4.2 某公司 IP 规划与配置案例

我们知道，对于在 Internet 和 Intranet 网络上，使用 TCP/IP 时每台主机必须具有独立的 IP 地址，有了 IP 地址的主机才能与网络上的其他主机进行通信。下面用一个简单的案例说明之前的理论知识。

4.2.1 网络组建需求

某科技公司成立，成立之初，这个公司只有数十人，每个人根据工作需要，都配备有电脑终端，有一台公用的服务器负责文件存储和打印机共享，这些设备要实现联网。另外，公司由于业务的需要，在内部联网之后要建立和 Internet 的连接。

要实现并配置这家公司的基本要求，在 IP 管理中需要包含如下范畴：

- 选择一个适合几十个网络终端的 IP 地址分配范围。
- 自动分配内部每台终端的 IP 地址。
- Internet 连接后要保证每台计算机都能够上网，并不需要 Internet 上的其他用户能够直接访问到内部网络。
- 所有客户端要进行测试。

4.2.2 地址规划与配置分析

在 IP 地址规划中有些 IP 地址是不能被配置到网络设备接口使用的，这些 IP 地址是网络地址和广播地址。另外，这家公司属于典型的小型网络，机器数量一般在 50 台以下，我们需要根据网络的规模考虑 IP 地址的分配与管理。

1．确定合法地址

网络中第一个不能使用的地址就是网络地址。网络地址用于表示网络本身，主机位部分为全“0”的 IP 地址代表一个特定的网络。网络地址对于网络通信数据量的控制非常重要，位于同一网络中的主机必然具有相同的网络号，它们之间可以直接相互通信。而网络号不同的主机之间则不能直接进行通信，必须经过第 3 层网络设备（如路由器）进行转发。

如图 4-9 的示例，上半部分的框架中表示网络 198.150.11.0。从局域网外部看，任何发往该网络主机 198.150.11.1~198.150.11.254 的数据，目的网络都是 198.150.11.0，只有数据到达上半部分的框架（局域网）时，才能进行主机位的匹配。下半部分的网络编号用 198.150.12.0 表示，数据进行比对的情况也是相同。

网络中第二个不能使用的地址是广播地址（Broadcast Address）。它用于向网络中的所有设备广播分组，具有正常的网络号部分，主机号部分为全“1”的 IP 地址代表一个在指定网络中的广播，被称为广播地址。

广播地址对于网络通信同样重要。在计算机网络通信中，经常会出现对某一指定网络中的所有机器发送数据的情形，如果没有广播地址，源主机就要对所有目的主机启动多次 IP 分组的封装与发送过程。

除了网络标识地址和广播地址之外，其他一些包含全“0”和全“1”的地址格式也是保留地址。图 4-10 中标明了这些特殊地址的用途。

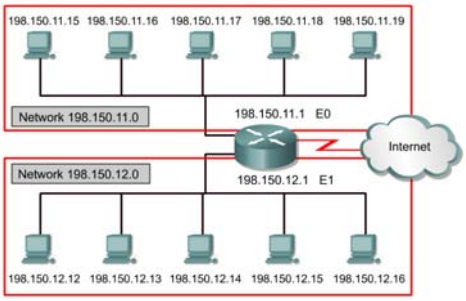

图 4-9　网络地址的与寻址

00...00	0000 ... 0000	本机
00...00	主机号	本网中的主机
11...11	1111 ... 1111	局域网中的广播
网络号	1111 ... 1111	对指定网络的广播
网络号	0000 ... 0000	网络地址
127	任意值	回路 Loopback

图 4-10　特殊的保留地址

2．选择专用 IP 地址

Internet 的稳定直接取决于网络地址的唯一性。这个工作最初由 InterNIC（Internet 网络信息中心）来分配 IP 地址，现在已被 IANA（Internet 地址分配中心）取代。IANA 管理着剩余 IP 地址的分配，以确保不会发生公用地址重复使用的问题。

1）公用 IP 地址

公用 IP 地址在 Internet 上是唯一的，因为公用 IP 地址是全局的和标准的，所以没有任何两台连到公共网络的主机拥有相同的 IP 地址。所有连接 Internet 的主机都遵循此规则，公用 IP 地址是从 Internet 服务供应商（ISP）或地址注册处获得的。如果需要到 Internet 的直接（路由）连接，则必须使用公用地址；如果需要到 Internet 的间接（代理或转换）连接，则可以使用公用地址或专用地址。

2）专用 IP 地址

随着 Internet 的发展，各个连接到 Internet 的组织需要为每台设备的每个接口获取一个公用地址。每个网络接口都需要有一个公有 IP 地址是不可能的，至少在 IPv4 版本中。这一需求对公用地址池提出了很高的要求，A、B、C 类地址的总数满足不了全世界所有网络设备的标识。Internet 的设计者注意到这个问题，所以保留了 IPv4 地址空间的一部分供专用地址使用。IANA 提供了一个为专用网际网络保留网络 ID 地址的方案，以下这些网络 ID 是内部网络中可任意部署的：

- 子网掩码为 255.0.0.0 的 10.0.0.0 网络地址池。
- 子网掩码为 255.240.0.0 的 172.16.0.0 网络地址池。
- 子网掩码为 255.255.0.0 的 192.168.0.0 网络地址池。

有关为专用 Intranet 保留的 IP 地址空间的详细信息，请参阅 RFC 1918，“专用 Internet 的地址分配”。

3．地址转换技术

有一种情况需要特别注意，如果公司网络没有以任何方式连接到 Internet，则可以使用任何 IP 地址。但这家公司网络需要连接到 Internet，所以应当使用公用地址或专用地址转换技术，以防止非法 IP 地址暴露在公网之上。

为了让使用专用 IP 地址的计算机能够访问 Internet，必须使用网络地址转换（NAT）和路由。NAT 使您能够把使用专用 IP 地址的客户端计算机连接到使用公共 IP 地址的 Internet。这需要有两个接口（或网络适配器）来隔离本地网络（使用专用 IP 地址）和 Internet 网络（使用公共 IP 地址）。这两个接口是必需的，因为两个网络之间的请求必须通过路由器服务或设备进行传送。当路由器接收到请求时，它在两个接口之间转发这些请求。NAT 服务帮助从源网络到目标网络，把 IP 地址转换成正确的地址。

例如，当客户端计算机发出访问 Internet 资源的请求时，路由器设备在本地网络上接收到该请求，客户端计算机的专用 IP 地址随后被转换成公共 IP 地址并路由到外部接口，从而

使请求能够被发送到 Internet。当在外部接口上接收到来自 Internet 的响应时，NAT 随后把公共 IP 地址转换回客户端计算机的专用 IP 地址，并把响应路由到本地接口。通过这种方法，路由和 NAT 服务提供了过滤功能，从而解决了这家公司针对网络安全的需求。

4．IP 地址配置方法

IP 地址的获得可以通过手工配置 TCP/IP 选项或者使用动态主机配置协议（DHCP）自动获取。客户端还需要配置的项目包括子网掩码、网关地址、DNS 地址等。

假设企业的服务器操作系统采用的是 Windows 2000/2003 Server 系统，客户端采用 Windows 2000/XP 系统。Windows 为 TCP/IP 客户端提供了 3 种配置 IP 地址的方法，用于满足 Windows 用户对网络的不同需求。具体采用哪种 IP 地址分配方式，可由网络管理员根据网络规模和网络应用等具体情况而定。

1）手工分配

手工设置 IP 地址是最常用的一种分配方式。在以手工方式进行设置时，需要为网络中的每一台计算机分别设置 4 项 IP 地址信息（IP 地址、子网掩码、默认网关和 DNS 服务器地址）。在通常情况下，手工设置 IP 被用于设置网络服务器、计算机数量较少的小型网络。

手工设置的 IP 地址为静态 IP 地址，在没有重新配置之前，计算机将一直拥有该 IP 地址。因此，既可以据此访问网络内的某台计算机，也可以据此判断计算机是否已经开机并接入网络。不过，默认网关必须是计算机所在的网段中的 IP 地址，而不能填写其他网段中的 IP 地址。

2）自动分配

动态主机配置协议（Dynamic Host configuration Protocol，DHCP）提供了自动的 TCP/IP 配置。DHCP 服务器为其客户端提供 IP 地址、子网掩码和默认网关地址等各种配置。网络中的计算机可以通过 DHCP 服务器自动获取 IP 地址信息。DHCP 服务器维护着一个容纳有许多 IP 地址的地址池，并根据计算机的请求而出租。DHCP 是 Windows 默认采用的地址分配方式。

在默认情况下，Windows 2000/XP 系统都使用 DHCP 请求来获得 IP 地址的分配。所以，如果仍然选择 DHCP 来分配和管理 IP 地址，网管工作将会减轻很多，而且可以很方便地配置客户机，我们所要做的就是维护好一台 DHCP 服务器。

4.2.3 确定 IP 规划方案

小型网络可以选择 192.168.0.0 地址段，大中型企业由于网络设备众多，有的可以达到上万台，那么则可以选择 172.16.0.0 或 10.0.0.0 地址段。经过前面的分析，确定使用子网掩码为 255.255.255.0，基于专用网络 ID 192.168.0.0 的分配 IP 地址方案，这种方案提供在每个网段上最多增加到 254 台计算机的容量，足够满足公司所有客户端的需求了。

由于公司刚刚起步，所以在连接 Internet 的网络带宽不是很大，而且也没有太多的网络业务往来。因此，可购买一个价格比较低廉的路由器，使用 NAT 技术将所有客户端共享上网，隐藏内部网络的结构，实现比较简单的安全防火墙作用。IP 地址配置要分别对待，文件服务器需要手工配置，这样所有用户都可以随时访问到这个静态 IP 地址，而其他客户端采用路由器上的 DHCP 功能，自动获得 IP。

这台路由器的内部接口需要设置成 192.168.1.1，这就是客户端需要指定的网关地址。而 DNS 服务器的地址可以使用 Internet 上的 DNS 服务器或者自行建立，这里使用外网的 DNS 服务器。

我们将这个公司的网络地址分配为 192.168.1.0，子网掩码为 255.255.255.0，那么它的主机范围就是：192.168.1.1~192.168.1.254，服务器使用固定的 192.168.1.2 的网络地址。其他主机采用自动分配的 IP 地址，但为了预留一些网络管理员和其他应用需求，只提供

192.168.1.100~ 192.168.1.199 这个范围的 IP。

4.2.4 实施与连通性测试

下面开始按照上面的 IP 规划方案进行实施，实施过程中需要让客户端获得 IP 地址还有子网掩码、网关地址、DNS 地址，完成之后要测试网络的连通性，可以利用 ipconfig、ping、tracert 等系统自带工具。

1．配置 IP 地址前的状况

在没有启用路由器 DHCP 和手工配置 IP 之前，这家公司的所有主机都能够相互访问，这是一个很怪异的现象。为什么在物理连接之后，就出现了这个状况呢？这是因为 APIPA 发挥了作用。

自动专用 IP 寻址（Automatic Private IP Addressing，APIPA）可以为没有 DHCP 服务器的单一网段的网络提供自动配置 TCP/IP 的功能。在默认情况下，运行 Windows 2000/XP 的计算机首先尝试与网络中的 DHCP 服务器进行联系，以便从 DHCP 服务器上获得自己的 IP 地址等信息，并对 TCP/IP 进行配置。如果无法建立与 DHCP 服务器的连接，则计算机改为使用 APIPA 自动寻址方式，并自动配置 TCP/IP。

使用 APIPA 时，Windows 将在 169.254.0.1~169.254.255.254 的范围内自动获得一个 IP 地址，子网掩码为 255.255.0.0，并以此配置建立网络连接，直到找到 DHCP 服务器为止。这也是计算机没有手工配置或利用 DCHP 指定 IP 时主机就能相互访问的原因。

值得注意的是：APIPA 分配的 IP 地址只适用于一个子网的网络。如果网络需要与其他的网段通信，或者需接入 Internet 时就不能使用 APIPA 这种分配方式了。

2．配置服务器地址

在 Windows 2000/XP/2003 系统下，具体的配置方法如下：

（1）在完成网卡驱动程序的安装之后，重新启动计算机进入系统。

（2）用鼠标右键单击桌面上的“网上邻居”图标，选择【属性】命令。

（3）检查是否已经自动安装好了 TCP/IP，选择并单击它下面的【属性】按钮，会弹出“Internet 协议（TCP/IP）属性”对话框。

（4）在“IP 地址”选项卡里，把“自动获取 IP 地址”改为“指定 IP 地址”，这时原本灰色的不能填写的 IP 地址和子网掩码就可以由自己来指定了，如图 4-11 所示，填入对应内容后单击【确定】按钮。

3．配置网关地址和 NAT

这里只说明了需要设置网关 IP 地址这个重要步骤，不同的路由器配置方法不同；尤其是低端的家用或者商用路由器可以参照说明书或者安装向导完成配置。很多路由器都自动开启了 NAT 功能，这台路由器默认已经启用了 NAT 服务，所以不需要进行配置。只需要将这台路由器的内部网络接口的 IP 地址配置为如图 4-12 所示的地址：192.168.1.1。

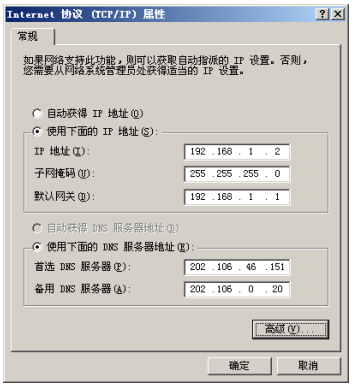

图 4-11　手工指定服务器 IP 地址

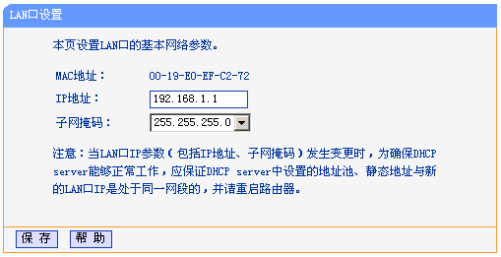

图 4-12　设置路由器 LAN 接口 IP

4．配置自动分配 IP 选项

根据方案中确定的内容，这里需要设置 192.168.1.100~192.168.1.199 作为客户端获得 IP 地址的范围。DNS 服务器的地址根据城市与地区的不同，需要填写不同的 IP 地址，图 4-13 中是北京地区常用的 DNS 服务器 IP 地址。

DHCP：DHCP 协议提供了主机 IP 地址的动态租用配置，并将其他配置参数分发给合法网络客户端的 TCP/IP 服务协议。DHCP 提供了安全、可靠、简便的 TCP/IP 网络配置，能避免地址冲突，并且有助于保留网络上客户端 IP 地址的使用。DHCP 使用客户端/服务器模型，通过这种模式，DHCP 服务器集中维持网络上使用的 IP 地址的管理。然后支持 DHCP 的客户端就可以向 DHCP 服务器请求和租用 IP 地址，作为它们网络启动过程的一部分。

DNS：DNS 域名则是一种分层的分布式数据库，它包含对 DNS 域名到各种数据类型的映射，例如，IP 地址。DNS 可以用来按友好用户名称查找计算机和服务的位置，也可以用来发现存储在数据库中的其他信息。

5．测试配置结果

在 IP 地址配置完成后需要测试网络的连通性，可以利用 Ipconfig、Ping、Tracert 等系统工具。

1）测试 IP 地址属性

要快速获取计算机的 TCP/IP 配置信息，打开“命令提示符”，然后键入：Ipconfig。在“Ipconfig”命令的显示中，要确保正在测试的 TCP/IP 配置的网卡不处于“断开”状态。

（1）使用不带参数的 Ipconfig

可以显示所有适配器的 IP 地址、子网掩码、默认网关。在没有该参数的情况下 Ipconfig 只显示 IP 地址、子网掩码和各个适配器的默认网关值。适配器可以代表物理接口（例如，安装的网络适配器）或逻辑接口（例如，拨号连接）。

（2）使用带参数的 Ipconfig

Ipconfig/All 显示所有适配器的完整 TCP/IP 配置信息。Ipconfig 显示所有当前的 TCP/IP 网络配置值、刷新动态主机配置协议（DHCP）和域名系统（DNS）设置。从图 4-14 中可以看到从 DCHP 服务器获得网络属性。

图 4-13　配置 DHCP 选项

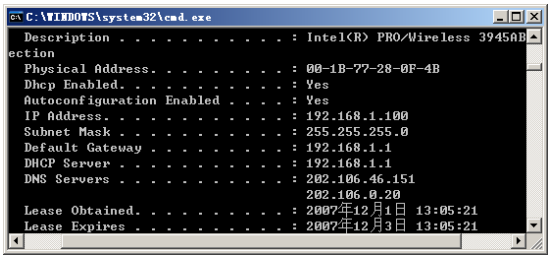

图 4-14　Ipconfig/All 输出结果

如果要释放和重新获得网络属性可以使用 release 和 renew 参数，Ipconfig 的使用方法可以从 Windows 系统帮助中查询。

2）测试网络连通性

（1）测试回环地址

Ping 命令使用 Internet 控制消息协议（ICMP）回响请求和回响答复消息。路由器、防火墙或其他类型安全性网关上的数据报筛选策略可能会阻止该通信的转发。使用 Ping127.0.0.1 测试回环地址的连通性。如果命令失败，本机的 TCP/IP 可能出现问题。图 4-15 中的输出结果表示网络之间可以正常访问。

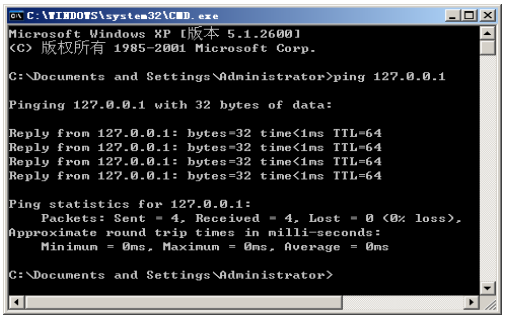

图 4-15　ping127.0.0.1 的输出结果

（2）测试内部服务器地址

使用 Ping 命令检测远程主机（不同子网上的主机）IP 地址的连通性。如果 Ping 命令失败，请验证远程主机的 IP 地址是否正确，远程主机是否运行，以及该计算机和远程主机之间的所有网关（路由器）是否运行。

（3）测试网关地址

使用 Ping 命令检测默认网关 IP 地址的连通性。如果 Ping 命令执行失败，验证默认网关 IP 地址是否正确，以及网关（路由器）是否运行。

（4）测试 DNS 服务器地址

使用 Ping 命令检测 DNS 服务器 IP 地址的连通性。如果 Ping 命令失败，验证 DNS 服务器的 IP 地址是否正确，DNS 服务器是否运行，以及该计算机和 DNS 服务器之间的网关（路由器）是否运行。

3）使用 Tracert 诊断工具

Tracert 通过递增“生存时间（TTL）”字段的值将“Internet 控制消息协议（ICMP）回响请求”消息发送给目标，并能显示网络路径中源主机与目标主机间的路由器的近侧路由器接口列表。不带任何参数时 tracert 显示帮助和使用格式：tracert [-d] [-h MaximumHops] [-j HostList] [-w Timeout] [TargetName]

例如，要跟踪名为“www.microsoft.com”的主机的路径，请输入：tracert www.microsoft.com。

在使用 Tracert 命令时，需要注意以下内容：

（1）Tracert 诊断工具通过更改“生存时间（TTL）”的值向目标发送“ICMP 回响请求”消息来确定到达目标的路径。

（2）要求路径上的每个路由器在转发数据报之前至少将 IP 数据报中的 TTL 递减 1。这样，TTL 就成为最大链路计数器。

（3）数据报上的 TTL 到达 0 时，路由器应该将“ICMP 已超时”的消息发送回源计算机。

（4）Tracert 发送 TTL 为 1 的第一条“回响请求”消息，并在随后的每次发送过程将 TTL 递增 1，直到目标响应或跃点达到最大值，从而确定路径。在默认情况下，跃点最大值

是 30，可使用-h 参数指定。

（5）检查中间路由器返回的“ICMP 超时”消息与目标返回的“回响答复”消息可确定路径。但是，某些路由器不会为使用到期 TTL 值的数据包返回“已超时（Request timed out）”消息，而且有些路由器对于 Tracert 命令不可见。在这种情况下，将为该节点显示一行星号“*”。

4.4 某大学 IP 管理规划案例

一个大型网络的 IP 地址管理结构设计要充分考虑，否则很容易引起整个网络地址重新设计和部署。这不仅会引起长时间的停机，而且还会在重新编址阶段引起不稳定，这会花掉很多的人力和财力。

使用子网划分技术，大部分网络能够获得较好的地址规划。但在大型网络中，由于网络的数量与主机的数量比例不平衡，这里就需要可变长的子网掩码（VLSM）技术作为规划的依据。

4.4.1 网络规划需求

海特大学的网络 ID 为 157.54.0.0/16，此次 IP 规划分配任务首先需要保留一半的地址空间供将来使用（这一点很值得推荐）。另外，海特大学共有 15 个分学院，每个学院可能包含 2 000 台主机和不同用途的服务器，为此需要将网络再划分出为子网。

当然，不能规范每个学院的分配方案，因此，需要为其中一所学院创建 8 个可拥有 250 个主机的子网，其他学院可参照这个模板执行。

4.4.2 VLSM 技术分析

严格按照 TCP/IP 中的 A、B、C、D 定义给 IP 地址分类的环境下，全 0 和全 1 网段都不让使用，这种环境叫做基于类的 IP（Classful）。在这种环境下，子网掩码只在所定义的路由器内有效，掩码信息无法传递到其他路由器。比如 RIP-1，它在做路由广播时根本不带掩码信息，收到路由广播的路由器因为无从知道这个网络的掩码，只好照标准 TCP/IP 的定义赋予它一个掩码。

子网划分的原始用途之一是将基于类的网络 ID 细分为一系列同等大小的子网。例如，对 B 类网络 ID 进行 4 位子网划分后，会生成 16 个同等大小的子网。基于类的网络 ID 或无类别的网络 ID 中可以存在不同大小的子网，这一规则正好适合现实世界中的环境。因为在现实网络中包含的主机数量不同，所以需要使用不同大小的子网来避免 IPv4 地址浪费的现象。从 IPv4 网络 ID 创建和部署不同大小子网的做法叫做可变长度子网划分，这种技术使用可变前缀长度，又叫做可变长度子网掩码（Variable Length Subnet Mask，VLSM）。

4.4.3 任务实施

假定你是海特大学的网络管理员，网络 ID 为 157.54.0.0/16，任务如下。

- 保留地址：需要保留一半的地址空间供将来使用。
- 分配各个学院地址：有 15 个地址前缀，供各个学院使用，海特大学中每个学院可能包含 2 000 台主机和不同用途的服务器。
- 创建 IP 地址模板：为其中一所学院创建 8 个可拥有 250 个主机的子网，其他学院可参照执行。

1．保留地址任务

为了达到保留一半地址空间供将来使用这一要求，应当对网络 ID 157.54.0.0 进行 1 位的子网划分。这种子网划分生成了 2 个子网 157.54.0.0/17 和 157.54.128.0/17，将地址空间平均分成了两部分。可以选择 157.54.0.0/17 作为保留的那一部分地址空间的网络 ID，从而满足上述要求。表 4-7 显示了保留的那一半地址空间。

表 4-7　第 1 次子网划分

子 网 编 号	网络 ID（点分十进制）	网络 ID（网络前缀）
1	157.54.0.0, 255.255.128.0	157.54.0.0/17

2．各学院地址分配

为了达到拥有 15 个地址前缀，每个前缀有大约 2 000 个主机这一要求，对子网网络 ID 157.54.128.0/17 执行 4 位子网划分。第 2 次子网网划分生成了 16 个地址前缀。

157.54.128.0/21、157.54.136.0/21…157.54.240.0/21 和 157.54.248.0/21，每个地址前缀可拥有多达 2 046 个主机。可以选择 15 个子网网络 ID（从 157.54.128.0/21~157.54.240.0/21）作为分院校的地址前缀，从而满足了这一要求。表 4-8 列出了这 15 个地址前缀，其中每个子网可拥有多达 2 046 个主机。

表 4-8　第 2 次子网划分

子 网 编 号	网络 ID（点分十进制）	网络 ID（网络前缀）
1	157.54.128.0, 255.255.248.0	157.54.128.0/21
2	157.54.136.0, 255.255.248.0	157.54.136.0/21
3	157.54.144.0, 255.255.248.0	157.54.144.0/21
4	157.54.152.0, 255.255.248.0	157.54.152.0/21
5	157.54.160.0, 255.255.248.0	157.54.160.0/21
6	157.54.168.0, 255.255.248.0	157.54.168.0/21
7	157.54.176.0, 255.255.248.0	157.54.176.0/21
8	157.54.184.0, 255.255.248.0	157.54.184.0/21
9	157.54.192.0, 255.255.248.0	157.54.192.0/21
10	157.54.200.0, 255.255.248.0	157.54.200.0/21
11	157.54.208.0, 255.255.248.0	157.54.208.0/21
12	157.54.216.0, 255.255.248.0	157.54.216.0/21
13	157.54.224.0, 255.255.248.0	157.54.224.0/21
14	157.54.232.0, 255.255.248.0	157.54.232.0/21
15	157.54.240.0, 255.255.248.0	157.54.240.0/21

3．创建地址分配模板

为了满足每个学员创建 8 个可拥有 250 个主机的子网模板要求，需要对子网网络 ID 157.54.248.0/21 进行 3 位的子网划分。第 3 次子网划分会生成 8 个子网。

157.54.248.0/24、157.54.249.0/24…157.54.254.0/24 和 157.54.255.0/24，每个子网可拥有 254 个主机。可以选择所有 8 个子网网络 ID 从 157.54.248.0/24~157.54.255.0/24，作为网络 ID 分配给单个子网，从而完成整个任务。表 4-9 列出了 8 个子网，其中每个子网可拥有 254 个主机。

表 4-9　第 3 次子网划分

子 网 编 号	网络 ID（点分十进制）	网络 ID（网络前缀）
1	157.54.248.0, 255.255.255.0	157.54.248.0/24
2	157.54.249.0, 255.255.255.0	157.54.249.0/24
3	157.54.250.0, 255.255.255.0	157.54.250.0/24

子 网 编 号	网络 ID（点分十进制）	网络 ID（网络前缀）
4	157.54.251.0, 255.255.255.0	157.54.251.0/24
5	157.54.252.0, 255.255.255.0	157.54.252.0/24
6	157.54.253.0, 255.255.255.0	157.54.253.0/24
7	157.54.254.0, 255.255.255.0	157.54.254.0/24
8	157.54.255.0, 255.255.255.0	157.54.255.0/24

当然，每个学院的内部还有可能对 250 台主机再次进行可变长子网掩码的操作，例如，划分 VLAN 等。这些利用 VLSM 操作之后进行的实际配置案例，我们会在“园区网与 VLAN 应用”一章中重点讲述。此次 IP 规划任务完成情况可以根据图 4-16 看到这次子网划分的流程图。

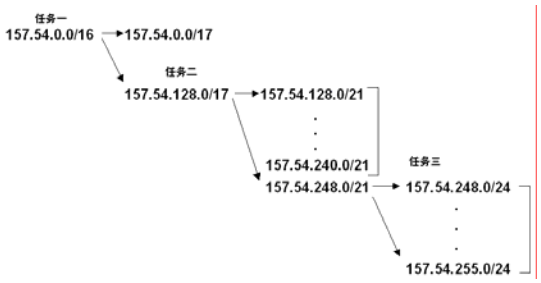

图 4-16　海特大学子网划分流程