第一部分　IP基础知识

第1章　为何要升级IP

我们都知道岁月的流逝并不会使一些美好的事物消失。但不幸的是，一些现在看来不错的事物并不意味着能够永远使用下去 —— 无论它现在是多么的辉煌，它或者将会过时，或者将被开发殆尽，总会有新鲜的事物遮盖它原有的光芒。而当这种好的事物已经成为基础设施的一部分的时候，对它的维护变得非常重要，而了解何时对它进行升级以及如何以最少的混乱、最低的代价进行升级则显得尤其重要。

IP第4版作为网络的基础设施而广泛地应用在 Internet和难以计数的小型专用网络上，这就是著名的IPv4。IPv4是一个令人难以置信的成功的协议，它可以把数十个或数百个网络上的数以百计或数以千计的主机连接在一起，并已经在全球 Internet上成功地连接了数以千万计的主机。IP协议诞生于70年代中期，可以用几种不同方式表示 IP的存在时间，本章以及本书的其他部分中将有更详细的描述。但是 ,就像被过度使用的桥或高速公路一样， IPv4已经走到了尽头并且必须马上升级。

本章将讨论以下议题：

- 什么是IPv4，为什么它如此重要？
- IPv4中存在哪些问题，它为什么需要升级？
- 为什么我们现在就需要修补 IP而不是等到将来？
- IP的升级对于用户、网络操作员、管理者和供货商究竟有哪些影响？

在本书中，IP用来指网际协议的各个版本，IPv4是指1998年及早些时候使用的IP。IPv6指的是由Internet工程任务组(IETF)制订的用来取代IPv4的新的IP版本，该协议公布在最近发表的IETF的RFC文档中。

1.1　IP的影响

元素、化合物及服务等已经融入了我们 (以及我们的父辈和祖父辈)的日常生活，但IP与此不同，在我们的印象中，它的使用还远不能像使用电力或道路网络一样的熟悉和必不可少。即便如此，无论是个人计算机产品还是大型主机产品，对于 IP的支持实质上已经成为新的计算机硬件、软件或网络设备最普遍的功能之一。网际协议及其相关协议已经取得了 IBM和苹果、微软、网景、 Sun、Novell、康柏、莲花及所有其他主要计算机厂商的共识。本节将介绍以下问题：

- 究竟什么是IP？
- IP可以应用在哪些地方？
- 有多少人、多少计算机和网络在使用 IP？

• 如果IP发生变化，我们能够预计到什么？

1.1.1 什么是IP

IP解决的最根本的问题是如何把网络连接在一起，也就是把计算机连接在一起，而且除了其他计算机的网络地址之外，这些连接起来的计算机无需了解任何的网络细节。这就有以下三个要求：首先，每个连接在“网络的网络”上的计算机必须具有唯一的标识；其次，所有计算机都能够与所有其他计算机以每个计算机都能识别的格式进行数据的收发；最后，一台计算机必须能够在了解另一计算机的网络地址后把数据可靠地传至对方，而无需了解对方计算机和网络的任何细节。IP实现了上述目标。详细的介绍参见第 2章，本节将进行扼要 (可能是非常简单)的介绍。

所谓“网络的网络”就是互联网络(internetwork)，也被简称为互联网(internet)。全球Internet与它们的区别在于它的第一个字母是大写的I。最近，内联网(intranet)逐渐取代互联网用于指称使用TCP/IP的机构网络。

TCP/IP网络协议集基于一个四层的网络互联模型来连接任意两个系统。最底层是物理层，位于物理层之上的是数据链路层，用于在网络媒体 (如以太网电缆或无线发送器)上传输计算机格式的数据。这一层协议使得连接在同种媒体上的两个系统可以通信，但不能与未连接在同一媒体上的系统通信。换言之，所有连接在办公室的以太网集线器上的 PC机之间可以在数据链路层直接进行通信，但也只有连接在该集线器上的计算机才能彼此通信。

在数据链路层，数据被发送到与计算机的网络接口相关联的地址。这意味着每个将计算机连接到网络的设备都有一个类似于序列号的地址：对该连接设备这个地址通常是唯一的，每个设备“侦听”目的地址与自己的地址相同的数据包。如果一个系统没有连接到特定网络上的设备，它就不能与网络上的其他系统在数据链路层上直接通信。

不在同一个物理网络上的系统不能在数据链路层直接进行通信的部分原因，在于连接在不同的网络上的计算机往往使用不同的协议。例如：使用令牌环网的计算机无法理解以太网上传输的数据。另一个原因是链接不同链路层协议的网络需要特殊类型的系统，这种系统被称为网关(gateway)。网关是一个同时连接两个或更多运行不同协议网络的计算机，它可以将来自一种数据链路层协议的数据翻译成另一种协议。但即便有了网关，仍然需要一些其他的办法来连接异构的网络。

数据链路层的上一层被称为网际层，正是在这一层，位于不同物理网络上的设备可以进行通信。每一个接口被分配了一个网际层地址，这个地址在连接在该互联网络上的所有系统中具备唯一性(使用IP连接到网络上的系统通常称为主机)。所有连接在同一个互联网络上的主机可以理解这些地址，并可以在必要时使用各种方法将这些地址与数据链路层的地址进行映射。路由器正是在 Internet层发挥作用的：这些系统 (也可以是网络协议网关)连接在两个或更多的网络上，并由连接到这些网络上的所有主机使用，以向远端网络上转发数据包。

一个需要全球唯一地址的网络示例是电话系统：每个电话用户必须具备一个唯一的电话号码。随着电话网络的扩展和用户数量的增加，电话公司用增加交换局和地区号来加长电话号码的做法并不少见。与电话号码不同，虽然 IP地址也是由数字组成，但它既不能多于也不能少于32位。正如在美国使用的10位电话号码把电话用户的数量

限制在了10^{10}之内，32位地址限制了Internet的地址数量不能超过2^{32}，即接近于40亿。与电话号码一样，真正可用的地址少于理论值(在Internet地址中更少)，这主要是由于一些号码被保留或具备了特殊意义。地址空间的限制是 IPv4的根本问题，本书将进一步讨论这个问题。

当一台主机需要向另一台主机发送数据时，它将检查目的主机的 Internet地址。如果该地址与自己连接在同一物理网络上，则发送端主机简单地通过数据链路层将数据包发送至目的地。在这种情况下，以太网上的发送端主机将通过以太网传输直接到达目的主机。

但是，如果发送端主机发现目的方主机与自己不是连接在同一物理网络上，那么发送端主机将把数据发给与自己连接在同一个物理网络上的路由器。然后，该路由器判断数据的目的地址是否属于与自己直接连接的网络。如果是，该路由器将简单地把数据交给目的主机；如果该数据的目的地址不属于与自己直接连接的网络，该路由器将把数据转发给连接在其他网络上的路由器。如此继续，如果一切顺利的话，直到将数据最终交给与目的主机在同一物理网络上的路由器为止。

其他TCP/IP网络互联操作在传输层和应用层上完成。在传输层上，数据在通信系统的实际进程之间移动；在应用层上，数据在应用自身之间移动。这些层以及网络层将在第2章中详细讨论。

1.1.2 IP应用在哪些地方

许多年以来，只有在大学或研究机构的网络中才能找到 IP的应用。而IP的商用产品直到80年代后期、90年代初期才出现，即使这样，这些产品仍被定位为专用产品。直到 1995年，TCP/IP才被普遍引入到个人计算机产品中，因为从那时起， Novell和微软开始选择IP作为连网协议来支持其打印和文件服务的网络传输。

这意味着正在使用IP的不仅包括每个连接到Internet的计算机，还包括所有使用这些网络操作系统来访问机构资源的所有计算机，而不论这些计算机是否连接到 Internet。

从手提式电脑到功能强大的超级计算机，目前使用的所有计算机几乎都支持 IP。另一方面，IP也越来越多地用于连接其他设备，从而可以任意地使用网页浏览客户机访问内置网页服务器以实现对家用电器和安全系统的远程控制。

使用IP的网络除了Internet之外还包括称作内联网的公司网络，其规模可以从一个办公室中连接在一起的几台主机到分布在全球范围内的所有分支机构的数以万计的主机。 IP网的另一个特例是外联网 (extranet)，它是出于某个共同目标在实体间提供安全连接的专用 IP网。例如，外联网可用于把不同公司的成员连接成一个工作组或把需要传递订货和执行信息的商业伙伴连接起来 (如需了解更多的关于外联网的信息，参见作者的另一本书《 Extranet Design and Implementation》(SYBEX,1997))。

从计算机硬件和软件到家庭娱乐产品、移动电话，甚至支持无线 Internet连接的汽车，这些支持IP的产品的数量体现出IP对于当今世界的通信基础设施的重要性。

1.1.3 有多少人在使用IP

“有多少人在使用连接到IP网络的系统”是一个复杂的问题。对于运行 IP和连接到Internet的网络数量，曾经一度有一个简单的计算方法：可以根据由不同网络授权机构指派的网络地址数量作出判断。可这种方法并不能保证其正确性，因为它忽略了那些运行 IP但没有连接

Internet的网络。

如今情况更加复杂，因为一个网络地址可以分为子网，由使用同一个 Internet服务供应商(ISP)的多个机构共享。与此类似，还有很多机构在连接到 Internet时采用了网络地址翻译技术(这种方法在内部主机 /网络与外部主机 /网络间使用网关作为媒介，网关把只有内部网才能识别的内部网络地址翻译为外部网络能够识别的地址)，在官方的统计数据中同样也不会包含这种网络。以上两种技术将在后续章节进一步讨论，使用这两种技术可以连接更多网络，但同时加大了准确统计Internet网络数量的难度。

即使网络数量的准确统计成为可能，每个网络中包含的主机也并非都可计数。今天，网络中越来越多的公司使用地址翻译技术和防火墙技术把公司的资源隐藏起来，任何一个网络所连接的主机名字和数量对于公司外部的人都很难辨别和获得。

最后，想要统计出通过这些系统访问 IP网络的个人用户数量更是难上加难。大型主机和超级计算机可能有数以百计甚至更多的用户，同时还有一些用户使用多台计算机。结果是必须推测每台计算机上的平均用户数量，实际的数目可能是高达每台计算机 300个用户也可能低至每台计算机1/3个用户。

根据过去十年中令人目瞪口呆的增长速度，研究分析者提出了一些不同的估计，但勿庸质疑的是，Internet上肯定有数千万台主机，且使用 IP的个人用户数量有一亿甚至更多。

1.1.4 当IP发生变化时会产生哪些影响

正如你看到的一样，IP的升级将影响许多人和机构。当从 IPv4向IPv6转变时，可能会发生一些事情，而这些都需要网络管理员来应付。首先，可能没有任何变化：没有软件 /硬件升级、服务不变、一切不变，只要网络管理员选择不进行任何升级或只升级与 Internet的连接。相反，也可能有很大变化，许多新的网络软件需要分发和配置，新的应用需要安装和升级，升级时出现的故障需要应付；此外，升级还会给用户、机构和网络管理员带来显著的好处。

过渡方案以及不同的过渡策略将在第 12章中进一步讨论。

1.2 IPv4的局限性及其缺点

在当前计算机工业飞速发展的步伐下，指出 IPv4的局限性和缺点如同指出小汽车和卡车的内燃机是有缺陷的动力源一样。 IP的确是一个非常强壮的协议，并已经证明了它能够连接小至几个节点，大至 Internet上难以计数的主机。为交通工具选择动力源时，只要能像汽油机或柴油机一样提供动力，任何人都可以使用包括电能、太阳能或是风能作为上路的动力而不会影响别人，与此不同的是， IP的升级将对所有使用IP的人产生重大影响。

TCP/IP的工程师和设计人员早在 80年代初期就意识到了升级的需求，因为当时已经发现IP地址空间随着 Internet的发展只能支持很短的时间。本节将介绍 IP必须升级的原因以及可以同时改进之处，其中包括：

- 地址空间的局限性：IP地址空间的危机由来已久，并正是升级的主要动力。
- 性能：尽管IP表现得不错，一些源自20年甚至更早以前的设计还能够进一步改进。
- 安全性：安全性一直被认为是由网络层以上的层负责，但它现在已经成为 IP的下一个版本可以发挥作用的地方。
- 自动配置：对于IPv4节点的配置一直比较复杂，而网络管理员与用户则更喜欢“ 即插即

用”，即：将计算机插在网络上然后就可以开始使用。 IP主机移动性的增强也要求当主机在不同网络间移动和使用不同的网络接入点时能提供更好的配置支持。

1.2.1 IP地址空间危机

Internet经历了核爆炸般的发展，在过去的10到15年间，连接到Internet的网络数量每隔不到一年的时间就会增加一倍。但即便是这样的发展速度，也并不足以导致 90年代后期IP地址的匮乏。

IP地址为32位长，经常以4个两位十六进制数字表示，也常常以 4个0至255间的数字表示，数字间以小数点间隔。每个 IP主机地址包括两部分：网络地址，用于指出该主机属于哪一个网络(属于同一个网络的主机使用同样的网络地址)；主机地址, 它唯一地定义了网络上的主机。这种安排一方面是IP协议的长处所在，另一方面也导致了地址危机的产生。

由于IPv4的地址空间可能具有多于40亿的地址，有人可能会认为Internet很容易容纳数以亿计的主机，至少几年内仍可以应付连续的倍增。但是，这只适用于IP地址以顺序化分布的情况，即第一台主机的地址为1，第二台主机的地址为2，依此类推。通过使用分级地址格式，即每台主机首先依据它所连接的网络进行标识， IP可支持简单的选路协议，主机只需要了解彼此的 IP地址，就可以将数据从一台主机上转移至另一台主机。这种分级地址把地址分配的工作交给了每个网络的管理者，从而不再需要中央授权机构为 Internet上的每台主机指派地址。到网络外的数据依据网络地址进行选路，在数据到达目的主机所连接的路由器之前无需要了解主机地址。

通过中央授权机构顺序化地为每台主机指派地址可能会使地址指派更加高效，但是这几乎使所有其他的网络功能不可行。例如，选路将实质上不可行，因为这将要求每个中间路由器去查询中央数据库以确定向何处转发包，而且每个路由器都需要最新的 Internet拓扑图获知向何处转发包。每一次主机的地址变动都将导致中央数据库的更新，因为需在其中修改或删除该主机的表项。

IP地址被分为五类，只有三类用于 IP网络，这三类地址一度被认为足以应付将来的网络互联。A类地址只有126个，用于那些最大的实体，如政府机关，因为它们连接着最多的主机：理论上最多可达一千六百万台。 B类地址大约16 000个，用于大型机构，如大学和大公司，理论上可支持超过65 000台主机。 C类网络超过两百万个，每个网络上的主机数量不超过 255个，用于使用IP网络的其他机构。

更小的公司，某些只有几台主机，它们对于 C类地址的使用效率很低；而大型机构在寻找B类地址时却发现越来越难；那些幸运地获得 A类地址的少数公司很少能够高效地使用它们的一千六百万个主机地址。这导致了在过去几年中一直使用的网络地址指派规程陷入了困境，在试图更有效地分发地址空间的同时，还要注意保存现有的未指派地址。与此同时，一些解决地址危机的办法开始得以广泛使用，其中包括无类域间选路 (CIDR)、网络地址翻译和使用非选路网络地址。

IP寻址将在第2章中详细解释，而与 IPv4地址短缺相关的问题、挑战和临时解决方案将在第3章中讨论， IPv6的地址空间将在第6章中详细介绍。

1.2.2 IP性能议题

IP刚开始时，从各方面看就像一个实验品，其主要目的在于为在异种网络间进行数据的

可靠、健壮和高效传输探索最佳机制，从而实现不同计算机的互操作。在很大程度上 IP实现了此目标，但这并不意味着 IP可以继续实现这些目标，也不意味着在对 IP进行修改后而不能更好。在过去的几年中，很明显不仅 IP有改进余地，同时新的开发也导致修改 IP的呼声越来越高。在这次升级中考虑了最大传输单元、最大包长度、 IP头的设计、校验和的使用、 IP选项的应用等议题。针对这些议题已经提出了专门建议并已引入 IPv6中，这将有利于提高 IPv6的性能并改进IPv6作为继续高速发展的网络的基础的能力。

与IPv4性能相关的问题和挑战将在第 3章中讨论，而IPv6的解决方法将在第 7章和第8章中详细解释。

1.2.3 IP安全性议题

刚开始时连入Internet的都是侧重于研究与开发的机构，至少其中的研究人员互相间了解各自的名声，而他们与军队和政府的密切关系也保证了安全性不是一个主要问题。更重要的是，很久以来人们认为安全性议题在网络协议栈的低层并不重要，应用安全性的责任仍交给应用层。在许多情况下， IPv4设计为只具备最少的安全性选项，而 IPv6的设计者们已在其中加入了安全性选项来强力支持IP的安全性。

IPv6安全性的增强无疑将改进虚拟专用网 (VPN)的互操作性。IPv6的安全性特性中包括数据的加密与对于所传输的加密数据和未加密数据进行的身份验证。这些功能也许将被证实是有价值的，但其价值(和功效)将主要体现在政治上而不是技术上。

IPv4的安全性议题将在第 3章中有所介绍，而IPv6对于安全和身份验证的解决方案将在第9章中详细解释。

1.2.4 自动配置

在IP还很年轻时，大部分计算机被放在雕花地板的房间里且其价格超过了大多数人一年(甚至更长时间)的收入。这些系统无法搬到任何其他地方去：它们年复一年地放在一个房间或建筑物中，它们与Internet的连接基本上是静态的，极少改变。那时也没有 ISP，它们通过电话公司提供的线路来链接至其他网络或 Internet骨干网。

现在事情有了些变化。有数百个 ISP可供选择，如果对于用户系统与网络间的选路和转发没有影响的话，理论上用户可以在不同的 ISP间切换，从而更好地利用不同的速率和服务。同样，越来越多用户的工作方式要求网络服务具有更大的移动性。他们可能在家中使用一个或多个系统，可能在世界各地使用所携带的膝上型或笔记本电脑，也可能使用办公室中的任何一部电脑。更复杂的事情在于，这些人可能不只受雇于一个雇主，也可能为多个雇主工作。即便是同一个人使用同一部计算机，该计算机也会频繁地升级或售出。

随着工作和计算机对于移动性要求的与日俱增， IP也必须做出一些改变以适应这种需求。针对这个问题， IPv4已经有了一些改变，动态主机配置协议 (DHCP)可以允许系统在启动甚至只在需要时才通过服务器获取其正确和完整的 IP网络配置。目前，主机 (无论是移动的还是固定的)仍然依赖于到网络的单点连接。当用户携带笔记本电脑出差时，只需给其 ISP打一个电话就可以恢复连接能力。如果该 ISP不能提供区域外的免费长途号码，就需要打长途电话来拨入该ISP。

但是，还可以进行更多的改进， IPv6应该能够旁路到单一ISP的静态连接，让用户系统能

够检测到最近的网络网关并通过它进行连接。目前尚不清楚这个功能如何实现，这里暂不讨论，但IPv6将可能实现该功能，其技术细节将在第 11章中解释。

1.3 紧迫感

对IP地址体系结构不足的官方认可可以参见 1991年发布的RFC 1287，其中定义了IP在成长过程中遇到的问题。至少从 1992年就已开始了网络地址的定量分配，那时候对新的 B类地址提出了要求，而不足以使用 B类地址的中型机构开始接受成块的 C类地址(参见RFC 1366和RFC 1466)。

与最后一分钟(或更晚)才开始的为2000年问题所做的努力不同， IPv6的升级工作体现了多年来许多专职工程师和计算机科学家的努力。他们已完成的工作使 Internet和其他IP网络继续高效地发挥作用并保持多年的增长。