第 1 章

企业网络规划

在当今高度信息化的社会中，对于一个企业而言，无论其企业性质及其企业经营方向存在什么区别，信息化都是其战略投资中必不可少的一部分，而信息化的核心则是起到支撑作用的企业网络。一个企业从创建伊始就需要构建自己的网络，而随着企业规模的扩大，企业网络的规模也会随之变大，以支撑整个企业的信息化。对于一个具备相当规模的企业而言，其网络也会具备一定的复杂度，需要各个层次上的多种不同协议协同工作才能保障网络通信的正常进行。为使读者能够了解网络中各种常用协议的配置以及各个协议之间的关系，进而掌握企业网络规划和设计的知识，本书将首先给出一个完整的企业网络规划，并通过网络功能分析将其拆解为多个项目，然后依次完成各个项目并最终完成整个网络的构建。

在企业网络的选择上，本书将选择一个高职学院的网络作为例子。选择依据主要为以下两点：首先，在高职学院中一般会有各个职能处室、教学系部等数十个部门，这些部门存在于办公楼、教学楼、图书馆等多栋不同的建筑中，而且很多高职学院还会有多个处于不同地域的校区，因此网络具有足够的复杂度，是中型企业网络中的典型代表；其次，以高职学院的网络为例能够使学生与自己学院实际的网络联系起来，更好地理解网络中的相关知识。

1.1 用户需求分析

在进行网络规划之前，首先需要与用户进行沟通，了解用户单位的具体情况以及用户的需求，包括该高职学院有几个校区、每个校区内的建筑情况以及具体的部门分布等信息，以作为网络规划的依据。

1.1.1 用户单位基本信息

经过与用户沟通，了解到用户所在的高职学院基本信息如下。

该高职学院由 3 个处于不同地域的校区组成，包括一个主校区和两个分校区。

学院由 30 余个部门组成，包括教务处、学生处、人事处等职能处室，计算机系、电信系、邮政通信管理系等教学系部以及中驿软件技术有限公司和惠远邮电设计公司两个院属公司。每个部门工作人员数量 10～50 人不等。

学院主校区有教学楼、图科楼、绿苑大厦、鸿雁宾馆以及体育馆等数栋建筑。其中，教学楼和图科楼均为 6 层，每层有信息点 15～20 个，共有信息点 250 个左右；绿苑大厦共有 18 层，每层有信息点 30～35 个，共有信息点 630 个左右；鸿雁宾馆共有 6 层，每层有信息点 30～35 个，共有信息点 210 个左右；体育馆共有信息点 10～15 个。

以上给出的只是与本书内容相关的部分信息，在实际与用户沟通的过程中，还需要详细了解并描述用户单位的组织机构、业务情况、各个组织机构的员工情况，以及用户单位的地理位置分布等信息。

1.1.2 用户总体需求

对于学院而言，其希望通过一次投入，建设起完善的校园内部网络，并且要求网络能够满足学校的不断发展和员工不断增多的需要，具体的需求如下。

学院的各个部门分散在多栋建筑中，一个部门可能有多个处于不同楼层的办公地点，而同一楼层可能有多个部门的办公室。要求按照部门进行网段的划分和路由，为学院的每一个员工分配一个静态 IP 地址，使所有员工均能连接网络，同时还需保证部门间的广播隔离。

要求所有的教室均可以连接网络，以保证教师上课时可以通过互联网进行资料查询或远程到办公室的计算机上进行操作。

在网络带宽需求方面，要求信息点的接入带宽达到主流的 100Mbps，上游主干链路带宽达到 1000Mbps。对于个别对带宽需求较高的部门要求能够提供高于 100Mbps 的带宽，以避免出现网络通信的瓶颈。

在学院的局域网内部，对于网络可靠性要求比较高的部门其网络必须要有冗余机制，以避免因为单点故障而导致断网事件的发生。而这种冗余机制对用户要求透明，即不能为了提高网络可用性而增加终端用户的使用难度。

为方便教师和学生的网络接入，在为教师办公室提供固定接入的同时，要求对校园内的热点区域（例如教学楼内的大厅等位置）进行无线网络的覆盖，使教师和学生使用笔记本电脑、智能手机等能够方便地接入网络。出于安全的考虑，必须要对无线网络的接入进行认证和加密，以避免诸如驾驶攻击等非法侵入攻击。

要求学院的网络在出现网络震荡或故障时能够及时被发现并能够快速修复故障，恢复网络服务。

对于网络规划和设计人员，与之进行沟通的企业代表往往是非网络专业人员，甚至是非计算机专业人员，因此用户基本上都是从实际的应用效果和实现效果角度提出需求。而网络规划和设计人员需要将这些需求进行专业的分析和归类，以确定网络中涉及的技术协议，从而给出网络的设计方案。

1.2 网络功能分析

结合用户单位的信息以及用户的需求信息进行分析，即可确定网络应具备的功能以及涉及的协议，具体如下。

1. 网络拓扑设计和设备选择

由于学院有多个校区，因此在各个校区之间必然会存在广域网的连接。

在每个校区内部的局域网中，由于要将处于不同楼层的同一个部门办公室划分到一个网段中，还需要实现多个建筑之间的连接，因此必然会涉及接入、汇聚和核心的三层网络拓扑结构设计，并且在接入交换机上进行 VLAN 的划分、汇聚交换机上进行 VLAN 间的路由以实现按部门进行的逻辑划分和路由。

为满足网络带宽的需求，接入交换机必须要具备 1000Mbps 的上连端口，而汇聚和核心交换机则应该是全千兆的端口。

2. IP 地址规划

由于要按照部门进行逻辑网段的划分，而每个部门中的员工数量并不相同，因此要求必须使用可变长子网掩码(Variable Length Subnet Mask，VLSM)技术进行子网的划分。一方面确保了子网的大小能够符合相应部门或连接对 IP 地址的数量要求；另一方面又能尽量避免 IP 地址的浪费。

而为了减少路由表中的路由条目，同一栋建筑中的多个部门使用的子网 IP 地址应尽量连续，以确保其可以在汇聚交换机上使用无类别域间路由(Classless Inter-Domain Routing，CIDR)技术进行路由的聚合。

对于教室，考虑到一般不会出现所有的教室同时使用的情况，而且教室也没有对 IP 地址长期持有的需求，因此可以使用动态主机配置协议(Dynamic Host Configuration Protocol，DHCP)对其进行 IP 地址的动态分配，在减少了地址分配工作量的同时还可以实现 IP 地址的节约。

3. 交换技术

对于有较高带宽需求的部门，为确保其上行链路的带宽能够满足需求，可以考虑使用链路聚合控制协议(Link Aggregation Control Protocol，LACP)将多条物理链路聚合成一条逻辑链路，以增加上行链路的带宽。

对于网络的可靠性要求比较高的部门，可以在数据链路层引入冗余链路并运行生成树协议(Spanning Tree Protocol，STP)。在主链路正常工作的情况下，逻辑上断开备份链路，而一旦主链路出现故障，备份链路将被启用以保障网络的连通性。

4. 路由技术

由于在 IP 地址规划中采用了 VLSM 技术，因此必须要选择无类别的路由选择协议进行不同网段之间的路由。在各个校区的局域网内部可以运行第二代路由信息协议(Routing Information Protocol version 2，RIPv2)来实现局域网内部各网段之间的路由；而在各个校区之间可以考虑运行开放式最短路径优先(Open Shortest Path First，OSPF)协议，以保证网络的快速收敛。

对于网络的可靠性要求比较高的部门，可以在网络层引入冗余设备和冗余链路并运行虚拟路由器冗余协议(Virtual Router Redundancy Protocol，VRRP)，使多台物理网关设备虚拟成一台逻辑网关设备，即使某一台物理网关设备出现故障，其他的物理网关设备依然可以保障网络的连通性。

5. 广域网技术

由于在多个校区之间需要使用到广域网的连接，因此可以在广域网连接上配置高级数据链路控制（High-level Data Link Control，HDLC）协议或者点到点协议（Point-to-Point Protocol，PPP）以进行数据链路层的封装，而且在采用 PPP 协议时还可以进行认证的配置以确保对端设备的可靠。

6. 无线热点覆盖

对于校园内的热点区域进行无线覆盖时，由于热点区域相对分散且没有太多的覆盖设计需求，可以考虑在接入交换机下连接 Fat AP 进行覆盖，并使用 Wi-Fi 网络安全接入（Wi-Fi Protected Access，WPA）技术对无线网络的接入进行认证和加密。

7. 网络设备管理与维护

为保证网络设备出现故障时能够快速地修复，要求所有的网络设备必须能够远程登录进行配置管理。同时，必须对所有的网络设备上的操作系统以及配置文件进行备份，以备设备上的系统文件出现故障时的恢复。

通过对网络应该具备的功能进行分析，即可依据这些功能进行网络的设计并逐项实现相应的功能。

1.3 网络拓扑设计

对于学院网络而言，其包括广域网和局域网两部分，广域网部分通过租用联通或者电信的线路即可，不会涉及网络拓扑的设计，因此本节的重点是讨论局域网的设计。

1.3.1 局域网分层网络设计

1. 分层网络设计模型

使用自备通信线路时，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时（例如给出的学院网络中的信息点达到了上千个），局域网的设计一般采用分层网络设计方法。同 ISO/OSI 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，且每层提供特定的功能，而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，即接入层、汇聚层和核心层，如图 1-1 所示。

在局域网分层网络设计模型中各层网络设备通常使用包转发速率较高的以太网交换机实现。

（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，其主要目的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，接入层设备一般是较低档次的以太网交换机或无线接入设备，而且所有的最终用户均由接入层连接到网络中。

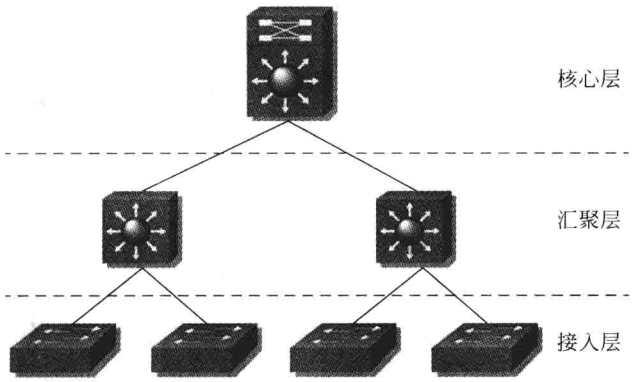

图 1-1　分层网络设计模型

（2）汇聚层

汇聚层位于接入层和核心层之间，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。其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，用以提供边界的定义，通过通信策略控制将核心层和网络的其他部分区分开，以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，它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。其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。在很多规模较小的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，形成一个“接入层＋核心层”的两层结构。

2. 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，并且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

此为试读，需要完整PDF请访问：www.ertongbook.com

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数据传递，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绑定技术来限制只允许特定 IP 地址和 MAC 地址的主机接入网络。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 List，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 2 层执行安全策略，即使某些接入层交换机支持第 3 层功能。第 3 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很多。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，因为所有的接入层交换机在该层上执行的功能都相同。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，即可利用同一层各交换机之间的一致性，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的配置的不一致，此时一定要妥善记录这些配置，以避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。

1.3.2 网络的可用性和高性能保证

1. 网络可用性保证

在网络系统设计中，通常引入冗余机制来提高网络的可用性。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，可以通过冗余机制设计来实现。

冗余机制包括增加冗余设备和增加冗余通信链路。增加冗余设备是为了保障当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。冗余机制能够在网络出现故障时确保网络的可用性，而在网络正常运行时，网络层的冗余链路和冗余设备还可以实现网络通信流量的负载分担功能。

冗余机制设计如图 1-2 所示，在 PC1 的上行链路上采用了冗余机制设计。当汇聚层、核心层的某个交换机出现故障，或者汇聚层、核心层的某一条链路出现故障时，都不会影响 PC1 的网络通信。

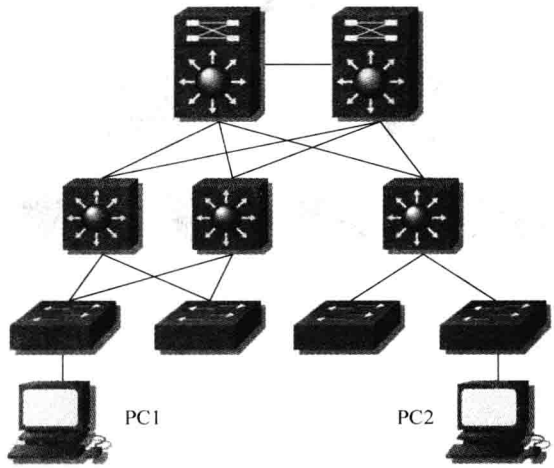

图 1-2　冗余机制设计

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，而是根据需要只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，且汇聚层设备和两个核心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。此类问题解决方法为在交换机上运行生成树协议，使网络的数据链路层在逻辑上形成一个树形结构，具体的解决方法详见 3.3 节的生成树协议。

2. 网络高性能保证

要保证网络的高性能传输，一方面需要尽可能减少信源和信宿之间经过的设备数量，以降低数据的传输延时；另一方面需要在逻辑上增大某些链路的带宽，以避免出现数据传输的瓶颈。

(1) 网络直径

在进行分层网络设计中，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 1-3 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，而网络直径越大，积累的延时就越大。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

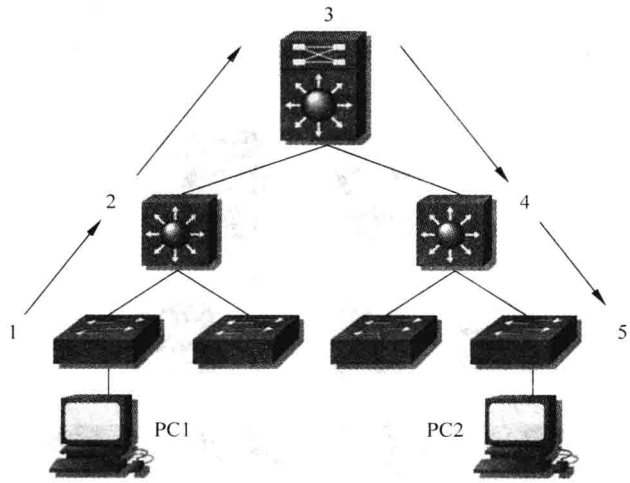

图 1-3 网络直径

许多交换机，则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，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，因此在网络设计中应该尽量降低网络直径。

(2) 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往往有着不同的需求，因此在通信链路设计中需要分别设计各条通信链路带宽。在分层网络的核心层、汇聚层一般要求较高带宽的通信链路，而接入层一般需要的通信链路带宽较低。一般情况下，局域网连接可以设计较高的链路带宽，例如几百兆位每秒、千兆位每秒，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。但无论如何，在通信链路设计中，都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 1-4 中，学院的人事处和教务处之间由于经常有较大的通信量，所以可能要求接入层和汇聚层之间的链路带宽要高于 100Mbps；汇聚层和核心层之间的通信链路也需要高于 100Mbps 的带宽。

在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。

在图 1-4 中，人事处主机和教务处主机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

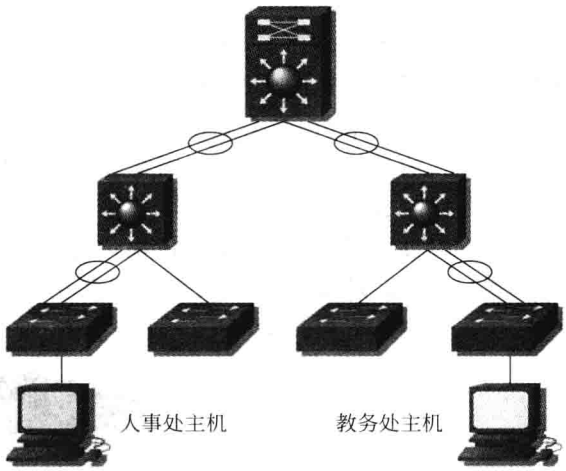

图 1-4　链路聚合

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用性。

1.4　网络设备选择

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，在给出的学院网络环境中，实际上包含了两部分网络。一部分是各校区之间的广域网连接，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。另一部分是各校区内部的局域网连接，使用的设备为交换机，在这里主要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、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网络的特定要求。下面就分别对以上几点进行介绍。

1.4.1　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，网络设备包括路由器、交换机等，它们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划分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就已经固定，不能够再为交换机增加出厂配置以

外的功能或配件，如 H3C S3100、S3600 系列、Catalyst 2960、3560 系列交换机等。不过一般同一型号的交换机会有不同的配置可供选择，如 H3C S3600 系列就有 24 口、48 口两种不同端口数量的交换机。固定配置交换机的外形如图 1-5 所示。

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 端口的模块化交换机上再添加一个 24 端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 H3C S7500、S9500 系列、Catalyst 4500、6500 系列等，如 H3C S7506 交换机拥有 6 个业务插槽，即最多可以支持 6 个网络模块。模块化交换机的外形如图 1-6 所示。

图 1-5 固定配置交换机

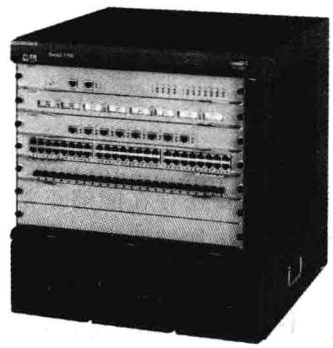

图 1-6 模块化交换机

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。所以在早期解决网络可扩展性的成本较低的方法是采用可堆叠的交换机。

可堆叠交换机可以使用专用的背板电缆将多个交换机连接起来当作一台交换机使用，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。但堆叠需要交换机的支持，并不是所有的交换机都支持堆叠。但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地被使用。

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设备最多支持 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。例如，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，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 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，所谓全线速通信即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 端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需要至少达到 48Gbps。但是考虑到成本的原因，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且支持全线速运行的交换机。

4. 交换机的 3 层功能

提到交换机自然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，往往成为网络通信中的瓶颈。而交换机通过增加路由模块就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设备。

1.4.2　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。

此为试读，需要完整PDF请访问：www.ertongbook.com

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，作为保护网络的第一道重要防线。

对于 VLAN 的支持也是对接入层交换机的基本要求。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提高数据传输的速度，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另一项功能，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出现在接入层交换机和汇聚层交换机之间的链路上，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，它们仅需要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则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需要具有第三层的功能。不同汇聚层交换机下的 VLAN 之间的通信需要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 List，ACL)，但使用 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 的某个规则匹配，这也就要求汇聚层交换机具有强大的数据处理能力。

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将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将可能导致整个网络的瘫痪。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，即包括设备、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。

1.4.3　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也大体相同。在进行用户群分析时，要考虑不同用户群的不同需求，对于人员增长可能比较快的用户群，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，流量分析更多地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的靠近服务器，以减少用户通信的网络直径，提高网络传输效率。

1.5 企业网络设计方案

学院网络中的广域网部分直接租用 ISP 的服务即可，在此不进行讨论。而学院局域网部分以主校区为例进行网络的设计。

1.5.1 局域网络拓扑结构

对于学院主校区的网络，可以采用分层网络的设计，由接入层、汇聚层、核心层 3 层构成。其拓扑结构如图 1-7 所示。

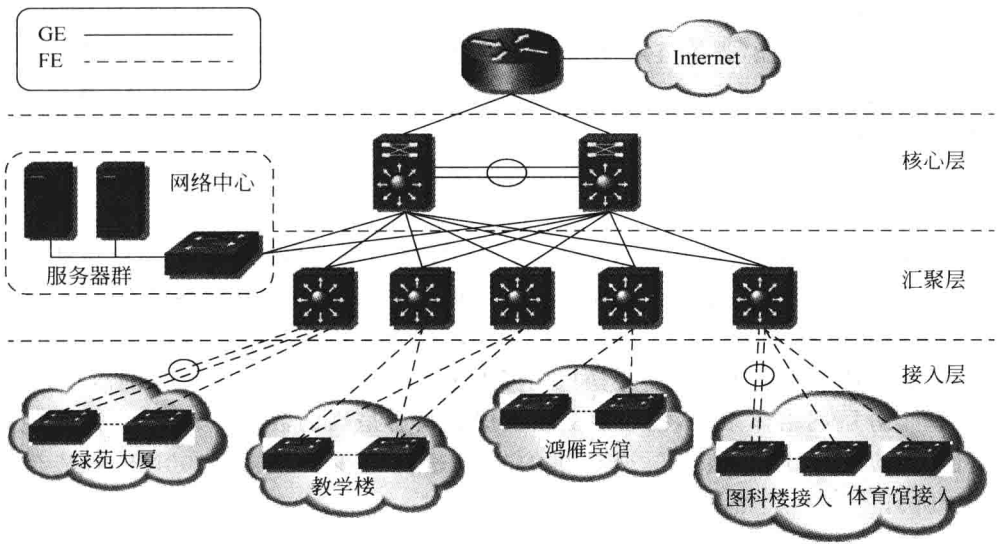

图 1-7 学院主校区网络拓扑结构

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，介质为超五类双绞线；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。

为满足位于绿苑大厦的人事处和位于图科楼的教务处主机对带宽的需求，分别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。

为保障网络的可用性，对教学楼的汇聚层交换机进行了冗余，并使用 VRRP 技术保障教学楼的终端接入不会因为某一台汇聚层交换机出现故障而导致网络中断。在核心层

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。

对于需要进行无线热点覆盖的区域，在相应的接入交换机下连接 Fat AP 进行覆盖，并通过 WPA-PSK 对无线网络进行安全防护。

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核心层交换机上。一方面，1000Mbps 的带宽可以确保流量的高速传输；另一方面，可以减少终端用户访问服务器的网络直径，提高网络传输效率。

1.5.2　局域网络设备选择

在确定了网络的拓扑结构以后，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厂家的设备，以保证技术上的兼容性。在这里，以 H3C 公司交换机为例进行选型。

1. 接入层交换机选型

对于学院的教学楼和图科楼，每层有信息点 15～20 个，需为每一层配备一台接入层交换机；体育馆共有信息点 10～15 个，需配备一台接入层交换机。教学楼和图科楼分别有 6 层，加上体育馆共需要 13 台交换机。选择交换机为 H3C E126A，该款交换机为 H3C 公司推出的一款教育网交换机，详细参数如表 1-1 所示。

表 1-1　H3C E126A 交换机详细参数表

产品类型	企业级二层可网管交换机
交换容量	19.2Gbps，所有端口支持线速转发
交换模式	存储转发模式(Store and Forward)
接口类型/数目	24 个 10/100Base-TX 以太网端口，2 个 10/100/1000Base-T 以太网端口和 2 个复用的 1000Base-X SFP 千兆以太网端口
VLAN	支持基于端口的 VLAN(4k 个) 支持 VLAN VPN(QinQ) 支持 GVRP
链路聚合	支持 LACP 支持手工汇聚 支持最大 13/8 个聚合组，每个聚合组支持 8 个端口汇聚
堆叠	最大支持 16 台设备堆叠
最大功率	17W
外形尺寸	440mm×160mm×43.6mm
重量	≤3kg

对于鸿雁宾馆和绿苑大厦，每层有信息点 30～35 个，分别为 6 层和 18 层，需为每层配备一台接入层交换机，共 24 台交换机，选择交换机为 H3C E152。该款交换机的参数与 H3C E126A 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。

对于网络中心的服务器配备一台接入层交换机，选择交换机为 H3C S5120-28P-SI，该款交换机为全千兆以太网交换机，详细参数如表 1-2 所示。

表 1-2 H3C S5120-28P-SI 交换机详细参数表

产品类型	企业级三层以太网管交换机
交换容量	192Gbps
接口类型/数目	24 个 10/100/1000 Base-T 以太网端口，4 个 1000Base-X SFP 千兆以太网端口
VLAN	支持基于端口的 VLAN(4k 个)
链路聚合	支持 LACP
堆叠	支持通过标准以太网接口进行堆叠、支持本地堆叠和远程堆叠
最大功率	31.5W
外形尺寸	440mm×160mm×43.6mm
重量	<3kg

2. 汇聚层交换机选型

对于绿苑大厦、鸿雁宾馆和图科楼分别配备一台汇聚层交换机，教学楼配备两台汇聚层交换机，体育馆由于只有一台接入层交换机，因此不再配备汇聚层交换机，而是将其接入层交换机连接到邻近的图科楼汇聚层交换机上。选择交换机型号为 H3C S3610-28P，详细参数如表 1-3 所示。其中快速以太网端口(100Mbps)用来连接接入层交换机，而千兆以太网端口(1000Mbps)用来上连核心层交换机。

表 1-3 H3C S3610-28P 交换机详细参数表

产品类型	盒式路由交换机
交换容量	32Gbps
接口类型/数目	24 个 10/100Base-TX 以太网端口，4 个 1000Base-X SFP 千兆以太网端口
VLAN	支持端口 VLAN(4094 个) 支持协议 VLAN 基于 IPv4 子网 VLAN 支持 Voice VLAN 支持 GARP/GVRP 支持 VLAN VPN(QinQ)，灵活 QinQ 支持 VLAN Translation
链路聚合	支持 LACP 支持手工聚合 支持最大聚合组：端口数/2，每个聚合组支持最大 8FE/4GE
堆叠	支持 IRF LITE 堆叠技术 最大支持堆叠 16 台
IP 路由	支持静态路由和默认路由 支持 RIPv1/v2，RIPng 支持 OSPFv1/v2，OSPFv3 支持 IS-IS，IS-ISv6 支持 BGP，BGP4+ for IPv6 支持策略路由，等价路由 支持 VRRP/VRRPv3
最大功率	35W
外形尺寸	440mm×260mm×43.6mm
重量	3.6kg

3. 核心层交换机选型

核心层选择的交换机为 H3C S7503，H3C S7500 系列交换机是 H3C 公司推出的高端多业务路由交换机，H3C S7503 是其中可以提供 3 个业务插槽和 1 个主控插槽的一款，该款交换机的详细参数如表 1-4 所示。

表 1-4　H3C S7503 交换机详细参数表

产品类型	高端多业务路由交换机
交换容量	96Gbps/384Gbps/768Gbps
槽位数量	4
业务槽位	3
冗余设计	电源冗余
VLAN 数量	4k
链路聚合	支持，每组最大支持 8 个 GE 口或 8 个 FE 口捆绑，支持跨板端口聚合
IP 路由	支持 IP、TCP、UDP、ICMP 协议 支持 IPX 协议 支持 OSPF 支持 RIP1/2 支持静态路由 支持 IS-IS 支持 BGP4 支持策略路由 支持等价路由 支持 VRRP
最大功率	350W
外形尺寸	436mm×480mm×352.8mm
重量	≤50kg

H3C S7503 作为一款模块化交换机，实际上只是一个可以提供 4 个模块化插槽的交换机机箱，还需要另外配置主控模块和业务模块才能够运行。为交换机配置主控模块（即交换路由处理板）“S7500-交换路由模块-Salience Ⅲ 384G”，并配置一块“4 端口千兆以太网电口＋12 端口千兆以太网 SFP 光口业务板”的业务接口模块，用来实现其与汇聚层交换机以及接入路由器之间的连接。

经过选型，最终确定学院主校区网络设备需求情况如表 1-5 所示。

表 1-5　学院主校区网络设备需求情况表

设 备 名 称	数量（台）
H3C E126A	13
H3C E152	24
H3C S5120-28P-SI	1
H3C S3610-28P	5
H3C S7503	2
S7500-交换路由模块-Salience Ⅲ 384G	2
4 端口千兆以太网电口＋12 端口千兆以太网 SFP 光口业务板	2

此为试读，需要完整PDF请访问：www.ertongbook.com