杭州师范大学

研究生学位课程试题及答卷

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 二级学院 | | 信息科学与技术 | | 专 业 | | | 计算机应用技术 | | |
| 研究生姓名 | | 王齐 | | 学 号 | | | 2021111011004 | | |
| 考试课程名称 | | 高级计算机网络 | | | | | | | |
| 授课时间 | | 2021-2022-1 | | | 周学时数 | 3 | | 学分数 | 1.5 |
| 评  语 | （保留） | | | | | | | | |
| 考核论题\* | |  | | | | | | | |
| 成绩 | 平时成绩 | （保留） | 任课教师签名：王伟坤  2021年11月30日 | | | | | | |
| 考试成绩 | （保留） |
| 总评成绩 | （保留） |

注：1、本封面由任课教师填写，并与考试试题、答卷一起装订，写完评语后二周（以论文形式考试的一个月）内交二级学院研究生秘书。由研究生秘书做好成绩登记，在学期结束前，将单科成绩登记表交校研究生处。

2、\*栏，以撰写论文为考核形式的填写；综合考试可不填。

3、学位课程总评成绩须以百分制计分。

4、考试答题一律使用研究生处统一印刷的“研究生课程考试答题纸”。

IPv6过渡技术

摘 要

为了解决IPv4地址即将耗尽的问题，人们提出了IPv6协议。使用IPv6协议可以具有更大的网络规模、更高的通信速度、更有效的网络管理以及更好的安全性。但在IPv6完全取代IPv4之前，必须使用过渡技术进行IPv4 网络和 IPv6网络间的通信。

本文首先对IPv6协议的基本原理进行介绍，接着讲述了当前主流的三种过渡技术：双栈技术、隧道技术和转换机制，最后通过Cisco Packet Trace网络模拟器进行模拟仿真IPv4到IPv6的过渡实验。

**关键字**： IPv6，过渡技术

**IPv6** **Transition Technology**

**Abstract**

In order to solve the problem that IPv4 addresses are about to run out, IPv6 protocol is proposed. Using IPv6 protocol can have larger network scale, higher communication speed, more effective network management and better security. However, before IPv6 completely replaces IPv4, transition technology must be used to communicate between IPv4 network and IPv6 network.

This paper first introduces the basic principle of IPv6 protocol, then describes three mainstream transition technologies: dual stack technology, tunnel technology and conversion mechanism, and finally simulates the transition from IPv4 to IPv6 through Cisco packet trace network simulator.

**Keywords**: IPv6, transition technology

**目 录**

[第1章 新型网络协议——IPv6 5](#_Toc88939087)

[1.1 IPv4与IPv6 5](#_Toc88939088)

[1.2 IPv6基本报头 6](#_Toc88939089)

[1.3 IPv6扩展报头 7](#_Toc88939090)

[1.4 IPv6地址 9](#_Toc88939091)

[1.5 IPv6地址类型 9](#_Toc88939092)

[1.5.1 IPv6单点传送地址 10](#_Toc88939093)

[1.5.2 IPv6多点传送地址 12](#_Toc88939094)

[1.5.3 IPv6任意点传送地址 13](#_Toc88939095)

[第2章 IPv6过渡技术 14](#_Toc88939096)

[2.1 双协议栈技术 15](#_Toc88939097)

[2.2 隧道技术 16](#_Toc88939098)

[2.3 转换机制 19](#_Toc88939099)

[第3章 仿真 20](#_Toc88939100)

[3.1 二进制指数退避算法（BEB） 20](#_Toc88939101)

[3.2 倍数增加线性减少退避算法（MILD） 20](#_Toc88939102)

[3.3 指数增加指数减少退避算法（EIED） 21](#_Toc88939103)

[3.4 倍数增加倍数/线性减少退避算法（MIMLD） 22](#_Toc88939104)

# 新型网络协议——IPv6

## 1.1 IPv4与IPv6

目前IPv4地址主要存在以下3个方面的问题，这些问题是由于Internet网络飞速发展而产生的。

① 超过一半的B类地址已被分配。

② 从Internet长期增长的角度来看，32比特的IP地址是不够的。

③ 当前的路由结构没有层次性，属于平面型结构，即每个网络都需要一个路由表项。随着网络数量的增长，一个具有多个网络的网站就必须分配多个C类地址，而不是一个B类地址，从而导致路由表的规模不断增加。

许多组织和研究人员针对当前IPv4版本存在的问题提出了许多解决方法。采用具有更大地址空间的新版本IP协议，即IPv6，是一种很好的解决方法。IETF早在1992年就提出要制订下一代的IP（IP Next Generation，IPNG），现正式称为IPv6。

IPv6仍支持无连接的传送，但将协议数据单元PDU称为分组，而不是IPv4的数据报。

IPv6所引进的主要变化如下：

① 更大的地址空间。IPv6将地址从IPv4的32bit增大到了128bit，使地址空间增大了296倍。这样大的地址空间在可预见的将来是不会用完的。

② 扩展的地址层次结构。IPv6由于地址空间很大，因此可以划分为更多的层次。

③ 灵活的报头格式。IPv6数据报的报头和IPv4的报头并不兼容。IPv6定义了许多可选的扩展报头，不仅可提供比IPv4更多的功能，还可以提高路由器的处理效率，这是因为路由器对扩展报头不进行处理（除逐跳扩展报头外）。

④ 改进的选项。IPv6允许数据报包含有选项的控制信息，因而可以包含一些新的选项。而IPv4所规定的选项是固定不变的。

⑤ 允许协议继续扩充。这一点很重要，因为技术总是在不断发展，而新的应用也还会出现。但IPv4的功能是固定不变的。

⑥ 支持即插即用（即自动配置）。

⑦ 支持资源的预分配。IPv6支持实时视频等要求一定带宽和时延的应用。

## 1.2 IPv6基本报头

IPv6将基本报头长度变为固定的40字节，称为基本报头（base header）。它将不必要的功能取消了，报头的字段减少到只有8个（虽然报头长度增大了一倍）此外，还取消了报头的检验和字段（考虑到数据链路层和传输层都有差错检验功能），这样就加快了路由器处理数据报的速度。

IPv6数据报在基本报头的后面允许有0个或者多个扩展首部（extension header），再后面是数据。但需注意，所以扩展的报头都不属于基本报头，所有的扩展报头和数据报合起来称为数据报的有效载荷（payload）或净负荷，如图1-1所示。

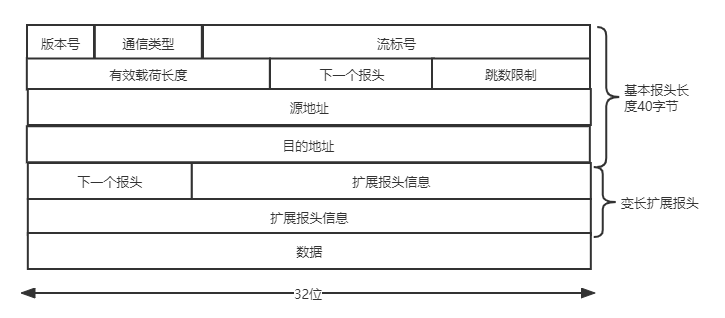


图1-1 IPv6报文格式

IPv6基本报文中各字段的作用如下。

① 版本号（version）：占4位。它指明了协议的版本，对IPv6该字段总是6。

② 通信类型（traffic class）：占8位。这是为了区分不同IPv6数据报的类别或优先级。

③ 流标号（flow label）：占20位。IPv6中一个新的机制是支持资源预分配，并且允许路由器将每一个数据报与给定的资源分配相联系。IPv6提出流（flow）的抽象概念。所谓“流”就是互联网上从特定源点到特定终点（单播或多播）的一系列数据报（如实时音频或视频传输），而在这个“流”所经过的路径上的路由器都保证指明的服务质量。所有属于同一流的数据报都具有相同的流标号。

④ 有效载荷长度（payload length）：占16位。它指明IPv6数据报除基本报头以外的字节数（所有扩展报头都算在有效载荷之内）。这个字段的最大值是64KB。

⑤ 下一个报头（next header）：占8位。它相当于IPv4的协议字段或可选字段。当IPv6数据报没有扩展报头时，下一个报头字段的作用和IPv4的协议字段一样，它的值指出了基本报头后面的数据应交付给IP上面的哪一个高层协议（例如，6或17分别表示应交付给TCP或UDP）。当出现扩展报头时，下一个报头字段的值就标识后面第一个扩展报头的类型。

⑥ 跳数限制（hop limit）：占8位。用来防止数据报在网络中无限期地存在。源站在每个数据报发出时设定某个跳数限制。每个路由器在转发数据报时，要先将跳数限制的值减1。当跳数限制的值为0时，就要将此数据报丢弃。

⑦ 源地址：占128位。是数据报发送站的IP地址。

⑧ 目的地址：占128位。是数据报接收站的IP地址。

## 1.3 IPv6扩展报头

IPv4的数据报如果在其报头中使用了选项，那么沿数据报传送的路径上的每个路由器都必须对这些选项进行一一检查。然而实际上很多选项在途中的路由器上是不需要检查的（因为它们并不使用这些选项的信息），这就降低了路由器处理数据报的速度。IPv6将原来IPv4报头中选项的功能都放在扩展报头中，并将扩展报头留给路径两端的源站和目的站的主机来处理，而数据报途中经过的路由器都不处理这些扩展报头（只有一个报头例外，即逐跳选项扩展报头），这样就大大提高了路由器的处理效率。通常，一个典型的IPv6包没有扩展头，仅当需要路由器或目的节点做某些特殊处理时，才由发送方添加一个或多个扩展头。与IPv4不同，IPv6扩展头长度任意，不受40字节限制，以便日后扩充新增选项，这一特征加上选项的处理方式使得IPv6选项能得以真正利用。但是为了提高处理选项头和传输层协议的性能，扩展头总是8字节长度的整数倍。

在RFC 2460中定义了以下6种扩展报头：逐跳选项报头、路由选择报头、分段报头、认证报头、ESP协议报头和目的站选项报头。

① 逐跳选项报头，包含分组传送过程中每个路由器都必须检查和处理的特殊参数选项。其中的选项描述一个分组的某些特性或用于提供填充。这些选项有：

* Pad1选项（选项类型为0），填充单字节。
* PadN选项（选项类型为1），填充2个以上字节。
* Jumbo Payload选项（选项类型为194），用于传送超大分组。使用Jumbo Payload选项，分组有效载荷长度可达4294967295字节。负载长度超过65535字节的IPv6包称为“超大包”。
* 路由器警告选项（选项类型为5），提醒路由器分组内容需要做特殊处理。该选项用于组播收听者发现RSVP（资源预留）协议。

② 路由选择报头，类似于IPv4 的松散源路由，IPv6的源节点可以利用路由选择扩展报头指定一个松散源路由，即分组从信源到信宿需要经过的中转路由器列表。

③ 分段报头，提供分段和重装服务。当分组大于链路最大传输单元（MTU）时，源节点负责对分组进行分段，并在分段扩展包头中提供重装信息。

④ 认证报头，提供数据源认证、数据完整性检查和反重播保护。认证包头不提供数据加密服务，需要加密服务的数据包，可以结合使用ESP协议。

⑤ ESP协议报头，提供加密服务。

⑥ 目的站选项报头，指明需要被中间目的地或最终目的地检查的信息。有两种用法:如果存在路由扩展报头，则每一个中转路由器都要处理这些选项;如果没有路由扩展头，则只有最终目的节点需要处理这些选项。  
 每一个扩展报头都由若干个字段组成，它们的长度也各不同。但所有扩展报头的第一个字段都是8位的“下一个报头”字段。此字段的值指出了在该扩展报头后面的字段是什么。当使用多个扩展报头时，应按以上的先后顺序出现。高层报头总是放在最后面。

## 1.4 IPv6地址

IPv4地址表示为点分十进制格式，32位的地址分成4个8位分组，每个8位写成十进，中间用点号分隔。而IPv6的128位地址则是以16位为一 分组，每个16位分组写成4个十六进制数，中间用冒号分隔，称为冒号分十六进制格式。IPv6地址中，每个16位分组中的前导零位可以去除做简化表示，但每个分组必须至少保留一位数字。

某些地址中可能包含很长的零序列，为进一步简化表示法， 还可以将冒号十六进制格式中相邻的连续零位合并，用双冒号“::”表示。“::”符号在一个地址中只能出现一次， 该符号也能用来压缩地址中前部和尾部相邻的连续零位。

在IPv4和IPv6混合环境中，有时更适合于采用另一种表示形式：x:x:x:x:d.d.d.d。.其中x是地址中6个高阶16位分组的十六进制值，d是地址中4个低阶8位分组的十进制值（标准IPV4表示）。要在一个URL中使用文本IPv6地址，文本地址应用符号“["和“]”来封闭。

IPv6协议支持地址自动配置，这是一种即插即用的机制。IPv6节点通过地址自动配置得到IPv6地址和网关地址。

IPv6支持无状态地址自动配置和状态地址自动配置两种地址自动配置方式。在无状态地址自动配置方式下，需要配置地址的网络接口先使用邻居发现机制获得一个链路本地地址。 网络接口得到这个链路本地地址之后，再接收路由器宣告的地址前缀，结合接口标识得到个全球地址。而状态地址自动配置的方式，如动态主机配置协议（DHCP）,需要一个 DHCP服务器，通过客户机/服务器模式从DHCP服务器处得到地址配置的信息。

## 1.5 IPv6地址类型

IPv6地址是独立接口的标识符，所有1IPv6地址都被分配到接口，而非节点。由于每个接口都属于某个特定节点，因此节点的任意一个接 口地址都可用来标识一个节点。IPv6 有3种类型的地址:

①单点传送（单播）地址。一个IPv6单点传送地址与单个接口相关联。发给单播地址的包传送到由该地址标识的单接口上。但是为了满足负载平衡系统，在RFC 2373中允许多个接口使用同一地址，只要在实现中这些接口看起来形同一个接口。

②多点传送（组播）地址。一个多点传送地址标识多个接口。发给组播地址的包传送到该地址标识的所有接口上。IPv6 协议不再定义广播地址，其功能可由组播地址替代。

③任意点传送（任播）地址。任意点传送地址标识一组接口(通常属于不同的节点)，发送给任播地址的包传送到该地址标识的一组接口中根据路由算法度量距离为最近的一个接口。如果说多点传送地址适用于one-to-many的通信场合，接收方为多个接口的话，那么任意点传送地址则适用于one-to-one-of-many的通信场合，接收方是一组接口中的任意一个。

### 1.5.1 IPv6单点传送地址

IPv6单点传送地址包括可聚集全球单点传送地址、链路本地地址、站点本地地址和其他一些特殊的单点传送地址。

（1）可聚集全球单点传送地址

可聚集全球单点传送地址，顾名思义是可以在全球范围内进行路由转发的地址，格式前缀为001, 相当于IPv4 公共地址。全球地址的设计有助于构架一个基于层次的路由基础设施。与目前IPv4所采用的平面与层次混合型路由机制不同，IPv6支持更高效的层次寻址和路由机制。可聚集全球单点传送地址结构如图1.2所示。

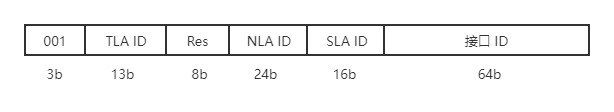


图1.2 可聚集全球单点传送地址

001是格式前缀，用于区别其他地址类型。随后分别是13 位的TLA ID、8位的Res、24位的NLA ID、16 位SLA ID和64位主机接口ID。TLA （Top Level Aggregator, 顶级聚合体）、NLA （Next Level Aggregator, 下级聚合体）、 SLA （Site Level Aggregator, 节点级聚合体）三者构成了自顶向下排列的3个网络层次。TLA是与长途服务供应商和电话公司相互连接的公共骨干网络接入点，其ID的分配由IANA严格管理。NLA通常是大型ISP,它从TLA处申请获得地址，并为SLA分配地址。SLA也可称为订户（subscriber）, 它可以是一个机构或一个小型ISP。 SLA负责为属于它的订户分配地址。SLA通常为其订户分配由连续地址组成的地址块，以便这些机构可以建立自己的地址层次结构以识别不同的子网。分层结构的最底层是网络主机。

Res是8位保留位，以备将来TLA或NLA扩充之用。

（2）本地使用单点传送地址

本地单点传送地址的传送范围限于本地，又分为链路本地地址和站点本地地址两类，分别适用于单条链路和一个站点内。

① 链路本地地址：格式前缀为1111 1110 10，用于同一链路的相邻节点间通信，如单条链路上没有路由器时主机间的通信。链路本地地址相当于当前在Windows 下使用169.254.0.0/16前缀的APIPA IPv4地址，其有效域仅限于本地链路。链路本地地址可用于邻居发现，且总是自动配置的，包含链路本地地址的包永远也不会被IPv6路由器转发。

② 站点本地地址：格式前缀为1111 1110 11，相当于10.0.0.0/8、 172.16.0.0/12 和192. 168.0.0/16等IPv4私用地址空间。例如，企业专用Intranet，如果没有连接到IPv6 Internet上，那么在企业站点内部可以使用站点本地地址，其有效域限于一个站点内部，站点本地地址不可被其他站点访问，同时含此类地址的包也不会被路由器转发到站外。一个站点通常是位于同一地理位置的机构网络或子网。与链路本地地址不同的是，站点本地地址不是自动配置的，而必须使用无状态或全状态地址配置服务。

站点本地地址允许和Internet不相连的企业构造企业专用网络，而不需要申请一个全球地址空间的地址前缀。如果该企业日后要连入Internet，它可以用它的子网ID和接口ID与一个全球前缀组合成一个全球地址。IPv6自动进行重编号。

（3）兼容性地址

在IPv4向IPv6的迁移过渡期中两类地址并存，我们还将看到一些特殊的地址类型。

① IPv4兼容地址：可表示为0:0:0:0:0:0:w.x.y.z或::w.x.y.z（w.x.y.z 是以点分十进制表示的IPv4地址），用于具有Pv4和IPv6两种协议的节点使用IPv6进行通信。

② IPv4映射地址：又一种内嵌IPv4地址的IPv6 地址，可表示为0:0:0:0:0:FFFF:w.x.y.z或::FFF:w.x.y.z。这种地址被用来表示仅支持IPv4 地址的节点。

③ 6to4地址：用于具有IPv4 和IPv6两种协议的节点在IPv4路由架构中进行通信。6to4是通过IPv4路由方式在主机和路由器之间传递IPv6分组的动态隧道技术。

### 1.5.2 IPv6多点传送地址

IPv6的多点传送（组播）与IPv4运作相同。多点传送可以将数据传输给组内所有成员。组的成员是动态的，成员可以在任何时间加入一个组或退出一个组。

IPv6多点传送地址格式前缀为1111 111，此外还包括标志(Flags)、 范围(Scope) 域和组(Group) ID等字段，如图1.3所示。

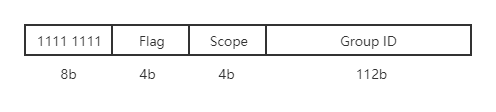


图1.3 IPv6多点传送地址

4位Flags 可表示为000T。其中高三位保留，必须初始化成0。T=0表示一个被IANA永久分配的多点传送地址；T=1 表示一个临时的多点传送地址。4位Scope是一个多点传送范围域，用来限制多点传送的范围。表1.1列出了在RFC 2373中定义的Scope 字段值。

表10.1 Scope 字段值

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 值 | 范围 | 值 | 范围 | 值 | 范围 |
| 0 | 保留 | 5 | 站点本地范围 | F | 保留 |
| 1 | 节点本地范围 | 8 | 机构本地范围 |  |  |
| 2 | 链路本地范围 | E | 全球范围 |  |  |

Group ID标识一个给定 范围内的多点传送组。永久分配的组ID独立于范围域，临时组ID仅与某个特定范围域相关。

### 1.5.3 IPv6任意点传送地址

一个IPv6任意点传送地址被分配给组接口 (通常属于不同的节点)。发往任意点传送地址的包传送到该地址标识的组接口中根据路由算法度量距离为最近的一个接口。目前，任意点传送地址仅被用做目标地址，且仅分配给路由器。任意点传送地址是从单点传送地址空间中分配的，使用了单点传送地址格式中的一种。

子网—路由器任意点传送地址必须经过预定义，该地址从子网前缀中产生。为构造一个 子网-路由器任意点传送地址，子网前缀必须固定，余下的位数置为全“0”，见图1.4 所示。

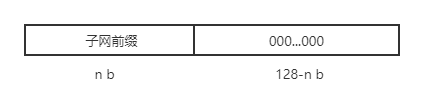


图1.4 子网-路由器任意点传送地址

一个子网内的所有路由器接口均被分配该子网的子网—路由器任意点传送地址。子网—路由器任意点传送地址用于一组路由器中的一个与远程子网的通信。

# IPv6过渡技术

IPv6 与IPv4相比具有诸多的优越性，因此，IPv4被IPv6替代也是一个不可逆转的过程，但是由于IPv4与IPv6协议的不兼容，使得IPv4到IPv6的过渡将是一个长期的过程，其过渡中主要存在的问题如下：

1）协议的兼容性：IPv4和IPv6都是网络层的传输协议，但是IPv4的地址是32位的，IPv6的地址是128位的，这使得二者网络不能直接通信;

2）应用的拓展性：目前网络上大部分业务都是在IPv4协议支持下运作的，虽然IPv6能够更好的支持各种多媒体业务，但是如何在耗费财力物力最小消耗的基础上转移这些业务是一个亟待解决的难题;

3）管理系统的支撑：当前网络上的管理系统不能满足下一代互联网的需求，没有完整的支撑IPv6业务的管理系统;

4）IPv6的安全性：虽然IPv6提供了IPSEC作为保护报文的工具，但是应用层的攻击(如WEB服务器攻击、数据库服务器攻击)、中间人攻击以及泛洪仍然存在。鉴于这些问题的存在，IPv4向IPv6过渡必然是一个长期的渐进的过程，其过渡技术主要有三种：双协议栈技术、隧道技术和转换机制。双协议栈技术指主机或路由器同时运行IPv4和IPv6两个协议栈，同时转发 IPv4和IPv6报文，分别于 IPv4 节点和 IPv6节点通信；隧道技术指将 IPv4 报文封装在 IPv6 隧道中或将 IPv6 报文封装在IPv4隧道中，以完成IPv4 孤岛和IPv6 孤岛间的通信；地址转换指将 IPv4 包头和 IPv6 包头互相转化，以完成 IPv6 节点和 IPv4 节点互相通信。这三种技术各有特点，用于解决不同过渡时期、不同环境的通信问题。

IPv4到IPv6 过渡是个长期渐进的过程要根据不同过渡时期采用不同的过渡技术。

第一阶段：IPv4“海洋”和 IPv6“孤岛”。这一阶段整个互联网仍以 IPv4 协议为主，但也出现了很多 IPv6 试验网，这些试验网规模都很小，就像一些“孤岛”，这时应采取隧道技术来互联各个 IPv6 孤岛。

第二阶段：IPv4“海洋”和 IPv6“海洋”。随着网络的发展出现了越来越多的 IPv6“孤岛”，这些“孤岛”实现互联逐步发展为 IPv6“海洋”，这个时期要综合利用三种过渡技术实现网络间的互联。

第三阶段：IPv6“海洋”和 IPv4“孤岛”。随着IPv6 技术的升级，IPv6成为当前互联网的主要协议，IPv6应用的扩大加速了IPv4应用的减少，最终形成大规模的 IPv6“海洋”和小范围的 IPv4“孤岛”。类似于发展初期，可利用隧道技术实现IPv4孤岛间的互联。

第四阶段：纯IPv6网络。

## 2.1 双协议栈技术

双协议栈技术是指网络中的设备同时支持IPv4和IPv6两种协议，其实现过程是：具有双协议栈的主机将物理截获的信息交给数据链路层，数据链路层检测包头中的信息，区分是IPv6数据包还是IPv4数据包，处理结束后继续向上层传递，网络层（IPv4 和 IPv6 共存）根据底层传上来的包是IPv4还是IPv6分别进行处理，处理结束后继续传给传输层，一直到上层用户应用。其具体模型如图2.1所示：



图2.1 双协议栈模型

双协议栈并行工作的主要难点在于需要同时处理两种不同的地址方案。首先，双协议栈技术要能独立配置IPv4和IPv6地址，双栈节点的IPv4地址可以使用传统的DHCP、BOOTP或手动方式配置来获得，IPv6地址应可以手动配置；其次，采用双协议栈还要解决域名服务服务器（DNS）问题。现有的32位的域名服务器不能解决 IPv6 使用128位地址的问题，为此，IETF定义了一个支持 IPv6 的DNS标准RFC 1886来实现主机域名和IPv6地址的映射。

双栈优点是互通性好、非常容易实现，是目前应用最广泛的过渡技术，缺点是需要给网络设备同时分配IPv6地址和IPv4地址，并没有解决当前IPv6地址的缺乏问题。

## 2.2 隧道技术

隧道（tunnel）技术是一种协议封装结束。随着 IPv6 的发展，会出现越来越多的IPv6“孤岛”，为了实现 IPv4“海洋”中这些“孤岛”的通信就可以利用隧道技术，这种技术要求隧道的两端节点同时支持 IPv4 协议和 IPv6 协议，其运行机制是：隧道入口节点将 IPv6 数据包封装在 IPv4 数据包中，IPv4 数据包的源和目的地址分别是两端节点的IPv4 地址，封装后的数据包经过 IPv4 网络传输到隧道出口节点再解封为 IPv6 数据包并传到目的地，这样便实现了两个 IPv6“孤岛”的通信。隧道的实现方式不同，隧道分组的封装格式也不同。IPv6 网络穿越 IPv4 网络如图2.2所示。

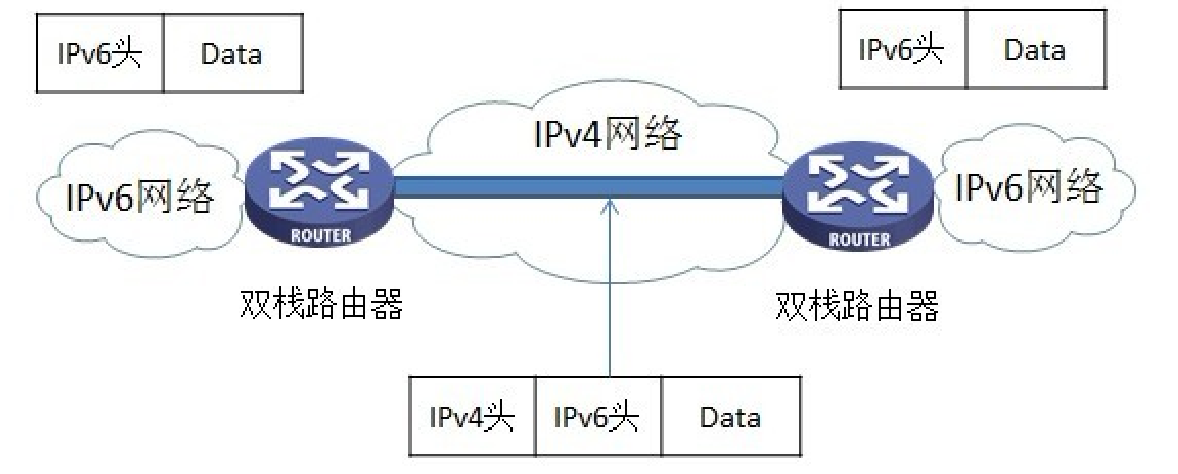


图 2.2 IPv6 穿越 IPv4 隧道

隧道技术本质上是一种封装和解封装的过程，图2.3表示了隧道封装和解封装的机制，图中隧道的端点入口C将IPv6数据包封装在IPv4报文中，将它作为IPv4报文的负荷，并将该IPv4的协议字段设置为41，以说明该IPv4封装报文的负载是IPv6报文，然后在IPv4网络上传输该封装报文，当封装报文达到隧道出口节点D时，该端点解开封装报文的IPv4报头，还原为IPv6数据包并传往目的地。

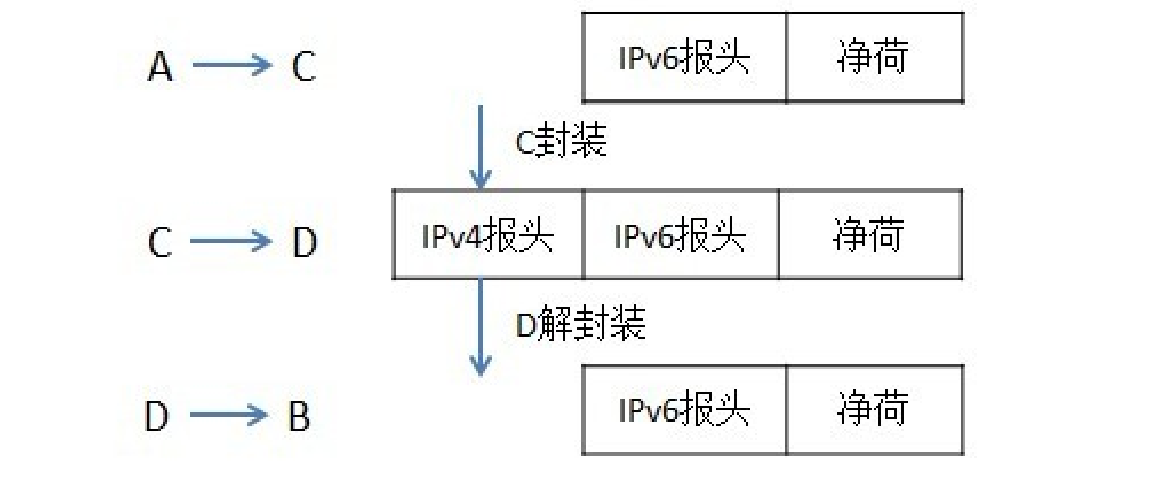


图 2.3 隧道的封装和解封装过程

隧道的类型多种多样，某些类型隧道取决于隧道的终结点（主机、路由器）和终结点的数量，根据这个可将隧道类型分为三种，包括路由器到路由器、主机到路由器或和路由器到主机、主机到主机。

1) 路由器到路由器：这类隧道的起点和终点都是IPv4/IPv6双栈路由器，可以把两个IPv6网络连接起来，对于IPv6网络内的主机来说只需要配置一条指向隧道路由器的IPv6路由即可，如图2.4所示：

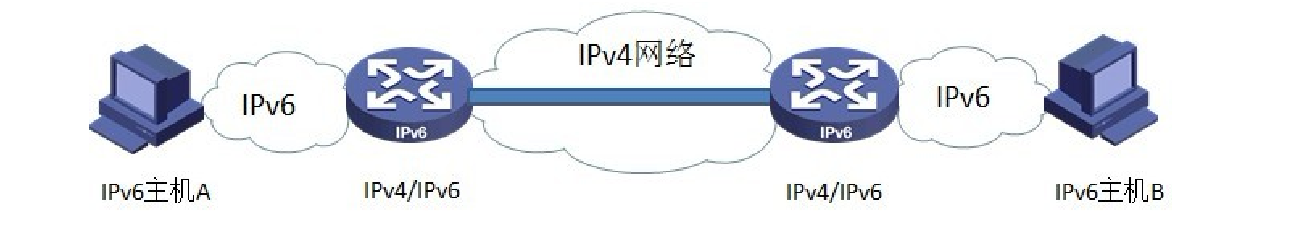


图 2.4 路由器—路由器隧道

当两个 IPv6 网络需要互联时可以采用这种方式，典型的例子包括6to4路由器或与6to4中继路由器互联。

2) 主机到路由器和路由器到主机：这种方式是指讲一个单独的双栈主机通过隧道接入到IPv6网络中，只是隧道的发起端不同。如图 2.5所示，在路由器—主机模式下，路由器首先创建IPv6 over IPv4的隧道接入到双栈主机，即路由器创建一个代表IPv6 over IPv4隧道的虚接口，并在路由表上添加一条到达特定子网的路由；而在路由器—主机模式下，IPv4/ IPv6 主机首先创建IPv6 over IPv4隧道接入到双栈路由器，并创建相应的虚接口，以及一条使用虚接口的路由以到达隧道终点。

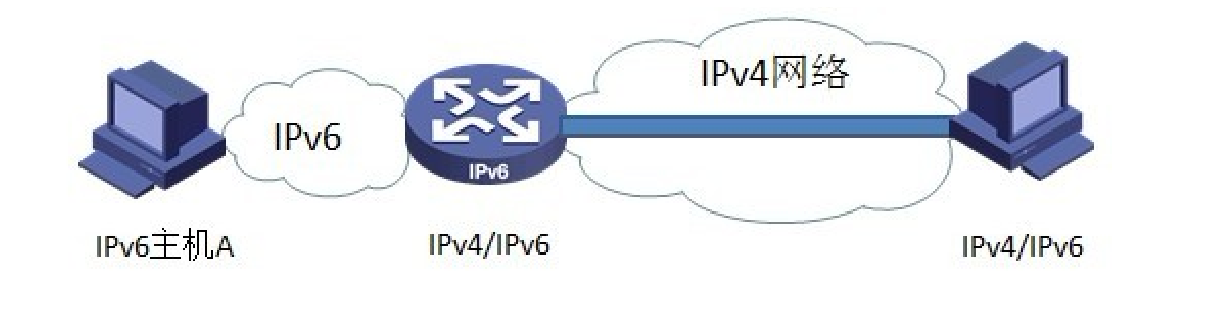


图 2.5 路由器—主机和主机—路由器隧道

这种类型的典型例子包括：ISATAP 主机跨越 IPv4 网络连接 IPv6 网络，以及 ISATAP 路由器跨越 IPv4 网络连接至 ISATAP 主机。

3) 主机到主机：这种模式下，通信的双方都是双栈主机，主机之间可以直接创建隧道而不使用路由器。在每个主机上都会创建一条隧道虚接口，并添加相应的路由条目，以便正确的传送 IPv6 流量到目的地，如图 2.6 所示。

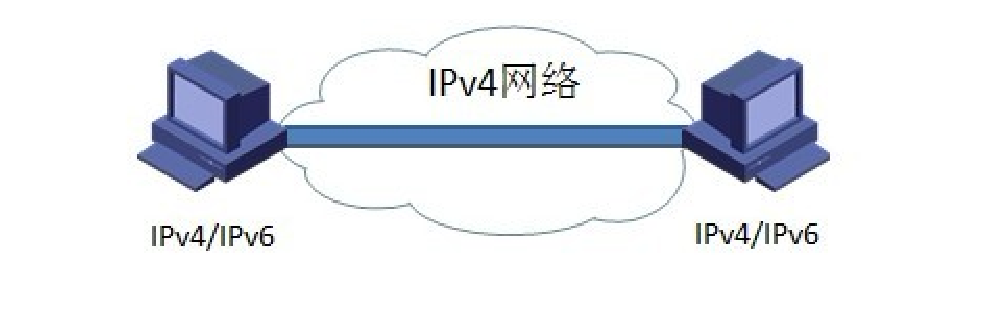


图 2.6 主机到主机隧道

通常双栈主机之间使用ISATAP地址跨越IPv4网络实现互通以及双栈主机之间使用IPv4兼容地址跨越IPv4网络都属于这种类型。

隧道还可以按照 RFC 4231标准分为两类：手工隧道和自动隧道。手工隧道是一种静态指定方式，它的出入口需要手工配置，常用于隧道出入口固定或隧道两端双栈节点的IPv4地址和IPv6地址没有特定关系的情况，在隧道两端节点的配置上，必须指明隧道另一端的IPv4地址，以及静态添加的路由条目；自动隧道则是使用时，隧道接口自动对报文进行封装和解封装，隧道的起点和终点也是不固定的，常见的自动隧道有以下几种形式：6over4、IPv4 兼容IPv6自动隧道技术、6to4、ISATAP、隧道代理等。

## 2.3 转换机制

隧道技术解决了 IPv4 海洋中 IPv6 和 IPv6 通信的问题，而转换机制解决的是纯 IPv6节点如何访问纯 IPv4 节点以及纯 IPv4 节点如何访问纯 IPv6 节点的问题。转换技术根据协议转换在网络中的位置可以分为网络层协议转换、传输层协议转换和应用层协议转换。

# 仿真

## 3.1 二进制指数退避算法（BEB）

二进制指数退避算法己经被广泛的应用于MAC层协议。在算法中每个节点发生冲突以后就使他们的退避间隔双倍直到最大(Bmax)而当成功传输以后就使他们的退避间隔最小(Bmin)。我们可以用下列公式来表示:

二进制指数退避算法(BEB)以它的简单和执行效率高而闻名，但它的公平性却很差。例如，网络中有两个节点争夺信道，每一个节点都有足够的数据要传输当一个节点传输成功，降低它的退避值到最小，因为别的节点传输没有成功，那么它必须以大的退避值和第一个节点竞争信道，第一个节点有很大的概率继续重复访问信道，而第二个节点则继续双倍退避值直到最大。结果，第一个节点独占信道，第二个节点则有很少的机会访问信道。当节点传输成功后，它的退避间隔马上降到最小，当传输失败以后，则以两倍的速度增长直到最大。这样退避间隔的大范围波动势必会影响网络的吞吐量、延迟等性能。

## 3.2 倍数增加线性减少退避算法（MILD）

为了解决BEB不公平的问题,在MACAW协议中介绍了一种新的退避算法倍数增加线性减少退避算法(MILD)。

MILD算法的退避思想为:当站点通信冲突时,竞争窗口CW按α倍增长;当站点通信完成时，竞争窗口CW按常数β线性递减，以这样的方式来控制竞争窗口变小的速度。

在MILD算法中,冲突节点的退避值会变为原来的1.5倍，而成功节点的退避值减1。因为MACAW协议假设一个成功传输的节点有一个与本地争夺层次相关的退避值,那么当前的退避值被包括在每一个传输的包当中，听到成功传输的每个节点都会复制当前的退避值作为自己的退避值，这就是MILD中所谓的复制机制。MILD算法可以用下列公式表示:

CWpacket:是包括在包头的当前退避值。

为了提高公平性，MILD对于每个流只用一个退避值。由于采用复制机制，MILD的公平性有很大的提高。但是这个算法的线性下降退避窗口的策略，在轻负载网络中又导致节点传输效率的降低。

## 3.3 指数增加指数减少退避算法（EIED）

针对前面所述BEB的和MILD退避算法的局限性，美国高级网络技术国家标准技术分局的Nah-Oak Song等人提出一种新的改进算法--增强型的指数增长指数下降退避算法EIED。

它是用来增强IEEE 802.11 DCF性能的退避算法。它执行起来和BEB、MILD算法一样简单，但却大大改善了它们的不足。

EIED是通过调整退避窗口的参数值来加以改进BEB和MILD算法的。主要弥补了BEB算法不合理的退避窗口重设机制和MILD算法的参数是否合适的问题。它的退避窗口是依据传输中是否碰撞或成功的节点，其各自的退避窗口值根据参数成倍增加或减少。与BEB以及MILD算法相比，更加合理地调整了CW值，很好的增强了IEEE 802.11 DCF的性能。

EIED引入了两个参数，分别作用在传输发生冲突或传输成功上。当从节点发出的帧传输时遇到冲突，该节点退避窗口的大小按上升参数Rcollsion(Rcollsion≥1)成倍增加，而不是BEB算法中固定以2，MILD算法中固定以1.5来倍乘。这个参数可以通过网络负载量合理地进行调整，当网络节点数较多即负载较重时，可将参数设为大于2；当然如果网络节点数较少即负载较轻时，可将参数设为小于2。

同样当成功传输顿后，退避窗口的大小按下降参数Rsuccess(Rsuccess≤1)成倍减少，这个参数同样可以根据网络负载量合理地进行调整。既不是BEB算法中统一将CW值重置为最小退避窗口，这在重负载网络中极易引起下一轮冲突；又不是MILD算法中将CW值都减1，这在较轻负载网络中又会导致系统的低效，使众数据倾等待不必要的时间，造成资源的浪费。EIED算法可以用下列公式表示:

EIED的性能是受Rcollsion、Rsuccess这两个参数影响的。也就是说，：当Rcollsion和Rsuccess取的值不同时，EIED退避算法的执行效果也是不一样的。

## 3.4 倍数增加倍数/线性减少退避算法（MIMLD）

倍数增加倍数/线性减少退避算法（MIMLD），这种算法具体实现如下：

在参数CWmin、CWmax的基础上，提出了一个新的参数CWbasic。这个新参数是无线信道竞争强烈与否的门限，它的值被置为接近CWmin。

当退避窗口CW>CWbasic时，就假定无线信道竞争强度很高。如果这时数据帧成功传输，不是把CW立即减为CWmin，而是把当前窗口值的一半与CWbasic比较，取最大值置为退避窗口值，这样做是的退避窗口设置的相对较大，潜在的竞争被最小化，这个阶段被称为“倍数递减阶段”。

当退避窗口CW≤CWbasic时，即信道竞争较小。在成功传输后，当前退避窗口就减1，而不是减半。在活动站数量较少或传输不均匀的时候，小的退避窗口能够带来好的性能。使用线性递减的目的是尽量长时间的保持退避窗口在这一小范围内，递减的太快可能会很快发生冲突，CW就会倍增，从而超出这个小范围。这个递减过程在CW到达CWmin的时候停止。这个阶段称为“线性递减阶段”。

当冲突发生时，如果CW>CWbasic，退避窗口就像原协议的算法一样乘以2。如果CW≤CWbasic，退避窗口就增加到CWbasic的2倍。这样做的原因是尽快从CWbasic以下的范围出来，在这个范围内CW值很小，再在该范围内会造成更多的冲突。这种方法的思想是，小于CWbasic的CW窗口只用于活动中数目很少的时候，这样避免信道的浪费。如果有冲突发生，冲突双方就从该范围跳出来。这种窗口增长阶段就称为“倍数增长阶段”。EIED算法可以用下列公式表示:

这种方法虽然解决了标准协议存在的问题，即竞争节点在成功发送帧后其

退避窗口迅速恢复为最小值，从而可能给信道增加负担。但它们还不能完全适应信道的忙闲程度来调整退避窗口值。而且MIMLD方法中CWbasic取值的确定也是难点。