



# 项目二

常用服务的配置和使用



## 项目导入

小刘作为某公司的网络管理员，其中一项工作任务是负责创建和维护公司的网站。在上一个项目中，小刘完成了服务器的安装工作。接下来，他需要在服务器上安装 Web 服务器软件，来作为公司对外网站的发布平台。除此而外，公司还需要为员工提供企业办公自动化平台(Web 版，内嵌电子邮件系统和 FTP 文件系统)和企业私有云存储平台(Web 版)。

## 项目分析

为了满足不同的业务需求，需要在操作系统上配置不同的应用服务器。

大多数企业都需要建设和发布管理企业的网站，网站需要发布在 Web 服务器上，所以搭建自己的 Web 服务器是每个公司必需的业务内容。

企业网站是企业的门面，既是对外宣传企业的必需，很多时候还会承载客户交流、网上电子商务等功能，对企业生存和发展来说，非常重要。

另一方面，企业内部办公基本已经电子化和 Web 化。多数企业的内部办公系统都依托 Web 平台建立和开发。

在公司的业务往来中，电子邮件是必不可少的业务工具。虽然网络上有各种不同类型的电子邮箱可以申请，但出于安全性、可靠性、经济性等原因，很多企业会建立自己的电子邮件服务器来向员工提供邮件服务。

在日常工作中，通知下达，文件转发，报告提交等都涉及大量的文件交流。企业需要提供文件交流共享平台来实现日常办公。很多办公商业软件可以满足企业的日常办公需求，即使如此，企业仍然有足够的理由建立自己的文件服务器，来作为必要的补充。

现代企业办公自动化平台基本上集成了各种必备的要素，采用模块化机制开发，把电子邮件、FTP 服务都容纳到自动化平台内部，无缝集成，构建了全 Web 化的统一平台。

就像眼睛满足视觉需要、鼻子满足嗅觉需要、耳朵满足听觉需要一样，各个器官各负其责，协同工作。对于企业来说，对外网站提供信息发布、客户交流、业务门户、企业形象等多种功能，是必需的要素存在；电子邮件作为稳妥可靠的交流手段，是企业主要的交流渠道之一；文件传输作为另一种常用服务，不可或缺，在多方面发挥作用。每个企业都需要这些服务来各负其责，协同工作，一个都不能少。另外，作为企业网络的基础服务，DHCP 服务和 DNS 服务通常也是需要提供的。

本项目首先简要介绍服务器的基本工作原理、常用服务及使用的端口地址，然后以 Apache 服务器为核心，对 LAMP 应用平台的安装、配置、使用进行介绍。

## 能力目标

掌握 DHCP 服务的配置和使用。

掌握 DNS 服务的配置和使用。

熟练掌握 Web 服务器的配置和使用。

## 知识目标

- 了解服务器的工作原理。
- 了解常见的网络服务和端口。
- 掌握服务器软件的安装和管理的方法。
- 能够根据需要对服务器进行合理的配置。

# 任务一：理解服务器和服务器软件

在这一部分，我们要关注三个问题：服务器是什么？为什么要使用服务器？怎样为服务器选择要提供的服务？

## 知识储备

### 2.1 了解服务器

- 服务器也是计算机，PC 是通用计算机，服务器是专用计算机。
- 服务器是提供服务的计算机，通常需要安装服务器专用的操作系统。
- 服务器采用 RASUM 设计标准：可靠性、可用性、可维护性、易用性、可管理性。

#### 2.1.1 服务器是什么

要充分了解服务器的含义，我们需要从两个方面来进行解析。

从物理上看，服务器首先是一台计算机，由 CPU、内存、主板、硬盘等部件构成，就像我们熟悉的个人电脑(Personal Computer, PC)一样。与个人电脑的用途不同，服务器的设计目的是为海量用户提供全天候的网络服务，所以在稳定性、可靠性、安全性等方面有强大的优势，属于专用领域强化计算机，如图 2-1 所示。我们可以使用 PC 充当服务器，但是在专业领域，性能远远不如专业服务器优越。

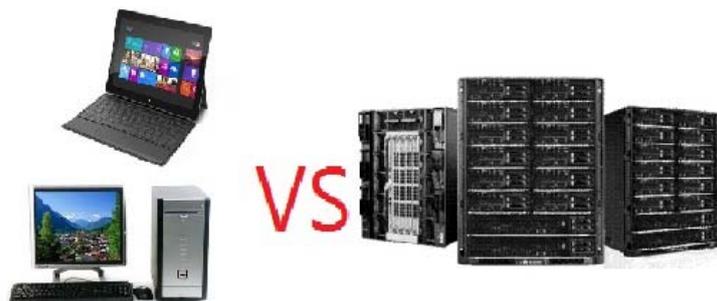


图 2-1 普通 PC 计算机和服务器



从功能上看，服务器就是提供服务的计算机。与个人电脑的家用娱乐目的不同，服务器就像卖商品的商场，而个人计算机的角色类似购买商品的顾客。在服务器上运行的功能软件，就是提供各种不同类型商品(服务)的软件了。

对于普通计算机而言，没有安装操作系统的计算机被称为“裸机”，只能识别执行二进制机器指令。想象一下面对外星人的感觉，不下命令外星人(计算机)什么都不会做；要下命令，你就得学会外星语言。普通人无法操作这样的计算机。

但安装了操作系统之后，通过用户接口，人们就可以操作计算机了。用户接口就像翻译官，把你的命令告诉计算机，让计算机干活；活干完了，再向你汇报任务的完成情况。为了让计算机完成更多的工作，在操作系统之上，我们安装各种专业化的软件来完成需要的功能，比如我们熟悉的文字处理软件、浏览器软件、媒体播放软件、网络聊天软件等。

服务器的工作原理和普通计算机没什么不同。在网络应用架构中，服务器主要应用于数据库和 Web 服务，而 PC 主要应用于桌面计算和网络终端，设计根本出发点的差异决定了服务器应该具备比 PC 更可靠的持续运行能力、更强大的存储能力和网络通信能力、更快捷的故障恢复功能和更广阔的扩展空间，同时，对数据相当敏感的应用还要求服务器提供数据备份功能。而 PC 在设计上则更加重视人机接口的易用性、图像和 3D 处理能力及其他多媒体性能。

由于服务器的功能倾向与 PC 完全不同，所以，虽然拥有相同的工作原理，类似的技术，但是看起来和使用起来差异巨大。

在服务器上，通常需要安装服务器专用的操作系统，例如我们学习的 CentOS。

## 2.1.2 服务器的五大设计标准

服务器需要向互联网用户提供 7×24 小时不间断的服务，常常几个月甚至几年不关机或重新启动。作为计算机，服务器的性能参数与 PC 类似，但是由于功能角色定位不同，因此，衡量服务器所采用的标准与 PC 差别很大。对于服务器来说，通常采用 RASUM 设计标准。

- R: Reliability(可靠性)。
- A: Availability(可用性)。
- S: Serviceability(可维护性)。
- U: Usability 易用性。
- M: Manageability(可管理性)。

### 1. 可靠性

可靠性是指定时间内系统正常工作的概率。增强可靠性可以帮助避免、检测和修复硬件故障。一个可靠性高的系统在发生故障时不应该默默地继续工作并交付结果。相反，它应该能自动检测错误，更好的情况是能修复错误。例如，通过重试操作修复间歇性错误，或者，针对无法改正的错误，隔离故障并报告给其他恢复机制(切换至冗余硬件)。可靠性

一般通过平均无故障时间(Mean Time Between Failure, MTBF)来衡量。

例如硬盘, 假如 MTBF 高达 120 万小时, 120 万小时约为 137 年, 这并不能理解成该硬盘每只均能工作 137 年不出故障(这不可能)。而是指该硬盘的平均年故障率约为 0.7%(1/137), 一年内, 平均 1000 只硬盘有 7 只会出故障。考虑到硬盘的销售量, 每年的故障硬盘数量其实也不少。

要知道, 电子产品的寿命一般都符合浴盆曲线, 如图 2-2 所示。可分为三个阶段。

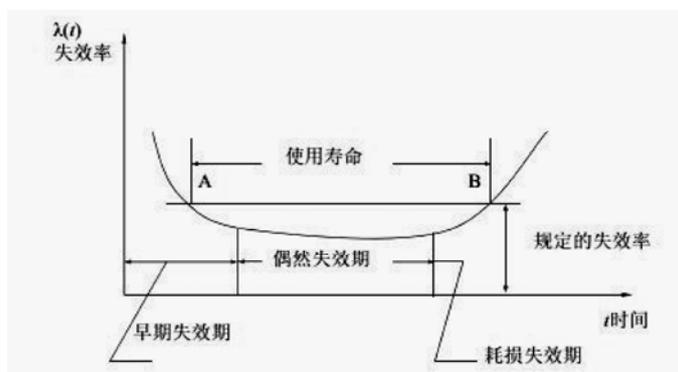


图 2-2 电子产品的浴盆曲线

(1) 早期失效期: 由于设计、原材料、生产等可能出现的原因而导致一个较高失效率的阶段, 也称失效率递减阶段。

(2) 偶然失效期: 这一阶段产品失效率近似一个常数, 只有随机失效(偶然失效)产生, MTBF 即要得到这一阶段(稳定期)的寿命。

(3) 耗损失效期: 硬件故障期, 产品这时已达到设计寿命, 进入报废阶段。

MTBF 是用来度量偶然失效期的, 所以, 数据看起来比我们想象的高是很正常的。

## 2. 可用性

可用性是指系统的有效可用运行时间, 代表系统的可用性程度。对于服务器而言, 一个非常重要的方面就是它的“可用性”, 即所选服务器能满足长期稳定工作的要求, 不能经常出问题。

因为服务器所面对的是整个网络的用户, 而不是单个用户, 在大中型企业中, 通常要求服务器是永不中断的。在一些特殊应用领域, 即使没有用户使用, 有些服务器也得不间断地工作, 因为它必须持续地为用户提供连接服务, 而不管是在上班, 还是下班, 也不管是工作日, 还是休息、节假日。这就是要求服务器必须具备极高的稳定性的根本原因。

可用性的度量方式是工作时间比总时间, 一般用百分比来表示, 例如, 我们常说的 99.999%(5 个 9)。

通过表 2-1 中的计算可以看出, 一个 9 和两个 9 分别表示一年时间内业务可能中断的时间是 36.5 天、3.65 天, 这种级别的可靠性, 企业一般是无法接受的; 而 6 个 9 则表示一年内业务中断时间最多是 31 秒, 这个级别的可靠性并非实现不了, 但是要真正做到从 5 个 9

到 6 个 9 的可靠性提升的话，需要付出非常大的成本，性价比不高，所以评价可用性都只谈 3~5 个 9。

表 2-1 可用性标准

1 个 9	$(1-90\%) \times 365 = 36.5$ 天
2 个 9	$(1-99\%) \times 365 = 3.65$ 天
3 个 9	$(1-99.9\%) \times 365 \times 24 = 8.76$ 小时，表示该软件系统在连续运行 1 年时间里最多可能的业务中断时间是 8.76 小时(526 分钟)
4 个 9	$(1-99.99\%) \times 365 \times 24 = 0.876$ 小时=52.6 分钟，表示该软件系统在连续运行 1 年时间里最多可能的业务中断时间是 52.6 分钟
5 个 9	$(1-99.999\%) \times 365 \times 24 \times 60 = 5.26$ 分钟，表示该软件系统在连续运行 1 年时间里最多可能的业务中断时间是 5.26 分钟
6 个 9	$(1-99.9999\%) \times 365 \times 24 \times 60 \times 60 = 31$ 秒(0.526 分钟)

理想的情况下，服务器要 7×24 小时不间断地工作。对于这些服务器来说，也许真正工作开机的次数只有一次，那就是它刚买回全面安装配置好后投入正式使用的那一次，此后，它不间断地工作，一直到彻底报废。如果动不动就出毛病，则网络不可能保持长久正常运作。为了确保服务器具有高的可用性，除了要求各配件质量过关外，还可采取必要的技术和配置措施，如硬件冗余、热插拔、在线诊断等。

我们经常会听到高可用性的系统(3~5 个 9)，这样的系统不仅在一年中可能只有几分钟的停机时间。而且，高可用系统通常可以在发生故障后继续运行，其方式可能是禁用故障部分，虽然系统性能可能会有一定降低，但保证了整个系统的可用性。

冗余和热插拔对于高可用性系统基本是必备的技术。硬件冗余技术指对重要部件配置两个以上，这可以确保当一个设备故障时，还有其他设备能够继续提供服务，保证服务不间断；热插拔技术指在不断电关机的情况下，替换服务器支持热插拔的部件。以防止此冗余部件全部损坏，造成系统瘫痪。

在有些情况下，比如银行和证券的交易系统，系统的高可用性是相当有价值的。

### 3. 可维护性

可维护性(Serviceability)是指系统发生故障时，检查和维修的便利程度。服务器需要不间断地持续工作，但再好的产品都有可能出现故障，拿人们常说的一句话来说就是：不是不知道它可能坏，而是不知道它何时坏。服务器虽然在稳定性、可靠性方面比普通计算机好得多，也应有必要的避免出错的措施，以及时发现问题，而且出了故障也能及时得到维护。这不仅可减少服务器出错的机会，同时还可大大提高服务器维护的效率。

系统的修复时间越长，那么其可用性必然随之降低。可维护性包括系统出现故障时快速诊断故障的难易程度。早期的报错检查能有效减少或避免系统宕机时间。例如，一些企业级系统发生故障时，可在无须人工干预的情况下自动调用服务中心，让设备厂商知晓故障并进行诊断、分析和解决。

#### 4. 易使用性

易使用性(Usability)是指人类对系统的易学和易用程度。易使用性设计的重点在于让系统或产品的设计能够符合使用者的习惯与需求。服务器的易使用性,主要体现在服务器是不是容易操作、用户导航系统是不是完善、机箱设计是不是人性化、有没有关键恢复功能、是否有操作系统备份,以及有没有足够的培训支持等方面。

对于服务器来说,它的用户主要是系统管理员。在服务器设计中,我们常见到的免工具拆卸设计;可以热插拔的电源模块、硬盘模块等;前端面板的可在绿色、琥珀色和红色之间变换的LED系统状态标识灯等,这些都是服务器在易用性方面的设计和实现。

服务器的功能相对于PC来说复杂许多,不仅指其硬件配置,更多的是指其软件系统配置。服务器要实现如此多的功能,没有全面的软件支持是无法想象的。但是软件系统一多,又可能造成服务器的使用性能下降,增大管理难度。

软件的易使用性也是非常重要的一个衡量标准,因为大多数软件都是人在使用。

易用性通常包含下列元素:可学习性(Learnability)、效率(Efficiency)、可记忆性(Memorability)、很少出现严重错误(Errors)和满意度(Satisfaction)。

#### 5. 易管理性

易管理性(Manageability)是指系统在运行过程中是否便于管理的程度。良好的易管理性可以有效地减少系统的管理和维护成本。

事实上,高素质的管理者严重稀缺,很难获得。中小企业通常会考虑把管理任务外包给专业公司,因为很难招聘到合适的人才来管理自己的系统。为了降低管理难度,服务器的易管理性是很重要的。比如,服务器中通常所设计的可通过远程管理来实现服务器的远程管理,通过智能平台管理接口来实现远程对服务器的物理健康特征的监控,包括温度、电压、风扇工作状态、电源状态等。

服务器的易管理性还体现在服务器有没有智能管理系统,有没有自动报警功能,是不是有独立于系统的管理系统等方面。有了方便的工具,管理员才能轻松管理,高效工作。

## 2.2 服务器的简单分类

### 2.2.1 从外形上分类服务器

虽然服务器也是计算机,但看起来和我们熟悉的PC感觉差异还是很大的。从外形上分,服务器可以分为机架式服务器、刀片式服务器、塔式服务器、机柜式服务器等。

#### 1. 机架式服务器

机架式服务器(如图2-3所示)安装在标准的19英寸机柜里面。机架式服务器的外形看起来扁而长,看起来类似交换机。



图 2-3 机架式服务器

相比不少企业的自建机房，大型专业信息中心更加正规和专业化，会统一部署和管理大量的服务器资源。大型信息中心通常设有严密的保安措施、良好的温湿度控制系统、多重备份的供电系统，机房的总体造价十分昂贵。对于专用机房来说，如何在有限的空间内部署更多的服务器，直接关系到企业的服务成本。

对于专业机房，选择服务器时首先要考虑服务器的体积、功耗、发热量等物理参数，通常会选用机架式服务器。

机架式服务器也有多种规格，例如 1U(4.45cm 高)、2U、4U、6U、8U 等。通常 1U 的机架式服务器最节省空间，但性能和可扩展性较差，适合一些业务相对固定的使用领域。4U 以上的产品性能较高，可扩展性好，一般支持 4 个以上的高性能处理器和大量的标准热插拔部件，管理也十分方便，厂商通常会提供相应的管理和监控工具，适合大访问量的关键应用，但体积较大，空间利用率不高。

## 2. 刀片式服务器

刀片式服务器(如图 2-4 所示)是指在标准高度的机架式机箱内可插装多个卡式的服务器单元，实现高可用和高密度。每一块“刀片”实际上就是一块系统主板。它们可以通过“板载”硬盘启动自己的操作系统，类似于一个个独立的服务器，在这种模式下，每一块母板运行自己的系统，服务于指定的不同用户群，相互之间没有关联。

相比机架式服务器和机柜式服务器，单片母板的性能较低。不过，管理员可以使用系统软件，将这些母板集成为一个服务器集群。在集群模式下，所有的母板可以连接起来提供高速的网络环境，并同时共享资源，为相同的用户群服务。通过在集群中插入新的“刀片”，就可以提高整体性能。而由于每块“刀片”都是热插拔的，所以，系统可以轻松地进行替换，并且将维护时间减少到最小。

## 3. 塔式服务器

塔式服务器(如图 2-5 所示)应该是大家最容易理解的一种服务器结构类型，因为它的外形以及结构都跟我们平时使用的立式 PC 差不多，当然，由于服务器的主板扩展性较强、插槽也多出一些，所以个头比普通主板大一些，因此塔式服务器的主机机箱也比标准的 PC 机箱要大，一般都会预留足够的内部空间，以便日后进行硬盘和电源的冗余扩展。

由于塔式服务器的机箱比较大，服务器的配置也可以很高，冗余扩展更可以很齐备，所以它的应用范围非常广，应该说使用率最高的一种服务器就是塔式服务器。我们平时常说的通用服务器一般都是塔式服务器，它可以集多种常见的服务应



图 2-4 刀片式服务器



图 2-5 塔式服务器

用于一身，不管是速度应用还是存储应用，都可以使用塔式服务器来解决。

#### 4. 机柜式服务器

在一些高档企业服务器中，由于内部结构复杂，内部设备较多，有的还具有许多不同的设备单元或几个服务器都放在一个机柜中，这种服务器就是机柜式服务器，如图 2-6 所示。机柜式通常由机架式、刀片式服务器再加上其他设备组合而成。



图 2-6 机柜式服务器

### 2.2.2 从应用规模分类

按应用规模分类，是服务器最为普遍的一种划分方法，它主要根据企业应用规模来进行服务器的划分。按这种划分方法，服务器可分为：入门级服务器、工作组级服务器、部门级服务器、企业级服务器。

#### 1. 入门级服务器(应用规模 $\leq 20$ )

这类服务器是最基础的一类服务器，也是最低档的服务器。许多入门级服务器与 PC 的配置差不多，或者就是使用高性能的品牌 PC。这类服务器所包含的服务器特性并不是很多，通常只具备以下几方面的特性。

- (1) 有一些基本硬件的冗余，如硬盘、电源、风扇等。
- (2) 通常采用 SCSI 接口硬盘，也有采用 SATA 串行接口的。
- (3) 部分部件支持热插拔，如硬盘和内存等。
- (4) 通常只有一个 CPU。
- (5) 内存容量最大支持 16GB。

图 2-7 是一家酒店的网络拓扑图，由于业务计算机数量只有几台，业务相对单一，应用规模也小，因此业务平台使用了入门级服务器(左上区域)，图示中心区域是酒店无线网络控制器，作为酒店网络的中心设备，向下通过交换机连接业务计算机以及无线接入设备，提供点餐、结算等服务。右上区域是网络接入，提供上网功能。

入门级服务器所连的终端比较有限(通常为 20 台左右)，在稳定性、可扩展性以及容错冗余性能方面较差，仅适用于没有大型数据库数据交换，日常工作网络流量不大，无需长期不间断开机的小型企业。

#### 2. 工作组级服务器(应用规模 $\leq 50$ )

工作组级服务器的应用规模，通常是连接一个工作组(50 台左右)规模的用户。因为网络规模较小，服务器的稳定性要求也不算高，在其他性能方面的要求也相应要低一些。工作组服务器具有以下几方面的主要特点。

- (1) 通常仅支持单或双 CPU 结构的应用服务器。
- (2) 可支持大容量的 ECC 内存和增强服务器管理功能的 SM 总线。
- (3) 功能较全面、可管理性强，且易于维护。

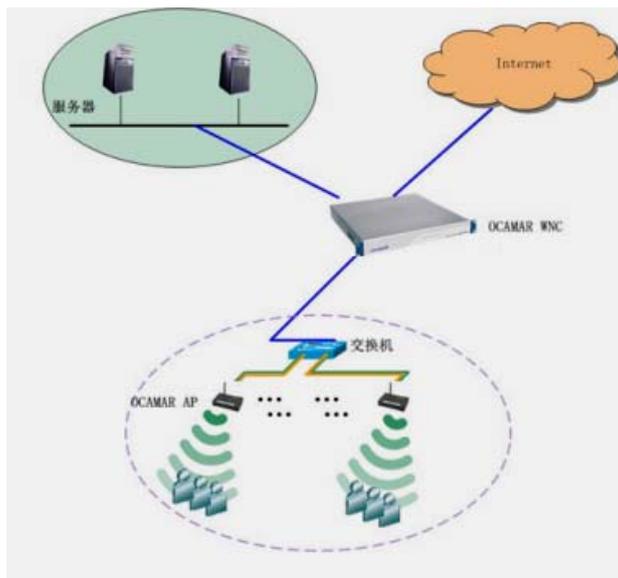


图 2-7 入门级网络拓扑

(4) 采用 Intel 服务器 CPU 和 Windows 网络操作系统，但也有一部分是采用 Linux 系列操作系统的。

(5) 可以满足中小型网络用户的数据处理、文件共享、Internet 接入及简单数据库应用的需求。

图 2-8 是一家企业的网络拓扑图，企业本身有几十台员工计算机，分属各个部门，图例右侧是工作电脑区域，由两台交换机进行联网；由于有多种业务需求，所以配置了多台工作组级服务器，图例的左上部分就是服务器区。左下连接互联网，提供上网功能。

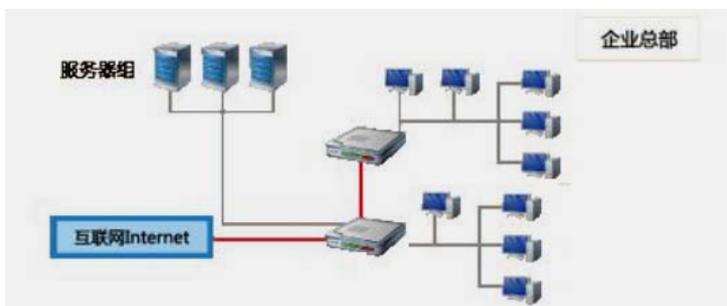


图 2-8 工作组级网络拓扑

工作组级服务器较入门级服务器来说性能有所提高，功能有所增强，有一定的可扩展性，但容错和冗余性能仍不完善，也不能满足大型数据库系统的应用，但价格也比前者贵许多，一般相当于 2~3 台高性能的 PC 品牌机总价。

### 3. 部门级服务器(应用规模≤100)

这类服务器是属于中档服务器之列，一般都是支持双 CPU 以上的对称处理器结构，

具备比较完全的硬件配置，如磁盘阵列等。

部门级服务器的最大特点就是，除了具有工作组服务器的全部服务器特点外，还集成了大量的监测及管理电路，具有全面的服务器管理能力，可监测如温度、电压、风扇、机箱等状态参数，结合标准服务器管理软件，使管理人员及时了解服务器的工作状况。

同时，大多数部门级服务器具有优良的系统扩展性，可让用户在业务量迅速增大时能够及时在线升级系统，充分保护了用户的投资。它是企业网络中分散的各基层数据采集单位与最高层的数据中心保持顺利连通的必要环节，一般为中型企业的首选，也可用于金融、邮电等行业。

部门级服务器一般采用 IBM、SUN 和 HP 各自开发的 CPU 芯片，这类芯片一般是 RISC(精简指令计算机)结构，所采用的操作系统一般是 Unix 系列操作系统，Linux 也在部门级服务器中得到了广泛应用。

图 2-9 是一家中等规模的网络公司，有接近百台员工计算机，右下区域是公司的业务区，由于应用规模较大，计算机数量较多，所以网络拓扑由核心层和接入层构建了两级体系结构，实现网络连接与网络管理。右上区域是服务器区，公司的核心业务很重要，所以采用了部门级服务器，并构建了双机热备，以备万一服务器出现问题，不会导致业务中断出错，业务数据量非常大，所以选择了外置大存储设备。左上区域提供互联网接入。

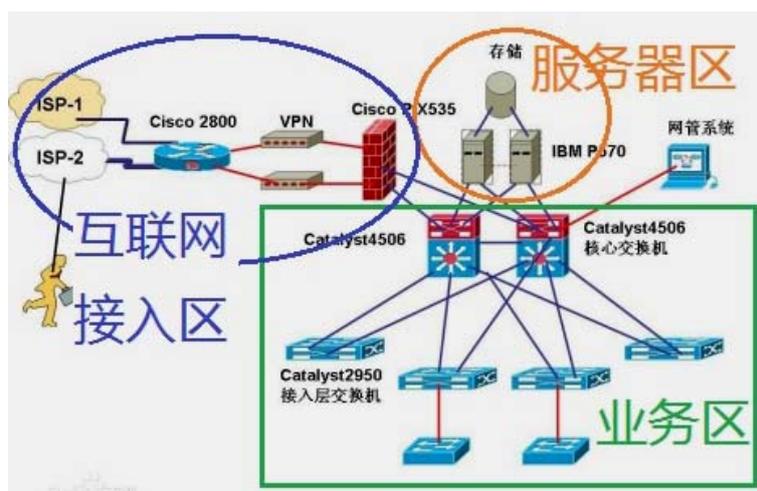


图 2-9 部门级网络拓扑

部门级服务器可连接 100 个左右的计算机用户、适用于对处理速度和系统可靠性高一些的中小型企业网络，其硬件配置相对较高，其可靠性比工作组级服务器要高一些，当然其价格也较高(通常为 5 台左右高性能 PC 机价格总和)。由于这类服务器需要安装比较多的部件，所以机箱通常较大，有的服务器会采用机柜式。

#### 4. 企业级服务器(应用规模≤?)

企业级服务器属于高档服务器行列，一般，企业级服务器最起码是采用 4 个以上 CPU 的对称处理器结构，有的高达几十个。另外，一般还具有独立的双 PCI 通道和内存扩展板

设计，具有高内存带宽、大容量热插拔硬盘和热插拔电源、超强的数据处理能力和群集性能等。

企业级服务器的机箱就更大了，一般为机柜式的，有的还由几个机柜来组成，像大型机一样。企业级服务器产品除了具有部门级服务器全部服务器特性外，最大的特点就是它还具有高度的容错能力、优良的扩展性能、故障预报警功能、在线诊断和 RAM、PCI、CPU 等具有热插拔性能。有的企业级服务器还引入了大型计算机的许多优良特性。这类服务器所采用的芯片也都是几大服务器开发、生产厂商自己开发的独有 CPU 芯片，所采用的操作系统一般也是 Unix(Solaris)或 Linux。

图 2-10 是一家大学的网络拓扑图。可以看出，学校采用了核心层→汇聚层→接入层的三级网络体系结构，用户计算机数量几千台，应用规模非常大，而且大学业务需求多种多样，需要大量的服务器，处理多种类别、海量的数据和业务，所以，应该选择企业级服务器支撑重要的业务，还有大量的中低端服务器作为补充。此图并没有标注服务器区域和互联网接入区域，但看了前面的几张简图后，我们也可以类比感受。

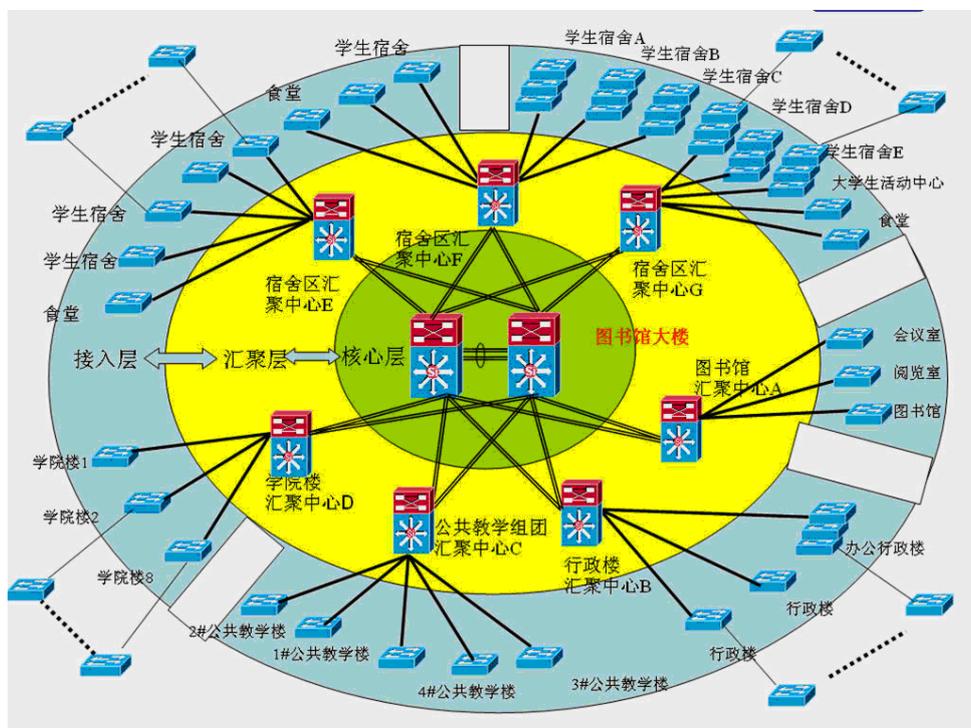


图 2-10 企业级网络拓扑

企业级服务器适合运行于需要处理大量数据、高处理速度和对可靠性要求极高的金融、证券、交通、邮电、通信或大型企业。企业级服务器用于应用规模在数百台以上、对处理速度和数据安全要求非常高的大型网络。企业级服务器的硬件配置最高，系统可靠性也最强。

## 2.3 常见服务与对应端口

要提供什么样的服务，就需要什么功能的服务器软件。

DHCP(动态主机分配协议)服务自动管理 IP 地址的分配和回收。

域名服务(Domain Name Service, DNS)把 IP 地址和域名关联起来，我们才可以正常使用域名访问服务器。

Web 服务就是平常说的网站服务。FTP 服务用于 Internet 上的文件的双向传输。电子邮件服务可以收发电子邮件。每个服务都有约定的端口。

服务器上运行着很多种服务，这些系统如果和谐共存，协同工作呢？

类比现实，似乎也不难理解。如果我们去商场转转，想买日常用品，就去超市区；想买衣物，就去衣物区；想吃饭，就去餐厅。我们所需要的，就是方便的指示牌，告诉我们要去的地方在哪里。

端口地址就是服务在服务器中的标识，有了它，我们就能找到服务，享受服务了。服务的端口地址是有默认约定的，虽然我们可以进行改动，但是改了，用户就可能找不到这个服务，因为他不知道改成了哪个端口，这可能会造成一些麻烦。

### 2.3.1 基础服务

#### 1. IP 地址和域名

服务器的设计目的就是为了向互联网用户提供服务，要提供什么样的服务，就需要什么功能的服务器软件。要接入网络，首先必须拥有合法的 IP 地址，这样网络用户才可以从网络找到服务器。

IP 地址用来作为网络节点(用户 PC、服务器以及所有的联网设备)的唯一标识，就像公民身份证一样。它是计算机或者其他网络设备在网络上的根本性的基础标识。

IP 地址是 32 位二进制数字，使用时用点分十进制来表示，用 3 个小数点把 32 位二进制数分割成 4 部分，每部分 8 位，然后把 8 位二进制数用十进制表示。这样，我们看到的 IP 地址就是由三个小数点分成的四个数字，每个数字最小是 0，最大是 255。

例如点分十进制的 IP 地址 114.114.114.114。0 是 8 位二进制数 00000000 的十进制表示，也是 8 位二进制数的最小值；255 是 8 位二进制数 11111111 的十进制表示，也是 8 位二进制数的最大值。

32 位 IP 地址由两部分构成，网络地址和主机地址。网络地址部分是标识属于哪一个网络，主机地址部分是标识网络中的哪一台主机。

就像身份证号和人名的关系，IP 地址是一串数字，记忆起来很不友好。因此，服务器也会起个名字，见文知意，比较友好，也容易记忆。在互联网中，这个名字被称为“域名”(Domain Name)，域名也由两部分构成，主机名+所属域。所属域标识属于哪一个组织部门，主机名标识哪一台服务器，例如 www.sohu.com，其中 sohu.com 是所属域，www 是



服务器的标识名称。

## 2. DHCP 与 DNS

用户的 IP 地址通常是动态获取的，每次上网都在变，但是服务器的 IP 是固定不变的。当用户知道服务器的 IP 后，就可以通过网络来访问服务器了，就如同拿着地址来找人一样。

互联网中有百万以上的服务器，有十亿以上的计算机，每个设备都需要一个 IP。

对于每个企业部门，少则几十台主机，多则几百几千，ISP 进行商业接入，客户主机数量更是以万计数，对这么多 IP 进行人工管理，效率是很低的，这时候我们需要一个服务来自动管理 IP 地址的分配和回收，这就是 DHCP(动态主机分配协议)服务。

通过 DHCP 服务，每台主机联网时，从 DHCP 服务器申请一个 IP 设置使用；使用完毕后，IP 设置可以回收，再提供给其他用户使用。只需要配置好 DHCP 服务，就再也不用操心 IP 设置的问题了。

访问服务器需要的是 IP 地址，用户平常使用的是域名，所以需要一种服务把 IP 地址和域名关联起来，这就是域名服务(Domain Name Service)。通过域名服务，我们才可以正常使用域名访问服务器。每次访问服务器时，DNS 服务会帮助我们吧域名解析成为 IP 地址，然后用 IP 地址去访问服务器。

### 2.3.2 常用服务

#### 1. Web 服务

Web 服务就是平常我们说的网站服务，是最为流行的网络服务，为我们提供网站发布运行的基础平台。我们制作的网站页面就像店铺里面的商品，把它们放到店铺里，就可以进行销售了。Web 服务就像是店铺，用户可以自由访问里面的网页。

Web 服务是“客户机/服务器”工作模式，用户使用浏览器作为客户端来访问服务器上的网站，这种模式也常常称为“浏览器/服务器”工作模式。

要提供 Web 服务，需要安装 Web 服务器软件。Linux 环境下最流行的 Web 服务器软件是 Apache Web Server。

#### 2. FTP 服务

文件传输协议(File Transfer Protocol, FTP)用于 Internet 上的文件的双向传输。支持 FTP 协议的服务器就是 FTP 服务器。

与大多数 Internet 服务一样，FTP 服务也是一个客户机/服务器系统。用户通过一个支持 FTP 协议的客户机程序，连接到在远程主机上的 FTP 服务器程序。用户通过客户机程序向服务器程序发出命令，服务器程序执行用户所发出的命令，并将执行的结果返回到客户机。比如说，用户发出一条命令，要求服务器向用户传送某一个文件的一份拷贝，服务器会响应这条命令，将指定文件送到用户的机器上。客户机程序代表用户接收到这个文件，将其存放在用户目录中。

### 3. 电子邮件服务

电子邮件在 Internet 上发送和接收的原理可以很形象地用我们日常生活中邮寄信件或包裹来形容：当我们要寄一个包裹时，我们首先要找到任何一个有这项业务的邮局或者快递公司，在填写完收件人姓名、地址等之后，邮件就寄出了，等到了收件人所在地的邮局或者快递公司，收件人就可以在任何自己适合的时间接收信件或包裹。同样地，当我们发送电子邮件时，这封邮件是由发信人的邮件服务器发出，并根据收信人的地址判断对方的邮件接收服务器，而将这封信发送到该服务器上，收信人要收取邮件时，可以随时访问自己邮件服务器上的信箱即可。

#### 2.3.3 服务与端口地址

在服务器上运行着多种服务，这些服务同时运行，各负其责，协作完成系统功能。当一个请求信息发送到服务器时，怎样识别信息是送给哪一个服务的呢？

服务器就像一座办公楼，里面有很多的房间可以进入，每个房间都有自己的编号。不同的服务也会有自己的编号，称为“端口地址”。网络服务运行时绑定端口，当用户发送信息时，标明是发送给哪个端口，系统会自动转送给对应的服务。

控制信息发送和接收的有两种传输协议：传输控制协议(Transmission Control Protocol, TCP)和用户数据报协议(User Datagram Protocol, UDP)，相应地，端口也有两种，TCP 端口和 UDP 端口，每种端口都在 0~65535 之间编号。

TCP 端口，就是使用传输控制协议进行传输时使用的端口地址，需要在客户端和服务端之间建立可信任连接，这样可以提供可靠的数据传输。常见的包括 FTP 服务的 21 端口，Telnet 服务的 23 端口，SMTP 服务的 25 端口，以及 HTTP 服务的 80 端口等。可以看出，远距离、大量数据传输、传输质量难以保证的情况适合使用 TCP 协议传输。TCP 协议多用于互联网传输，因为距离远，传输质量不可控，大量数据传输出错几率高。

UDP 端口，就是用户数据报协议端口，不需要在客户端和服务端之间建立连接，传输可靠性得不到保障，但是传输开销较小。常见的有 DNS 服务的 53 端口，SNMP(简单网络管理协议)服务的 161 端口等。UDP 协议多用于局域网内，因为网络传输质量好，不易出错，此时 UDP 的简单和低开销可以提高传输效率和性能。

常见的服务和端口如表 2-2 所示。

表 2-2 常见服务和端口

TCP 端口	服 务	说 明
20	FTP-DATA	文件传输协议 - 数据(File Transfer Protocol-Data)
21	FTP	文件传输协议 - 控制(FTP-Control)
22	SSH	SSH 远程登录协议(SSH Remote Login Control)
23	TELNET	Telnet 远程登录

续表

TCP 端口	服 务	说 明
25	SMTP	简单邮件传输协议(Simple Mail Transfer Protocol)
80	WWW	Web 服务器(World Wide Web)
110	POP3	E-mail 邮局协议版本 3(Post Office Protocol ver 3)
UDP 端口	服 务	说 明
53	DNS	域名服务(Domain Name System)
68	DHCP	动态主机配置协议
69	TFTP	简单文件传输协议
161	SNMP	简单网络管理协议

## 任务实践

## 2.4 软件管理工具 yum 的使用

### 2.4.1 yum 简介

在 Linux 环境下，有海量的软件支持。基本上，这个世界上曾存在过的各种功能的软件，只要还没过时，都可以在 Linux 下找到。为了管理海量的软件，Linux 形成了一个系列的文件管理方法。

把相关功能的文件聚合成组，打包成一个软件包；相关软件包聚合在一起，就形成了一个完整的功能软件；把相关的功能软件聚合在一起，就形成了一个功能软件集合，把很多功能软件集合都放在一起，就形成了一个软件仓库。

一个软件按照功能划分，通常会分成若干个软件包，当安装一个软件包时，需要把它所有依赖的软件包先进行安装，否则自己无法运行。之后才可以安装自己。有时候，依赖的软件包又会需要其他的支撑包；有时候，要安装的软件包运行所需要的软件包不存在；有时候，库文件版本不对也无法安装运行。

很长时间以来，依赖和软件版本把 Linux 用户折磨得焦头烂额，幸好，现在有了很好的解决方案。

现代 Linux 的软件管理的理念是使用一个中心仓库(repository)来管理一部分甚至一个完整发行版(distribution)的应用程序间的相互关系，根据分析出来的软件依赖关系进行相关的升级、安装、删除等操作，减少 Linux 用户一直头痛的依赖(dependencies)的问题。

yum 是现在 Linux 下最流行的软件管理工具之一，也是 CentOS 7 的默认软件包管理器。yum 可以自动化地升级、安装和移除 rpm 包，收集 rpm 包的相关信息，检查依赖性并自动提示用户解决，这就解决了系统软件管理中遇到的大问题。

常用的 yum 操作命令如表 2-3 所示。

表 2-3 yum 的常用命令

命令选项	功能描述
yum search 关键字	能够在已启用的软件包仓库中，对所有软件包的名称、描述和概述进行搜索
yum list	列出要查找的包，没有指定参数时列出所有包
yum grouplist	列出所有软件包组
yum repolist	列出所有启用的软件仓库的 ID，名称及其包含的软件包的数量
yum info 软件包	命令可查看一个或多个软件包的信息
yum provides 要查的命令	查看命令所在的软件包
yum group remove 程序组	卸载程序组
yum list installed	列出所有已安装的软件包
yum localinstall ~	从硬盘安装 rpm 包并使用 yum 解决依赖

例 1，查找 net-tools 包：

```
#yum search net-tools
#yum list |grep net-tools
```

例 2，查找 nmap 命令所在的包：

```
#yum provides nmap
```

例 3，查看 net-tools 包的信息：

```
#yum info net-tools
```

例 4，安装 net-tools 包：

```
#yum install net-tools
```

例 5，卸载 net-tools 包：

```
#yum remove net-tools
```

## 2.4.2 yum 配置

yum 可以检测软件间的依赖性。发布的软件放到 yum 服务器，通过分析这些软件的依赖关系，将每个软件相关性记录成列表。当客户端有软件安装请求时，yum 客户端在 yum 服务器上下载记录列表，然后通过列表信息与本机已安装软件数据对比，明确软件的依赖关系，从而能够判断出哪些软件需要安装。

列表信息保存在 yum 客户端的/var/cache/yum 中，每次 yum 启动都会通过校验码与 yum 服务器同步更新列表信息。

使用 yum 需要有 yum 软件仓库(yum repositories)，用来存放软件列表信息和软件包。yum 仓库可以是 HTTP 站点、FTP 站点、本地站点。

yum 仓库的路径格式如表 2-4 所示。

表 2-4 yum repo 的路径

HTTP 站点	ftp://主机地址或域名/PATH/TO/REPO
FTP 站点	http://主机地址或域名/PATH/TO/REPO
本地站点	file:///PATH/TO/REPO (注意是三个/)

yum 的全局配置文件是/etc/yum.conf，存放对所有仓库都适用的配置信息。

通常，我们会为每一个软件仓库或者相关的几个仓库单独设置一个配置文件，名称为“\*\*\*.repo”，放置在/etc/yum.repos.d/目录下。

要设置仓库文件，需要指定几项关键属性，如表 2-5 所示。

表 2-5 repo 文件的设置

属性名	功能描述
[base]	用于区别各个不同的 repository，唯一性
name=	对 repository 的描述
mirrorlist=	指定一个镜像服务器的地址列表
enabled=1	表示这个 repo 中定义的源是启用的，0 为禁用
gpgcheck=1	启用 gpg 的校验，确定 rpm 包的来源安全和完整性，0 为禁止
gpgkey=文件	定义用于校验的 gpg 密钥
cost=	cost 为开销，默认是 1000，开销越大，使用优先级越低

使用 cat 命令查看已有的 repo 文件：

```
#cat CentOS-Base.repo
```

repo 文件的格式如图 2-11 所示。

```
[base]
name=CentOS-$releasever - Base
mirrorlist=http://mirrorlist.centos.org/?release=$relea
#baseurl=http://mirror.centos.org/centos/$releasever/os
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-7
```

图 2-11 repo 文件的格式

### 2.4.3 使用光盘作为本地库

我们使用 yum 管理自己的软件系统，当 CentOS 7 安装好后，如果使用原始仓库的话，因为仓库在国外，速度会比较慢，所以通常需要添加国内 yum 仓库，也可以直接使用安装盘建立本地仓库。

为了方便安装软件，可以用安装光盘，来建立本地仓库。建立此仓库的目的是一是本地安装远远快于网络安装，目的二是解决软件包安装时的依赖问题。

首先，需要把光盘挂载至某目录下，或者把光盘文件复制到磁盘某目录下，这样就省去挂载的步骤了。

接下来修改配置，添加新仓库的定义文件，在文件中使用 `file:///path/to/mount` 指明访问路径即可。新仓库设定完成后，检查是否配置成功。如果成功的话，接下来就可以来安装一个软件包，测试新的软件仓库是否正常工作了。

### (1) 挂载光盘。

把光驱挂载到指定目录，如果目录还不存在，可以使用 `mkdir` 命令创建。光盘必须已经插入光驱，在虚拟机里，ISO 文件应该已经挂载的虚拟光驱里。

```
#mkdir /mnt/localiso
#mount -r /dev/cdrom /mnt/localiso/
#ls /mnt/localiso
```

这样配置每次重新启动都要重新挂载，建议在 `/etc/fstab` 文件中添加一行挂载内容，这样，每次启动，系统会自动挂载光盘。或者把光盘复制到硬盘上也可以。

### (2) 定义仓库。

`yum` 的总配置文件是 `/etc/yum.conf`，可以新建一个配置文件放在 `/etc/yum.repos.d/` 目录下，此目录下的仓库定义会自动识别加载。

```
#cd /etc/yum.repos.d/
#vim /etc/yum.repos.d/centos7-ISO.repo
```

把以下内容输入文件：

```
[centos7-ISO]
name=centos-local-iso
baseurl=file:///mnt/localiso
enabled=1
gpgcheck=0
cost=100
```

`[centos7-ISO]` 是仓库的名称，要保证唯一；`name` 设置描述信息；`baseurl` 设定仓库存放的位置；`enable` 设置为 1，启用此 `repo` 仓库；`gpgcheck` 设置为 0，不进行 `gpg` 校验，省事；`cost` 设置为 100，这样可以优先使用此仓库。

### (3) 查看可用 repository，检查是否配置成功。

执行命令查看配置好已启用的仓库，如图 2-12 所示。

```
#yum repolist enabled
```

```
repo id                               repo name
!centos7-ISO                          centos-local-iso
!base/7/x86_64                         CentOS-7 - Base
!extras/7/x86_64                       CentOS-7 - Extras
!updates/7/x86_64                      CentOS-7 - Updates
repolist: 14 291
```

图 2-12 查看已启用的 repo 仓库

可以看到 `Centos7-ISO` 名称前面有感叹号，说明 `centos7-ISO` 仓库启用成功。



(4) 使用 yum 命令测试软件安装。

执行命令：

```
#yum list
#yum install net-tools
```

如果软件包能快速安装成功，那么本地 yum 就可以用了。

## 任务二：配置 DNS 和 DHCP 服务器

在这一部分内容中，我们要关注三个问题：DNS 服务器和 DHCP 服务器是什么？为什么要使用 DNS 和 DHCP 服务器？怎样配置和管理 DNS 和 DHCP 服务器？

### 知识储备

## 2.5 DNS 服务器和 DHCP 服务器

DHCP 服务和 DNS 都是网络的基础服务，掌握了这些服务，就可以解决对应的具体问题。灵活使用掌握的技术，可以高效地完成管理任务。

### 2.5.1 IP 地址和子网掩码

IP 地址是 32 位二进制数据，通常以十进制表示，并以“.”分隔。IP 的点分十进制表示法如图 2-13 所示。IP 地址是一种逻辑地址，用来标识网络中的一个主机，IP 有唯一性，即每台机器的 IP 在全世界是唯一的。

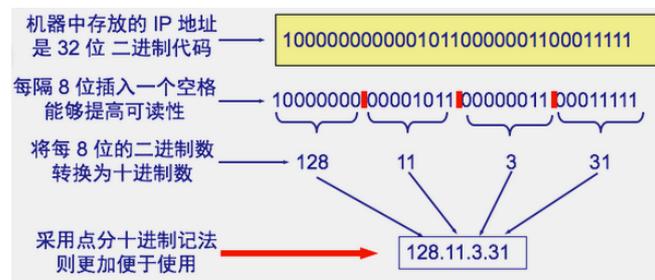


图 2-13 点分十进制表示法

互联网是由许多小型网络构成的，每个网络上都有许多主机，这样便构成了一个有层次的结构。IP 地址在设计时就考虑到地址分配的层次特点，将每个 IP 地址都分割成网络地址和主机地址两部分，以便于 IP 地址的寻址操作。

IP 地址的网络地址和主机地址各是多少位呢？如果不指定，就不知道哪些位是网络地址、哪些是主机地址，这就需要通过子网掩码来实现。

什么是子网掩码？子网掩码不能单独存在，它必须结合 IP 地址一起使用。子网掩码只有一个作用，就是将某个 IP 地址划分成网络地址和主机地址两部分。子网掩码的设定必须遵循一定的规则。与 IP 地址相对应，网络位用二进制数字 1 表示；主机位用二进制数字 0 表示。IP 地址和子网掩码如表 2-6 所示。

表 2-6 IP 地址和子网掩码

	字节一	字节二	字节三	字节四
子网掩码	11111111	11111111	11111111	00000000
IP 地址	11000000	10101000	00000001	00000001
点分十进制	192	168	1	1
地址划分	网络地址			主机地址

书写 IP 设置信息时，IP 地址和子网掩码通常一起书写。

例如：192.168.125.1/255.255.255.0 或者 192.168.125.1/24。

这两种写法意思是一样的，前面是 IP 地址，后面的 255.255.255.0，转成二进制，255 就是二进制的 11111111(八个 1)，三个 255 就意味着前面  $8 \times 3 = 24$  位都是 1，而子网掩码位为 1 表示 IP 地址的对应位是网络地址位，剩下的  $32 - 24 = 8$  位就是主机地址了。第二种写法看起来比较友好，“/24”表示前 24 位是网络地址，后面的是主机地址。

## 2.5.2 默认网关

网关是一个网络通向其他网络的出口地址。两个网络即使连接在同一台交换机上，也不能直接通信，必须通过网关转发。

有了 IP 地址和子网掩码，我们就可以计算出来网络地址。比如 192.168.125.1/24，前面三个字节段是网络地址位，把主机地址位置为全 0 后，得到网络地址 192.168.125.0/24，这就是我们需要的网络地址。

当 A 主机向 B 主机发送信息时，A 主机会计算自己的网络地址和对方的网络地址是否在同一个网络，如果网络地址相同，那么就直接发送；如果网络地址不同，那么就发送到网关，由网关通过路由机制转发到目的主机。默认网关如图 2-14 所示。因此，只有设置好网关的 IP 地址，才能实现不同网络之间的相互通信。

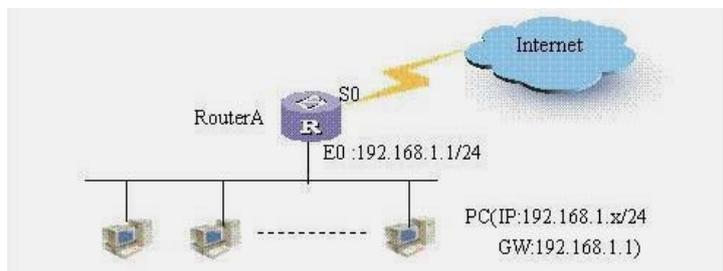


图 2-14 默认网关

如图 2-14 所示，路由器 RouterA 是整个局域网连接互联网的出口，任何一台计算机要上网，首先需要经过 RouterA，所以，RouterA 就是整个局域网的网关，RouterA 的 IP 地址就是整个局域网的网关地址。

如果出口只有一个，那么它肯定就是默认网关。有时候，一个网络有可能不止一个网络出口，比如移动和联通两条线路同时接入，此时，默认网关指的是当主机发送数据时，如果系统设置中没有明确指定送去哪里，那么就会把数据包发给我们设定为默认的网关，由这个网关来处理数据包。例如所属网络有中国移动 ISP 接入和中国联通网络 ISP 接入两个出口，网管可能设置一部分信息从移动出口转发，另一部分从联通出口转发，至于没说明的部分，就送给设定的默认网关来转发。

### 2.5.3 DHCP 动态主机配置协议

动态主机配置协议(Dynamic Host Configuration Protocol, DHCP)是 TCP/IP 协议中的一种，主要是用来给网络客户机分配动态的 IP 地址。这些被分配的 IP 地址都是 DHCP 服务器预先配置好的一个由多个地址组成的地址集，并且它们一般是一段连续的地址。

使用 DHCP 时，必须在网络上有一台 DHCP 服务器，而其他机器作为 DHCP 客户端从服务器获得 IP 地址信息。当 DHCP 客户端程序发出一个信息，要求一个动态的 IP 地址时，DHCP 服务器会根据目前已经配置的地址，提供一个可供使用的 IP 地址设置信息给客户端。通常这些信息包括 IP 地址、子网掩码、默认网关、本地 DNS 服务器地址等。

DHCP 使服务器能够动态地为网络中的其他服务器提供 IP 地址，通过使用 DHCP，就可以不再给网络中除服务器外的任何服务器设置和维护静态 IP 地址。大大简化配置客户机的 TCP/IP 的管理维护工作，尤其是当某些 TCP/IP 参数改变时，如网络的大规模重建而引起的 IP 地址和子网掩码的更改。

DHCP 服务的基本思路就是为了排除手工配置可能出现的差错，由服务器自动进行 IP 地址和其他网络配置信息的分配。每一台客户机启动时，都需要向网络中发出 DHCP Discovery 广播，来寻找 DHCP 服务器；当服务器收到信息后，会从自己的地址池中取出一个可用的 IP 地址回送给客户端，这就是 DHCP offer 信息；客户机收到 IP 地址后，向服务器提交申请 DHCP request，要求获得这个 IP 地址的使用权；服务器审核请求，把 IP 等信息送给客户机，这就是 DHCP ACK 信息。整个 DHCP 工作过程如图 2-15 所示。

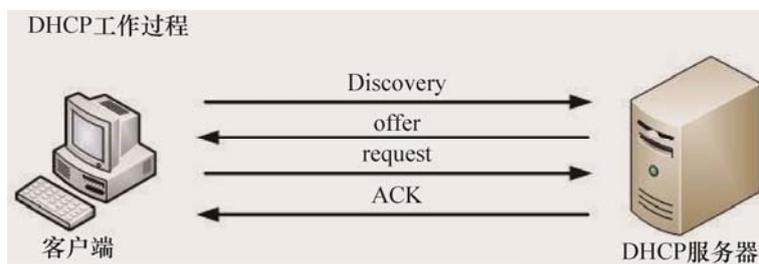


图 2-15 DHCP 的工作过程

看起来好像挺乱的，实际上就好像你去小卖店。

你喊一声：“有人在吗”？ <-----> DHCP Discovery  
 店主出来说：你看这个东西不错，要不？ <-----> DHCP offer  
 你看看说：挺好，就它吧！给你钱。 <-----> DHCP request  
 店主说：刚刚好，给你。 <-----> DHCP ACK

要注意的是，你得到的不是 IP 地址等的终身使用权，而是一个租约。在租约到期前，你要续租，否则一旦到期，你就不能够使用这个 IP 地址了。客户机会在到期前自动续租，成功了租约更新，继续使用；如果失败了，会过一段时间自动申请；如果直到租期到了，却还没续租成功，就只能放弃使用这个 IP 地址了。

DHCP 基本上是必配的基础服务，它可以大大简化配置客户机 IP 地址设置的工作量，并减少 IP 地址冲突的可能性，此外，如果网络配置需要大范围的修改，也不需要一个个主机地去改了，只需要重新配置一下服务器，就可以完成这个任务。

#### 2.5.4 DNS 域名服务

域名服务(Domain Name Service, DNS)的作用是域名解析，可以把域名解析成为 IP 地址，也可以反向解析。这样，我们在访问网站时，可以不需要输入难记的 IP 地址，相对来说，有意义的名字更为容易记忆和使用。

就像每个人都有身份证号，也有名字。我们会用身份证号码来称呼记忆别人吗？是不是使用名字更适合我们呢？

使用 DHCP 服务器，是为了让主机向所在网络的 DHCP 服务器申请从指定的 IP 范围内自动获取 IP 地址设置。而使用 DNS 服务器，是为了能够更友好地访问主机。

互联网是由许许多多的局域网互联而成的世界范围的网络。这些网络属于不同的公司或者其他组织部门，由各组织部门自行管理。各组织部门向互联网管理机构申请 IP 地址和域名后，配置 DHCP 服务器或者手动来分配 IP 地址，配置 DNS 服务器为每台服务器甚至普通主机进行域名解析。

IP 地址有 32 位，理论上说，可以提供  $2^{32}$ (约 43 亿)个 IP 地址。如果每个主机都有个名字，那么也就有几十亿的名字要管理，想起来就觉得好累，是不是？

就像中国有十几亿人，那么按照地域，分成若干个省级单位；每个省级单位下面再分成若干个地区；每个地区下面再分成县。按照这样的模式，最底层的部门，例如居民委员会，来具体管理所在区域的人口，其他的各级分别管理自己直属的下级并接受上级的管理，最高级由中央政府总管全局。

互联网并不按照国家地区来管理网络，但是也采用类似的管理思路。如图 2-16 所示，最上层称为根域，是大总管，就像中央政府；下面分为若干分支，称为顶级域；然后各域下面再进行细分。每一级也是逐层管理的关系。

当你邮寄信件填写地址时，你会写类似“河北省廊坊市固安县\*\*\*街\*\*\*号某某人收”这样的地址。在互联网中，地址也是这样的，不过要倒过来写。