用划分 VLAN（局域网）、加密通信（远程网）等手段。

3) 网络层的安全：网络层的安全要保证网络只给授权的客户使用授权的服务，保证网络传输正确，避免被拦截或监听。

4) 操作系统的安全：操作系统安全要求保证客户资料、操作系统访问控制的安全，同时能够对该操作系统上的应用进行审计。

5) 应用平台的安全：应用平台是指建立在网络系统之上的应用软件服务，如数据库服务器、电子邮件服务器、Web 服务器等。由于应用平台的系统非常复杂，通常采用多种技术（如 SSL 等）来增强应用平台的安全性。

6) 应用系统的安全：应用系统为用户提供服务，应用系统的安全与系统设计和实现关系密切。应用系统使用应用平台提供的安全服务来保证基本的安全，如通信内容安全、通信双方的认证和审计等手段。

(5) 安全产品的选型。

网络安全产品主要包括防火墙、用户身份认证、网络防病毒系统等。安全产品的选型工作要严格按照用户信息与网络安全产品的功能规范要求，利用综合的技术手段，对产品功能、性能与可用性等方面进行测试，为用户选出符合功能要求的安全产品。

【拓展训练】

读者根据以上知识，独立完成以下任务：

(1) 进行×××大学校园网的需求调查。

(2) 进行×××大学校园网建设方案的规划设计，画出网络拓扑图。

【分析和讨论】

(1) 如何进行需求调查？

(2) 网络规划设计应包含哪些主要部分？