《Introduction to IP Address Management》第一章翻译

**前言：**

随着新的IP服务和技术的部署，当今的IP网络日益复杂化。 IP设备和应用程序日益增长只能用来强调支持这些关键业务相关的应用程序运行的IP网络性能是有多么重要。 如果终端用户设备（如笔记本电脑或VoIP电话）无法通过DHCP（动态主机配置协议）获取IP地址，则这些设备将无效，不过可以用户致电帮助台寻找解决办法。 同样，如果DNS（域名系统）关闭，按名称，电话号码或网址进行的应用导航同样会损害其功能性并且引起很多人去呼叫帮助台寻求帮助。 因此，有效的IP地址管理（IPAM）对于维护数据，视频和IP语音（VoIP）等高性能IP业务至关重要。

IPAM的实践需要将网络管理学科应用于IP地址空间和相关网络服务，即DHCP和DNS。 DHCP的不正确配置的结果会导致最终用户可能无法获取访问网络的IP地址。 没有适当的DNS配置，网络的可用性也会受到极大的困扰，然后名称到地址的查找过程的那些功能就都可能会失败。 想象一下，不得不通过IP地址导航到网站或发送电子邮件或即时消息！ 同样重要的是，这些DHCP和DNS配置基于通用的IP地址计划，其中映射了IP地址层次结构，子网，地址池和域。

IP地址计划，DHCP服务器配置和DNS服务器配置是不可分割的; 更改IP地址也会影响DNS信息，也可能会影响DHCP。 这些关键网络功能为今天的融合服务IP网络提供了基础，这些网络构成了大多数企业和服务提供商网络，因此必须使用严格的方法进行管理。

本书简要介绍了IP寻址技术，DHCP和DNS技术，以及IPAM实践和技术管理技巧。 IP地址管理原则的一本伴侣书和实践，更深入地介绍了IPAM技术和技术。 本书的目的是帮助您：

1. 了解IPv4和IPv6寻址和子网划分，DHCP和DNS网络技术的基础知识
2. 了解IPAM实践，包括管理您的IP地址清单并跟踪地址事务，**如分配和拆分地址空间，发现网络占用，管理故障和性能**
3. **了解正确实施**IPAM战略的成本和理由
4. 了解IPv4 - IPv6共存技术

**约定：**

这本书是以Times Roman字体排版的。 时代罗马斜体字体用于术语第一次引入或强调。

区分散文中的示例配置信息，例如，DHCP或DNS服务器，Courier字体使用方式如下：

Courier plain font - 表示配置文件或屏幕中的关键字或文字文字。

Courier italic font - 表示在实际中代替反映表示的数据元素或类型的值的参数名称。

**IP网络概述**

**IP网络101**

各方进行沟通，无论是两个人交流信息，还是两台电脑交换信息，都必须遵守一套管辖这种沟通规则的公约。语言和文化通常指导人类对话的这种惯例。而协议为计算机定义了这些约定。计算机通常比人们更容易遵守这些惯例。协议规定了通信的顺序和语法以及错误条件下所需的恢复机制。实际上在计算机通信期间使用几个协议层或协议层，每个提供特定的一组功能以支持通过各种媒体进行通信的通用级别。我们将在本章稍后深入研究，但让我们先来简单的类比一下人类通信，介绍互联网协议（IP）寻址的关键方面，以及为什么地址管理很重要。当两个人交谈时，一个人可以通过多种方式开始讨论：通过身体接近另一个人，说话，打电话给他或她，发送他或她的即时消息，等等。在这些情景的每一种情况下，对话的发起者识别并定位预期的接收者，然后尝试使用所选择的媒体开始对话。例如，当我想和我的朋友史蒂夫谈话时，我可以看看他在线号码或在电话簿中拨打他的号码，当他接起电话时，我可以通过声音去识别是否是本人，然后我们便可以开始谈话。在基层，知识产权通信遵循类似的过程。当IP设备寻求与另一个设备进行通信时，它必须识别并定位预期的接收者，然后通过链路启动通信，同时还向接收者标识自身的过程。

也许最好的IP通信的类比是邮递信，虽然这个类比可能被滥用了很多次了。 不过，让我们考虑一下这个过程“运动鞋邮件”，然后将其与IP通信相关联。 基本的邮递过程如图1 - 1所示，从我写信给史蒂夫和通过邮件通信。

写完我的信后，我把它放在信封里。 这是第1步。接下来，我写我的回复（From）地址和Steve的（To）地址在信封上，盖章支付我的邮政服务提供商。 在这一点上，我准备邮寄了。步骤3包括将我的信存入我的外发邮箱。 在我的邮件-工作人员拿起我的信，第四步需要转发这封信，邮政系统到当地邮局服务史蒂夫的地址。 在信已经被交付给邮局或配送中心服务，一个本地派送邮件员将信丢在史蒂夫的邮箱中。 史蒂夫走出门，看到邮箱，他可以打开信件并阅读我的信。 信息交付就完毕了！

所以我们来映射这个邮件消息流通过IP发送一个消息网络，参考图1-2。 在这种情况下，我们以电子方式进行沟通，通过互联网，虽然这种比喻保留了通过私有企业，服务提供商，家庭IP网络或其组合进行通信。 正如史蒂夫和我有邮政地址一样，我们都需要IP地址来互联互通。 世界上没有其他人与史蒂夫拥有相同的邮寄地址; 同样，世界上没有其他人拥有与史蒂夫相同的IP地址（从技术上讲，当我和史蒂夫之间的IP地址被翻译时，这不一定是正确的，但现在我就简单的这么假设）。 我们假设我们每台计算机都配置了各自的IP地址，并且我知道Steve的IP地址。

步骤1需要创建或输入我给Steve的消息。 在第二步，我的计算机，知道我的IP地址和史蒂夫，将我的消息放在一个数据包中，或者一个IP包中。 一个IP包就是要传送的消息，前缀有一个IP头。 IP报文头就像我们的信封，包含我的（源）源IP地址以及史蒂夫（To）目的地IP地址等。 制定了我的IP包后，我现在准备发送了。 从我的家庭网络，我有一台宽带路由器，我的电脑传输我的IP包作为步骤3.这种传输可能通过电缆或我的计算机和路由器之间的无线连接发生。

在步骤4中，我的路由器通过我的宽带将我的IP包转发到互联网服务提供商（不需要邮票，他们会稍后通知我）。 互联网中的设备即所谓的路由器将我的IP包转发到Steve的宽带服务提供商和家中的宽带路由器。 路由器检查每个IP包的头信息，以确定转发数据包到达目的IP地址的位置。 当IP包已经送达到史蒂夫的宽带路由器后，步骤5包括将数据包转发到史蒂夫计算机，其IP地址与IP数据包的目标IP地址字段相匹配。 在步骤6中，史蒂夫的电脑剥离IP头，以产生我输入的消息。 消息就这么成功的送达到了史蒂夫手中

在邮件和IP通信中，源地址和目标地址都是指定的，并且是唯一的，人员和/或机器的基础设施将消息连续地转发到寻址的目的地，并且最终将其传递给接收者。 表1-1总结了邮政和IP通信示例的关键相似之处。

这些通信类比通用的两个核心概念是路由和寻址。 正如我们迄今为止所暗示的，路由依赖于正确的寻址！ 接下来我们来更详细地研究这种关系。

**IP路由**

邮政系统通过“路由”信件和包裹尽可能高效地运行到区域配送中心，本地中心，最后到路边。扫描和跟踪系统沿途通过一个或多个配送中心，通过各种交通工具将包裹更接近其最终目的地。通常，这种路由是通过首先检查“目的地”（目的地）所在国家，邮政编码，城市和州或省，最后是街道地址来执行的。 “To”地址中的一般（国家，邮政编码）和特定（街道地址）的编码使得邮政系统中的不同实体能够使用地址的不同部分有效地路由。分销中心只能根据国家和邮政编码信息转发包裹;一旦包裹到达服务目的地邮政编码的当地中心，当地中心然后需要检查街道地址进行最终交付。

如果史蒂夫住在街上，我的信将简单地穿过我当地的邮局，也许是一个配送中心，然后回到史蒂夫的本地邮局。 如果史蒂夫住在全国各地，我的信可能会从本地邮局通过一个或多个区域中心，然后到史蒂夫的当地配送中心交货。 如果史蒂夫住在不同的国家，我的信可能需要通过海关代理进入该国。 海关代理人可以分析该信件，并允许在国内进一步交货，或者将其退还给发件人或者没收或者处理该信件。

路由器在路由IP包中执行类似的功能。 路由器通过检查每个IP包中的目的地IP地址的网络部分并将其转发，模拟邮政系统的扫描系统，每一次转发都会离目的地进一步。 到达本地服务路由器后，该路由器检查完整的IP地址，以便将其传递给预期

接受者。 因此，IP地址由网络部分和主机组成\*部分，连接在一起，我们将在下一章讨论。

如果分组的目的地是私人运行的网络，例如a公司或企业，包可能会遇到类似的检查到海关代理。 而且像海关代理商一样，这个企业网关或防火墙可以允许或者拒绝将数据包进一步传输到目的地。顺便说一句，正如风暴或其他事件可能导致邮政系统中的航班延误或邮件重新路由，路由器可以检测到类似的中断或拥塞事件，以便根据需要重新路由IP数据包。 是的，既不是下雨也不是雪，也不是夜晚的黑夜会停止邮件或IP包的传送！

**IP地址**

如我们所见，IP网络上的每个设备都必须通过IP地址进行唯一标识。 因此，希望在IP网络上通信的每个设备需要IP地址。 所以你的电脑在家里，你的IP语音电话在工作，甚至你的手机可能有一个IP地址，至少在它的电源和准备沟通的时候。 在上面的例子中，我们假设每个计算机的IP地址已经被编程了，但是这个IP地址是如何进入的呢？ 其实我们可以手动或自动地在每个设备中分配和配置每个设备的IP地址。

使用固定IP地址的手动地址分配方法适用于固定基础设施IP设备（如路由器和服务器）。 但对于绝大多数IP可寻址设备（如笔记本电脑和移动电话）而言，固定地址分配方式不能正常工作。 这是因为分配的IP地址必须与IP设备连接的当前网络或子网相关。 如果这些IP设备移动，他们需要在IP网络上的当前位置的上下文中进行IP寻址，使手动方法非常麻烦。 即使邮政服务也没有提供“找到我”的服务，无论我发生什么事情，都可以向我发送邮件！

为了说明这个位置敏感度要求，我们来考虑一个小型组织，具有三个办公室，如图1-3（a）所示。 为了实现这些站点之间的网络通信，我们通过广域网（它们可能是互联网）或在这种情况下，来自服务提供商的私有网络进行互连。 为了实现通信和路由，我们在每个位置安装了至少一个路由器，如图1-3（b）所示。 该图显示了这些位置之间的简单IP网络的覆盖。

要启用这些位置之间的路由，我们需要为每个位置分配一组唯一的IP地址。 以这种方式，分公司将成为一套IP地址（或一个IP网络），零售店不同的集合以及总部，另一个独特的IP地址集。 让我们使用每个路由器显示的一组IP地址，如图1-3（c）所示。 每个路由器将支持一组IP地址，从该位置将单独的IP地址分配给该位置的打印机，笔记本电脑，IP电话语音和其他IP设备。

我们将在第2章中更详细地描述IP地址的结构和格式，但IP地址由四个数字组成，用小数点或点分隔。 四个数字中的每一个可以从0到255的值范围。在我们的示例中，IP地址集10.0.1.0 - 255，10.0.2.0 - 255和10.0.3.0 - 255已分配给总部10.1.1.0 - 255 到分公司，10.2.1.0-255到零售店。 这些IP地址集合中的每一个称为子网或子网，因为每个IP地址集合表示整个企业的IP地址集合的一部分或子集。

请注意，每组地址落在与每个集合内的IP地址的网络部分相对应的连续IP地址范围内。 回想起我们的邮政类比，地址的网络部分用于高效路由，直到IP分组被传递到本地服务路由器。

互联广域网（WAN）也有一个网络地址（10.254.1.0 - 255）。 每个位置的路由器必须配置此网络信息才能正确路由IP通信流量。 这样，我们的分公司路由器负责IP地址10.1.1.0 - 255，所以目的IP地址落在这个范围内的所有IP数据包将被分配给分支机构路由器。 将IP地址划分到特定站点或路由器类似于通过邮政编码和相应的邮政配送中心分割地理位置。

现在我们按照我们的解决方案分配了我们的IP地址并配置了我们的路由器，让我们来看看给定的地址分配设备，比如说我的笔记本电脑。 假设我星期一在分公司被指示由图1 - 3（c）中的笔记本电脑。 我将需要10.1.1.0 - 255子网中的IP地址，我们说10.1.1.52。 这是因为Branch路由器“拥有”10.1.1.0 -255子网，并作为我的“本地邮局”，用于将IP数据包传送到分支机构的设备。 当我发送即时消息给同事的时候，总部，我的消息被路由到总部路由器，响应通过分支路由器路由到我这里。

现在我们假设我星期二在零售商店打电话给会议室。当我到达零售商店并使用我手动配置的10.1.1.52 IP地址连接到商店的网络时，我将很快意识到我无法在网络上通信。这是因为我的IP地址是10.1.1.0 - 255网络的一部分，由Branch路由器提供。因此，当我开始发送IP通信时，\*通过打开网页，输入www地址，我的网络浏览器使用我的笔记本电脑的IP地址10.1.1.52向目标网站IP地址发送IP包，作为源IP地址。网络服务器确认通信并用所请求的网页进行响应，将其寻址回IP地址10.1.1.52。路由器全部“知道”分支路由器将IP数据包传递到10.1.1.0 - 255子网的IP地址，因此他们将打算用于我的Web浏览器的响应IP数据包发送回分支机构！

\*从技术上讲，我的IP通信甚至不会超过零售路由器，因为我的源IP地址对零售子网无效。 但这个简化的例子说明了这种通信尝试的谬误，即使它在技术上是可行的。

从我的角度来看，我没有得到Web服务器的响应。 网络关闭还是网络服务器关闭？ 当我呼叫帮助台抱怨网络中断时，网络团队最终会发现我的IP地址不适合我所连接的子网。 他们通知让我手动将笔记本电脑的IP地址更改为10.2.1.187的繁琐过程（只有当我星期三回到分公司时，才能让我回到相反的过程）。 一旦我的地址与我的位置相关，我就能够与Web服务器和其他IP应用服务器（如电子邮件服务器）进行双向通信，因为我的地址在分配给本地服务路由器的集合内。

地址分配问题解决后，我们的下一个目标是消除IP地址的人为错误输入。 早些时候，我们掩盖了一个事实，即我已经知道Steve的IP地址，或者我输入的www地址被神奇地翻译成一个IP地址，以创建一个IP包。 因此，如果IP网络上的通信需要IP地址，我们如何避免输入文本名称来发送电子邮件或连接到网站？ 解决方案是域名系统（DNS），使用户可以输入服务，网站或电子邮件箱的名称，从而避免输入IP地址。

我们一般认为这是理所当然的，这是一件好事！ 想象一下，相当于一个互联网电话簿与网站和相关的IP地址。 DNS在幕后工作，提供一个名称到地址查找机制，以弥补人类消费品名称与网络耗材IP地址之间的差距。 除非您是数字向导，否则在您的网页浏览器中输入http://www.ipamworldwide.com比输入（并记住）http://192.0.2.201更简单。 幸运的是，这个可用性问题在互联网的发展早期得到了认可，DNS被设计为使这个目录查找功能自动化。

输入www地址后，您的计算机将查找DNS中的www地址，并获取相应的IP地址，然后将其用作IP头中的目标IP地址。 多年来已经开发了其他形式的名称到地址转换，包括主机文件，黄页（YP）和Windows Internet命名服务（WINS），但DNS已经成为事实上的生产网络的主导地位 - 当今知识产权通信的地址转换服务。 在进一步探索IP地址管理（IP地址分配，DHCP和DNS）的核心要素之前，我们将通过探索路由器如何将IP报文传送到各自目的地的内部工作，来更详细地了解IP网络的基础知识。

**IP网络102**

在查看了我们上面简单的IP地址示例之后，您可能会想，为什么我们不消除路由器，然后使用一个可以共享的大型网络，而不是使用这种子网划分过程，导致笔记本电脑在我移动时的阅读 从这里到那里？ 毕竟，我可以在网络中的任何地方使用一个IP地址。 虽然这种方法在理论上可以利用跨越所有这些站点的桥接网络，但是由于网络上的站点间距离和设备数量的增加，通信的性能将受到影响，因此这种方法不能很好地扩展。 这是因为在共享或桥接网络中，每个设备的消息被发送到网络上的每个其他设备。 并且因为网络是共享介质，所以当两个或多个设备尝试同时发送消息时，可能会导致冲突。

网络世界中的冲突与人际沟通中的冲突相同。随着更多的成员加入“对话”，碰撞频繁发生。由于冲突发生在对话（至少有礼貌的人）之间，在重新启动通信之前暂时退出。参与谈话的人越多，碰撞越频繁，等待通信的信息积压越多。这种尝试/退避/重试进程会迅速升级，直到最终没有任何一方尝试通信才能向收件人发送消息。随着积压的反复沟通建设，就只剩下挫败的升级还有一个僵局的结果。当太多设备尝试在大型，单片式共享介质上进行通信时，会发生相同的效果。而对于人类对话组成的相同的一般解决方案可以应用于IP网络，这些群组自然地从主要对话分支到较小群体的子群体中。

通过减少和限制在同一媒体上进行通信的方式，可以对冲突域进行本地化，减少整个网络上的冲突和积压次数。 交换机和路由器的部署支持将网络划分为单独的冲突域。 交换机通过互连成对的交换机端口，其中每个端口物理连接到主机，使得能够对冲突域本身进行分区。 路由器通过终止互连冲突域来提供冲突域边界点。 路由器特别利用协议分层的概念来分离冲突域。 我们来看看协议分层的概念，这将引导我们更详细地讨论交换机和路由器的角色。

**协议分层**

国际标准化组织（ISO）定义了分层协议模型，分离了控制通信不同方面的责任（1）。分层模型由七层组成，分为开放系统互连（OSI）模型。术语协议栈是指几个协议层彼此“堆叠”的事实，以将数据和命令从我的Web浏览器引导到有线或空中，并通过网络到达目的地。事实上，互联网协议在各种媒体（如这些和其他媒体）上运行的能力是使用分层协议栈的强大后果。 OSI模型使得能够在各种下层数据链路和物理层（包括电缆，数字用户线路（DSL），光纤，以太网，无线等）上实现互联网协议的通用实现。图1-4说明了OSI模型，并简要介绍了每个层的关键功能。

应用层 。 应用层提供主要的最终用户寻找曝光和功能。 Web浏览器，文件传输程序或电子邮件客户端是应用层的示例。

表示层 。表示层负责定义通信中应用程序端点之间的数据格式和语法。 例如，该层为网络上的通信规定了标准图形格式和翻译。

会话层（第5层）。会话层负责调整网络端到端的应用通信，提供这样的功能服务作为安全和认证。 NetBIOS是会话层的一个示例协议。

传输层（第4层）。 传输层负责端对端通信的完整性，确保两个端点之间的流量控制，以及数据检查，请求重传以及信息的正确排序。 传输控制协议（TCP）和用户数据报协议（UDP）是TCP / IP协议栈内的传输层协议。

网络层（第3层）。网络层负责将信息格式化为数据包和/或数据包片段，用于通信和通过一个或多个网络路由。 IP是一种网络层协议。

数据链路层（第2层）。数据链路层负责将信息格式化为帧，用于通过物理网络进行通信，包括数据完整性的错误检查。 以太网，令牌环，ATM和帧中继是数据链路层协议的例子。 数据链路层通常分为逻辑链路控制（LLC）和媒体访问控制（MAC）子层。 熟悉的术语“MAC地址”是指设备的第2层或媒体访问控制地址。

物理层（层1）。物理层定义电子接口和特性，包括用于传输数据和控制（例如，前导码）位的电压和电流规范。 EIA-232（RS-232）提供了物理层指定的示例。

**OSI和TCP / IP层**

这些协议层不仅允许多个应用的互操作性和底层物理网络，它们也分割了所需的责任，用于通过数据网络成功通信。 一些层例如数据链路和网络层，提供错误检查和纠正以方便准确的通信和减少重传的要求。其他的，如传输层，负责端到端通信的完整性和信息的正确排序。 总体而言，协议层定义的标准化使得成功的端到端通信同时促进了互操作性

图1 - 4所示的七层堆叠有时也被描述为在Internet上下文中的五层模型，应用层分别位于TCP，IP，数据链路和物理层之上，如图1-5所示。协议分层不仅可以实现IP分组在各种媒体上的传输，还可以使各种最终用户应用通过IP进行通信，IP又通过各种低层协议进行通信。例如，电子邮件客户端应用程序可以使用分层在TCP上的邮局协议版本3（POP3）应用程序，然后可以将IP分层在以太网，令牌环，帧中继，或其他第2层协议，最终是特定的物理层。图1-5所示的另一个例子是HTTP（web浏览），TFTP（简单的文件传输协议）和POP3运行在各自的传输协议以及IP，以太网和100BaseT上。无论通过以太网100BaseT网络，802.11无线网络还是基于ATM的DSL网络进行通信，这提供了使用常见“桌面应用程序”的无缝终端用户体验。

分层还使堆栈的组件能够被不同的组织开发和提供。 实际上，协议分层在应用于TCP / IP边界以及TCP / IP到数据链路边界方面一直在有效地工作着，尽管TCP和UDP通常在传输网络层边界处以IP为特色。 应用程序编程接口（API）使来自不同供应商的各种应用程序可以将通用功能调用利用到通常包含在操作系统中的TCP / IP协议栈中。 用于TCP / IP应用程序的API事实上是最初在BSD UNIX（最初实现DNS BIND）上实现的套接字接口。 套接字接口定义程序调用，以使应用程序能够与TCP / IP层接口，以通过IP网络进行通信。 Microsoft的Winsock API也是基于socket接口。

Intra-Link通信。 要了解数据如何在协议栈中流经这些层，请参考图1-6。 从图左上角的应用程序数据开始，当应用程序数据负载穿过堆栈的时候，请注意添加IP报文头。 在本地网络上发送的数据链路帧包含应用数据和上层报头。 图的右侧的帧接收者随后将数据从堆栈传递到目标应用程序，处理并剥离相应层上的每个标题。 每个层边界显示的报头和有效载荷在这个链路内通信的两端是完全相同的。

随着应用数据准备在IP网络上使用一个TCP / IP协议栈进行传输，应用程序调用sockets API顺着不同层堆叠下来来传送数据。同时要 基于应用程序选择去添加TCP或UDP头，然后附加IP头。 回想起我们以前的邮政类比，我们可以现在看到IP头只是一个类似的报文被添加到网络消息中。附加IP标头的“消息”包括应用程序数据（例如，即时消息文本）加上传输层（TCP或UDP）头。 在这个多层堆栈模型中，每个层都添加一个报文头来启用它，去执行其各自的功能。

应用程序通常规定UDP或TCP头参数，它由应用程序（特定的端口号）以及留控制和其他数据组成。 正如我们所讨论的，IP头包含发件人和接收者的IP地址。 发送方的IP地址是手动分配的 自动（例如通过DHCP）输入收件人的IP地址通过应用程序用户界面或从DNS服务器获取。

在IP层之下，IP包（其自身包括IP头），一个TCP或UDP报头以及应用数据被包含在数据链路层内。通过物理网络进行传输。 沟通给定数据链路需要在数据链路帧内封装IP分组。本身需要源地址和目的地数据链路（MAC）地址。 发送数据链路帧内的IP包，发送主机必须确定收件人的数据链接（MAC）地址。 因此，设备必须将目标IP地址映射到目标MAC地址，以便在物理网络上的第2层帧内进行传输。 但是，另一个问题会根据目的地IP地址是否与发送方相同的数据链路而出现。

我们是否在同一条连路上呢？通常，每个设备可以通过其配置的IP地址和子网地址范围来确定预期接收者是否驻留在同一链路上。因此，如果目标IP地址与发件人的IP地址在同一子网范围内，则该设备被认为在同一个链路上。否则，如果目标收件人不在同一子网上，则源设备必须标识链路上可以将数据转发或路由到目的地的路由器。使用路由表或大多数非路由器设备配置的默认路由，设备可以确定发送数据的下一跳。默认路由是在没有向目的地址的已知下一跳的情况下发送所有数据包的下一跳目的地。这就像我在邮政类比中的传出信箱一样，这是我把我所有传出的公报的地方。这个默认路由（通常会被称为为一个默认网关），通常是为所有非链路本地分组发送到的子网服务的路由器的IP地址。

例如，如图1-3所示，如果笔记本电脑将数据传输到分支机构内的其他设备，也就是说，目的IP地址范围为10.1.1.0 - 10.1.1.255，可以直接发送（内联）; 如果将数据发送到总部或零售店的设备，则必须将其发送到分支路由器进行路由。 无论是将数据发送到内部链路目的地还是路由器，发送设备必须确定接收方或路由器的数据链路（MAC）地址，以便在数据链路层帧内制定和发送IP数据包。 该MAC地址是指定设备的数据链路层地址。 但是我们确定了DNS的目标IP地址，而不是MAC地址; 那么MAC地址如何确定？

地址解析协议（ARP）使设备能够确定与IP地址对应的同一链路上的设备的MAC地址。发送消息的设备知道预定的下一跳IP地址（接收者在链路或路由器上）制定请求MAC地址的MAC解析的ARP数据链路广播帧。广播帧是指向链路上所有设备的数据链路帧。对于以太网数据链路，例如，广播帧使用所有1的目标以太网地址，这意味着连接到此以太网链路的所有设备的广播地址。配置有寻址IP地址的设备以指示其对应的二层地址的ARP响应帧进行响应。这使得源设备能够制定用于IP分组传输的以太网帧。大多数设备将此信息缓存在ARP缓存中，提供这种IP到MAC地址相关性的临时存储，以减少例如多帧通信的重复ARP查询。

限制广播域名 诸如以太网的数据链路包括我们之前提及的冲突域（也称为广播域）。 数据链路层主要涉及访问网络进行传输，检测冲突，并对帧执行错误检查。 连接到公共以太网的所有设备，会接收从其他所连接设备发送过来的帧。 因此，我们很容易看到我们早期的关于积压和僵局的类比，都是因为尝试通信的方面的数量造成的。 随着冲突域内的设备数量的增加和/或每个设备的通信尝试次数增加和/或每个设备的通信量增加，数据冲突可能会更可能发生，降低网络性能。 如果我们可以限制每个碰撞域中的参与者人数，我们可以提高整体性能，最终提高用户的生产力和满意度。

这使我们回到如何用交换机和路由器去约束广播域。以太网局域网（LAN）部署了布线，每个办公室，机柜或终端站汇集回一个或多个以太网集线器。集线器将任何给定端口上接收的帧广播到每个其他端口，从而包含不可分割的冲突域。交换机被开发以在源端口和目的端口之间直接互连（或交换）业务，而不盲目地将所有数据广播到所有端口。交换机端口有效地提供终端设备与其交换机端口之间的直接点对点连接。交换机检测每个连接设备的MAC地址，然后利用该信息将帧进入的端口直接互连到适当的目的端口。这最大限度地减少了所有其他端口上设备的多余的广播流量。当然，第2层广播流量广播到所有交换机端口，但这肯定是一个改进！

现代的第二层交换机已进一步发展，以便能够定义给定广播域的物理端口子集。 因此，代替在广播域或LAN内的硬接线集线器端口，可以划分属于独立广播域的哪个交换机端口。 这些独立广播域被称为虚拟LAN（VLAN），因为交换机在一个物理交换机设备上支持多个逻辑LAN。 例如，在VLAN 1内的端口上的广播流量将不会广播到与VLAN 2关联的端口。 考虑图1 - 7的VLAN分段示例。 该图显示了将不同VLAN与不同子网地址相关联的常见实现。 \*与图左侧显示的每个集线器的单个广播域形成对比。

互通通讯。交换机肯定有助于减少冲突域的范围，但不管怎么说，交换机端口就只有这么多！所以我们要采用第二个方法，用于限制广播域的第二种方法利用了协议分层概念，并采用路由器来分离第二层网络。考虑图1 - 8，这是图1-6的重新设计，中间路由器。该图的左侧与图1-6中的相同。每个协议层随着应用程序数据向下移动堆叠而添加其各自的头。最后，以太网帧通过物理[层]网络发送到路由器。路由器还有一个协议栈，但它只包含1-3层（路由器通常提供一个配置“应用程序”层，但为了讨论的目的，我们将考虑它们的路由功能）。当路由器的数据链路层检查帧的完整性时，它将剥离第2层帧头（和页脚），然后将IP包传递到IP层。路由器分析源和目标IP地址（以及潜在的其他IP报头字段）以确定下一步路由数据包的位置。也就是说，路由器只是到达终端目的地的中间点，因此其协议栈限制到第1-3层。

在路由器确定下一步路由IP数据包之后，它会附加一个修改的IP头（注意图中不同的阴影IP头 - 源和目标IP地址保持不变，但至少有一个其他字段被更改， Live（TTL）字段，其沿着分组路径的每个路由器递减，使得分组不会无限地漫游在互联网上。）路由器然后将IP包传递到数据链路层。数据链路层将IP数据包封装在适合于路由消息的相应链路和物理层的链路层帧内。路由器根据其选择的出接口使用其源链路层（MAC）地址，并根据下一跳IP地址的ARP或ARP缓存映射到相应的MAC地址来识别目的链路层地址。因此，路由器可以通过无线链路在左侧接收输入分组，然后通过以太网链路适当地进行传输。

在接收到链路层的帧时，Device 2的协议栈处理每个连续的层，将其堆栈传递给预期应用。 请注意，数据链路和IP层帧和数据包分别变化链接。 然而，传输层消息和应用数据本身在连接的发送端和接收端是相同的。 当然，目标是完整地发送应用数据，并且相同的TCP / UDP层消息能够实现传输层所需的端到端处理。

我们现在可以得出结论，路由器用于终止图中左侧的数据链路层或冲突域，仅修改IP和MAC头，然后将消息转发到图右侧的第二个冲突域。 因此，路由器也被称为网关，作为第2层冲突域和IP网络之间的网关。 当交换机利用端口VLAN配置在第2层分离冲突域时，路由器使用IP子网来区分第3层的冲突域。

全球IP通信。 我们从图1 - 8中推断出两个通过单个网关互连的设备，通过我的宽带连接在家中使用我的电脑访问世界各地的网络服务器，如图1所示-9。 当我浏览服务器上托管的网站时，我输入或点击的站点地址被捕获并配制成IP数据包，然后通过我的宽带路由器发送到我的服务提供商的路由器Router A。

该传输遵循与图1至图8左侧所示相同的过程。 路由器A然后通过互联网将额外的中间路由器路由我的数据包到由路由器G服务的最终目的地。在路由器的每个链路上，每个路由器终止第2层帧和IP分组，确定下一个路由的下一个 从特定出站接口跳转IP地址），并且制定相应的帧以传输到下一跳。 请注意，图1 - 9中有多条从PC到Web服务器的路径。 我的一个包可能会通过路径A-B-E-F-G从一端到另一端行进，而下一个包可能采取不同的路径，例如A-C-D-F-G，等等。 每个IP包通过网络独立路由。

与传统电话网络从我的电话临时连接到我打过去的的电话的老式电话交换电话对比。 由于我们的语音对话需要在我们讨论期间建立包括通过电话网络的物理路径的连接，所以这种类型的连接被称为“面向连接”。 “在IP层，IP在通信之前不建立连接，并且每个IP数据包都是独立路由的：所有数据包都可能遵循一个共同的端到端路径，它们可能都采取不同的路径，或者更有可能， 在这两个极端之间的某个地方。 因此，IP被认为是“无连接的”。”

面向连接的通信通常提供更可靠的通信方法，代价是绑定网络资源，而不是在连接会话期间围绕中间故障点动态重新路由。在这种情况下，可靠的术语意味着存在检测和从丢弃的分组或分组片段中恢复的方法。 “ 对不起？ “通常在语音通话中工作，某些协议（如TCP）包括具有肯定确认的类似结构。虽然IP本身被认为是不可靠的数据报服务，IP上的传输层（即TCP）可用于覆盖面向连接的控制以提供两个设备或主机之间的可靠通信。 TCP不提供物理连接，提供正确订购传入IP数据包的机制，并且一旦有一个或多个丢失，就要求重新发送IP数据包。 UDP是TCP / IP协议组中的替代无连接传输层协议，提供不可靠的数据传输。相反，可以使用伪层2技术，多协议标签交换，MPLS来逻辑地“钉住”在两个端点之间可以传输IP分组的连接路径。最后，可以沿着干预路由器的路径配置IP静态路由，以确定性地路由数据包。静态路由模拟面向连接的会话，牺牲了无连接重路的优势。

动态路由。 采用IP无连接方案的优点是可以自动检测通信路径中的路由器之间的链路是否中断，并重新路由数据包，保持通信线路的开放。 如果您曾经打过电话并且掉话，那么您就已经遇到了面向连接的通信的缺点：如果路径上的链路发生故障，整个会话将失败。 无连接通信提供了关于中断的自动路由，这种弹性实际上是互联网协议的关键设计目标之一。

沿着IP包的通信路径上的每个路由器检查IP报头中的目的地IP地址，以识别它是否直接服务于目的地IP地址所在的网络，否则将转发到离目的地更近的路由器上。每个路由器都会查询一个内部路由表，该路由表存储有关发往各种IP网络的路由数据包的下一个信息。每个路由器内的路由表管理每个进入的IP分组的路由决策，并且通常指示给定目的网络的路径中的一个或多个下一跳。下一跳是给定路由器可以直接转发数据包的另一个路由器。也就是说，下一跳是相邻或直接连接的路由器，其本身可以直接连接或者距离目的地是多个（希望更少）跳数。以这种方式，每个路由器不需要知道互联网上的每个其他路由器;相反，给定的路由器必须简单地知道其直接连接的对等体中的下一个发送分组以使其更接近其最终目的地。

每个路由器使用路由协议来周期性地与其相邻路由器进行通信，以获得它们当前的路由和可达性信息，以使路由表保持最新。 因此，动态路由使用最近更新的路由信息来进行下一跳路由决策。 如果链路或路由器发生故障，将检测到可达性更改，并通过所选择的路由协议更新可达性指标将通过路由基础架构。 路由协议定义了管理路由器之间的这种“后台”通信的格式和规则，这使得每个路由器能够利用最新的可达性信息维护其路由表。

例如，考虑到图1-9，路由器B将接收来自路由器D，E和F的网络服务器驻留的网络的可达性的广告。这些路由器都不直接用于该网络，而是提供中间路径。使用简单的跳数距离度量，路由器F通告跳数为2，而路由器D和E发布跳数3.推测所选择的下一跳将更接近于预期目的地，即，路由器F，尽管其他数据包流量拥塞等因素可能会发挥作用。现代路由协议现在考虑到超越跳数的更复杂的指标。当接收到来自RouterB的数据包时，所选择的下一跳路由器然后执行相同的基本算法，以确定它是直接服务于IP网络还是将数据包发送到另一个路由器，例如Router G.最终，数据包应到达提供目的地IP地址的路由器进行交付。

组织通常使用两种类型的路由协议。 内部路由协议使组织内的路由器能够传达子网可达性。 流行的内部路由协议包括路由信息协议（RIP / RIP-2），增强内部网关路由协议（Cisco Systems Inc.的EIGRP）和开放最短路径优先（OSPF）。 外部路由协议，例如中间系统到中间系统协议（IS-IS）或边界网关协议（BGP），可以跨组织或路由域更新可达性和度量信息。 我的网络的可达性由我的路由器（或我的互联网服务提供商）使用外部路由协议传送。 BGP是事实上的因特网标准外部路由协议。

组织通常在其内部路由网络上运行内部路由协议，并在其外部路由器接口上运行BGP，例如连接到其Internet服务提供商（ISP）的路由器接口。 然而，对于具有单个ISP连接的组织不向其他组织提供下游路由，BGP不是必需的。 例如，对于具有单ISP连接的小型办公室，不需要BGP。 与一个或多个ISP具有多个互联网连接的多宿主组织相比，这样的最终用户被认为是单一归属的。 BGP总结了通过自治系统（AS）号码识别的组织的可达性信息。 AS号码只是组织标识符，由区域互联网注册管理机构（见第2章）进行分发和管理，以唯一标识组织或更准确地确定路由域。

“BGP总结可达性信息”的说法是什么意思？当使用外部路由协议与互联网进行通信（技术上称为广告）子网可达性时，路由器不会按跳数列出每个子网。这将创造大量的消息传递。称为汇总或聚合的过程使得能够为每个这样的连续的IP地址组在因特网上去通信到单个的网络地址。这样就像路由单词到邮政编码分发中心。国家另一端的中心只需要直到目的地邮政编码中心的路线，然后允许该中心执行本地交付。同样，总结使得路由器能够将连续的一组IP地址与其相对接近度或距离一起识别为单个网络地址，而不是为每个单个IP地址或子网传达这种可达性。通常，组织从Internet注册或ISP获取一组Internet地址，并通过网络地址简单地通告所有这些地址的可达性。然后由组织根据需要在内部开展网络分配以实现Internet可达性。这个块分配过程是IP地址管理的关键过程之一，我们将在第6章中详细讨论。内部路由协议也采用类似的汇总过程。

路由器和子网。 由于路由器作为互连网关和转发或基于层3（IP）信息的路由数据，每个链路需要被分配一组IP地址，子网地址。 给定链路上的每个设备将需要与链接相关联的相应子网地址的IP地址，并且将利用ARP来识别与通过链路传输IP分组的IP地址对应的MAC地址。 IP子网划分的过程需要将IP网络划分成连续的IP地址集或块，然后与每个链路或子网相关联。 基于子网规划，IP地址管理的关键要素就是可以相应地配置路由器。

在路由器上配置子网类似于添加一个新的邮政交付中心。 就像邮政系统必须更新一样，反映新的可用地址，Internet路由器必须同样更新。 幸运的是，在这两种情况下，这通常是一个简单的过程。 在邮政案件中，大多数新的社区都属于现有的邮政编码，只要“邮政系统”的其余部分可以继续向提供此邮政编码的邮政发送中心发送信件，则更新仅限于内部的系统和人员 当地中心或邮政编码。

在互联网世界中，希望在互联网上进行通信的每个组织都需要一套 唯一的IP地址。 组织的IP地址集或块可以比作邮政编码。 发往组织地址集中的设备的任何IP通信将路由到组织的路由器，类似于邮政编码分发中心。 然后路由器处理组织内的“本地传送”。 因此，添加的子网到路由器的配置只影响组内路由器，需要通过内部路由协议进行更新，以识别哪些路由器服务新的子网。

参考图1-3（c）中的示例网络，分公司路由器向10.1.1.0/24网络通告直接可达性，而不是列出0 - 255个IP地址; 这将每个这样的子网将路由表的大小和更新消息从256减少到1，从而减少开销并提高路由器性能。 这就是为什么我们不允许零售商路由器与分公司路由器竞争，为10.1.1.52的IP地址提供服务我在零售商店呆了一天：路由协议消息的开销将创造不必要的流量，牺牲最终用户的生产力流量。 由于路由器只能分析协议栈中的IP层，所以开销也被最小化。 无需完全消化每个帧，它便能够快速识别下一步路由消息的位置。

在我们的总部网络中，如果这三个网络由一个单路由器，路由器可以将其与这些网络的接近度通信在一个路由器中，替代了IP地址的768种可能。甚至每个网络只有三个，有一个为网络服务。 组织您的地址空间以促进此路由器聚合对于保持路由协议通信小，加快更新和路由中断的通信同时实现可扩展性非常重要。

在组织内，地址空间规划必须考虑组织路由拓扑结构中IP设备群体的地址容量需求。 正如我们将在后面的章节中看到的那样，地址分配与路由拓扑的对齐产生了一个有效的地址计划，它将最小化路由协议，更新流量和路由表大小。

互联网协议历史的亮点。互联网协议（IP）是全球最广泛部署的网络层协议。美国国防部在20世纪60年代开始实施的一个美国政府赞助的网络项目，TCP / IP套件最初是在20世纪80年代早期实施的，并且已经发展壮大，以支持从数百台计算机到今天数亿的网络。事实上，根据互联网系统联盟（ISC）调查（2），截至2010年初，互联网上的设备或主机数量已经超过了7.3亿，每年平均每年增加约7500万个主机年（见图1-10）。互联网从研究项目到超过7.3亿台计算机的网络无缝扩张的事实证明了其开发人员的愿景和其基础技术设计的鲁棒性。

互联网协议是在1980年由着名的Jon Postel编辑的请求评论（RFC）760（3）和791（4）中定义的。我引用“最初”，因为Postel先生在序言中指出，RFC 791是基于早期版本的ARPA（美国国防部高级研究计划署，互联网协议），尽管它被提及在RFC中作为版本4（IPv4）。 RFC 791指出，互联网协议执行两个基本功能：寻址和分段。虽然这可能会使实现的互联网协议的许多附加功能和特征变得简单化，并且由此实际上突出了任何协议设计者的这两个主要主题的重要性。分段处理将消息分解成多个IP分组，使得它们可以通过具有有限的分组大小约束的网络来传输，并且以适当的顺序重新组合目的地的分组。寻址当然是本书的主要议题之一，因此确保需要可达性的主机的独特可寻址性对于基本的协议操作至关重要。

互联网已经成为日常个人和企业生产力不可或缺的工具，包括电子邮件，即时通讯，网页浏览以及无线，视频和语音通信等应用。 互联网确实已成为现代社会的关键要素。 术语“互联网”从互联网技术早期开发人员使用的术语小写形式演变而来，指互连网络或“互联网”之间的通信。”

今天，资本化的“互联网”是指我们每天使用的全球互联网，它确实是一个庞大的互联网网络。 大多数企业网络还使用TCP / IP协议栈，宽带，无线和固定电话服务提供商也是如此。 使所有这些网络和其上的主机高效地合作和交换用户通信需要一套强大的这种通信规则。 互联网协议已被证明是非常强大的，以及极其通用和可扩展的。

IP - 地址子网跟踪（IPv4 / IPv6寻址） - 维护一个有力的IP地址分配计划，促进路由聚合，维护准确的IP地址库存，并提供一个自动化的个人IP地址分配和跟踪机制。 这还需要跟踪每个子网上的单个IP地址分配，一些由硬编码分配的IP地址分配，例如路由器或服务器，以及其他动态分配的其他IP地址，如笔记本电脑和VoIP电话。

DHCP - 与之相关的自动IP地址和参数分配位置和设备类型。 这需要在设备上配置的跟踪地址分配，并拨出动态分配的地址池。 这些地址池可以在DHCP服务器上进行配置，以使设备能够请求IP地址并接收位置相关的地址。

**致谢**

首先，我要感谢以下提供的评论者,非常有用的反馈，建议和鼓励：Janet

Hurwitz（开发者和工作/生活平衡者特别），Alex Drescher（真的世界顶级DNS专家之一），Brian Hart（不知疲倦的IP网络天才）和迈克尔·杜利（整体伟大的家伙与独特的混合优秀技术，管理和个人技能 - 感谢您的想法书！）。      我也要感谢以下与我曾经认罪的人，肯定工作，我从中学到了很多关于通信的知识技术和IPAM特别是：John Ramkawsky，Greg Rabil，Steve汤普森，安迪·安布罗西奥，肖恩·费舍尔，克里斯·斯瓦莫，大卫·克罗斯，斯科特梅德拉诺，马可·梅卡雷利，弗兰克·詹宁斯，吉姆·尤特，罗伯·伍德拉夫，拉尔夫Senseny，以及我在BT Diamond IP，INS和阿尔卡特朗讯合作的人。从贝尔实验室的过去的生活中，我感谢安东尼的约翰·马西谢夫斯基（John Marciszewski）Longhitano，Sampath Ramaswami，Maryclaire Brescia,Krishna Murti，GastonArredondo，Robert Schoenweisner，Tom Walker，Ray Pennotti，尤其是我的导师，朱镕基。      我也要感谢我的家人，我的妻子李安娜和我的女儿马耶夫和苔丝，为了忍受我无尽的时间在作家的隔离和sup-

移植我这个经验！