

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扩大,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以最终实现整个网络构建。

在企业网络的结构上,为了使教学内容更贴近企业的实际网络,本书将模拟一个学院网络。该模拟学院网络在机构设置上包括各个职能处室、教学系部等数十个部门,这些部门分别位于办公楼、教学楼、图书馆等多栋不同的建筑中,而且学院还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。同时,以模拟学院网络为例能够让学生将其与实际网络联系起来,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,包括学院有几个校区、每个校区内的建筑情况,以及部门的具体分布等信息,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,假定了解到该模拟学院的基本信息如下。

学院共有三个处于不同地域的校区,包括一个主校区和两个分校区。

学院由三十余个部门组成,包括教务处、学生处、人事处等职能处室,计算机系、通信系、金融系等教学系部,以及慧创软件技术有限公司和惠远咨询服务公司两个院属公司。每个部门的工作人员数量 10~50 人不等。

学院主校区有教学楼、图科楼、清苑大厦、校园宾馆及体育馆等数栋建筑。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;清苑大厦共有 18 层,每层有信息点 30~35 个,共有信息点 630 个左右;校园宾馆共有 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。

以上只给出了与本教材内容相关的部分信息,在实际与用户沟通的过程中,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,希望通过一次投入,建设起完善的学院网络,并且要求网络能够满足学校不断发展和员工不断增多的需求。具体的需求如下。

学院的各个部门分散在多栋楼宇中,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,为学院的每一位员工分配一个静态 IP 地址,使所有员工均能连接网络的同时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网络进行资料查询或远程登录到办公室的计算机上进行操作。

在网络带宽方面,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 1 000Mbps。对于个别对带宽需求较高的部门能够提供高于 100Mbps 的带宽,以免出现网络通信的瓶颈。

在学院的局域网(LAN)内部,对网络可靠性要求比较高的部门其网络必须有冗余机制,避免因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透明,即不能为了提高网络的可用性而增加终端用户的使用难度。

为方便教师和学生接入网络,在为教师办公室提供固定接入的同时,还要对学院内的热点区域(如教学楼的教室内、大厅等位置)进行无线网络的覆盖,使教师和学生能够使用笔记本电脑、智能手机等方便地接入网络。出于安全考虑,必须对无线网络的接入进行认证和加密,以免网络被非法侵入。

要求学院的网络在出现网络震荡或故障时能够及时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,与之进行沟通的用户代表往往是非网络专业的人员,甚至是非计算机专业的人员,用户代表基本上都是从实际的应用效果和实现效果角度提出需求。网络规划和设计人员需要对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。

在完成了用户需求分析之后就要进行网络功能分析、网络拓扑结构设计、网络设备选择,并最终给出企业网络设计方案。在企业网络设计中需要考虑的问题、需要使用的技术只靠网络技术基础课程中的知识是不够的。本教材的设计会使用很多没有遇到过的概念和技术,这些内容可以在后续章节中逐步学习掌握。

1.2 网络功能分析

结合用户单位的信息及用户的需求进行分析,即可以确定网络应该具备的功能,以及涉及的技术协议,具体内容如下。

1. 网络拓扑设计和设备选择

学院有多个校区,在各个校区之间必然存在广域网的连接。

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,还需要实现多个楼宇之间的连接,因此必然会涉及接入、汇聚和核心的 3 层网络拓扑结构设计,还要在接入交换机上进行虚拟局域网(VLAN)的划分,并在汇聚交换机上进行 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,接入交换机必须具备 1 000Mbps 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. 综合布线需求

网络设计应该充分考虑网络综合布线的需求,布线系统一般会在遵循兼容性、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进行设计,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)、管理系统(administration subsystem)和建筑群子系统(campus subsystem)6 个部分分别进行设计和实现。为了确保各子系统之间相对独立,相邻子系统之间通过跳线进行交连和互连。本教材主要介绍实际网络中的高级路由交换技术,综合布线技术请参考相关教材。

3. 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,因此必须使用可变长子网掩码(variable length subnet masks, VLSM)技术进行子网的划分。这样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。

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 地址应该尽量连续,以确保其可以在汇聚交换机上使用无类别域间路由选择(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,这样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。

4. 交换技术

由于网络中存在数十个 VLAN,而这些 VLAN 需要配置在每台交换机上,因此,可以通过 GARP VLAN 注册协议(GARP VLAN registration protocol, GVRP)实现 VLAN 在交换机之间的传播,以方便 VLAN 的配置和管理。

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。

5. 路由技术

由于在 IP 地址规划中采用了 VLSM 技术,因此必须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通过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采用开放最短通路优先协议(open shortest path first, OSPF),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采用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。

6. 广域网技术

多个校区之间的连接需要使用广域网,可以在广域网连接上配置高级数据链路控制(highlevel data link control, HDLC)协议或者点到点协议(point-to-point protocol, PPP)来进行数据链路层的封装。在采用 PPP 时还可以进行认证配置以确保对端设备的可靠。

7. 无线热点覆盖

对于学院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 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。

8. 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,必须对所有网络设备的操作系统及配置文件进行备份,以便设备的系统文件出现故障时可以进行恢复。

通过对网络应该具备的功能进行分析,即可以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

模拟学院网络,包括广域网和局域网两部分。广域网部分租用互联网服务提供商的线路即可,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。当一个局域网内部的信息点较多时(例如,本教材给出的模拟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。同国际标准化组织/开放系统互连(ISO/OSI)模型的理念类似,分层网络设计模型把网络逻辑结构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。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

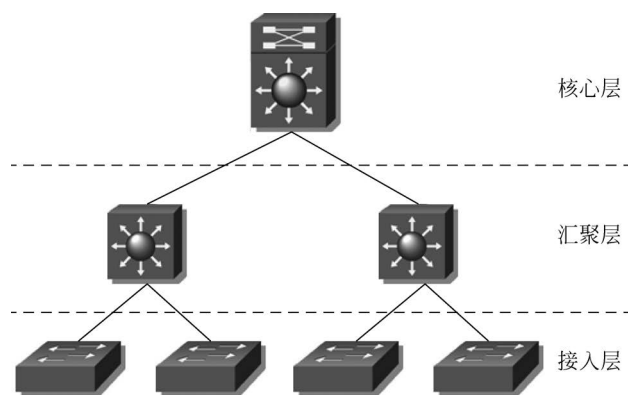


图 1-1 分层网络设计模型

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。接入层的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,所有的用户终端均由接入层连接到网络中。

(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。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,用以提供边界的定义。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,以达到禁止不必要的流量进入核心层的目的。汇聚层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,而不是整个网络系统的核心骨干网络。局域网分层网络设计模型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。核心层的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。这三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,分层网络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,分层网络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,大大提高了网络的通信性能。

(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,分层网络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,分层网络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,分层网络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地址和介质访问控制(MAC)地址的主机接入网络。在汇聚层交换机上它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2层执行安全策略,即使接入层的某些交换机支持第3层功能。第3层的安全策略通常由汇聚层交换机来执行,因为汇聚层交换机的处理效率要比接入层交换机高很多。而核心层不必定义任何安全策略。

(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,则可以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所执行的功能都相同。由于几乎无须修改即可在同层不同交换机之间复制配置,因此还可以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的配置不一致,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,从而实现成本的控制。

1.3.2 网络的可用性和高性能保证

1. 网络的可用性保证

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,可以通过冗余机制来实现。

冗余机制包括增加冗余设备和增加冗余链路。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,网络中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。PC1 的上行链路采用了冗余机制。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,都不会影响 PC1 的网络通信。

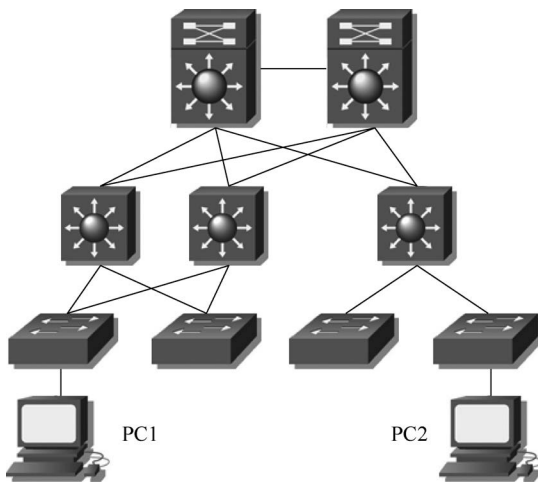


图 1-2 冗余机制设计

考虑到成本和接入层流量较少、终端设备功能有限等问题,一般不会对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,汇聚层设备和两台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。此类问题的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 3.4 节的生成树协议。

2. 网络的高性能保证

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量的最大值,而不是指通信的最大距离。如图 1-3 所示,PC1 和 PC2 之间进行通信最多经过 5 台交换机,即网络直径为 5。

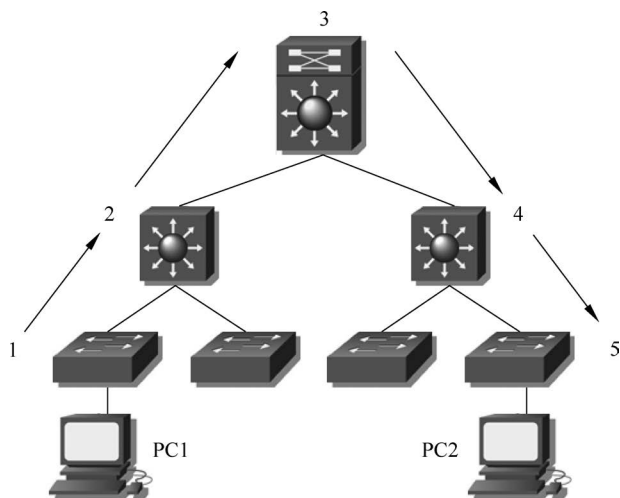


图 1-3 网络直径

在进行分层网络设计时,应该尽可能地降低网络直径,因为数据在经过网络设备时都会产生延时,网络直径越大,积累的延时就越长。例如,数据帧在经过交换机时,交换机需要确定数据帧的目的 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方法。

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,而跳数是可以预测的。在局域网中,即使网络采用了冗余机制,在汇聚层和核心层引入了冗余设备和冗余链路,网络直径也一般会被控制在 6 以内;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,在通信链路的设计中需要分别设计每条通信链路的带宽。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,局域网线路可以设计较高的链路带宽,如百兆级、千兆级;但是在广域网线路中,链路带宽的设计需要兼顾通信线路的费用。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对带宽可能会有比较高的要求。例如图 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通信链路带宽要高于 100Mbps;汇聚层和核心层之间的通信链路带宽也需要高于 100Mbps。

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。

如图 1-4 所示,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,对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

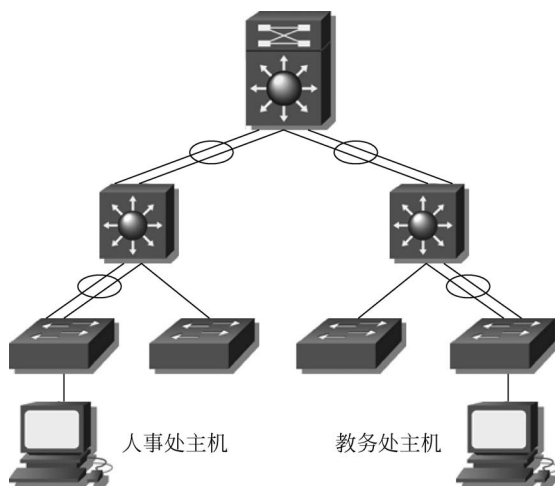


图 1-4 链路聚合

的要求。

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,在给出的模拟学院网络环境中,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互联网服务提供商(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,本节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于交换机功能的要求,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。

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和其是否可以模块的扩展等。

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”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,而高端的核心层交换机会达到 18U 甚至更高。

按照是否可以进行物理扩展来划分,可以将交换机分为固定配置交换机(盒式交换机)和模块化交换机(框式交换机)。固定配置交换机在出厂时物理配置已经固定,不能够再增加出厂配置以外的功能或配件,如华为 S3700、S5720 系列等。不过,一般同一型号的交换机会有不同的配置可供选择,例如,华为 S3700 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。



图 1-5 固定配置交换机

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华为 S7700、S12700 系列等,如华为 S7706 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 1-6 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,网络规模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交换机。