第 1 章

计算机网络工程模拟环境

本章主要给出一个模拟的计算机网络工程环境。为了比较全面地介绍计算机网络工程中必备的知识和常用的技术，这个模拟环境需要复杂一些。然后根据环境中的用户需求，分析得出该网络工程项目需要完成的任务。以后的章节都是围绕一个个任务项目介绍必备的知识、技术，介绍完成任务项目的设计方案，最终完成任务的设计或实现。

考虑到教学环境和模拟工程环境的差异，第 2 章到第 5 章的最后在给出模拟网络工程环境任务实现的同时，都给出了一个实验室的模拟实训环境，以便在实验室环境下验证相应任务的设计和实现。

1.1 概述

假设某新兴产业公司新近成立，公司目前有上万名职工，预计年产值上百亿元，预计利税有 20 亿元。公司总部设在 A 市，在 B 市和 C 市设有分公司，并且在 A 市、B 市、C 市都有分支机构。该公司的地理分布如图 1-1 所示。

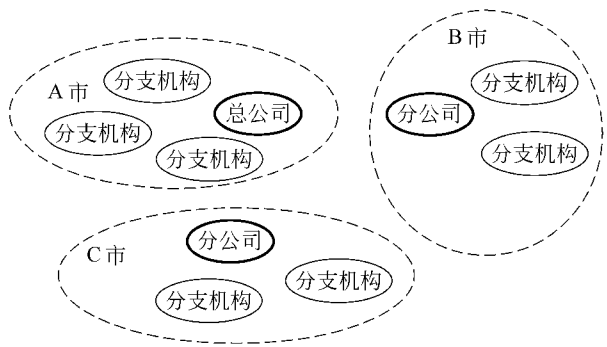

图 1-1 公司的地理分布

总公司和分公司都由管理部门、研发部门、市场部门、售后服务部门和生产部门组成，占地面积在 $1km^2$ 左右。各部门分布在 5～8 座楼宇和厂房内。各分支机构一般由市场部门、售后服务部门和部分管理部门组成，一般分布在一座楼宇内。

为了适应现代管理和生产的需要，公司购置了大量的计算机设备。总公司的信息点

有800多个，两个分公司和分支机构根据规模的不同分别有20～200个不等的信息点。目前公司在信息化建设方面的主要任务是建设公司内部网络，实现公司内部的管理网络化，达到利用公司内部网络实现信息资源共享和信息管理的目的。

1.2 任务需求分析

对于网络工程项目而言，首先需要进行用户需求分析，对用户的管理目标需求、技术目标需求以及应用目标需求等进行调查，并对调查结果进行分析，最终根据需求分析结果确定网络设计方案。

在给出的模拟网络工程环境中，假定该公司并没有任何的网络基础，需要进行全新网络的搭建。通过与公司的相关部门和人员进行沟通交流，收集了相关需求信息，并对需求信息进行分析。

1.2.1 总体需求分析

随着该公司业务规模的不断扩大，出于管理和发展的需要，信息化建设成为必须要面对的问题。公司信息化建设的目标是建设公司内部网络，将总公司、分公司和各分支机构通过网络进行连接，实现公司内部的信息化管理。

1. 管理目标需求

通过沟通，了解到该公司的组织机构如下：该公司在A市设有总公司和3个分支机构，在B市和C市分别设有一个分公司和两个分支机构。总公司和分公司主要负责产品的研发和生产，主要有管理部门、研发部门、市场部门、售后服务部门和生产部门，各部门分布在5～8座楼宇和厂房内，楼宇间的直线距离不超过1500m。分支机构主要负责产品的市场拓展和售后服务，主要有市场部门、售后服务部门和部分管理部门，一般分布在一座楼宇内。

总公司的1号办公楼共25层，每层有信息点15～20个，共计有信息点400个左右；在1号办公楼上办公的部门有管理部门、研发部门以及公司内部网络建成后的总公司网络中心。总公司的2号办公楼共7层，每层有信息点30～35个，共计有信息点200个左右；在2号办公楼上办公的部门有市场部门和售后服务部门。总公司共有厂房4座，所有厂房都只有一层。每个厂房分成了10个生产区，每个生产区有信息点5个，每个厂房共计有信息点50个左右；生产部门分散在各个厂房中。

A市的分支机构1所在的办公楼共7层，每层有信息点10～20个，共计有信息点100个左右；在该办公楼上办公的部门有市场部门、售后服务部门和分支机构管理部门。A市的分支机构2仅占用所在办公楼的一层，共计有信息点30个左右；在该办公楼上办公的部门有市场部门、售后服务部门和分支机构管理部门。

公司的决策者希望能够通过一次投入，建设起完善的公司内部网络，并且要求网络能够满足公司业务不断发展和员工不断增多的需要。

实际工程方案中的管理目标需求需要详细地描述客户公司的组织机构、业务情况；客

户公司的地理位置分布，包括总公司、分公司和各分支机构的地理位置与距离，总公司、分公司和各分支机构内部建筑物的位置与距离，各建筑物内办公区的分布情况，各办公区内的信息点数目和规模，各建筑物内弱电井、配电室的位置等；客户公司的员工情况；客户公司决策者的建设思路及预算等。而本部分出于教学的需要，只给出了其中的一部分需求，并非完整的管理目标需求描述，希望读者注意。

2. 技术目标需求

在网络的可扩展性方面，考虑到该公司以后的发展，在总公司、分公司和各分支机构的局域网设计中，均做了局域网设备接口、信息接入点和布线的预留，预留比例根据具体情况在 10%～20%之间。另外，考虑到技术的兼容性，网络中使用的协议均为开放式协议，以确保对不同厂家生产的网络设备的支持。

在网络的带宽方面，信息点的接入带宽采用主流的 100Mbps，楼宇间采用 1000Mbps 的光纤连接。对于对带宽需求较高的总公司市场部门的部分主机，其汇聚层链路采用链路带宽聚合技术增加可用带宽。总公司网络中心的网站服务器、邮件服务器等由于并发连接数较高，采用链路冗余技术与负载均衡技术来提高网络的可靠性和访问速度。

在网络设备的选择方面，所有设备都应具有可管理功能，并为网络设备划分专门的子网，确保网络管理员可以在公司内任一地点通过远程管理软件对所有的网络设备进行管理。

在安全性要求方面，一方面要确保网络连接及网络设备的物理安全；另一方面需要通过定义相关策略确保网络应用和信息传输的安全，具体内容可参考《计算机网络安全与管理》一书。

总体需求分析一般还包括应用需求，以明确企业的应用服务类型及其对网络功能指标的要求。由于其涉及的知识不在本书的范围内，在此不再进行介绍，具体内容可参考《网络操作系统》一书。

1.2.2　具体需求分析

在了解了该公司的总体需求，包括公司的管理目标需求和技术目标需求后，以总体需求为依据，分别对网络工程涉及的各方面技术进行具体的需求分析。

1. 局域网设计需求

该公司包括了总公司、两个分公司和 7 个分支机构，共 10 个局域网，对于每一个局域网需要根据其规模分别进行分析和设计。考虑到部分局域网实现上的重复性，本书仅对其中有代表性的 3 个局域网进行分析。

总公司局域网包含了 5 个部门、1 个网络中心和 800 多个信息点，并且跨越了 6 座建筑。在局域网设计上采用接入、汇聚和核心 3 层网络连接：在接入层将信息点连接到网络中，在汇聚层设置安全策略，在核心层实现局域网各子网间数据的高速交换和与公司广域网的连接。

A 市的分支机构 1 在一座建筑内，包含了 3 个部门和 100 多个信息点。在局域网设计上采用接入、核心两层网络连接：在接入层将信息点连接到网络中，在核心层实现安全

策略、局域网各子网间数据的交换和与公司广域网的连接。

A 市的分支机构 2 在一座建筑的一层内，包含了 3 个部门和 30 多个信息点。由于信息点较少，且在同一楼层，局域网不再做分级设计，直接由接入交换机连接到公司的广域网。

2. 综合布线需求

本部分只包括数据网络布线部分，不讨论语音及其他弱电系统的布线。布线系统要求在遵循兼容性、开放性、灵活性、可靠性和先进性等原则的基础上采用模块化和分层星型拓扑结构设计，将布线系统分割成工作区子系统(Work Area Subsystem)、配线子系统(Horizontal Subsystem)、干线子系统(Backbone Subsystem)、设备间子系统(Equipment Room Subsystem)、进线间子系统(Lead-in Room Subsystem)、管理子系统(Administration Subsystem)和建筑群子系统(Campus Subsystem)7 部分，并分别进行设计和实现。为了确保各子系统之间的相对独立，相邻子系统之间通过跳线进行交连和互连。在管理上要求采用双点管理双交连的方式，以确保网络的易管理性。

3. IP 地址规划需求

在 IP 地址规划上，原则上按照部门进行子网的划分，并且要求为网络设备划分专门的管理子网、为点对点连接划分子网。通过使用可变长子网掩码(Variable-Length Subnet Masks，VLSM)技术，确保子网的大小既符合相应部门或连接对 IP 地址的数量要求，又尽量避免了 IP 地址的浪费。同一个公司或分支机构的多个子网 IP 地址应尽量连续。

4. 路由需求

对于网络中的不同部分采用不同的路由方式。对于规模较小的局域网采用直连路由、静态路由实现；对于规模相对较大的局域网采用路由选择信息协议(Routing Information Protocol，RIP)实现；总公司、分公司和各分支机构之间采用多区域的开放式最短路径优先协议(Open Shortest Path First，OSPF)实现，在区域的边界上采用无类别域间路由选择(Classless Inter-Domain Routing，CIDR)技术进行路由汇聚，以减少路由条目。不同路由选择协议之间使用路由重分布技术进行路由信息的共享。

通过对模拟网络工程环境进行简要的具体需求分析，可以了解到完成该网络工程任务需要具备的知识主要有网络设计、综合布线、IP 地址规划、路由协议等网络设备配置以及网络设备管理等几个方面，在后续的章节中将分别对它们进行介绍。

1.3 小结

本章给出了拟定的模拟网络工程环境，并对其进行任务需求分析，包括总体需求分析和具体需求分析。通过需求分析对网络工程中需要完成的各方面的任务以及涉及的技术知识进行介绍，为后续各个章节知识的展开做好铺垫。

1.4　习题

1. 任务需求分析主要包含哪两部分?
2. 总体需求分析一般包括哪 3 部分?
3. 管理目标需求主要是对网络工程的哪些方面进行需求分析?
4. 技术目标需求主要是对网络工程的哪些方面进行需求分析?

第 2 章

网络系统总体设计

本章的任务

根据第 1 章给出的工程任务需求分析进行全公司的网络系统总体设计。

必备的知识

(1) 网络设计方法。

(2) 网络通信链路带宽设计与网络性能设计。

(3) 网络设备的选型。

达到的目标

完成总公司、分公司和各分支机构之间的网络逻辑结构的规划和设计。

计算机网络系统设计的一般方法是从基层信息点接入开始完成各个局部局域网的设计,然后将各个局域网连接形成一个整体网络。下面介绍在网络设计中经常使用的技术方法。

2.1 局域网分层网络设计

2.1.1 局域网分层网络设计模型

使用自备通信线路,地理覆盖范围较小的一个单位内部网络一般都使用局域网技术实现。当一个局域网内部信息点较多,例如模拟公司环境中一个分支机构内的信息点上千个时,局域网的设计一般采用分层网络设计方法。同 ISO/OSI 参考模型的理念类似,分层网络设计模型把网络逻辑结构的设计这一复杂的网络问题分解为多个小的、更容易管理的问题。它将网络分成互相分离的层,每层提供特定的功能,这些功能界定了该层在整个网络中扮演的角色。通过对网络的各种功能进行分离,可以实现模块化的网络设计,从而提高网络的可扩展性和性能。典型的分层网络设计模型可分为 3 层:接入层、汇聚层和核心层,如图 2-1 所示。在局域网分层网络设计模型中,各层网络设备间的连接通常使用包转发速率较高的以太网交换机来实现。

1. 接入层

接入层负责将终端设备,如 PC、服务器、打印机等连接到网络中。接入层的主要作用是提供一种将设备连接到网络并控制允许网络中的哪些设备进行通信的方法。根据网络接入方式的不同,接入层设备一般采用较低档次的以太网交换机或无线接入设备。所有的最终用户均由接入层连接到网络中。

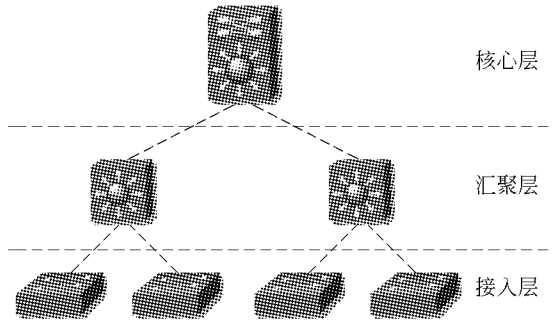

图 2-1　分层网络设计模型

2. 汇聚层

汇聚层位于接入层和核心层之间，它先汇聚接入层发送的数据，再将其传输到核心层，并最终发送到目的地。汇聚层通过定义通信策略控制网络中的通信流，尤其是进入核心层的通信，来提供边界的定义。汇聚层通过通信策略控制将核心层和网络的其他部分区分开，达到禁止不必要的流量进入核心层的目的。汇聚层设备一般使用具有较高包转发速率和路由功能的三层交换机，在汇聚层交换机上除了完成较高速率的数据转发之外，还需要为下层交换机提供 VLAN 之间的路由。

3. 核心层

核心层是局域网分层网络中的高速主干，是局域网分层网络设计模型中的一个层次定义，而不是指整个网络系统的核心骨干网络。局域网分层网络设计中的核心层主要用于汇聚所有下层设备发送的流量，进行大量数据的快速转发。核心层不承担任何访问控制、数据加密等影响快速交换的任务。核心层设备通常需要具备极高的数据转发速率。

需要注意的是，局域网分层网络设计模型只是一个概念上的框架，实际的网络设计结构会因网络的具体情况而异。这 3 层可能位于清晰明确的物理实体中，也可能不是。在很多的小型网络中，通常采用紧缩核心型的网络设计，即将核心层和汇聚层合二为一。

2.1.2　局域网分层网络设计中的网络直径

在分层网络设计中，网络直径是指网络中任意两台终端之间进行通信需要经过的网络设备数目的最大值，而不是指通信的最大距离。如图 2-2 所示，PC1 和 PC2 之间进行通信至多可能经过 5 台交换机，即网络直径为 5。

在进行分层网络设计时，应该尽可能地降低网络直径的值，因为数据在经过网络设备时都会产生延时，网络直径越大，积累的延时越长。例如，数据帧在经过交换机时，交换机需要确定帧的目的 MAC 地址，从“端口—MAC 地址映射表”中查找转发端口，再将数据帧转发到相应的端口上。这个过程虽然只有几分之一秒的延时，但如果数据帧要经过许多台交换机，累加后的延时将不容忽视，而数据报文经过路由器的延时将会更长。因此将网络直径保持在较低的水平是提高网络传输性能的一个重要因素。

在分层网络设计中，网络直径总是源设备和目的设备之间的跳数，而跳数是可预测的。在局域网中，一般即使网络采用冗余技术，在汇聚层和核心层引入了冗余设备和冗余

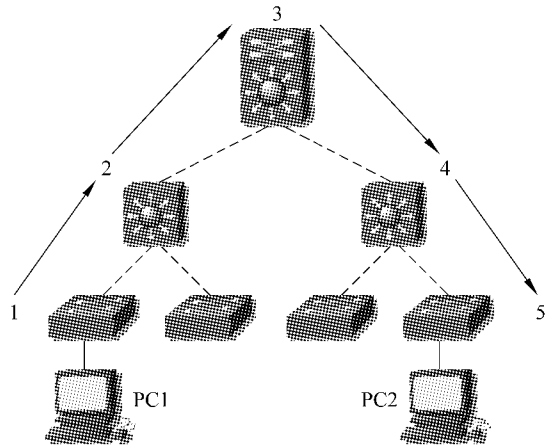

图 2-2 网络直径

链路，网络直径也会被控制在 6 之内；但是在涉及广域网的大型网络中，网络直径往往会较大，网络设计时应该尽量降低网络直径。

2.1.3 局域网分层网络设计的优点

1. 可扩展性好

分层网络具有很好的可扩展性。由于采用了模块化的设计，以及同一层中实例设计的一致性，当网络需要扩展时，可以很方便地将某一部分的设计直接进行复制。例如，如果网络设计中为每 8 台接入层交换机配备了 2 台汇聚层交换机，则在网络接入点增多时，可以不断地向网络中增加接入层交换机，直到有 8 台接入层交换机交叉连接到 2 台汇聚层交换机上为止。如果网络接入点继续增多，则可以重复上述过程，通过增加汇聚层交换机和接入层交换机来确保网络的可扩展性。

2. 网络通信性能高

改善通信性能的方法是避免数据通过低性能的中间设备传输。在局域网分层网络设计中，一般通过使用转发速率较高的交换机设备将通信数据以接近线速的速度从接入层发送到汇聚层。随后，汇聚层交换机利用其高性能的交换功能将此流量上传到核心层，再由核心层交换机将此流量发送到最终目的地。由于核心层和汇聚层选用高性能的交换机，因此数据报文可以在所有设备之间实现接近线速的速度传递，大大提高网络的通信性能。

3. 安全性高

局域网分层网络设计可以提高网络的安全性。在接入层可以通过端口安全选项的配置来控制允许哪些设备连接到网络。在汇聚层则可以使用更高级的安全策略来定义在网络上部署哪些通信协议以及允许这些协议的流量传送到何方。例如，可以在接入层交换机上通过端口粘滞功能来限制只允许特定 MAC 地址的主机接入到网络；在汇聚层交换机上则可以通过定义并应用访问控制列表（Access Control Lists，ACL）来限制允许或禁止特定高层协议（如 IP、ICMP、TCP、HTTP 等）数据流量的通过。

接入层交换机一般只在第二层执行安全策略，即使某些接入层交换机支持第三层功

能。第三层的安全策略通常由汇聚层交换机来执行，因为汇聚层交换机处理的效率要比接入层交换机高得多。而在核心层不必定义任何的安全策略。

4. 易于管理和维护

由于局域网分层网络设计的每一层都执行特定的功能，并且整层执行的功能都相同，因此分层网络更容易管理。如果需要更改接入层交换机的功能，则可在该网络中的所有接入层交换机上重复此更改。由于几乎无须修改即可在同层不同交换机之间复制配置，因此还可简化新交换机的部署。利用同一层各交换机之间的一致性，可以实现快速恢复并简化故障排除。当然也可能因为网络的特殊需求造成两台同层交换机之间配置的不一致，此时一定要妥善记录这些配置，以免出现管理上的混乱。

另外，在局域网分层网络设计中，每层交换机的功能并不相同。因此，可以在接入层上使用较便宜的交换机，而在汇聚层和核心层上使用较昂贵的交换机来实现高性能的网络，从而实现成本上的控制。

2.2　广域网连接设计

在模拟公司网络环境中，除对总公司、分公司和各分支机构的局域网进行设计之外，还需要通过广域网进行连接，以实现整个公司网络的通信。在广域网连接的设计中，一般同样采用分层网络设计模型，将网络分为接入层、汇聚层和核心层，每层的功能与局域网分层网络模型中各层的功能类似。不同的是，在广域网连接设计中使用的网络设备为路由器。通过路由器将各个局域网络使用广域网链路连接起来，形成一个整体的网络。而广域网链路通常是根据用户的具体需要向服务提供商如联通、电信等租用线路，在此不再进行介绍。

2.3　通信链路带宽设计

在网络设计中，各个部分之间的通信链路有着不同的需求，在通信链路设计中需要设计各条通信链路的带宽。在分层网络的核心层、汇聚层一般要求带宽较高的通信链路，而接入层一般需要带宽较低的通信链路。一般情况下，局域网连接可以设计较高的链路带宽，例如几百兆 bps、千兆 bps，但是在广域网线路中，链路带宽设计需要兼顾通信线路费用。无论如何，在通信链路设计中，必须满足用户的链路带宽需求。

在有些情况下，网络中的某一部分通信链路可能会对带宽有比较高的要求。例如在图 2-3 中，公司的市场部门和研发部门之间由于经常有较大的通信量，所以可能要求汇聚层链路的带宽要高于 100Mbps；核心层通信链路的带宽也要高于 100Mbps。

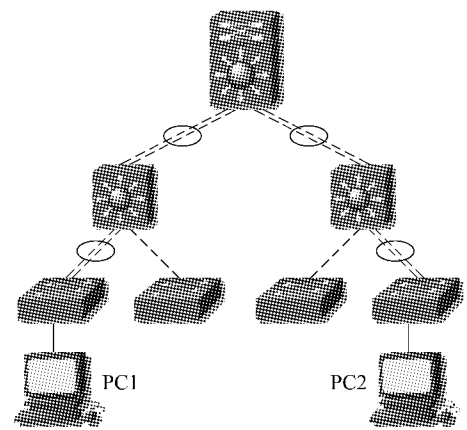

图 2-3　链路聚合

当通信链路需要的带宽大于网络设备接口提供的最高带宽时，可以使用链路聚合技术来解决问题。链路聚合技术是将多个网络设备端口链路组合在一起，在逻辑上形成单个高带宽链路，从而在低带宽通信接口之间实现高速数据传输的技术。

例如在图 2-3 中，PC1 和 PC2 之间需要较高的带宽，而网络中使用的交换机端口速率只有 100Mbps。因此将它们进行通信经过的接入交换机—汇聚交换机、汇聚交换机—核心交换机之间的链路使用链路聚合技术，通过使用两条通信链路来达到链路带宽要求。

在链路聚合中，同一逻辑链路中的物理链路成员彼此互为冗余，共同完成数据通信并相互备份。只要还存在能够正常工作的物理链路成员，整个逻辑链路就不会失效。因此链路聚合技术在增加链路带宽的同时也提高了链路的可靠性。

目前链路聚合技术的国际标准为 IEEE802.3ad，Cisco 公司有专有的 EtherChannel 技术，链路聚合的具体配置实现详见 5.2 节的链路带宽聚合。

2.4 网络性能设计

在网络系统设计中，另一种通常用来提高网络可用性的方法是冗余机制。冗余机制通过在网络中提供冗余设备和冗余链路来保障网络的可靠运行。在实际网络设计中，网络中的某一部分可能会要求比较高的可用性，例如某一部分网络不允许出现通信中断故障，为了保证部分网络的安全畅通，可以使用冗余机制来设计。

冗余机制包括增加冗余设备和增加冗余通信链路两部分。增加冗余设备是为了保障网络中某些设备出现故障时网络的可用性；增加冗余链路是为了保障网络中某些链路出现故障时网络的可用性。实际上冗余设备和冗余链路往往是同时存在的，使用了冗余设备就需要使用冗余链路连接。冗余机制不仅能够在网络出现故障时确保网络的可用性，而且在网络正常运行时，冗余链路和冗余设备还可以实现网络通信流量的负载均衡功能。

冗余机制设计如图 2-4 所示。在 PC1 的上行链路上采用了冗余机制设计。某个汇聚层或核心层的某台交换机，或者某一条链路出现故障，都不会影响 PC1 的网络通信。

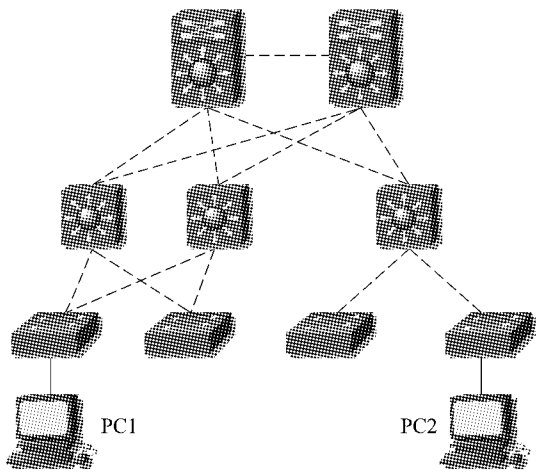

图 2-4 冗余机制设计

考虑到成本和接入层流量较少、终端设备功能有限等问题，一般不会在接入层采用冗余机制。在汇聚层和核心层也不会去做整个网络的完全冗余，而是根据需要做可用性要求较高的那一部分。在较大型的网络中，对于可用性要求比较高的部分会增加汇聚层设备，并在接入层和汇聚层之间增加冗余链路；而在核心层往往会采用“双核心”，即使用两台核心层设备，两台核心层设备和汇聚层设备之间均有链路连接，两台核心层设备互为备份并进行负载的分担。

冗余机制在提高网络可用性的同时也造成了网络中数据链路层环路的存在，从而可能引起广播风暴等一系列问题。具体的解决方法详见 5.1 节的生成树协议。

2.5　网络设备选型

如何为网络中的每一层选择合适的网络设备是一个非常复杂的问题，在给出的模拟网络工程环境中，实际上包含了两部分网络：一部分是总公司、分公司和各分支机构之间的广域网连接，使用的网络设备为路由器，对于不同的应用需求需要向网络服务提供商(Internet Server Provider，ISP)租用不同的广域网链路，并添加相应的路由器模块；另一部分是总公司、分公司和各分支机构内部的局域网连接，使用的设备为交换机，在这里只讨论局域网设备即交换机的选型。

在进行局域网设备选型时，不但要了解交换机的各种技术参数和特性以及分层网络中每一层对交换机功能的要求，还需要考虑网络中的某些部分对于网络的特定要求。下面就分别对以上几点进行介绍。

2.5.1　交换机的技术参数和特性

1. 交换机的物理特性

在选择交换机时，首先需要考虑的就是交换机的物理特性，包括交换机的物理尺寸、是否可以进行模块的扩展等。

在实际网络中，路由器、交换机等网络设备往往会被集中放置在配线间和设备间的机柜中，因此在选择交换机时，物理尺寸成为一个需要考虑的因素。一般交换机的设计宽度为 48.26cm(19in)或 58.42cm(23in)，而高度则是使用“机架单元”即“U”来进行衡量，1U 的高度大约等于 4.445cm。交换机的高度均为 U 的整数倍，大部分低端的接入层、汇聚层交换机高度为 1U，而高端核心层交换机会达到 18U 甚至更高。

从是否可以进行物理扩展上可以将交换机分为固定配置交换机和模块化交换机。固定配置交换机即在出厂时物理配置已经固定，不能够再为交换机增加出厂配置以外的功能或配件，如 Catalyst 2960、Catalyst 3560 系列和 H3C 3100、H3C 3600 系列等交换机。不过一般同一型号的交换机会有不同的配置可供选择，如 Catalyst 3560 系列就有 24 口和 48 口两种不同端口数量的交换机。固定配置交换机外形如图 2-5 所示。

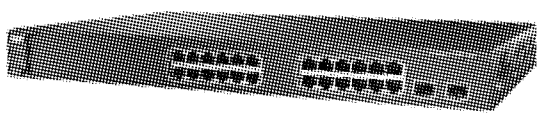

图 2-5　固定配置交换机外形

模块化交换机则拥有开放性的插槽，在网络规模增大时可以通过向空闲插槽添加相应的网络模块来提高网络的接入容量。例如，可以向原本拥有 24 口的模块化交换机上再添加一个 24 口的网络模块，使交换机的端口数量增加到 48 个。另外，还可以根据具体的网络需求选择不同的模块，如光纤模块等。典型的模块化交换机有 Catalyst 4500、Catalyst 6500 系列和 H3C 9500 系列等，如 Catalyst 4510 交换机拥有 10 个模块化插槽，即最多可以支持 10 个网络模块。模块化交换机外形如图 2-6 所示。

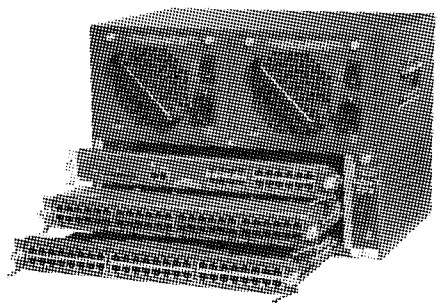

图 2-6 模块化交换机外形

相比较而言，固定配置交换机的成本较低，而模块化交换机的可扩展性更好。对于一个企业或单位而言，网络会随着业务的发展而不断地增大，因此在网络建设的初期就需要考虑到网络的日后扩展。如果网络前期建设采用了固定配置交换机，则当网络需要扩展时就需要新增交换机，这样不但会造成连接线路的复杂度增高，还会因为每台交换机都需要独立管理而造成管理成本的增加。而如果采用模块化交换机就可以很好地解决网络扩展的问题。但是另外一个问题是模块化交换机往往价格比较高，所以早期解决网络可扩展性的成本较低的方法是采用可堆叠交换机。

可堆叠交换机是使用专用的背板电缆将多个交换机连接起来当做一台交换机使用，当网络需要扩展时增加堆叠交换机的个数即可，而在管理上仍然作为一台交换机，如 Cisco 公司的 StackWise 技术允许最多将 9 台交换机进行堆叠。堆叠需要交换机的支持，并不是所有的交换机都支持堆叠。随着模块化交换机成本的降低以及固定配置交换机端口的增加，交换机的堆叠技术越来越少使用。

2. 交换机的端口密度

端口密度是指一台交换机上可用的端口数。通常一台固定配置交换机最多支持 48 个端口，部分机型还提供 2 个或 4 个附加端口用于连接小型可插拔(SFP)设备。在空间和电源接口有限的情况下，较高的端口密度可以更有效地利用这些资源。比如两台 24 口交换机最多可以支持 46 台设备，因为每台交换机都至少要有一个端口用于将交换机本身连接到网络的其他部分，而且还需要两个电源插座。但是，一台 48 口交换机则可支持 47 台设备，它只需要使用一个端口将交换机本身连接到网络的其他部分即可，并且只需要一个电源插座来为交换机供电。

对于大型企业的网络而言，在某一物理点如配线间、设备间，可能有数量庞大的网络接入需求。如果使用端口密度较低的交换机，一方面需要配置大量的交换机，占用许多电源插座和大量的空间；另一方面为了解决交换机间链路的带宽问题，还需要额外占用大量的端口来提供交换机之间的链路聚合。而使用端口密度较高的交换机则不存在上述问题。一般模块化交换机都可以通过增加网络模块来提高交换机的端口密度，如一台 Catalyst 6500 交换机最多可以支持 1000 多个端口。

3. 交换机的转发速率

转发速率是指交换机每秒能够处理的数据量，它用来定义交换机的数据处理能力。

转发速率越高则交换机的数据处理能力越好，最佳情况是交换机的转发速率可以支持其所有端口之间实现全线速的通信。线速是指交换机上每个端口能够达到的数据传输速率，如 100Mbps、1000Mbps 等。所谓全线速通信是指所有端口之间都可以进行完全无阻塞的数据交换。例如，一台 48 口的千兆交换机全线速运行时能够产生 48Gbps 的流量，如果要实现全线速的通信，则该交换机的转发速率至少需要达到 48Gbps。但是考虑到成本的原因，实际上很多的低端交换机并不支持全线速通信。

在分层网络中，一方面部分终端用户流量较少；另一方面受到通往汇聚层的上行链路的限制，接入层交换机通常不需要全线速运行。因此在进行设备选择时，在接入层就可以选择转发速率较低，同时成本也较低的交换机。而在汇聚层和核心层由于数据流量大，则需要选择成本较高但支持全线速运行的交换机。

4. 交换机的三层功能

一般人们提到交换机就会想到其工作层次为数据链路层，即二层交换机。但是，在实际应用中为实现不同广播域之间的路由，往往需要交换机具有第三层的功能。典型的三层设备为路由器，但是由于路由器通过软件来实现数据报文的路由，延时时间长，常常成为网络通信中的“瓶颈”。而交换机通过增加路由模块可以实现第三层路由，并且突破了路由器的速率限制。另外，由于三层交换机可以提供更多的端口并且成本比路由器要低，因此在局域网中通常使用三层交换机来实现路由功能。

当然，三层交换机并不能完全取代路由器，因为路由器对于一些高级路由协议有着更好的支持，并且路由器在支持广域网接入方面也更加灵活。因此，路由器依然是广域网连接的首选设备，在某些情况下甚至是唯一的可选设备。

2.5.2　分层网络对交换机功能的要求

在了解了交换机的部分技术参数和特性后，还需要了解分层网络中每一层对于交换机功能的要求，从而可以依据具体要求来为每一层选择适合的交换机。

1. 接入层交换机的功能

接入层交换机负责将终端节点设备连接到网络，它们需要支持端口安全功能、VLAN 和链路聚合等功能，还要根据终端用户的具体需求支持相应的端口速度和转发速率。

端口安全功能允许交换机决定允许多少设备或哪些设备连接到交换机。它通过在交换机的端口下绑定接入设备的 MAC 地址来实现。如果为某一个交换机端口分配了安全 MAC 地址，那么当数据包的源地址不是已定义地址组中的地址时，端口不会转发这些数据包。端口安全功能应用于接入层，是保护网络的第一道重要防线。端口安全的具体配置见《计算机网络安全与管理》一书。

支持 VLAN 也是对接入层交换机的一个基本要求。在实际的网络中，通常存在不同部门的终端设备连接到同一台接入层交换机上或者同一部门的终端设备连接到不同接入层交换机上的情况，而同一部门的终端设备一般划分到一个子网中。因此要求接入层交换机必须能够进行广播域即 VLAN 的划分。

在选择接入层交换机时还需考虑交换机的端口速度。端口速度必须能够满足网络的性能需求。在网络中，不同的终端设备可能对于带宽有着不同的需求。对于大多数终端

设备的数据流量来说，快速以太网端口(100Mbps)已经足够，但是部分终端设备如应用服务器等可能需要千兆以太网端口(1000Mbps)。与仅支持快速以太网端口的交换机相比较而言，千兆以太网端口交换机可以大大加快数据传输的速度，提高用户的工作效率，但是千兆以太网端口交换机的成本也比仅支持快速以太网端口的交换机高出很多。

链路聚合是大多数接入层交换机所共有的一项功能，接入层交换机通过链路聚合可以增加接入层交换机到汇聚层交换机上行链路的带宽。

由于通信的“瓶颈”通常在接入层交换机和汇聚层交换机之间的上行链路连接，因此接入层交换机对转发速率的要求并不太高，一般的接入层交换机都不能达到而且也不需要达到所有端口全线速的通信，它们仅处理来自终端设备的流量并将其转发到汇聚层交换机。

2. 汇聚层交换机的功能

汇聚层交换机负责收集所有接入层交换机发来的数据并将其转发到核心层交换机。它们需要具有第三层的功能，支持安全策略、链路聚合，并且具有一定的冗余和较高的转发速率。

在接入层交换机上实施了 VLAN 的划分，而在汇聚层交换机上需要实现其下连接的接入层交换机上的 VLAN 之间的路由，以实现同一汇聚层交换机下不同 VLAN 之间的通信。因此要求汇聚层交换机具有第三层的功能。不同汇聚层交换机下的 VLAN 之间的通信由核心层交换机来实现，但核心层交换机需要学习到各个汇聚层交换机下 VLAN 的路由，这就要求在核心层交换机和汇聚层交换机之间运行路由选择协议。因此要求汇聚层交换机必须支持至少一种动态路由选择协议，如路由选择信息协议(Routing Information Protocol，RIP)等。

汇聚层为网络中的流量应用高级安全策略，以控制流量如何在网络上传输，因此要求汇聚层交换机必须支持安全策略的应用。典型的安全策略为访问控制列表(Access Control Lists，ACL)，使用 ACL 需要占用大量的处理资源，因为交换机需要检查每个数据包并查看该数据包是否与交换机上定义的 ACL 的某个规则相匹配。这也就要求汇聚层交换机具有强大的数据处理能力。ACL 的具体原理和配置见《计算机网络安全与管理》一书。

汇聚层交换机同样需要支持链路聚合功能。通常，接入层交换机使用多条链路连接到汇聚层交换机，来确保为接入层上产生的流量提供足够的带宽。而由于汇聚层交换机要接收多个接入层交换机发送的流量，并且需要尽快将所有流量转发到核心层交换机上，因此汇聚层交换机还需要回连核心层交换机的高带宽聚合链路。

另外一个需要考虑的问题是汇聚层交换机的冗余功能。由于汇聚层交换机是所有接入层流量的必经之路，因此一旦汇聚层交换机出现故障会严重影响到网络的其他部分。为确保网络的可用性，汇聚层交换机通常成对使用，互为冗余，并且在每一台汇聚层交换机上都应该有一部分冗余端口。同时汇聚层交换机还应该支持多个可热插拔电源，以确保在其中某个电源出现故障时，交换机仍可继续运行。

与接入层交换机相比，汇聚层交换机要求更高的转发速率和更高的可用性。通常汇聚层交换机的端口速度都要达到 1000Mbps。

3. 核心层交换机的功能

核心层交换机负责汇聚所有下层交换机发送的流量，并实现高速的数据交换。它们需要具有第三层的功能，支持链路聚合，并且需要高度的冗余和极高的转发速率。

核心层交换机用来实现整个网络的数据路由，因此需要具有第三层功能，并且支持动态路由选择协议。

核心层交换机通过链路聚合功能增加汇聚层交换机到核心层交换机上行链路的带宽。

核心层交换机必须具备高度的冗余，因为一旦核心层交换机出现故障，可能导致整个网络瘫痪。一般核心层都会采用比汇聚层更加完善的冗余，甚至是完全冗余，包括设备、线路以及设备组件的冗余。另外，由于核心层交换机的传输负载很高，所以它运行时的温度通常比接入层或汇聚层交换机的温度更高，因此应该配备更完善的冷却方案。

在整个分层网络体系中，核心层交换机应该具有最高的数据转发速率，以实现整个网络的高速运转。通常核心层交换机的端口速度至少要达到 1000Mbps，甚至达到 10000Mbps。

2.5.3　其他因素

实际上，在进行交换机的选型时，还需要考虑到网络的具体情况和要求，并对其进行分析。一般需要进行用户群分析、流量分析、服务器分析等，以选择适合某些特定要求和应用的交换机，保障网络的可扩展性和可用性。

通过用户群分析可以确定各类用户群体对网络性能的影响和需求。通常将一个职能部门划分为一个用户群，因为相同职能的用户所需访问的资源和应用程序大体相同。在进行用户群分析时，要考虑不同用户群的不同需求。对于人员增长比较快的用户群，要选择端口密度较大的交换机，以确保有足够多的闲置交换机端口用来扩展；对于流量较大的用户群，要选择转发速率较高的交换机，以避免产生数据传输的“瓶颈”。

通过流量分析可以了解网络中各部分的流量大小，确定其对带宽的具体需求，以选择合适的交换机。实际上，流量分析更多的用于网络投入运行后，用来测量网络带宽的使用率，以确定是否需要调整和升级网络。

另外需要考虑的是各种应用服务器和数据存储服务器，一般服务器的数据流量总是很大，因此要选择转发速率较高的交换机，并且应该具备高度的冗余，以确保可用性。

在逻辑上，对于经常访问服务器的用户群应该尽量靠近服务器，以减少用户通信的网络直径，提高网络传输效率。

2.6　模拟网络设计方案

在具备了网络设计的基础知识后，就可以对模拟网络工程环境进行网络的整体设计。

2.6.1　公司网络整体设计

总公司、分公司和各分支机构之间通过路由器使用广域网链路连接，路由器同时连接本地的局域网。公司网络整体拓扑结构如图 2-7 所示。

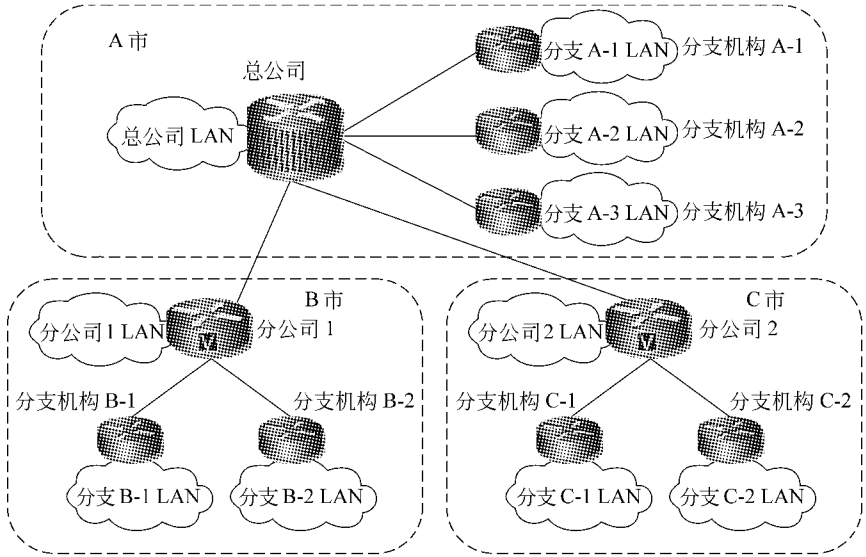

图 2-7 公司网络整体拓扑结构

2.6.2 总公司局域网设计

1. 总公司局域网拓扑结构

总公司的局域网采用了分层网络的设计，由接入层、汇聚层和核心层 3 层构成，其拓扑结构如图 2-8 所示。

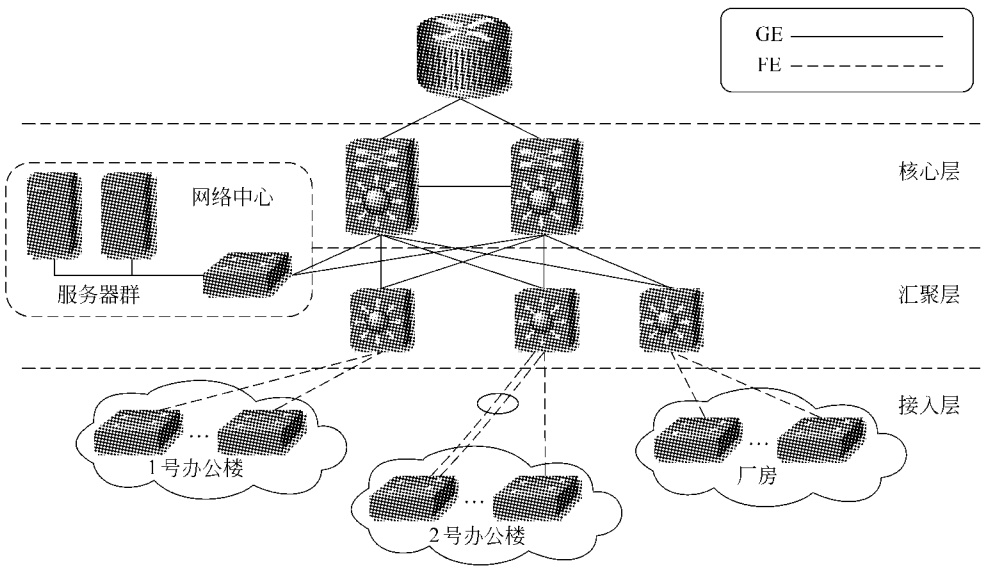

图 2-8 总公司局域网拓扑结构

在汇聚层交换机上进行 VLAN 的创建，并在接入层交换机上通过将接入端口指定到相应的 VLAN 中来按部门划分广播域，由汇聚层交换机实现其下的接入层各 VLAN 之

间的路由。在汇聚层交换机和核心层交换机之间运行动态路由选择协议，由核心层交换机实现整个局域网的路由。

在链路带宽上，接入层交换机和汇聚层交换机之间采用了 100Mbps 的快速以太网连接，介质为超 5 类双绞线；汇聚层交换机和核心层交换机之间采用了 1000Mbps 的千兆以太网连接，介质为多模光纤。

为满足位于 2 号办公楼市场部门的部分主机对带宽的需求，在其接入层交换机与汇聚层交换机之间的链路上进行链路聚合，将两条带宽为 100Mbps 的物理链路聚合成一条带宽为 200Mbps 的逻辑链路。

为保障可用性，网络采用了双核心的设计，并在汇聚层和核心层之间采用线路的完全冗余。使用两台完全相同的核心层交换机互为备份，并进行负载的均衡。

考虑到终端用户对服务器的访问流量较大，为避免产生网络“瓶颈”，将各个服务器通过一台端口带宽为 1000Mbps 的接入层交换机直接连接到两台核心层交换机上。一方面，1000Mbps 的带宽确保流量的高速传输；另一方面，可以减小终端用户访问服务器的网络直径，提高网络传输效率。

2. 总公司局域网设备选型

在确定了网络的拓扑结构以后，就可以开始对网络中的交换机进行选型。在选型时应尽量选择同一个厂家的设备，以保证技术上的兼容性。在这里，以思科公司交换机为例进行选型。

(1) 接入层交换机选型

对于总公司局域网中的 1 号办公楼，每层有信息点 15～20 个，共 25 层。为每层配备一台接入层交换机，共 25 台交换机。选择交换机为 Catalyst WS-C2960-24TT-L，该款交换机的详细参数如表 2-1 所示。

表 2-1　Catalyst WS-C2960-24TT-L 详细参数

产品类型	企业级二层可网管交换机
转发速率	16Gbps
最大 DRAM 内存	64MB
MAC 地址表	8KB
接口类型/数目	10/100Mbps 端口/24 个，10/100/1000Mbps 端口/2 个
支持网络标准	IEEE 802.3、IEEE 802.3u、IEEE 802.1x、IEEE 802.1Q、IEEE 802.1p、IEEE 802.1D、IEEE 802.1s、IEEE 802.1w、IEEE 802.3ad、IEEE 802.3z
VLAN	支持
链路聚合	支持
堆叠	不支持
最大功率	30W
外形尺寸	236mm×445mm×44mm
重量	3.6kg

对于总公司局域网中的2号办公楼，每层有信息点30～35个，共7层。为每层配备一台接入层交换机，共7台交换机。选择交换机为Catalyst WS-C2960-48TT-L，该款交换机的参数与Catalyst WS-C2960-24TT-L的基本相同，只是10/100Mbps端口有48个，以满足每层30～35个信息点接入的需求。

对于总公司局域网中的4个厂房，每个厂房分成了10个生产区，每个生产区有信息点5个。为每3个或4个生产区配备一台接入层交换机，即一台接入层交换机负责15～20个信息点的接入，1个厂房共配备3台接入层交换机，4个厂房共配备12台交换机。选择交换机为Catalyst WS-C2960-24TT-L。

为网络中心的服务器配备一台接入层交换机，选择交换机为Catalyst WS-C2960G-24TC-L。与Catalyst WS-C2960-24TT-L相比，Catalyst WS-C2960G-24TC-L提供了更高的数据转发速率24Gbps，并且所有的端口均为千兆以太网端口(1000Mbps)。

(2) 汇聚层交换机选型

为1号办公楼、2号办公楼和厂房分别配备一台汇聚层交换机，其中2号办公楼和厂房选择交换机为Catalyst WS-C3560-24TS-S，该款交换机的详细参数如表2-2所示。其中，快速以太网端口(100Mbps)用来连接接入层交换机，而千兆以太网光端口(1000Mbps)用来上连核心层交换机。1号办公楼选择交换机为Catalyst WS-C3560-48TS-S，该款交换机的参数与Catalyst WS-C3560-24TS-S的基本相同，只是10/100Mbps端口有48个，10/100/1000Mbps光端口有4个。

表2-2 Catalyst WS-C3560-24TS-S详细参数

产品类型	企业级三层可网管交换机
转发速率	32Gbps
最大DRAM内存	128MB
MAC地址表	12KB
接口类型/数目	10/100Mbps端口/24个，10/100/1000Mbps光端口/2个
支持网络标准	IEEE 802.3、IEEE 802.3u、IEEE 802.1x、IEEE 802.1Q、IEEE 802.1p、IEEE 802.1D、IEEE 802.1s、IEEE 802.1w、IEEE 802.3ad、IEEE 802.3z
VLAN	支持
链路聚合	支持
堆叠	不支持
最大功率	45W
外形尺寸	301mm×445mm×44mm
重量	3.9kg

(3) 核心层交换机选型

核心层使用两台完全相同的交换机来实现整个网络数据的高速传输。选择的交换机为 Catalyst WS-C4506,该款交换机的详细参数如表 2-3 所示。

表 2-3　Catalyst WS-C4506 详细参数

产品类型	企业级四层可网管交换机
转发速率	100Gbps
处理器	400MHz
MAC 地址表	32KB
模块化插槽数	引擎插槽 1 个,线卡插槽 5 个
支持网络标准	IEEE 802.3、IEEE 802.3u、IEEE 802.1x、IEEE 802.1Q、IEEE 802.1p、IEEE 802.1D、IEEE 802.1s、IEEE 802.1w、IEEE 802.3ad、IEEE 802.3z
VLAN	支持
链路聚合	支持
堆叠	不支持
最大功率	2800W
外形尺寸	440mm×317mm×440mm
重量	18.37kg

Catalyst WS-C4506 作为一款模块化交换机,实际上只是一个可以提供 6 个模块化插槽的交换机机箱,还需要另外配置引擎和线卡才能够运行。为交换机配置 WS-X4515 引擎,并配置一块 WS-X4418-GB 线卡,可以提供 18 个千兆以太网光端口,以实现与汇聚层交换机、另一台核心层交换机以及接入路由器之间的连接。

经过选型,最终确定总公司局域网设备需求情况,如表 2-4 所示。

表 2-4　总公司局域网设备需求情况

设 备 名 称	数量/台	设 备 名 称	数量/台
Catalyst WS-C2960-24TT-L	37	Catalyst WS-C3560-48TS-S	1
Catalyst WS-C2960-48TT-L	7	Catalyst WS-C4506	2
Catalyst WS-C2960G-24TC-L	1	WS-X4515 引擎	2
Catalyst WS-C3560-24TS-S	2	WS-X4418-GB 线卡	2

两个分公司的局域网与总公司的类似,在此不再赘述。

2.6.3　分支机构 A-1 局域网设计

1. 分支机构 A-1 局域网拓扑结构

由于分支机构 A-1 的网络规模较小,因此采用了紧缩核心型的网络设计,即将核心

层和汇聚层合二为一，其拓扑结构如图 2-9 所示。

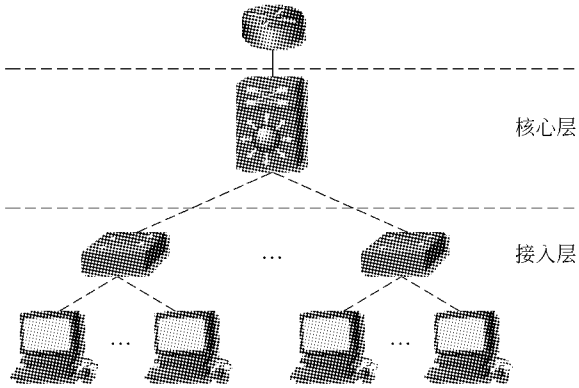

图 2-9 分支机构 A-1 局域网拓扑结构

在核心层交换机上进行 VLAN 的创建，并在接入层交换机上通过将接入端口指定到相应的 VLAN 中来按部门划分广播域，由核心层交换机实现其下的接入层各 VLAN 之间的路由。在链路带宽上，所有链路均采用 100Mbps 的快速以太网连接，介质为超 5 类双绞线。

2. 分支机构 A-1 局域网设备选型

分支机构 A-1 的办公楼每层有信息点 10～20 个，共 7 层。为每层配备一台接入层交换机，共 7 台交换机，选择交换机为 Catalyst WS-C2960-24TT-L。整个网络配备一台核心层交换机，选择交换机为 Catalyst WS-C3560-24TS-S。

2.6.4 分支机构 A-2 局域网设计

由于分支机构 A-2 的网络规模非常小，仅有 30 多个信息点，并且处在同一楼层内，因此在网络设计上不再分层，其拓扑结构如图 2-10 所示。

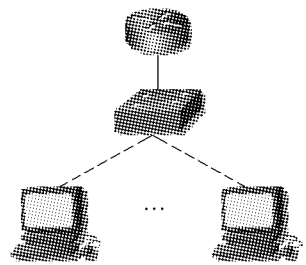

图 2-10 分支机构 A-2 局域网拓扑结构

使用一台二层交换机将终端用户接入网络，在交换机上创建 VLAN，并通过将接入端口指定到相应的 VLAN 中来按部门划分广播域，通过在接入路由器上划分子接口来实现路由。在链路带宽上，所有链路均采用 100Mbps 的快速以太网连接，介质为超 5 类双绞线。

选择的交换机型号为 Catalyst WS-C2960-48TT-L。

其他各个分支机构的局域网情况与分支机构 A-1 或分支机构 A-2 的情况类似，在此不再赘述。

2.7 小结

本章主要介绍了网络设计的基础知识，包括分层网络设计模型及分层网络设计需要遵循的原则、网络设备选型等方面的知识，并针对模拟网络工程环境给出了公司网络整体