第 7 章　组网方案设计与案例分析

随着网络技术的迅速发展，各种类型的网络产品也在不断出现。因此，在设计局域网组网方案时就有了众多选择，同时也增加了网络系统规划的难度。如何根据自身的需求，规划和设计一个功能完善、设备先进、性能优良、安全可靠的计算机网络系统，使其既能充分发挥计算机网络的作用，满足用户的实际应用，又能最大限度地适应未来网络和应用需求的发展，已成为当前网络建设的主要任务，这也是本章所要讨论的问题。

7.1　局域网组网方案设计

局域网组网方案设计主要分为网络需求分析和网络系统方案设计两个步骤。

7.1.1　网络需求分析

在局域网组建之前要进行需求分析，根据用户提出的要求，如网络的功能、性能、运行环境、可扩充性和可维护性等要求进行网络设计。网络组建的成败很大程度上取决于网络实施前的规划设计工作。

1. 网络的功能要求

任何网络都不可能是一个能满足各项需求的“万能网”。因此，必须针对网络所具备的功能，依据使用需求，完成对运营成本、未来发展、总预算等因素的分析，对网络的组建方案进行规划和设计。局域网一般具备的功能包括子网划分、VLAN 划分、QoS 设定、用户接入多 ISP、NAT、DHCP、AAA 认证、设备和线路备份、组播等。

2. 网络系统性能要求

网络系统性能要求主要包括系统连通性、链路传输速率、吞吐率、传输时延、广播率、错误率、线路利用率、冲突率。根据网络系统性能要求，分析各网络的工作站权限、容错程度、网络安全性等，确定采取何种措施及方案。

3. 网络运行环境的要求

根据整个局域网运行所需的环境，确定使用的网络操作系统和应用软件。

4. 网络的可扩充性和可维护性要求

如何增加工作站，如何与其他网络联网，对软硬件的升级换代有何要求与限制等，这些都要在网络设计时加以考虑，以保证网络的可扩充性和可维护性。通常新建网络时都会针对该网络提出一些有关使用寿命、维护代价等问题的要求。企事业单位的局域网一般不会追赶潮流（除了特殊行业，如 IT 等），系统的更新换代也有一定的时间规律。

7.1.2　网络系统方案设计

在完成了需求分析后，应产生规范的需求分析报告。有了需求分析报告，就可以进入网

络系统方案的设计阶段，这个阶段的工作内容包括确定网络总体目标和设计原则，设计网络通信平台、网络资源平台、网络安全体系结构，配置网络操作系统与服务器等。

1. 网络总体目标和设计原则

1）确定网络总体实现目标

确定网络建设的总体目标，首先应明确采用的网络技术和网络标准，以及网络功能和网络规模。如果网络工程分期实施，还应明确每个分期工程的目标、建设内容、所需工程费用、时间和进度等。网络设计人员不仅要考虑网络实施成本，还要考虑网络运行成本。

2）网络总体设计原则

网络设计应遵循一定的原则，网络总体设计原则包括实用性、开放性、可靠性、安全性、先进性、易用性和可扩展性。针对不同网络应侧重于某一个或几个原则，对这些设计原则进行选择和平衡，并排定其在设计方案中的优先级，这对网络的设计和工程实施将具有指导意义。网络总体设计原则如下：

(1)实用性原则。计算机、外部设备、服务器、网络通信设备等在技术性能逐步提升的同时，价格却在逐年下降，因此，不可能也没必要实现“一步到位”。所以，网络方案设计中应把握“够用”和“实用”原则。网络系统应采用成熟可靠的技术和设备，以达到实用、经济、有效的目的。

(2)开放性原则。网络系统应采用开放的标准和技术，资源系统建设要采用国家标准，有些网络系统(如财务管理系统、电子商务系统)还要遵循国际标准。其目的包括两个方面：一方面，有利于网络工程系统的后期扩充；另一方面，有利于与外部网络互联互通，切不可闭门造车，形成信息化孤岛。

(3)可靠性原则。无论是企业还是事业单位，也无论网络规模大小，网络系统的可靠性都是一个工程的生命线。例如，一个网络系统中的关键设备和应用系统偶尔出现的死锁，对于政府、教育、企业、税务、证券、金融、铁路、民航等行业将造成灾难性的后果。因此，应确保网络系统尽可能长的平均无故障时间和尽可能低的平均无故障率。

(4)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、电子商务网站以及 VPN 等网络中，应重点体现安全性原则，确保网络系统和数据的安全运行。在社区网、城域网和校园网中，安全性的需求相对较弱。

(5)先进性原则。建设一个现代化的网络系统，应尽可能采用先进成熟的技术，保证其在一段时间内的主流地位。网络系统应采用当前较先进的技术和设备，符合网络未来发展的潮流，如目前较主流的千兆以太网和全交换以太网。但是，太新的技术也有不足之处，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够。

(6)易用性原则。网络系统的硬件设备和软件程序应易于安装、管理和维护。各种主要的网络设备，如核心交换机、汇聚交换机、接入交换机、服务器、大功率长延时 UPS 等设备均要支持流行的网管系统，以方便用户管理、配置网络系统。

(7)可扩展性原则。网络总体设计不仅要考虑到近期目标，还要为网络的进一步发展留有扩展的余地，因此，要选用主流产品和技术。如果有可能，最好选用同一品牌的产品或兼容性好的产品。在一个系统中切不可选用技术和性能不兼容的产品。例如，对于多层交换网络，如果选用两种品牌的交换机，一定要注意它们的 VLAN 干道传输、生成树协议等是否兼容，是否可“无缝”连接。这些问题解决了，可扩展性自然会水到渠成。

2.网络通信平台设计

通信平台设计主要包括拓扑结构与网络总体规划，核心层、分布层和接入层的设计，广域网连接与远程访问设计，无线网络设计五个方面。

1)拓扑结构与网络总体规划

确立网络的拓扑结构是整个网络方案规划设计的基础，拓扑结构的选择往往和地理环境、传输介质、介质访问控制方法，甚至网络选型等因素紧密相关。选择拓扑结构时，应该考虑的主要因素有以下几点：

(1)费用。不同的拓扑结构所配置的网络设备不同，设计施工及安装的费用也不同。要关注费用，就需要对拓扑结构、传输介质、传输距离等相关因素进行分析，选择合理的方案。例如，冗余拓扑结构可提高网络可靠性，但费用也高。

(2)灵活性。在设计网络时，考虑到设备和用户需求的变迁，拓扑结构必须具有一定的灵活性，以方便重新配置。此外，还要考虑信息点增加、删除等问题。

(3)可靠性。网络设备损坏、光缆被挖断、连接器松动等故障可能时有发生，网络拓扑结构应避免因个别结点损坏而影响整个网络的正常运行。

在以太网占主导地位的今天，计算机局域网一般采用星型、树型拓扑结构及这两种结构的变形。

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主干网和外围网之分。规模较大的网络采用分层拓扑结构，一般分为核心层、分布层和接入层，如图 7-1 所示。

核心层又称为主干网络，用来将服务器群、建筑群与网络中心连接，或在一个较大型建筑物内连接多个交换机管理间到网络中心设备间。接入层用于连接信息点的“毛细血管”线路及网络设备。根据需要，可以在核心层和接入层中间设置分布层或汇聚层。分布层和接入层又称为外围网络。

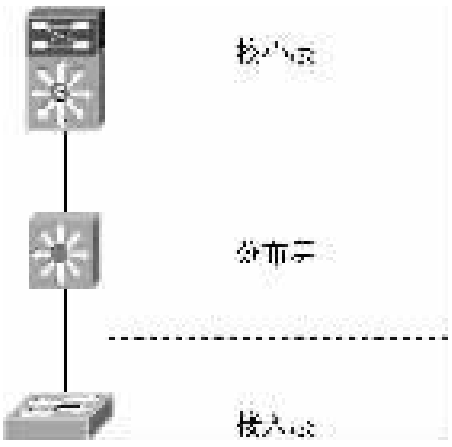

图 7-1　星型(树型)网络分层示意图

分层设计规划的好处是可以有效地将全局通信问题分解考虑，就像软件工程中的结构化程序设计一样。分层还有助于分配和规划带宽的使用。

2)核心层的设计

主干网技术的选择，要根据需求分析中的地理距离、信息流量和数据负载而定。一般而言，主干网一般用来连接建筑群和服务器群，可容纳网络 40%～60%的信息流，是网络的大动脉。连接建筑群的主干网一般以光缆作为传输介质。目前，局域网典型的主干网技术主

要有千兆以太网、10 G 以太网等。

FDDI(Fiber Distributed Data Interface,光纤分布式数据接口)局域网技术基本属于过时的技术,支持该技术的厂商越来越少。ATM(Asynchronous Transfer Mode,异步传输模式)是面向连接的网络技术,能保证一些突发重负载在网络中传输,但由于 ATM 在局域网的所有应用需要 ELAN 仿真来实现,不仅技术难度大,而且带宽效率低,不适宜用作局域网,但如果用户对实时传输要求比较高,也可以使用它。

主干网的焦点是核心交换机或路由器。如果考虑提供较高的可用性,而且经费允许,主干网可采用双星(树)结构,即采用两台同样的交换机,与接入层/分布层交换机分别连接。双星(树)结构解决了单点故障失效问题,不仅抗毁性强,而且通过采用最新的链路聚合技术,如快速以太网的 FEC(Fast Ethernet Channel)、千兆以太网的 GEC(Giga Ethernet Channel)等技术,可以允许每条冗余连接链路实现负载分担。单星(树)结构则采用一台核心交换机与与接入层/分布层交换机分别连接,网络构造简单,但容易造成单点故障失效问题。图 7-2 为主干网双星(树)结构和单星(树)结构示意图。

千兆以太网一般采用光缆作为传输介质。多种波长的单模和多模光纤分别用于不同场合和传输距离。由于建筑群布线路径的复杂性,一般直线距离超过 300 m 的建筑物间的千兆以太网线路就必须要用单模光纤。单模光纤本身并不贵,昂贵的是光端口及组件。骨干网及核心交换机经常会利用下列技术来改善网络设计或对旧网进行升级改造:

(1)FEC/GEC(Fast/Giga Ethernet Channel):即快速以太网/千兆以太网链路聚合技术,该技术来自 Cisco。多个以太网链路组合起来,组成一个逻辑链路,提供多倍 100/1000 Mb/s的全双工连接。FEC/GEC 不仅提高了连接带宽,而且提高了链路可靠性,逻辑链路中任一物理链路失效只会降低链路带宽,不影响正常工作。

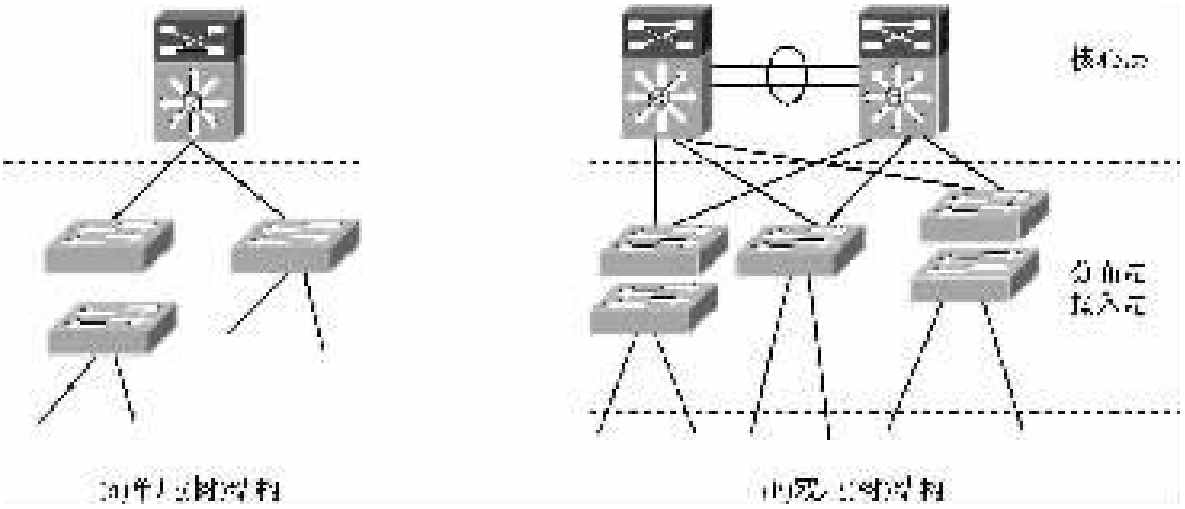

图 7-2　单星(树)结构和双星(树)结构

(2)CGMP(分组管理协议):是一种在 Cisco 交换机上智能发送组播(Multicast)包的技术,它能保证组播包仅送到应该接收的站点,使交换机能够向目标多媒体终端工作站有选择地传送 IP 多播流量,从而降低了网络的总体通信流量。尤其是在多媒体应用中,可避免不必要的数据包在网络上流动,占用其他用户的可用带宽。

(3)GBIC(千兆位集成电路):千兆以太网接口一般有一个 GBIC 卡槽,可插 SX/LX/LH/ZX GBIC 卡。LX/LH GBIC 在单模光纤上的传输距离不小于 10 km,ZX GBIC 的传输距离为 50 km～80 km。

(4)HSRP(热备份路由协议):这是 Cisco 的一种专有技术。HSRP 提供自动路由热备份技术,当局域网有两台以上路由器时,该局域网中的主机只能有一个默认路由器,如果该路由器失效,HSRP 可以使另一个路由器自动承担失效路由器的工作。

3)分布层和接入层的设计

分布层直接连接信息点,使网络资源设备(PC 等)接入网络。分布层的存在与否,取决于外围采用的扩充互联方法。当建筑物内的信息点超出了一台交换机所容纳的端口密度,而不得不增加交换机扩充端口密度时,如果采用级联方式,即将一组固定端口的交换机向上连接到一台背板带宽较大和性能较好的二级交换机上,再由二级交换机向上连接到主干,这种连接方式为三层结构,如图 7-3(a)所示;如果采用多个并行交换机堆叠方式扩充端口密度,其中一台交换机向上连接到主干,则网络中就只有接入层,没有分布层,这种连接方式为二层结构,如图 7-3(b)所示。

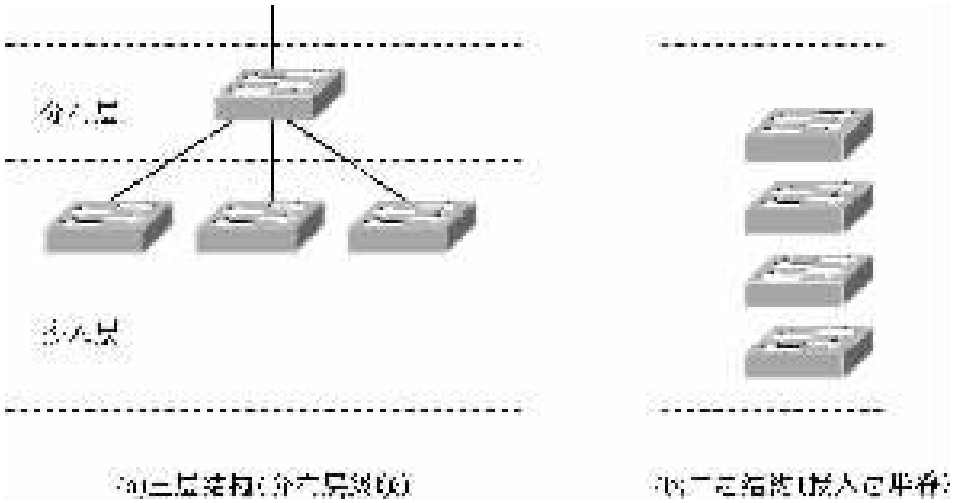

图 7-3 分布层与接入层的两种形式

要不要分布层,采用级联还是堆叠,要视网络信息流的特点而定。堆叠能够保证充足的带宽,适合本地(楼宇内)信息流密集、全局信息负载相对较轻的情况;级联适合全网信息流较平均,且分布层交换机大都具有组播和初级 QoS(Quality of Service,服务质量)管理能力的场合,能更好地处理一些突发的重负载(如 VOD 视频点播),但增加分布层的同时也会使成本提高。

分布层/接入层一般采用 100Base-T(X)快速(交换式)以太网,采用 10/100 Mb/s 自适应传输速率到桌面计算机,传输介质一般采用双绞线。接入层交换机可选择的产品很多,但一定要注意接入层交换机必须支持 1～2 个光端口模块和堆叠方式,如果主干为千兆以太网,接入层交换机还必须支持 GBE 模块。

4)广域网连接与远程访问设计

由于布线系统费用和实现上的限制,对于零散的远程用户接入,利用 PSTN 电话网络进行远程拨号访问几乎是唯一经济、方便的选择。远程拨号访问需要设计远程访问服务器和交换机设备,并申请一组中继线。由于拨号访问是整个网络中唯一的窄带设备,因此这部分在未来的网络中会逐步减少使用。远程访问服务器(RAS)和交换机组的端口数目一一对应,一般按一个端口支持 20 个用户来配置。

广域网连接是指园区网络与外部网络的连接。一般采用路由器连接外部网络,根据网络规模的大小、网络用户的数量来选择对外连接通道的带宽。如果网络用户没有 WWW、

E-mail等具有 Internet 功能的服务器，用户可以采用 ISDN 或 ADSL 等技术连接外网，也可采用 DDN(或 E1)专线连接、ATM 交换及永久虚电路连接外网。其连接带宽可根据内外信息流的大小选择，例如，上网并发用户数在 150～250 之间，可以租用 2 Mb/s 线路，通过同步口连接 Internet。如果用户与网络接入运营商在同一个城市，也可以采用光纤 10 Mb/s 或 100 Mb/s 的速率连接 Internet。外部线路租用费用一般与带宽成正比，速度越快费用越高。网络工程设计方和用户方必须清楚的一点就是，能给用户方提供多大的连接外网的带宽受两个因素的制约，一是用户方租用的外连线路的速率，二是运营商提供给用户方的连接 Internet 的速率。

5)无线网络设计

无线网络的出现就是为了解决有线网络无法克服的困难。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)。校园也是一个很重要的应用场所，使用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。另外，因为无线网络支持十几千米的区域，因此也适用于城市范围的网络接入，可以设想一个采用无线网络的 ISP 可以为一个城市的任何角落提供高达 10 Mb/s 的互联网接入。

6)网络通信设备选型

设备选型是指从多种可以满足相同需要的不同型号、规格的设备中，经过技术、经济的分析评价，选择最佳方案以做出购买决策。合理选择设备，可使有限的资金发挥最大的经济效益。

(1)网络设备选型原则。网络设备选型应遵循以下原则：

厂商的选择：所有网络设备尽可能选取同一厂家的产品，这样在设备可互联性、协议互操作性、技术支持、价格等方面都更有优势。从这个角度来看，产品种类、型号齐全，技术认证队伍力量雄厚，产品市场占有率高的品牌是网络设备品牌的首选。其产品经过更多用户的检验，成熟度高，而且这些品牌出货频繁，生产量大，售后服务体系完备。但作为系统集成商，不应依赖任何一家的产品，应根据需求和费用公正地评价各种产品，选择最优的产品。在制定网络方案之前，还应根据用户的经济能力来确定网络设备的品牌。

扩展性考虑：在网络的层次结构中，主干设备应预留一定的扩展能力，而低端设备则够用即可，因为低端设备更新较快，且易于扩展。

根据方案和实际需要选型：主要是在参照整体网络设计要求的基础上，根据网络实际带宽性能需求、端口类型和端口密度选型。如果是旧网改造项目，应尽可能保留并延长用户对原有网络设备的投资，避免在资金投入方面的浪费。

选择性价比高、质量过硬的产品能使资金的投入产出达到最大值，能以较低的成本、较少的人员投入来维持系统运转，能为用户提供稳定、高品质的服务。

(2)核心交换机的选型策略。核心网络骨干交换机是宽带网的核心，应满足下列要求：

高性能和高速率：第二层交换最好能达到线速交换，即交换机背板带宽不小于所有端口带宽的总和。如果网络规模较大，需要配置 VLAN 时，要求必须有较出色的三层交换能力。

定位准确便于升级和扩展：具体来说，具有 250 个信息点以上的网络，适宜采用模块化(插槽式机箱)交换机；具有 500 个信息点以上的网络，交换机还必须能够支持高密度端口和大吞吐量扩展卡；具有 250 个信息点以下的网络，为降低成本，应选择具有可堆叠能力的固

定配置交换机作为核心交换机。

高可靠性：除考察、调研产品本身的品质外，还应根据经费许可选择冗余设备，如冗余电源、风扇等；设备扩展卡要支持热插拔，以便于更换、维护。

强大的网络控制能力：提供 QoS 和网络安全，支持 RADIUS（Remote Authentication Dial In User Service，远程用户拨号认证系统）、TACACS＋（Terminal Access Controller Access Control System，终端访问控制器访问控制系统）等认证机制。

良好的可管理性：支持通用网管协议，如 SNMP、RMON、RMON2 等。

（3）分布层/接入层交换机的选型策略。分布层/接入层交换机也称为外围交换机或边缘交换机，一般都属于可堆叠、可扩充式固定端口交换机。这种交换机在大中型网络中常用来构成多层次、结构灵活的用户接入网络，在中小型网络中也可用来构成网络骨干交换设备。分布层/接入层的交换机应满足下列要求：

- 灵活性：提供多种固定端口数量搭配供组网选择，可堆叠、易扩展，以便增加信息点。
- 高性能：作为大型网络的二级交换设备，应支持 100/1000 Mb/s 高速上联，以及同级设备堆叠，当然还要注意与核心交换机品牌的一致性。如果是用作小型网络的中央交换机，应具有较高的背板带宽和第三层交换能力等。
- 在满足技术性能要求的基础上，尽可能选用价格便宜，使用方便，即插即用，配置简单的产品。
- 具备较高的网络服务质量和控制能力以及端到端的 QoS。
- 如果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。
- 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。在现今的网络连接中，一般采用同步接口或以太网接口连接 Internet，采用异步接口连接远程拨号用户。

3. 网络资源平台设计

网络资源平台设计主要包括服务器、服务器子网连接方案、网络应用系统的设计三个方面。

1）服务器

服务器系统是网络的核心设备，它在网络中的位置直接影响网络应用效果和网络运行效率。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，为企业网提供集中、统一的数据库服务，它由网络中心管理维护，服务对象为网络全局，适宜放在网管中心；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，例如，大学的图书馆服务器和企业财务部门的服务器，适宜放在部门子网中。服务器是网络信息流较集中的设备，其磁盘系统数据吞吐量大，传输速率高，要求绝对的高宽带接入。服务器接入方案主要有以下几种：

（1）千兆以太网端口接入。服务器需要配置而且必须支持各种 GBE 网卡。GBE 网卡采用 PCI 接口，使用多模 SX 连接器接入交换机的多模光纤端口中。其优点是性能好、数据吞吐量大。缺点是成本高，对服务器硬件有要求。此方法适用于企业级数据库服务器、流媒体服务器和较密集的应用服务器中。

(2)并行快速以太网冗余接入。即采用两块以上的 100 Mb/s 服务器专用高速以太网网卡分别接入网络中的两台交换机,通过网络管理系统的支持,实现负载均衡或负载分担,如果其中一块网卡失效也不会影响服务器正常运行。

(3)普通接入。采用一块服务器专用网卡接入网络,是一种经济、简单的接入方式,但可用性低,信息流密集时可能会因主机 CPU 占用(主要是缓存处理占用)而使服务器性能下降。适合数据业务量不是太大的服务器(如 E-mail 服务器)使用。

2)服务器子网连接方案

图 7-4 为服务器子网连接的两种方案。图 7-4(a)为直接接入核心交换机,优点是直接利用核心交换机的高带宽;缺点是需要占用太多的核心交换机端口,使成本上升。图 7-4(b)所示的方案是在两台核心交换机上外接一台专用服务器组交换机,优点是可以分担带宽,减少核心交换机的端口占用,可为服务器组提供充足的端口数量;缺点是容易形成带宽瓶颈,且存在单点故障。

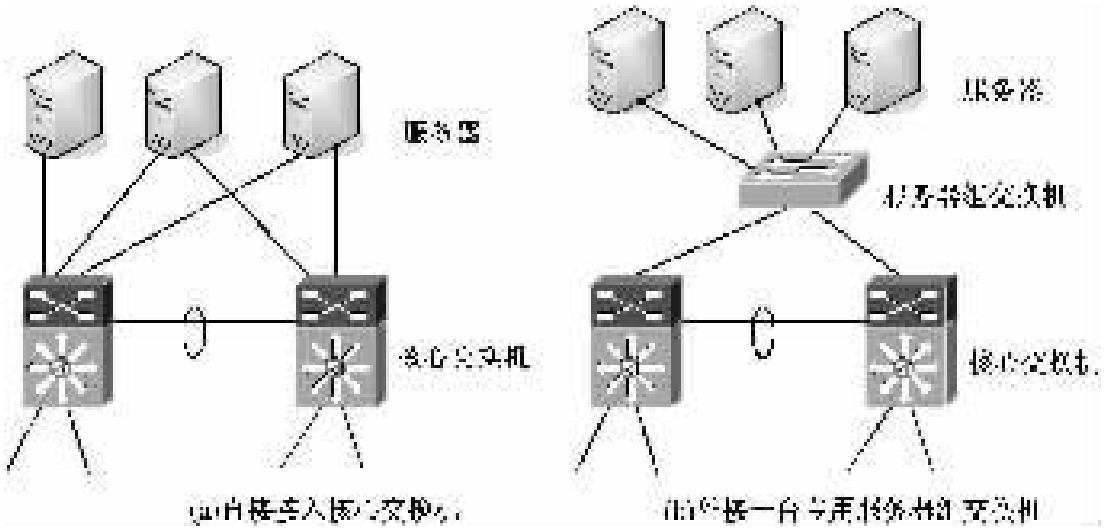

图 7-4　服务器子网的两种接入方案

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的选择是非常关键的环节,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于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,才发现与应用软件不配套或不够用,这样必然会造成资源浪费,使预算超支,直接导致网络方案失败。

选择服务器首先要看其具体的网络应用,网络应用的框架结构由底层到高层依次为服务器硬件、网络操作系统、基础应用平台和应用系统,如图 7-5 所示。虽然从理论上,应用系统与服务器硬件无关,但由于应用系统所采用的开发工具和运行环境建立在基础应用平台上,基础应用平台与网络操作系统紧密相关,其支持的操作系统是有选择的(如 SQL Server 数据库不支持 Tru64 UNIX 操作系统等),有时基础应用平台甚至是网络操作系统的有效组成部分(如 IIS Web 服务平台就是 Windows 2000 Server 的一部分),因此,选择服务器硬件实际上需要先确定所采用的网络操作系统。

图 7-5 网络应用框架结构

4. 网络操作系统与服务器配置

目前，网络操作系统产品较多，为网络应用提供了良好的可选择性。操作系统对网络建设的成败至关重要，要依据具体的应用选择操作系统。一般情况下，系统集成商在网络项目中要完成基础应用平台以下三层的搭建，选择什么操作系统，还要视公司内部的系统集成工程师，以及用户方系统管理员的技术水平和网络操作系统的使用经验而定。使用大家都比较生疏的服务器和操作系统是不明智的，这样做的结果会使工期延长和不可预见的费用加大，可能还要请外援，系统培训、维护的难度和费用也要增加。

网络操作系统分为两大类：面向 IA 架构 PC 服务器的操作系统家族和 UNIX 操作系统家族。

1）网络操作系统选择要点

与网络设备选型不同，在同一个网络中不一定需要采用相同的操作系统，在选择时可结合 Windows 2000 Server/Server 2003、Linux 和 UNIX 的特点，在网络中使用混合平台。通常，在应用服务器上采用 Windows 2000 Server/Server 2003 平台，在 Mail、Proxy、Web 等 Internet 应用中可使用 Linux/UNIX。这样，系统既具有 Windows 系统应用丰富、界面直观、使用方便的优点，又有 Linux/UNIX 稳定、高效的特点。

在网络方案规划设计中，选择操作系统要考虑的主要因素如下：

（1）服务器的性能和兼容性。Windows 2000 Server/Server 2003、Linux、NetWare 网络操作系统构建于主流的 PC 芯片上，既节约成本，又便于扩展，在系统兼容性和应用软件支持上占有优势，几种系统间均有互通互联协议，彼此间的互操作性较好。UNIX 虽然在性能、可靠性和稳定性方面具有优势，但只兼容某些型号的专用芯片及服务器，这使其只能用于金融、电信、政府、工业等少数行业。

（2）安全因素。Windows 系列是非常流行的操作系统，所以黑客、病毒经常对 Windows 操作系统进行各种攻击。该系统的密码加密方式 ACL 很严密，但加密步骤过于简单，容易被破解。Linux 继承 UNIX 在安全方面的成功技术，性能更为优越，但由于它是免费产品，容易引起用户的不信任。NetWare 操作系统的安全性、可靠性、运行稳定性都比较好。

（3）价格因素。操作系统的市场价格由高至低依次为 UNIX、NetWare、Windows 2000 Server、Windows Server 2003、Linux。除了操作系统本身的价格外，还要关注需要引进或开发的应用软件的成本。另外，培训的难易程度也是必须考虑的，因为过多的培训会带来不必要的支出。

（4）第三方软件。由于 Windows 2000 Server/Server 2003 为开放式结构，其第三方软

件十分丰富，加上与 Windows XP 等操作系统同属于微软公司的产品，客户端的桌面 Windows 系统在许多方面给 Windows 2000 Server/Server 2003 留了位置。Linux 的各种应用软件都可在网上获得，升级很快并且免费。

(5)市场占有率。市场占有率是衡量操作系统成熟度和发展势头的标尺。人们不愿意看到在下一代强有力的应用程序出现时还用着一个不能支持它的操作系统。NetWare 的应用领域只限于证券系统和部分中小网络，已没有了扩张势头；Windows Server 2003 目前已成为网络操作系统的标准配置；而 Linux 尽管到目前为止只有部分网站在用，但反响很好。随着新产品与新问题的不断出现，不同网络操作系统的市场占有率将会发生很大的变化。

2)Windows 系列操作系统服务器配置要点

首先，要根据需求分析阶段的要求，如网络规模、客户数据流量、数据库规模、所使用的应用软件等，决定需要采用的 Windows 系列操作系统服务器的档次、配置。

其次，选择 Windows 系列操作系统服务器时，对服务器上几个关键部分的选件一定要严格把关，因为 Windows 系列操作系统虽然是兼容性相对不错的操作系统，但兼容并不保证 100％可用。选购服务器组件时要注意以下几点：

(1)服务器的内存必须支持 ECC，如果使用非 ECC 的内存，就很难保证 SQL 数据库等软件能稳定、正常地运行。

(2)服务器的主要部件，如主板、网卡等，一定要通过微软公司认证，只有通过微软公司认证的产品才能保证其在 Windows 系列系统中具有 100％可用性；还要确定服务器的电源是否可靠，因为服务器不可能经常关机。

另外，在升级已有的 Windows 系列操作服务器时，要仔细分析原有网络服务器的瓶颈所在，此时可简单借用 Windows 系列操作系统中集成的软件工具，如性能监视器等，查看系统的运行状况，分析系统各部分资源的使用情况。一般来说，可供参考的 Windows 系列操作服务器升级的顺序是：扩充服务器内存容量、升级服务器处理器、增加系统的处理器数目。之所以这样，是因为对于 Windows 系列操作系统服务器上的典型应用，如 SQL 数据库、E-mail服务器来说，这些服务占用的系统资源是主要内存，而对处理器资源的要求并不多。通过扩充服务器内存容量提高系统可用内存资源将大大提高这些服务的性能。增加处理器数目往往要到整个系统升级时才考虑。

3)服务器群的综合配置与均衡

PC 服务器、UNIX 服务器及小型机服务器的概念主要局限于物理服务器(硬件)的范畴。在网络方案、系统资源集成等的应用中，通常会把安装了各类服务程序的服务器冠以相应的服务程序名称，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(偏向软件)范畴。

有关服务器群配置与均衡的建议如下：

(1)小型网络功能齐全。小型网络由于缺乏专业的技术人员，资金相对紧张，所以要求服务器组必须易于维护、功能齐全，而且还必须考虑费用的限制。建议在费用许可的情况下，尽可能提高硬件配置，利用硬件共享的特点，均衡网络应用负载，把网络中所需的所有服务压缩到 1～2 台服务器的服务范围内。例如，把对磁盘系统要求不高、对内存和 CPU 要求较高的 DNS、Web 和对磁盘系统和 I/O 吞吐量要求高、对缓存和 CPU 要求较低的文件服务安装在一台配置中等的部门级服务器内，而把对硬件整体性能要求较高的数据库服务和

E-mail服务安装在一台配置较高的部门级或企业入门级服务器中。当然，Web服务器对系统I/O的需求也较高，当用户访问数量增加时，系统的实时响应和I/O处理需求也会急剧增加，但FTP访问偶发性强，Web访问密度比较均匀，二者正好可以互补。另外，如果采用Linux操作系统，利用其资源占用低、Internet服务程序丰富的特点，可将所有Internet服务集中到一台服务器上，另外再配置一台应用服务器，这样网络效率可能会成倍提高。

(2)中型网络重应用。中型网络注重实际应用，可选择将应用分布在更多的服务器上。宜采用功能相关性配置方案，将相关应用集中在一起。例如，当前网络应用重心已开始转移到Web平台，Web服务器需要频繁地与数据库服务器交换信息，把Web服务和数据库服务安装在一台高档服务器内，毫无疑问会提高效率，减轻网络I/O负担。对于企业网络，可能需要一些工作流应用系统(如公文审批流转、文件下发等)，如果需要底层E-mail服务，就可以采用群件服务器，把E-mail和News服务集成进去。对于像VOD这样的流媒体专用服务器，需要单独使用一台服务器，并发用户多时还要采用服务器集群技术。

(3)大型网络或ISP/ICP的服务器群方案。大型网络要求安全可靠、稳定高效、功能强大。大型网站需要向用户提供全面的服务，如提供免费E-mail服务、免费软件下载、免费主页空间等，所以要求网站必须功能完备，且具有高度的可用性和可扩展性，以保证系统连续、稳定地运行。如果服务器数量过多，则会为管理和运行带来沉重负担，导致环境恶劣(仅机房噪声就令人无法忍受)。因此，建议采用机架式服务器，其Web、E-mail和防火墙等应用均采用负载均衡集群系统，以提高系统的可用性。专业的数据库系统为用户提供了强大的数据库底层支持，可提供大规模邮件服务，防火墙系统可以保证用户网络和数据的安全。

5.网络安全设计

网络安全就是网络信息的安全，是指网络系统的硬件、软件及系统中的数据受到保护，不因偶然或恶意的原因而遭到破坏、更改、泄露，系统能连续、可靠、正常地运行，网络服务不中断。广义来说，凡是涉及网络信息的保密性、完整性、可用性、真实性和可控性的相关技术和理论都是网络安全所要研究的内容。网络安全涉及的内容既有技术方面的问题，也有管理方面的问题，两方面相互补充，缺一不可。技术方面主要侧重于防范外部非法用户的攻击，管理方面则侧重于内部人为因素的管理。网络安全体系设计的重点在于根据安全设计的基本原则，制定出网络各层次的安全策略和措施，然后确定应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循相应的原则，网络系统的安全和保密就会更加有保障。从工程技术角度出发，在设计网络方案时，应该遵循以下原则：

(1)网络信息系统安全与保密的“木桶原则”。木桶原则来源于“木桶的最大容积取决于最短的一块木板”，它强调对信息进行均衡、全面的安全保护。网络信息系统是一个复杂的计算机系统，它本身在物理、操作和管理上的种种漏洞造成了系统安全的脆弱性，尤其是多用户网络系统自身的复杂性、资源共享性使单纯的技术保护防不胜防。攻击者使用的是“最易渗透原则”，即对系统中最薄弱的地方进行攻击。因此，充分、全面、完整地对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)网络安全系统的整体性原则。网络的安全防护、监测和应急恢复要求在网络被攻击

的情况下，必须尽快恢复网络信息中心的服务，以减少损失。所以网络安全系统应该包括安全防护机制、安全监测机制、安全恢复机制三种。安全防护机制是根据具体系统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；安全监测机制是监测系统的运行情况，及时发现和制止对系统进行的各种攻击；安全恢复机制是在安全防护机制失效的情况下，进行应急处理和尽量及时地恢复信息，减少攻击的破坏程度。

(3)网络安全系统的有效性与实用性原则。网络安全应以不影响系统的正常运行和合法用户的操作活动为前提。网络中的信息安全和信息利用是矛盾的两方面：为了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，同时，这势必给系统的运行和用户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。网络安全应采用分布式监控、集中式管理。

(4)网络安全系统的等级性原则。良好的网络安全系统应分为不同级别，包括对信息保密程度(绝密、机密、秘密、普密)、用户操作权限(面向个人及面向群组)、网络安全程度(安全子网和安全区域)、系统实现结构的分级(应用层、网络层、数据链路层等)，从而针对不同级别的安全对象提供全面、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。

(5)设计为本原则。强调安全与保密系统的设计应与网络设计相结合。由于安全与保密问题是一个相当复杂的问题，因此必须设计周密，才能保证网络的安全。

(6)自主和可控性原则。网络安全与保密问题关系着一个国家的主权和安全，所以网络安全产品不能依赖国外进口。

(7)安全有价原则。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，必须考虑性能和价格的平衡，不同的网络系统所要求的安全侧重点也不相同，例如，国家政府机关、国防部门的计算机网络系统安全侧重于存取控制功能；金融部门侧重于身份认证、审计、网络容错等功能；交通、民航部门侧重于网络容错等。因此，必须有的放矢，具体问题具体分析，把有限的经费用在关键领域。

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。网络安全系统的设计和实现必须根据具体的系统和环境，考察、分析、评估、检测(包括模拟攻击)和确定系统存在的安全漏洞和安全威胁。

(2)明确安全策略。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。安全策略要综合考虑以下几方面：

- 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。
- 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)。
- 便于网络管理人员进行控制、管理和配置。
- 可扩展的编程接口，便于更新和升级。
- 用户界面友好和使用方便。
- 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化，更好地解决与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。

- 安全体制：包括安全算法库、安全信息库和用户接口界面。
  - 安全算法库：包括私钥算法库、公钥算法库、Hash 函数库、密钥生成程序、随机数生成程序等安全处理算法。
  - 安全信息库：包括用户口令和密钥、安全管理参数及权限、系统当前运行状态等安全信息。
  - 用户接口界面：包括安全服务操作界面和安全信息管理界面等。
- 网络安全连接：包括安全协议和网络通信接口模块。
  - 安全协议：包括安全连接协议、身份验证协议、密钥分配协议等。
  - 网络通信接口模块：网络通信接口模块根据安全协议实现安全连接。一般有两种实现方式，一种是安全服务和安全体制在应用层实现，经过安全处理后的加密信息送到网络层和数据链路层，进行透明的网络传输和交换，这种方式的优点是实现简单，不需要对现有系统做任何修改，用户投资数额较小；另一种是对现有的网络通信协议进行修改，在应用层和网络层之间加一个安全子层，实现安全处理和操作的自动性、透明性。
- 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。
  - 网络安全管理系统：安全管理系统安装于用户终端或网络结点上，由若干可执行程序所组成的软件包组成，提供窗口化、交互的“安全管理器”界面，由用户或网络管理员配置、控制和管理数据信息的安全传输，兼容现有通信网络管理标准，实现安全功能。
  - 网络安全支撑系统：整个网络安全系统的可信任方是由网络管理员维护和管理的安全设备和安全信息的总和，包括密钥管理分配中心，负责身份密钥、公钥和私钥等密钥的生成、分发、管理和销毁；认证鉴别中心，负责对数字签名等信息进行鉴别和裁决。网络安全支撑系统的物理和逻辑安全都是至关重要的，必须受到最严密和全面的保护。同时，也要防止管理人员内部的非法攻击和误操作，在必要的应用环境，可以引入秘密分享机制来解决这个问题。
  - 网络安全传输系统：包括防火墙、安全控制、流量控制、路由选择和审计报警等。

(4)选择并实现安全服务，具体包括以下几个方面：

- 物理层的安全：物理层信息安全，主要防止物理通路的损坏、对物理通路的窃听和攻击(干扰等)。
- 数据链路层的安全：数据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。
- 网络层的安全：网络层的安全需要保证网络只允许授权的客户使用授权的服务，保证网络路由正确，避免被拦截或监听。
- 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。
- 应用平台的安全：应用平台指建立在网络系统之上的应用软件服务器，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，通常采用多种技术来增强应用平台的安全性。
- 应用系统的安全：应用系统完成网络系统的最终目的——为用户服务。应用系统的安全与系统的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，如通

信内容安全、通信双方的认证和审计等手段来保证系统的基本安全。

(5)安全产品的选型测试。安全产品的选型测试工作严格按照企业信息与网络系统、安全产品的功能规范要求,利用综合的技术手段,为企业测试出符合功能规范的安全产品。测试工作原则上应该由中立组织进行;测试方法必须科学、准确、公正,必须有一定的技术手段;测试标准应该是国际标准、国家标准与企业信息和网络系统安全产品功能规范的综合;测试范围是产品的功能、性能与可用性。

7.2　网络组建方案

目前,主流的组网技术有:局域网采用 1 000 Mb/s、10 Gb/s 以太网为主干网,采用 1 000/100 Mb/s连接各个汇聚结点,每个汇聚结点分别用 100 Mb/s 端口连接各个接入结点,10/100 Mb/s 以太网接入用户桌面;城域网采用 1 000 Mb/s、10 Gb/s 以太网组网技术和10 Gb/s POS(Packet Over SONET,SONET 上的数据包)组网技术,且 10 Gb/s 以太网将逐渐取代 10 Gb/s POS 成为城域网主流组网技术;广域网骨干链路主要采用 2.5 Gb/s POS 和 10 Gb/s POS 组网技术,POS 技术被广泛用于广域网骨干网中。

7.2.1　小型局域网组建方案

小型局域网的概念没有明确的定义,从几台计算机到几百台计算机所组成的网络,都可以称作小型局域网。如果按路由协议来分,通常小型局域网运行静态路由协议或 RIP 路由协议。下面以某网吧局域网的组建为例,分析小型局域网的建设方案。

该网吧现有计算机 350 台,其组网方案如图 7-6 所示。采用 RG-NBR1000E 作为出口路由器,在 RG-NBR1000E 上插单模光纤模块,电信 50 M 光纤直接连接到 RG-NBR1000E 上,RG-NBR1000E 提供端口镜像功能,公安部门的监控服务器连接 RG-NBR1000E 的四个 LAN 口中的某个 LAN 口。

核心交换机采用 RG-S3512G 的 1 000 M 三层交换机,接入交换机选用 RG-S2126。游戏服务器和电影服务器通过 1 000 Mb/s 以太网线路直接连接到 RG-S3512G 上。根据需要将网吧划分五个不同的网段,其中电影、游戏服务器在一个网段;内部计算机划分为四个网段,分别为普通上网区、视频上网区、游戏区和 VIP 区,不同区采用不同的计费标准。内部不同网段数据通过 RG-S3512G 进行线速转发。

在 RG-S2126 上启用了 ACL 防病毒功能,能够防止冲击波和震荡波,同时启用了 MAC+IP+端口绑定功能,能够防止 ARP 地址欺骗病毒。

在 RG-NBR1000E 上启用了防冲击波、防震荡波、防 ping 等外网攻击的保护功能;启用对内部计算机的限速功能,根据不同的分区限制不同的上传、下载速度;同时还启用了 NAT 的会话限制,每台计算机最多允许 500 个 NAT 会话。通过限速和限 NAT 会话数的策略,可以避免某些计算机感染病毒、过度 BT 下载等占用大量的 NAT 会话和带宽,影响其他用户的上网速度。

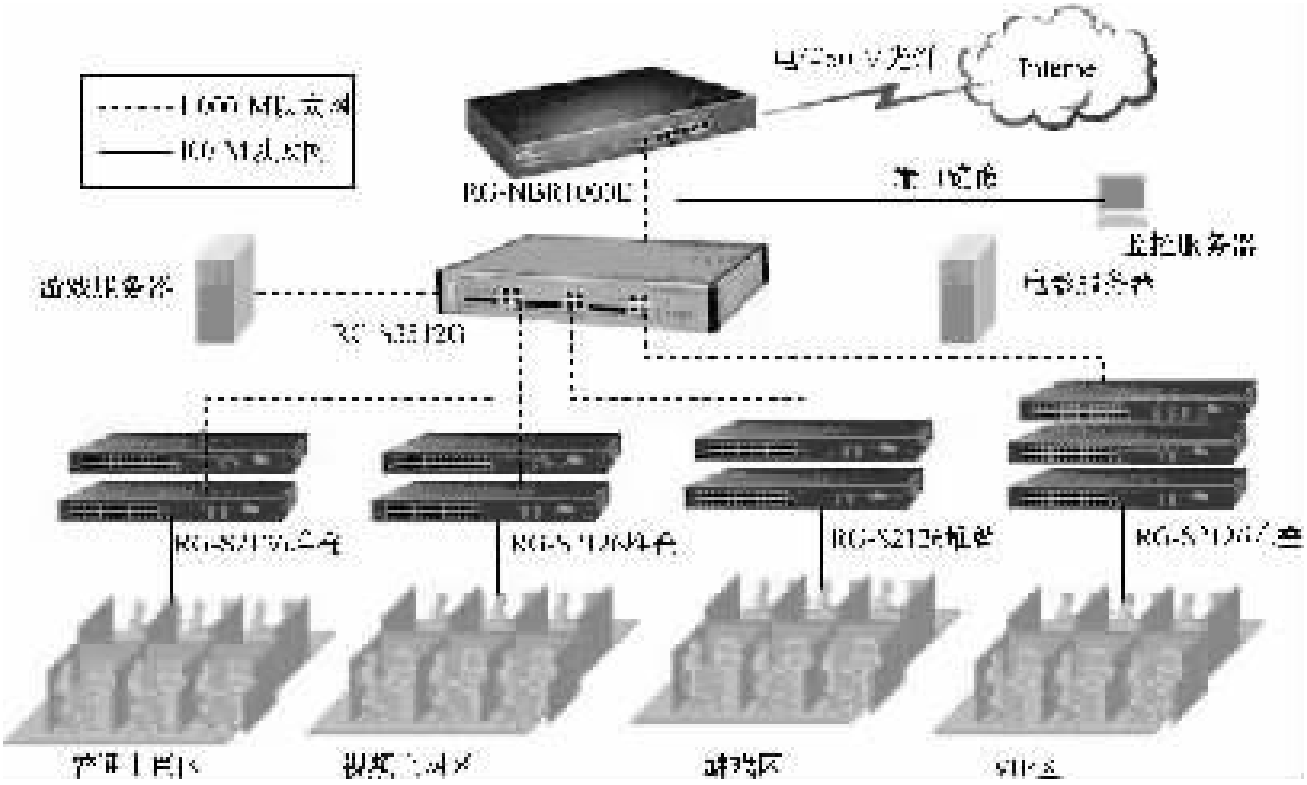

图 7-6 某网吧组网方案

1.主要设备的选择

采用国内领先的网络设备及解决方案提供商锐捷网络公司的产品作为网络连接的主要设备，该网络采用二层网络结构设计，其主要设备的选型如下：

(1)核心层交换机采用锐捷三层交换机 RG-S3512G。

(2)接入层交换机选用锐捷 RG-S2126。

(3)出口路由器选用锐捷 RG-NBR1000E，以 50 M 光纤接入 Internet。

2.采用的组网技术

该网络选用 1 000 Mb/s 交换技术为主干组网，用 100 Mb/s 交换技术接入用户桌面。

3.方案特点

(1)稳定可靠。RG-NBR1000E 采用 64 位 Motorola Power PC RISC 高性能处理芯片，稳定可靠不掉线。同时它具有 PC 133 MB 内存，FLASH ROM 达到 8 MB，Boot ROM 达到 2 MB，线速转发，能满足网络用户对高速网络的需求。核心交换机提供基于硬件的线速转发，数据包路由的任务由板卡上的 ASIC 来执行，在速度上比传统的基于 CPU 的路由快很多倍，使整个网络更加高效、稳定。

(2)直接连接光纤。RG-NBR1000E 通过模块扩展，可以直接连接多模光纤或单模光纤，无须配光纤收发器，从而减少了设备的占用空间和网络故障点，还解决了设备兼容性问题，提高了网络的可靠性。

(3)扩充性好。RG-NBR1000E 支持 VRRP 热备份协议，如果今后网吧扩充，则可以采用两台或多台 RG-NBR1000E 来进行 VRRP 的负载均衡和线路备份，网络速度和终端数量可成倍提升。

7.2.2 中型局域网组建方案

中型局域网所包括的计算机数量从几百台到几千台，一般情况下，综合性大学的校园网

是比较典型的中型网络。中型局域网从简单的信息承载平台转变成一个公共服务提供平台。终端用户希望能时刻保持与网络的连接，因此，高效、可靠成为中型局域网组建的重要目标。要保证网络的可靠性，就需要使用冗余技术。高冗余网络最大的优点是，在网络设备、链路发生中断或变化时，用户几乎感觉不到。为了达到这一目标，需要在网络的各个环节上实施一定的冗余，包括网络设备、链路、网络出口等。从运行的路由协议方面来看，中型局域网通常运行动态路由协议 RIP、OSPF 或 Cisco 的专用动态路由协议 IGRP/EIGRP 等。下面以某大学校园网为例分析中型局域网的组建。

1. 高校校园网现状分析

目前高校校园网的建设有若干需求，以下几点是建设校园网应考虑的关键因素：

(1)安全的需求。越来越多的报道表明，高校校园网已逐渐成为黑客的聚集地。一方面是由于网络病毒、黑客工具的泛滥；另一方面是高校学生——这群精力充沛的年轻一族对新鲜事物有着强烈的好奇心，他们有着探索的冲劲和高智商，却缺乏全面思考的责任感。据有关数字显示，目前校园网遭受的恶意攻击 90％来自高校网络内部。如何保障校园网络的安全，成为高校校园网络建设时需要首先考虑的问题。

(2)运营的需求。众所周知，学校不是运营商，其运营的模式和业务流程并不清晰。而学校收费和学生缴费是一对天然的矛盾，当前不少学校采用的运营模式与学校的实际情况差距太大，无法有效杜绝学生逃避缴费，这一问题一直困扰着学校的网管人员。

(3)管理的需求。由于高校网络结点众多，因此无法一体化管理众多的设备和用户。网络故障无法快速定位，IP 地址被盗用和 IP 地址冲突等问题日益严重，如何利用有限的人力、物力对网络进行高效管理也成为校园网建设需要考虑的重点之一。

(4)性能的需求。高校校园网的网络用户很多，并且随着网络应用技术的不断丰富，高校校园网应用也愈发复杂。例如，FTP 文件传输等大量数据的访问，产生了巨大的网络流量。高速进行网络传输，对网络设备提出了很高的要求。

(5)特殊业务的考虑。随着远程教育、视频会议和 VOD 等越来越多的多媒体业务在高校校园网上运行，尤其当业务量猛增时，会造成网络时延、抖动、丢包等现象，而这对于实时的、时延敏感的网络应用，如视频会议、IP 电话等会产生严重的影响。因此，保障特殊业务的正常使用，是高校网络建设中必须要考虑的因素。

(6)接入方式的考虑。高校校园网中不仅需要有线网络，在某些环境(如电子阅览室、体育馆、阶梯教室等)中还需要无线网络。目前，购买笔记本电脑的大学生越来越多，无线网络接入方式可以避免传统网络对用户接入的限制，实现随时随地上网。

2. 校园网解决方案

针对上述校园网建设中出现的问题与需求，下面给出一个较为安全、易管理、可运营的校园网建设方案，其网络拓扑如图 7-7 所示。

1)主要设备的选型

该校园网采用三层网络结构设计，核心层采用双交换机的冗余设计，这样既可以实现双机容错，又可以实现负载均衡。各层交换机的选型如下：

- 核心层交换机：SW 1、SW 2 为核心层交换机，选用三层交换机 Cisco 6509。
- 分布层交换机：SW 3～SW 10 为分布层交换机，选用 Cisco 3550-12G。
- 接入层交换机：选用 Cisco 2900、RG-S2150G 等。
- 出口路由器：选用 Cisco 7200，分别以 1 000 Mb/s 接入 CERNET(中国教育和科研计

算机网)和 100 Mb/s 接入 CNC(中国网通)。

2)采用的组网技术

主干网选用 10 Gb/s 交换技术,分支网采用 1 000 Mb/s 交换技术,采用 100 Mb/s 交换技术接入用户桌面,保证了校园网的高速数据路由交换,且具有很好的可扩展性。

3)该校园网方案的特点

(1)高安全性。高安全性表现在以下几个方面:

- 安全认证到桌面。采用 IEEE 802.1x、PPOE 或 Web/Portal 认证技术,可以确保用户入网时身份唯一,且避免了 IP 冲突。
- 管理分级授权。不同职能的管理者使用同一套系统时可以得到不同的操作界面及使用权限,避免了管理的安全隐患。
- 控制网络病毒。统一对接入层交换机动态下发安全策略,轻松有效地控制网络病毒,使网络保持畅通。
- 抵御网络攻击。结合网络攻击的检测系统,能够抵御日益增多的内部网络攻击,并且自动对用户做出相应的控制动作,保证网络安全。

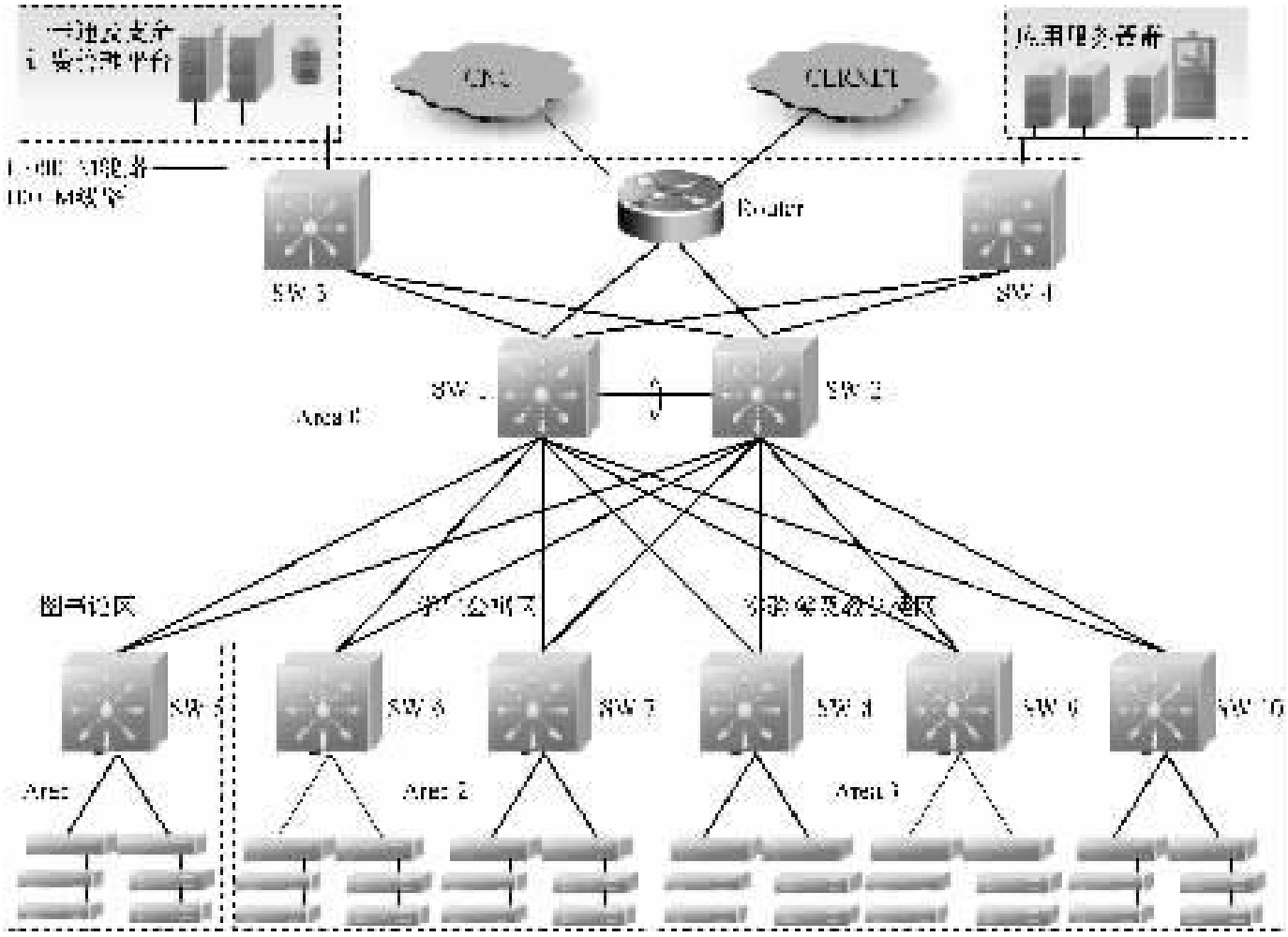

图 7-7 某校园网络的拓扑结构

(2)可运营性。可运营性表现在以下几个方面:

- 符合校园的运营模式。结合校园的实际运营,在原有电信策略的基础上开发出最适合校园的运营模式,从最大程度上解决收费和缴费的矛盾。
- 丰富的运营管理功能。保证管理者可以随时获得运营所需的记录和统计信息,从而为运营提供足够的数据支持。

- 完善的自助服务系统。能够让用户方便地对自身账号的信息以及账务情况进行自助查询，极大减轻了管理者的负担。

(3)易管理。易管理性表现在以下几个方面：

- 全网设备统一管理。对事件、性能、日志的统一管理，可以方便地对全网设备进行统一管理。
- 接入时段管理。通过对日常、周末以及节日的一次性设置，轻松灵活地管理用户能够使用网络的时段，提高用户管理的力度。

(4)高性能。网络中采用高吞吐量、线速转发的核心路由器和三层交换机；对所有关键器件进行了冗余，包括主控板、交换网板、电源等；支持板件的热插拔，保证了网络的高效运转。

对于 ACL、QoS 等针对单独端口的数据行为，通过为 ASIC 芯片各端口增加独立的 FFP(Fast Filter Processor)模块进行硬件处理，各端口可以同步进行硬件处理。

对于 L2/L3/组播等涉及不同端口之间的数据处理行为，通过存放在线卡 ASIC 芯片的统一硬件查表项对所有端口进行统一处理，提供数据在不同端口之间的线速转发。

(5)端到端 QoS。从接入层交换机到核心设备，全面覆盖端口速率限制、应用流分类识别、关键业务流量保证带宽等多层交换质量保证。

基于交换机时间、物理端口、MAC 地址、IP 地址、TCP/UDP 端口号的应用流分类识别和带宽限速机制，完成了全网端到端的 QoS 保证。

7.2.3　大型局域网建设方案

大型局域网通常处于核心位置，网络稳定、可靠是其网络业务正常运行的关键。为此，通常设置较多的冗余备份和热切换。在路由协议上，通常使用 OSPF 等动态路由协议。城域网其实就是一种大型的局域网，通常使用与局域网相似的技术。下面以“郑州教育城域网”为例，分析大型局域网的网络建设方案。

1. 郑州教育城域网建设的总体目标

郑州教育城域网建设的总体目标是利用各种先进、成熟的网络技术和通信技术，采用统一的网络协议，建设一个可实现各种综合网络应用的高速计算机网络系统，将郑州市区各高校及省教育厅各直属学校通过网络连接起来，并与 CERNET、Internet 相连。郑州教育城域网要求建成后除实现一般的 Internet 功能外，如 E-mail、FTP、网络论坛、网络图书馆、搜索引擎、网上聊天、数据传输管理、处理与查询等，还应实现如视频点播、实时远程教学、网络学校、电视会议和网络电话等功能，形成一个高速、多媒体 Internet，实现郑州整个教育系统的资源共享，做到网内资源全市大、中、小学都能共享。

2. 郑州教育城域网建设方案

郑州教育城域网建设方案如图 7-8 所示。网络主干由连接郑州市区的 1 000 Mb/s 网络主环和连接各骨干学校的光缆组成。选择 1 000 Mb/s 以太网为教育城域网的主干网，还需要选择适当的 1 000 Mb/s 以太网交换机作为网络的主干核心，这关系到网络的整体性能和系统的灵活性。

在本方案中，环形主干上的结点有省网络中心(郑州大学)、东区中心(省教育厅)和北区中心(农业大学)。

选择 Avaya P882 路由交换机来构造网络高速主干，它属于三层 1 000 Mb/s 以太网交

换机，内部集成路由功能，具有高容量、无阻塞、优质的管理能力和可靠的多媒体支持等特点。Avaya P882 拥有高达 139 Gb/s 的背板带宽和 106 Mb/s 的交换/路由性能，可支持最多 768 个 10/100 Mb/s 以太网端口、128 个千兆位以太网端口或 384 个 100Base-FX 端口，将 1 000 Mb/s 以太网交换、快速以太网交换、以太网交换以及路由都集成到一个交换机中，这使得交换机的功能十分强大。

Avaya P882 通过多模室外铠装光缆相互连接，构成环状。考虑到主干交换机所在楼宇均为高密度结点楼宇，以及环形主干的流量和标书的要求，将环形主干设计成双链路连接。这样，其他分布在各学校的 1 000 Mb/s 以太网交换机或 100 Mb/s 以太网交换机就近与环上的主干交换机进行 1 000 Mb/s 或 100 Mb/s 交换式连接，从而构成城域网的主干网络。

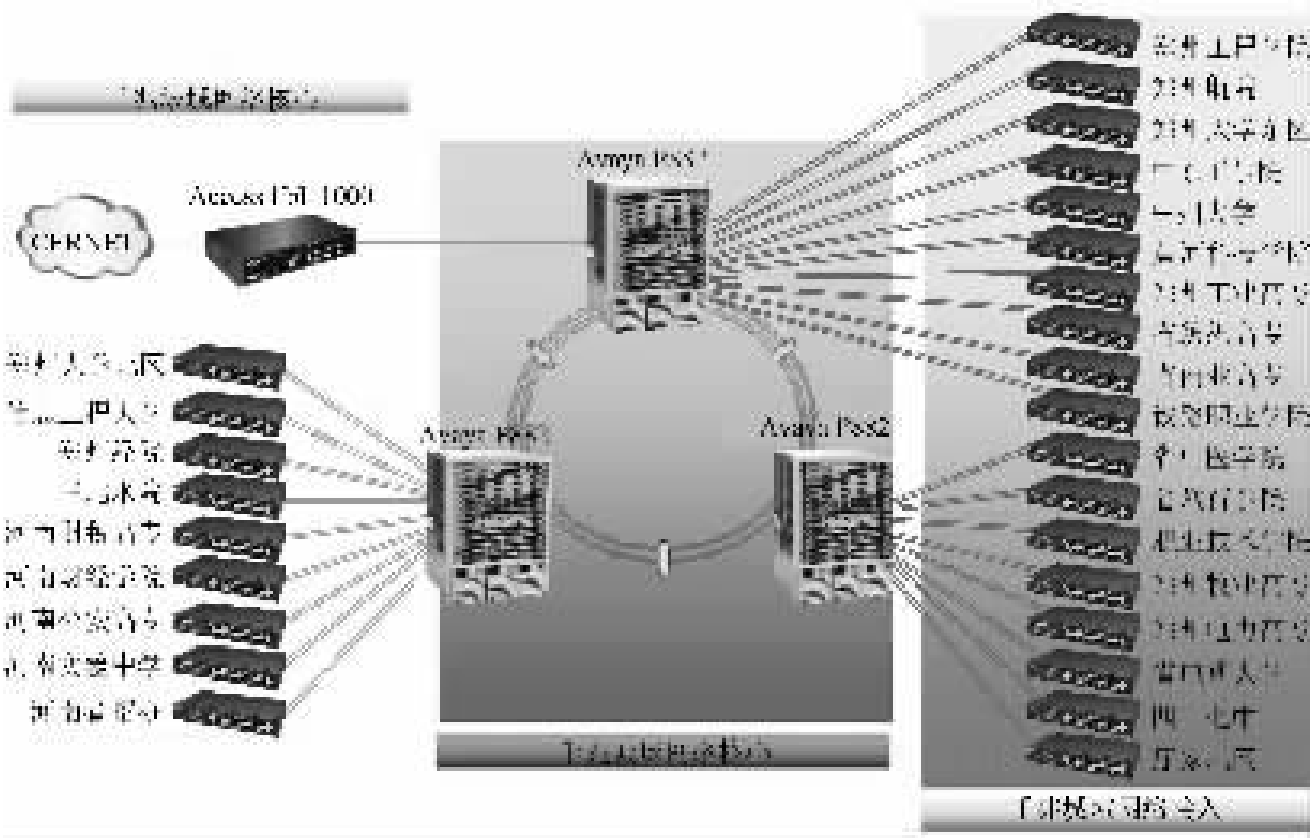

图 7-8　郑州教育城域网组网方案

7.3　案 例 分 析

下面以 7.2.2 小节的中型局域网建设方案（见图 7-7）为例，分析该组网方案的网络组成，并给出主要设备的具体配置命令。

7.3.1　组网方案分析

下面对 7.2.2 小节的中型局域网的组网方案进行详细介绍。

1. 网络组成

该网络是某大学的校园网络，它由以下五个部分组成：

(1)网络出口由边界路由器 Router 组成。

(2)核心层由两台核心层交换机 SW 1、SW 2 组成。

(3)Area 1 是图书馆区,由一台分布层交换机和若干接入层交换机组成。

(4)Area 2 是学生公寓区,由男生公寓分布层交换机和女生公寓分布层交换机及若干接入层交换机组成。

(5)Area 3 是实验楼及教学楼区,由三台分布层交换机及若干接入层交换机组成。

为保证网络的稳定运行,一定的冗余设备是必不可少的,在设备级,核心路由交换机采用双主控板、双电源,保证核心的稳定;在分布层和接入层,采用冗余链路,关键接入层交换机均采用双链路连接分布层交换机。

注意:该网络采用的是多区域的 OSPF 路由协议,其中 Area 0 为骨干区域,Area 1、Area 2 以及 Area 3 统称为非骨干区域。各非骨干区域间不可以直接交换信息,它们只有与骨干区域相连,通过骨干区域才能相互交换信息。

2.IP 地址规划

根据校园建筑物布局和不同部门的用户数量,合理划分有限的 IP 地址。该校园网各部门 IP 地址的分配情况见表 7-1。

表 7-1　校园网 IP 地址分配表

区　　域	IP 地址分配
网管中心	125.219.48.0～125.219.48.62
教学楼	125.219.48.64～125.219.48.158
学生活动中心	125.219.48.160～125.219.48.254
图书馆楼	125.219.49.0～125.219.50.254
男生公寓	125.219.51.0～125.219.56.254
女生公寓	125.219.57.0～125.219.58.254
1 号实验楼	125.219.59.0～125.219.61.254
2 号实验楼	125.219.62.0～125.219.63.254

3.路由协议

在三层协议上,使用动态路由协议 OSPF,当任何一台核心交换机出现问题时,能保证网络的正常运行,简化了路由表的管理;分布层也采用具有路由功能的三层交换机,保证在某个 VLAN 出现故障时,不至于影响整个网络。在边界路由器处,启用基于目的地址的策略路由,来自 CERNET 的数据通过 CERNET 出口出入,其余通过 CNC 出口出入,并启用动态检测功能,在一条出口出现故障时,所有流量走另一出口。

7.3.2　典型设备的配置命令

由于整个网络中的设备比较多,下面仅以其中的典型代表,如边界路由器、核心层交换机 SW 1、分布层交换机 SW 8 为例,给出相关的配置命令。

1.路由器的配置

路由器的配置比较复杂,这里只列举其配置的要点。

首先设置用于连接 SW 1 的接口地址 172.16.1.2/30 和连接 SW 2 的接口地址 172.161.6/30,然后启用 OSPF 路由协议,再设置到 CERNET 的静态路由和到 CNC 的默认

路由，最后启用 NAT 转换等功能。

2. SW1 的配置

具体命令如下：

```
sw1＞enable
sw1＃config terminal
sw1(config)＃interface gigabitethernet 1/1  (进入端口 1 槽 1 口，连接路由器)
sw1(config-if)＃ip address172.16.1.1 255.255.255.252
sw1(config-if)＃no shutdown
sw1(config-if)＃exit
sw1(config)＃interface gigabitethernet 1/2  (进入端口 1 槽 2 口，连接 SW 3)
sw1(config-if)＃ip address 172.16.3.1 255.255.255.252
sw1(config-if)＃no shutdown
sw1(config-if)＃exit
sw1(config)＃interface gigabitethenet 1/3  (进入端口 1 槽 3 口，连接 SW 4)
sw1(config-if)＃ip address 172.16.4.1 255.255.255.252
sw1(config-if)＃no shutdown
sw1(config-if)＃exit
sw1(config)＃interface gigabitethenet 6/1  (进入端口 6 槽 1 口，连接 SW 5)
sw1(config-if)＃ip address 172.16.5.1 255.255.255.252
sw1(cofig-if)＃no shutdown
sw1(config-if)＃exit
sw1(config)＃interface gigabitethernet 6/2  (进入端口 6 槽 2 口，连接 SW 6)
sw1(config-if)＃ip address 172.16.6.1 255.255.255.252
sw1(config-if)＃no shutdown
sw1(conflg-if)＃exit
sw1(config)＃interface gigabitethernet 6/3  (进入端口 6 槽 3 口，连接 SW 7)
sw1(config-if)＃ip address 172.16.7.1 255.255.255.252
sw1(config)＃no shutdown
sw1(conflg-if)＃exit
sw1(config)＃interface gigabitethernet 6/4  (进入端口 6 槽 4 口，连接 SW 8)
sw1(conflg-if)＃ip address 172.16.8.1 255.255.255.252
sw1(conflg-if)＃no shutdown
sw1(conflg-if)＃exit
sw1(config)＃interface gigabitethenet 6/5  (进入端口 6 槽 5 口，连接 SW 9)
sw1(conflg-if)＃ip address 172.16.9.1 255.255.255.252
sw1(conflg-if)＃no shutdown
sw1(conflg-if)＃exit
sw1(config)＃interface gigabitethenet 6/6  (进入端口 6 槽 6 口，连接 SW 10)
sw1(conflg-if)＃ip address 172.16.10.1 255.255.255.252
sw1(conflg-if)＃no shutdown
```

```
sw1(conflg-if)#exit
sw1(config)#router ospf 1                          (启用 OSPF 路由协议进程)
sw1(config-router)#network 172.16.1.0 0.0.0.3 area 0
                                                   (指定与该交换机相连的网络)
sw1(config-router)#network 172.16.3.0 0.0.0.3 area 0
sw1(conflg-router)#network 172.16.4.0 0.0.0.3 area 0
sw1(config-router)#network 172.16.5.0 0.0.0.3 area 1
sw1(config-router)#network 172.16.6.0 0.0.0.3 area 2
sw1(config-router)#network 172.16.7.0 0.0.0.3 area 2
sw1(config-router)#network 172.16.8.0 0.0.0.3 area 3
sw1(config-router)#network 172.16.9.0 0.0.0.3 area 3
sw1(config-router)#network 172.16.10.0 0.0.0.3 area 3
```

3. SW8 的配置

具体命令如下：

```
sw8>enable
sw8#config terminal
sw8(config)#interface vlan 1
sw8(config-if)#ip address 172.16.8.254 255.255.255.240
sw8(config-if)#no shutdown
sw8(config-if)#exit
sw8(config)#interface vlan 10                      (进入 VLAN 10)
sw8(config-if)#ip address 10.10.8.126 255.255.255.128
sw8(config-if)#no shutdown
sw8(config-if)#exit
sw8(config)#interface vlan 11
sw8(config-if)#ip address 10.10.8.254 255.255.255.128
sw8(config-if)#no shutdown
sw8(config-if)#exit
sw8(config)#interface gigabitethernet 0/1  (进入 1 000 Mb/s 1 口,连接 SW 1)
sw8(config-if)#no switchport
sw8(config)#ip address 172.16.8.2 255.255.255.252
sw8(config-if)#no shutdown
sw8(config-if)#exit
sw8(config)#interface gigabitethernet 0/2  (进入 1 000 Mb/s 2 口,连接 SW 2)
sw8(config-if)#no switchport
sw8(config-if)#ip address 172.16.8.6 255.255.255.252
sw8(conflg-if)#no shutdown
sw8(conflg-if)#exit
sw8(config)#interface range gigabitethernet 0/3-12
sw8(config-if)#switchport mode dynamic desirable
```

```
sw8(config-if)#switchport trunk encapsulation dot1q
                                        (以 IEEE 802.1q 协议封装 Trunk)
sw8(config-if)#exit
sw8(config)#router ospf 1
sw8(config-router)#network 172.16.8.0 0.0.0.3 area 3
                                        (指定与该交换机相连的网络)
sw8(config-router)#network 172.16.8.4 0.0.0.3 area 3
sw8(config-router)#network 172.16.8.240 0.0.0.15 area 3
                                        (此网段为交换机管理网段 )
sw8(config-router)#network 10.10.8.0 0.0.0.255 area 3
                                        (此网段为 VLAN 10、VLAN 11 汇聚)
```

对于连接到 SW 8 交换机的接入层交换机，需要设置其与 SW 8 交换机相连的端口为 Trunk 端口，其余的端口可以划分到 VLAN 10 或 VLAN 11 中。

本 章 小 结

本章主要介绍组网方案设计与案例分析。首先介绍了局域网组网方案设计的一般方法，组网方案设计主要包括网络需求分析和网络系统方案设计两个阶段。网络需求分析对于建立一个功能完善、安全可靠、性能优越的网络系统至关重要。然后介绍了小型、中型、大型局域网的组建方案，最后以一个中型局域网组建方案为例，详细介绍了局域网的组网方案和典型设备的配置。本章中的各个案例融入了作者的实际工作经验，有助于读者更好地把握网络组建中遇到的关键问题。本章所提供的案例具有典型性，可以应用到实际的网络环境中。

习 题 7

1. 网络组建方案中的需求分析包括哪些方面？

2. 网络系统方案设计包括哪些方面？

3. 请对一个有 40 台计算机的局域网进行网络系统设计，并列举出主要设备的类型及配置命令。

4. 参观所在学校的网络管理中心，了解学校的网络系统方案，列出所用的网络设备，并绘制出相应的网络拓扑结构图。