第10章 IPv6

作者：Tim Parker

本章内容包括：

- IPv6数据报
- 多IP地址主机
- 单播、组播及任一广播头
- IPv4到IPv6的过渡

在IPv4(当前版本)开发之时，32位的IP地址似乎足够Internet需要。但随着Internet的增长，32位的地址被证明有问题。正在开发之中的 IP下一代，通常称为IP版本6(IPv6)，就是为了克服这个不足而设计的。

现在人们正针对 IPv6的实现进行研究，其中最流行的是 TUBA(大地址TCP和UDP)、CATNIP(Common Architecture for the Internet, Internet通用体系结构)和SIPP(Simple Internet Protocol Plus，简单Internet协议＋)。三者之中没有一个能满足版本6的所有变化，但是基于其中一个进行改进或折衷却好像可以。

IP下一代必须提供什么？以下变化列表能简单地告诉读者 IPv6的主要特征：

- 128位而不是32位的网络地址。
- IP头中更有效的应用和选项扩展。
- 无头校验和。
- 用于服务质量要求的流标识。
- 不允许有数据报分段。
- 内嵌式的授权和加密安全。

下一节会稍仔细的考查 IPv6，以使这些将影响绝大多数用户、网络程序员以及网络管理员的变化更加清楚。首先看一下IPv6头。

10.1 IPv6数据报

如前所述，IPv6数据报头已经发生了改变。变化主要是提供对新的、更长的128位IP地址的支持以及去掉作废的和不用的域。图10-1显示了IPv6头结构。为比较方便，Ipv4头结构在图10-2中示出。

IP数据报头中的版本号4位长，记录数据报的版本号， IPv6中此数为6。优先级域4位长包括一个说明数据优先级的数值。用于定义传输顺序的优先级，首先设置一个粗略分类值，然后在每一类中再设置范围更精细的标识 (参考10.1.1节)。

流标识24位长并且还在实验阶段。流标识和源机器 IP地址一起提供网络流标识。比如，用户正在使用网络上的UNIX工作站，那么，流标识就和其他如 Windows 95 PC等机器上的流标识不同。这个域能用于标识流特性并提供一定的调节功能。这个域也能帮助大流量的数据传输标识目的机器，在这种情况下缓存系统能在源和目的之间更有效地路由。流标识将在

10.1.2节中更详细地讨论。

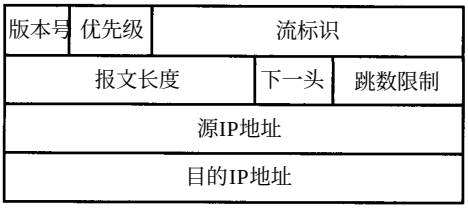

图10-1 IPv6头结构

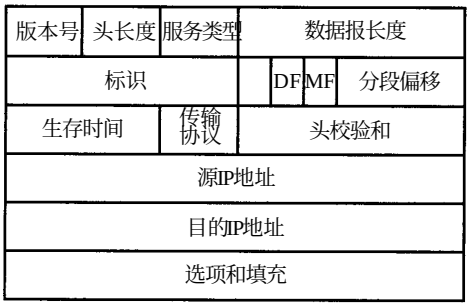

图10-2 IPv4头结构

数据长度域16位，用于指示整个IP数据报的长度，以字节为单位。整个长度不包括 IP头自身。16位域的使用使最大值限制在 65 353之内，但使用扩展头能提供对发送大数据报的支持(参考10.1.4节内容)。

下一个头域用于标识哪一个应用跟在 IP头之后。表10-1列出了为下一个头域定义了几个值。

表10-1 IP下一头域值

值	描 述
0	跳-跳选项
4	IP
6	TCP
17	UDP
43	路由
44	分段
45	域间路由
46	资源预约
50	封装安全
51	认证
58	ICMP
59	没有下一头
60	目的选项

跳数限制域决定了数据报经过的最大跳数。每一次转发，该数值减 1、当跳数限制减少到0时，数据报被丢弃。

最后，128位的源和目的IP地址放置在头中。新的IP地址格式会在10.1.3节中作详细讨论。

10.1.1 优先级分类

IPv6头中的优先级分类首先把数据报分成两类中的一种：有拥塞控制 (congestion-controlled)和非拥塞控制(non-congestion-controlled)。非拥塞控制的报文总是比拥塞控制的报文优先路由。有几种非拥塞控制子类型，但是它们都还没有被接受为标准。

如果数据报是拥塞控制的，它会对网络的拥塞问题很敏感。如果拥塞发生时，会减慢数据的处理。报文会暂时存放在Cache中直到问题解决。拥塞控制这一大类之中，又有几个子类

用于定义数据报的优先极。子类优先级列在表 10-2中。

表10-2 拥塞控制报文优先级

优 先 级	描 述
0	无优先级定义
1	后台流量
2	非特殊照顾的数据传输
3	没分配
4	特殊照顾的块数据传输
5	没分配
6	交互式流量
7	控制流量

非拥塞控制的报文有优先级8到15，但是如前所述，它们没有定义。

每个基本子类的例子可以帮助读者理解数据报优先级。路由和网络管理报文具有最高优先级，给它们分配类7。交互性应用如Telnet和Remote X会话分配交互式报文优先级(类6)。非实时传送，但仍采用交互式控制，如 FTP应用，被分配为类 4。电子邮件被分配为类 2，低优先级如新闻被分配优先级1。

10.1.2 流标识

如前所述，新加到IPv6头中的流标识域能帮助识别一系列 IP数据的发送方和接收方。使用Cache来处理流数据报能更有效地路由。不是所有的应用都能处理流标识，在这种情况下，此域被置为0。

一个简单的例子能说明流标识的用处。例如，一台运行 Windows 95的PC和另一网络上的UNIX服务器连接，并且发送大量的数据报。通过设置一个特殊的流标识给所有传输的数据报，则沿途上的路由器能在路由 Cache中放置一项指出对相同流标识的报文如何路由。当后续具有相同流标识的数据报到达时，路由器不必重新计算路由；路由器仅仅检查 Cache并且取出保存的信息即可。这样加速了通过每一个路由器的数据报处理速度。

为了防止Cache过大或出现一些过时的信息，IPv6规定Cache中维护的信息不能超过6秒钟。如果一个具有相同流标识的数据报在 6秒钟内没到达时， Cache项会被删除。为了防止发送机器产生重复值，发送方必须等6秒钟才能使用相同的到另一目的机的流标识值。

IPv6流标识用于给对时间要求严格的应用保留路由。比如实时应用必须在相同的路由上发送大量数据报且需要尽快地发送 (如视频和音频要求)，可以先在发送数据报之前建立路由。注意在中间路由器上不要超过6秒的限制。

10.1.3 128位IP地址

或许IPng的最重要方面是提供更长 IP地址的能力。版本 6把IP地址从32位增大到128位。这样可以有更多的地址，或许永远也用不尽。

新IP地址支持3类地址：单播、组播和任一广播。

- 单播地址(unicast address) 用于标识一台特定机器的接口，这样可以使 PC使用几种不同的协议，每一种有自己的地址。因此，用户能给特定机器的 IP接口地址发消息而不是NetBEUI接口地址。

- 组播地址(multicast address) 标识一组接口，能使组中的所有机器接收相同的报文。这非常像版本4中的广播，但是定义组更加灵活。用户的机器接口可以属于几个组播组。
- 任一广播地址(anycast address) 用于识别一个组播地址上的一组接口。换句话说也就是同一台机器上的多个接口可以接收报文。

在10.3节中会更加详细地考查这三种类型地址。

版本6的IP头有很大变化，提供更多信息和灵活性。分段和重组的处理也发生了变化，为IP提供更多功能。IPv6的认证性机制能确保数据在发送与接收之间没被破坏，并且发送端和接收端是正确的、不被冒充的。

10.1.4 IP扩展头

IPv6能在IP头上提供附加的头。当到目的地的简单路由不可能时，或者当需要特殊服务如认证时，扩展头就是必要的。所需的额外信息封装在扩展头中并附加在 IP头上。

IPv6定义了几种扩展头类型，用放在 IP头中下一头域中的一位数标识，当前接受的值及其含义列于表10-1中。IP头中可以附加几种扩展头，每个扩展头中的下一头域标识下一个扩展头。正常情况下，扩展头按数值递增的顺序排列，这样便于路由器分析扩展头。

1. 跳-跳(Hop-by-Hop)头

扩展类型0是跳-跳头，这种类型给报文经过的每一台机器提供 IP选项。包括在跳-跳扩展头中的选项包含下面三部分：类型、长度和类型值 (Padl选项除外，Pad1类型为0，没有长度和值域)类型和长度域为1个字节长，值域的长度是可变的，由长度字节指明。

到目前为止，有三种跳-跳扩展头类型：Pad1、PadN和Jumbo Payload。Pad1选项是单字节，类型为0，没有长度和值域，它用于在必要时改变其他选项的顺序和位置，通常由一个应用发出命令。PadN选项是类似的，只是值域中有N个0和一个计算出的长度。

Jumbo Payload扩展选项用于处理大小超过 65 535个字节的数据。IP头的长度域限制为16位，因此数据报大小限制在 65 535个字节内。要处理更大的数据报文，IP头长度域置为0，使路由器重新定向扩展头，找到正确的长度值。扩展头中的长度域使用 32位，超过4TB。

2. 路由头

当发送机器想控制数据报的路由，而不是靠路径上的路由器时，IP头要附加上路由扩展。路由扩展(包括整个路由的IP地址)，给出到达目的地的路由。

3. 分段头

分段头允许一台机器把大的数据报分段成更小的一部分。设计 IPv6的一个目的是防止分段，但是在一些情况下，为了沿着网络发送报文，必须允许分段。

4. 认证头

认证头用于保证数据报的内容没有被改变过。缺省情况下，IPv6使用称为信息摘要5(MD5)的认证策略，只要连接双方达成一致意见，也可以使用其他的认证策略。

认证头包括安全参数索引 (SPI)，SPI和目的IP地址一起定义认证策略。SPI之后跟着认证数据，对MD5而言是16字节长。MD5开始于一个密钥(如果比128位短会填充)，之后附加上整个报文。密钥在末尾标记，MD5算法可以运行。为了防止跳数问题和认证头自身改变值，它们应该置为0，以便于计算认证值。MD5算法产生一个128位的值放在认证头中，在接收端，重复相反步骤。两端必须有相同的密钥，这样策略才能工作。

数据报在产生认证值之前可以使用缺省的 IPv6加密策略Cipher Block Chaining(CBC)进行加密，CBC是数据加密标准(DES)的一部分。

10.2 多IP地址主机

除了潜在的地址耗尽问题，研究人员为什么花这么大力气开发完全不同的 IP地址结构？从IP头的组成，读者或许能看出，在新版本中有许多内在的特点。一个最重要的想法是让每一台主机有多个IP地址。

今天的TCP/IP系统，几乎每台主机都只有单一 IP地址。例外情况是作为网关或路由器的机器，这些设备在每一个相连的局域网接口上有一个 IP地址。单穴主机有一系列优点：通过计算网络上的IP地址数，我们知道存在的机器数。每台主机一个 IP地址，配置网络比多IP主机情况更容易。对用户而言，记住 FTP和Telnet的单一地址比记住大量不同的地址更容易些。DNS和其他服务为了映射要求单 -IP地址，这些服务不得不随着 IPv6而改变。但是使用多地址模型有许多原因。

最有用的一个优点是在多用户机器上提供多地址。如果用户和四个其他用户共享一台工作站(可能是无盘工作站或其他设备)，每个用户使用不同的IP地址会更方便些。这样会使连接到他们自己的文件系统更容易，同时提供更好的跟踪记录和收费功能。每个用户使用不同的IP地址，这样可以使用一些IPv6的加密技术。每个用户使用不同的密钥，加强了安全性。

加密也是多主机地址的一个重要好处。考虑到今天的绝大多数服务器通过各种各样的域实现通信(ftp.tpci.com是FTP域；http://www.tpci.com是WWW域)，所有这些服务在具有相同安全机制的单一主机上运行。使用 IPv6，用户可以让每种服务具有不同的 IP地址(虽然名字可以映射到相同的字母名)。但是基于IP地址可以使用不同的加密或安全认证策略。比如，一个地址可以指向http://www.tpci.com，几乎不需要加密和认证检查；而另一个地址指向 ftp.tpci.com，却使用严格的认证机制来保证只有有效系统允许传输文件。这种服务处理方式基于今天的 IP是可能的，但是IPv6加入了许多新功能。IPv6的缺点是需要许多地址映射到名字。

IPv6的TCP端口号比今天的IP更容易添加。比如，假如想连接服务器上的端口 14，需要使用IP地址和端口号(如255.150.89.1:14)寻址系统。作为用户，要知道端口号。在 IPv6中TCP端口可以很容易地解析为多地址。一个地址可以指向一个 FTP端口，比另一地址指向的FTP端口具有更严格的保护。

当子网汇聚时，多地址可以很好地工作。如果公司有两个局域网，一个用于研究和开发，另一个用于管理，恰好一个管理员管理开发组，那么这个管理员的机器需要在每个网上有一个IP地址。在一些情况下，用户的机器可能作为路由器使用，并且通常需要指出想工作于哪个局域网。使用 IPv6，可以分配IP地址使得用户能立即把信息发送到两个局域网上，或者在两个局域网之间很快地移动数据(实际上去掉了一个路由器)。

10.3 单播、组播和任一播头

单播地址以各种形式得到支持，包括到所有提供者的全局单播地址，以及特定网络的针对于某一站点的单播地址，还有和 IPv4机器兼容的单播地址。 IPv6规范允许其他类型的单播地址，为将来使用。

全局单播地址用于连接Internet上的每一个提供者。这种全局的，或称为基于提供者的单

播地址格式如图10-3所示。

在图10-3中，前3位为010，标识单播地址是基于提供者的类型。 REG ID(Registry ID)域是分配给提供者ID(PROV ID)的Internet地址注册，再由提供者把地址给用户 (提供者ID在绝大多数情况下是ISP)。SUBSC ID允许在提供者的网络中识别多个用户， SUBNET ID允许使用一个特殊地址。最后， INTF ID是接口号，使用它可以标识一个特定用户接口。

一个特定站点的或局部的用户单播地址仅仅在一个网络或子网中使用。因此，它需要的信息较少。局部用户单播地址头如图 10-4所示。INTF ID是网络或子网上的接口号。局部用户单播地址的一些小变化是在头中加入子网号，从 INFT ID域中移去空间。当使用时， SUBNET ID域能用于指定一个网络中的特定子网。

图10-3 基于提供者的单播地址头结构

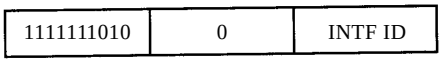

图10-4 局部用户单播头结构

最后，具有嵌入式IPv4地址的单播地址头如图10-5所示。IPv4地址附加在单播头后面，可以让IP的旧版本使用。

任一播地址使用和单播头相同的结构，并且在绝大多数情况下，不能和单播的广播加以区别。

组播头如图10-6所示。

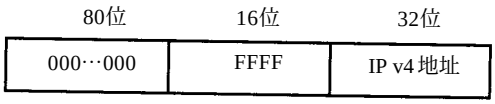

图10-5 嵌入IPv4单播头结构

图10-6 组播头结构

高8位为1标识头为组播。标志域有 4位，前3位为0(为将来使用保留)，最后一位为trailing位，如果此位为 0说明是永久性分配的组播地址；如果此位为 1，说明是非永久性分配的组播地址。

范围域4位用于限制组播到达的范围。范围的合法值如表 10-3所示。最后，组号标识一个特定的组播组。

表10-3 组播范围域的合法值

值	描 述
0	保留
1	局部结点
2	局部链路
3，4	没分配
5	局部站点
6，7	没分配
8	局部组织
9，A，B，C，D	没分配
E	全局
F	保留

10.4 从IPv4到IPv6的过渡

虽然从技术上讲，IPv6优于当今的IP版本(IPv4)，但在全球范围内实现IPv6存在潜在的问题。不可能在某一天简单地从旧的IP版本切换到更新的版本。因此，过渡必须在一段时间内提供两个版本的兼容性。因为在全球范围内建立IPv6仍需几年。因此，二者的过渡就是一个非常重要的问题。

从IPv4向IPv6的过渡会出现的问题是：IPv4嵌入到TCP/IP组件的许多层和许多应用程序中。如果实现到IPv6的切换，那么使用IP的各个应用、驱动程序和TCP栈不得不进行改变。这会涉及到成百上千的变化，牵扯到数以百万行代码的改动。这么多的生产商，不可能在一个特定的时间范围内改变它们的代码。这也意味着IPv4和IPv6必定会共存相当一段时间。

所有现在的机器(主机、路由器、桥等等)使用Ipv4。当机器转向运行IPv6(通过软件或硬件更新)时，所有的机器将会需要两组IP软件，一组用于旧的版本，一组用于新的版本。在一些情况下，这样实现会由于存储或性能问题而变得很困难，所以一些设备不得不只有一个IP版本(或使用功能更强大的设备)。

必须为不能或不会更新至IPv6的应用开发转换软件。比如，一些使用IPv4进行通信的设备和应用，仍需要和IPv6系统进行通信时，会需要一个转化或翻译应用程序，在两部分之间进行翻译。这会增加系统的开销，降低性能，但这可能是惟一的解决合法软件和硬件的方法。

IPv4和IPv6之间的过渡看起来不像是个大问题，但它确实会带来问题。基本问题是头翻译，这个过程中发生的一个极小问题就会导致数据丢失。IPv6是以IPv4为基础的，但二者的头非常不同。IPv6头中的任何不被IPv4支持的信息(如优先级分类)会在转化过程中被丢失。相反的，由IPv4主机生成的报文转化为IPv6报文时将会丢失大量信息，其中有一些可能是重要信息。

地址映射(IPv4地址转换为IPv6地址，或相反)需要一些特殊处理。如果用户有一台主机，此主机具有多个IPv6地址而只有一个IPv4地址，那么转换器、路由器或其他的转发设备必须具有一个大的地址映射来完成一个版本到另一个版本的转换。在大型的组织内这将是不现实的，并且当从IPv4向IPv6转化时可能会导致不正确地目的地。一个IPv4地址可以嵌入到IPv6头中，但这会给基于IPv6的系统带来路由问题。

一些TCP/IP服务到IPv6的转变需要很长的时间。比如DNS，保存了通用名字到IP地址的映射。当IPv6出现时，DNS将不得不处理两个IP版本，并且要为每个主机解析多个IP地址。用户的PC在IPv6下可以有10个IP地址(比如，在机器上不同的服务有不同的IP地址)，DNS必须能够正确地路由报文。

IPv4的广播是一个问题，因为经常性地会出现局域网范围或广域网范围的用IPv4发出的广播报文(ARP最常见)。IPv6使用组播来减少广播，这个特性允许广播报文在局域网或广域网上只经过一次。在转化期间涉及到两个广播系统也会成为问题。

当把整个的网络结构从IPv4转变到IPv6时，会涉及到更多的问题。当公司和网络从一个版本的IP转向另一个版本的IP时会有许多技术问题需要解决，以提供最大化的灵活性。这个过程不会很容易，并且需要许多年。但最终的结构应该是网络完全以IPv6为基础(虽然看起来许多旧的设备将不能升级到IPv6，因此需要某种形式的转译器)，对绝大多数人而言，从IPv4到IPv6的变化将是透明的。网络管理员会小心地为用户做好转换工作。但是对于负责网络管

理的人员而言，从IPv4到IPv6的转化需要经验。

10.5 小结

虽然IPv6要经过许多年才能被广泛使用，但是 IPv6的广泛使用必将发生。无论是一下子就改变还是采取慢慢改变的策略，最终需要实现 IPv6。对绝大多数用户而言，尤其是那些通过ISP连接的用户，实际的改变还要有相当长的时间。然而对公司而言，变化要快一些。 IPv6和IPv4之间的兼容性，会使得旧的IP系统在相当长一段时间内得到支持。