YD

中华人民共和国通信行业标准

YD/T 1442-2006

IPv6 网络技术要求
——地址、过渡及服务质量

The Technical Requirement for IPv6
——Address,Transition and Quality of Service

2006-06-08 发布　　2006-10-01 实施

中华人民共和国信息产业部　发布

目　次

前　言

本标准是“IPv6协议”系列标准之一，该系列标准的结构及名称预计如下：

1. YD/T 1341-2005　IPv6基本协议——IPv6协议
2. IPv6技术要求——支持计算机移动部分
3. YD/T 1442-2006　IPv6技术要求——地址、过渡及服务质量
4. YD/T 1344-2005　IPv6地址结构协议——IPv6无状态地址自动配置
5. YD/T 1343-2005　IPv6邻居发现协议——基于IPv6的邻居发现协议
6. 《IPv6协议一致性测试方法》

本标准非等效采用IETF的RFC 2460、RFC 2463以及RFC 2473等标准制定。

本标准的附录A为资料性附录，附录B是规范性附录。

本标准由中国通信标准化协会提出并归口。

本标准起草单位：信息产业部电信研究院

本标准主要起草人：魏　亮　姜吕良　杨　崑　柳　扬　薛　宁　王　浩

IPv6网络技术要求
——地址、过渡及服务质量

1 范围

本标准规定了IPv6协议的地址结构、IPv4向IPv6过渡和IPv6网络QoS机制。

本标准适用于使用IPv6协议的设备。

2 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本标准，然而，鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本标准。

RFC1887	IPv6单播地址分配结构
RFC2373	IPv6协议的地址结构
RFC2374	IPv6的可聚合全球单播地址格式
RFC2375	IPv6 组播地址分配
RFC2460	互联网协议——第六版（IPv6）规范
RFC2463	用于 IPv6 的 ICMP 协议
RFC2471	IPv6 实验地址分配
RFC2473	IPv6 规范中的一般分组隧道传送
RFC2474	在 IPv4 与 IPv6 的区分业务字段（DS）的定义
RFC2475	区分业务（DiffServ）体系结构
RFC2529	在IPv4域中不使用显式隧道传输IPv6
RFC2893	IPv6主机，路由器过渡机制
RFC2928	初始IPv6 Sub－TLA ID分配
RFC3053	IPv6隧道代理
RFC3056	通过IPv4云连接IPv6域
RFC3073	基于运营商的单播IP地址格式
RFC3089	基于SOCK的IPv6/IPv4网关机制
RFC3142	IPv6－IPv4中继传输翻译器
RFC3168	附加显式拥塞通知
RFC3177	IAB/IESG关于IP地址的建议
RFC3260	DiffServ 新术语及澄清
RFC3307	IPv6 组播地址分配指导
draft-ietf-ngtrans-satap-24.txt	站内自动隧道寻址协议

3 定义与缩略语

下列定义与缩略语适用于本标准。

3.1 定义

IPv6：互联网协议版本 6。

单播地址（Unicast Address）： 分配给单个接口的标识符，目标地址是一个单播地址的数据包并被发送到该地址所标识的接口。

泛播地址（Anycast Address）：分配给一组接口的地址，该组接口可以属于不同的节点，以泛播地址为目的地址的数据包会被转发到根据路由协议测量的距离最近的一个接口上。

组播地址（Multicast Address）：分配给一组接口的地址，该组接口可以属于不同的节点，目标地址是组播地址的包并被发送到所有由该地址标识的接口。IPv6 中没有广播地址，而是由组播地址代替。

3.2 缩略语

ALG	Application Level Gateway	应用层网关
CIDR	Class-less InterDomain Routing	无类域间路由
DSCP	DiffServ Code Point	DiffServ编码点
DTI	Dynamic Tunnel Interface	动态隧道端口
EUI	Extended Unique Identifier	扩展的惟一性标识
FIB	Forwarding Information Base	转发信息表
FTP	File Transmission Protocol	文件传输协议
HDLC	High level Data Link Control	高级数据链路控制协议
ICMP	Internet Control Message Protocol	因特网消息协议
IGMP	Internet Group Message Proyocol	因特网组消息协议
IGP	Interior Gateway Protocol	内部路由协议
IP	Internet Protocol	因特网协议
IPv4	Internet Protocol Version 4	因特网协议第4版
IPv6	Internet Protocol Version 6	因特网协议第6版
IPX	Internetwork Packet Exchange	网间包交换
MPLS	MultiProtocol Laber Switch	多协议标记交换
NAT	Network Address Translate	网络地址翻译
NAT – PT	Network Address Translate – Port Translate	网络地址翻译—端口翻译
NLA	Next Level Address	下级可聚合地址
NSAP	Network Service Access Point	网络服务接入点
OSPF	Open Shortest Path First	开放最短路径优先
PHB	PerHop Behavior	每一跳行为
PPP	Point to Point Protocol	点到点协议
RPF	Reverse Path Forwarding	反向路径转发
RSVP	Resource ReserVation Protocol	资源预留协议
SLA	Site Level Address	站点级可聚合地址

SLA	Service Level Agreement	服务等级协议
SNMP	Simple Network Management Protocol	简单网络管理协议
SIIT	Stateless IP/ICMP Translation	无状态IP/ICMP翻译
TB	Tunnel Broker	隧道代理
TCP	Transmission Control Protocol	传输控制协议
TEP	Tunnel End Point	隧道末端
TFTP	Trivial File Transfer Protocol	简单文件传输协议
TLA	Top Level Address	顶级可聚合地址
TOS	Type Of Service	服务类型
TTL	Time To Live	生存时间
VOD	Video On Demond	视频点播
WFQ	Weighted Fair Queuing	加权的公平排队算法
WRED	Weighted Random Early Detection	加权的随机早期探测

4 IPv6 地址

4.1 IPv6 地址概述

IPv6地址是为接口或一组接口分配的一个128比特的标识符。IPv6地址有单播地址、泛播地址和组播地址3类。

4.2 地址模型

所有类型的IPv6地址都分配给接口而不是节点。IPv6单播地址与单个接口对应。由于每个接口都属于一个单一节点，所以节点的任何一个接口的单播地址可以当作该节点的一个标识符。

所有的接口都需要至少一个链路本地单播地址。单个接口可以同时被分配任何类型或范围的多个IPv6地址。不作为任何IPv6数据包的源或目的的接口不需要超出链路范围的单播地址，这对于点到点接口来说有时候是方便的。这种地址模型有一个例外：在执行中如果将多个物理接口当作一个来对待，在呈送给网络层时可能会给多个物理接口分配一个单播地址或一组单播地址。这对于多个物理接口上的负载共享是有用的。

当前IPv6继承了IPv4的子网前缀与一个链路关联的模型。多个子网前缀可能属于同一条链路。

4.3 IPv6 地址的语法

IPv6地址有3种通用形式：

首选形式是*x*:*x*:*x*:*x*:*x*:*x*:*x*:*x*，这里*x*是地址中的8个16进制的16比特组。如：

FEDC:BA98:7654:3210:FEDC:BA98:7654:3210

1080:0:0:0:8:800:200C:417A

地址的每个区中前面的0不需要写，但是每个区里至少要有一个数字。

由于分配不同类型IPv6地址的方法不同，通常地址中都会包含长串连续0比特的情况。为便于书写这种地址形式，本标准指定了专门的语法来压缩连续的0比特，即用“::”来代替连续的多组16比特的0。但是“::”在一个地址中只能出现一次，“::”也可以用来代替地址中开头和末尾的连续0比特。

如下列地址：

1080:0:0:0:8:800:200C:417A　　单播地址

FF01:0:0:0:0:0:0:101　　组播地址

0:0:0:0:0:0:0:1　　环回地址

0:0:0:0:0:0:0:0　　未指定地址

它们可以由下列形式代替：

1080::8:800:200C:417A　　单播地址

FF01::101　　组播地址

::1　　环回地址

::　　未指定地址

在既有IPv6节点又有IPv4节点的环境中，采用*x:x:x:x:x:x:d.d.d.d*的地址格式，其中“*x*”是十六进制的数值，用在地址的高位6个16比特组，“*d*”是十进制的数值，用在地址的低位4个8比特组。

例如：

0:0:0:0:0:0:13.1.68.3

0:0:0:0:0:FFFF:129.144.52.38

或者写成省略格式：

::13.1.68.3

::FFFF:129.144.52.38

4.4　地址前缀的语法

IPv6地址前缀的语法类似于将IPv4的地址前缀写入CIDR符号中，IPv6地址前缀由下面形式来表示：

IPv6 地址/前缀长度。

其中IPv6地址是4.3节中任何形式表示的IPv6地址；前缀长度是一个十进制的数值，它表示地址中组成前缀的最左边相邻位的比特数。

下例中给出 60bit 前缀 12AB00000000CD3（十六进制）的合法表示方法：

12AB:0000:0000:CD30:0000:0000:0000:0000/60

12AB::CD30:0:0:0:0/60

12AB:0:0:CD30::/60

而如下表示方法则是非法的：

12AB:0:0:CD3/60 它可能会丢掉了前面的 0，而不是末尾的。

12AB::CD30/60 “/”左边的地址可能会被理解成这样的形式：12AB:0000:0000:0000:0000:000:0000:CD30

12AB::CD3/60 用“/”左边的地址可能会被理解成：12AB:0000:0000:0000:0000:000:0000:0CD3

当需要同时写一个节点地址和该节点地址的一个前缀（如该节点的子网前缀）时，两者可以结合成下面的形式：

节点地址：　　12AB:0:0:CD30:123:4567:89AB:CDEF

子网号：　　12AB:0:0:CD30::/60

也可以省略为：　12AB:0:0:CD30:123:4567:89AB:CDEF/60

4.5　地址类型表示法

地址中前导的比特表示IPv6地址的类型，长度可变的前导比特称作格式前缀，前缀的分配方法见表1。

表1 地址前缀的分配方法

分配情况	前缀（二进制）	占地址空间的比例
保留	0000 0000	1/256
未分配	0000 0001	1/256
留作NSAP地址	0000 001	1/128
留作IPX地址	0000 010	1/128
未分配	0000 011	1/128
未分配	0000 1	1/32
未分配	0001	1/16
可聚合的全局单播地址	001	1/8
未分配	010	1/8
未分配	011	1/8
未分配	100	1/8
未分配	101	1/8
未分配	110	1/8
未分配	1110	1/16
未分配	1111 0	1/32
未分配	1111 10	1/64
未分配	1111 110	1/128
未分配	1111 1110 0	1/512
链路本地单播地址	1111 1110 10	1/1024
站点本地单播地址	1111 1110 11	1/1024
组播地址	1111 1111	1/256
注：1）“未指定地址”（见4.6.2）、环回地址（见4.6.3）和内嵌IPv4地址的IPv6地址（见4.6.4）都在0000 0000格式前缀空间之外进行分配。 2）在EUI-64格式中，除了组播地址（1111 1111）的格式前缀001到111，都必须有64比特的接口标识符，详见4.6.1中的定义。		

这种地址前缀的分配方法支持聚合地址、本地地址和组播地址的直接分配，同时为NSAP地址和IPX地址作了预留。剩余的地址空间留给将来的需要。这可以用作对已有应用（比如：附加的可聚合地址等）或新的应用（比如：分离定位符和标识符）的扩展，初次分配的地址占整个地址空间的15%，其余的85%留作将来使用。

单播地址通过地址高位字节的值与组播地址区分开来，高位字节值为FF（11111111）表示该地址是组播地址，其他值则表示该地址是单播地址。泛播地址是单播地址空间中的一部分，并且在语法构成上与单播地址并没有区别。

4.6 单播地址

4.6.1 单播地址格式

IPv6单播地址是连续的、以比特为单位的可掩码地址。单播地址和带有CIDR的IPv4地址很相似。

在IPv6中，有以下几种类型的单播地址：可聚合全球单播地址、NSAP地址、IPX分级地址、链路本地地址、站点本地地址、可能的IPv4主机地址以及可能在将来另外定义的地址。

IPv6节点对IPv6地址的内部结构的了解可多可少，取决于该节点的功能。最简单的情况下，一个节点可能把一个IPv6地址当成一个128比特长的字符串，如图1所示。

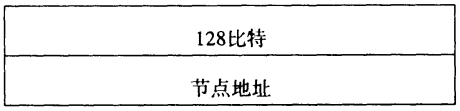


图1 IPv6 地址的内部结构

稍微复杂的节点可能会通过表示子网的前缀来把IPv6地址结构分成两部分，由网络前缀和接口标识组成，如图2所示，不同的地址*n*有不同的值。

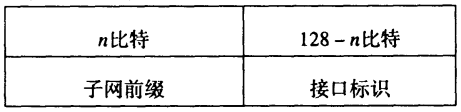


图2 IPv6 地址的内部结构

单播地址中更复杂的节点可以有其他的分级方式。路由器可以更具体地了解一级或多级结构的边界。了解的程度取决于路由器在路由结构中所处的位置。

4.6.2 接口标识

在IPv6单播地址中，接口标识用来分辨在一个链路中的多个接口。在同一链路中标识必须惟一，在更广的范围内标识也可能惟一。大多数情况下，接口的标识与接口的链路地址是相同的。在同一节点上多个接口可以使用相同的接口标识。

不同节点使用同一接口标识并不影响该接口的全球惟一性（使用该接口标识的每个IPv6地址的全球惟一性）。

在很多格式前缀中，接口标识要求64比特长并按IEEE EUI-64格式构建。当全球令牌可用时，基于接口标识的EUI-64号码可以是全球范围的；不可用时，可以是本地范围的。当从EUI-64形成接口标识时，需要进行“u”比特（IEEE EUI-64术语中的universal/local比特）置换。“u”比特被设为“1”说明是全球范围；设为“0”说明是本地范围。在EUI-64的二进制标识中，前三个8位字节如图3所示。

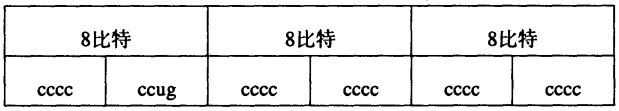


图3 EUI-64 的二进制标识中前三个 8 位字节

在因特网标准的比特顺序书写中，“u”代表universal/local 比特，“g” 代表 individual/group 比特，“c”代表 company_id比特，参见附录A。

在构建接口编号时对“u”比特进行转换，主要是考虑到硬件令牌失效时，管理员程序手动配置本地范围的标识可以更容易。可以想象，在串行链路，隧道端点有这种情况发生。方法是使用0200:0:0:1，0200:0:0:2等形式替代::1，::2。

在IEEE EUI-64标识中使用universal/local位，未来技术发展就可以在全球范围内使用接口标识。

4.6.3 未指定地址

地址 0:0:0:0:0:0:0:0 称为未指定地址。该地址不能被分配给任何节点。节点在初始状态如果不知道自身的地址，可以把它作为数据包的源地址。未指定地址不能作为目标地址，也不能用于路由报头。

4.6.4 环回地址

单播地址0:0:0:0:0:0:0:1称为环回地址。节点可以用它来给自己发IPv6的信息包。它不能被分配给任何实际接口，但可以被认为是一个虚拟接口。

在IPv6信息包中，环回地址不能作为源地址向外传送。目的地址为环回地址的IPv6的包不能被送到该节点以外，也不能被IPv6的路由器转发。

4.6.5 内嵌有 IPv4 地址的 IPv6 地址

对主机和路由器来说，IPv6的传送机制还包括在IPv4路由结构上动态的隧道传送IPv6包。使用这种技术的IPv6节点需要分配特殊的IPv6单播地址，在该地址的低32比特携带IPv4地址。这种地址称作IPv4兼容的IPv6地址，格式如图4所示。

80比特	16比特	32比特
0000……0000	0000	IPv4地址

图4 IPv4 兼容的 IPv6 地址

这里还定义一种内嵌有IPv4地址的IPv6地址。这种地址代表IPv6中的只能是IPv4类型的节点的地址，称为IPv4映射IPv6地址。格式如图5所示。

80比特	16比特	32比特
0000……0000	FFFF	IPv4地址

图5 内嵌有 IPv4 地址的 IPv6 地址

4.6.6 NSAP 地址

在RFC1888中定义了如何将NSAP地址映射成IPv6地址。本标准推荐那些已经计划或开展OSI NSAP编址计划和希望开展或转变到IPv6的网络实施者，应重新设计一个本地的IPv6编址方案以适应其需要。然而，RFC1888也定义了一系列的机制用来在IPv6网络中支持OSI NSAP编址。如果必须在IPv6网络中支持OSI NSAP编址，那么这些机制就是必须的。RFC1888还定义了在OSI地址格式中IPv6的地址映射。

4.6.7 IPX 地址

IPX 地址到 IPv6 地址的映射如图 6 所示。

7比特	121比特
000010	待定义

图6 IPX 地址到 IPv6 地址的映射

4.6.8 可聚合全球单播地址

可聚合全球单播地址定义见附录B。这种地址格式既支持基于聚合常规提供者的聚合，又支持一种新的称为交换的聚合。这样可以为与提供者直接相连的站点和与交换相连的站点提供足够的路由聚合。站点可以选择连到任一聚合点。

IPv6聚合全球单播地址格式如图7所示。

3比特	13比特	8比特	24比特	16比特	64比特
FP	TLA ID	RES	NLA ID	SLA ID	Interface ID

图7 IPv6 聚合全球单播地址格式

这里：

001　　可聚合全球单播地址格式前缀（3 比特）

TLA ID　　顶级可聚合标识

RES　　预留

NLA ID　　下级可聚合标识

SLA ID　　站点级可聚合标识

Interface ID　接口标识

具体定义见附录B。

4.6.9 IPv6的单播地址的本地使用

有两种类型的本地使用单播地址：链路本地和站点本地。链路本地是指在单个链路上使用，站点本地是指在单个站点上使用。链路本地地址格式如图8所示。

10比特	54比特	64比特
1111111010	0	接口标识

图8　链路本地地址格式

链路本地地址可以用于自动地址配置、邻居发现或者在没有路由器时使用。

路由器不需要传送任何源或目的地址为链路本地的信息包给其他链路。

站点本地地址格式如图9所示。

10比特	38比特	16比特	63比特
1111111011	0	子网标识	接口标识

图9　站点本地地址格式

站点本地地址用来在站点内部进行编址，而不需要考虑全球的前缀。

路由器不需要把任何源或目的地址为站点本地的信息包送出该站点。

4.7 泛播地址

一个泛播地址可以被同时分配给多于一个的属于不同节点的网络接口。其特点是以泛播地址为目的地址的数据包会被转发到根据路由协议测量的距离最近的接口上。

泛播地址从单播地址中划分出来。可以使用任意已定义的单播地址格式。因此，泛播地址从语法上无法与单播地址区分。当一个单播地址被配置在多个接口上时，该单播地址就变为泛播地址，同时该节点必须被明确的配置以明白该地址是一个泛播地址。

对任意已分配的泛播地址，都有一个最长的地址前缀P。该地址前缀标识了属于同一泛播地址的所有接口所在的拓扑区域。在这个由 P 标识的区域中，泛播地址的每个成员必须作为一个单独的个体在路由系统中进行广播（通常作为主机路由来进行引用）；而在该区域之外，该泛播地址必须以地址前缀P而聚合到路由广播中去。

需要指出的是，在最坏的情况下，一个泛播地址集合的地址前缀可能是一个空的前缀。也就是说，该集合的成员可能没有本地的拓扑区域。在这种情况下，该泛播地址必须作为单独的路由项在整个因特网上广播。必须对因特网该支持多少个这种“全球”性的泛播地址提出严格的要求。

泛播地址的一个预期应用是用来标识同属一个因特网业务提供商的路由器集合。泛播地址可以作为IPv6路由包头中的一种中间地址，用来强制该数据包经过某个特定的聚合或聚合系列而被转发。其他一些可能用途包括：标识那些连接在某个特定子网的路由器集合；标识提供到某个特定路由域的入口的路由器的集合。

在因特网上还没有广泛、任意使用泛播地址的经验；而且有一些已知的大量使用泛播地址带来的复杂性和危险性。基于这些理由，关于IPv6泛播地址有以下严格要求，直到能获得更多的经验和解决这些问题的方案。这些限制如下：

——泛播地址不能作为一个 IPv6 数据包的源地址；

——一个泛播地址不能分配给一个主机，也就是说泛播地址只能分配给路由器。

4.7.1 必须的泛播地址

子网路由器泛播地址是预定义的。其地址格式如图10所示。

*n*比特	128 - *n*比特
子网前缀	接口标识

图10 泛播地址格式

泛播地址中的子网前缀是指标识一个特定链路的一个泛播地址。此泛播地址与该链路上的接口部分设为零的单播地址等同。

以子网泛播地址为目的地址的数据包会被转发到该子网的一个路由器上。所有路由器要求支持其所有接口的子网对应的子网路由器泛播地址。

提出子网路由器泛播地址目的是用于那些需要与一个远程子网中的路由器集合中的一个路由器进行通信的应用。例如，当移动主机需要与其“家乡”子网上的移动代理进行通信。

4.8 组播地址

一个IPv6的组播地址用于标识一组节点。一个节点可以属于多个组播地址组。组播地址格式如图11所示。

8比特	4比特	4比特	112比特
11111111	标志	范围	组标识

图11 组播地址格式

该格式中起始的 11111111 表示该地址是一个组播地址。

标志域中含 4 个标志：

0	0	0	T

其中高位的三个标志被预留，在初始化时需为零。

T 标志若为“0”，则表示该地址是一个永久分配的（知名的）组播地址,；由全球因特网权威组织统一分配；T 标志若为“1”，则标识该地址是一个非永久分配的组播地址。

长度为 4 比特的范围域决定该组播地址的有效范围。详细情况如下：

0 预留

1 节点本地范围

2 链路本地范围

3 未分配

4 未分配

5 站点本地范围

6 未分配

7 未分配

8 组织本地范围

9 未分配

A 未分配

B 未分配

C 未分配

D 未分配

E 全球范围

F 预留

组标识域（group ID）在该地址的指定范围内永久性或者临时性地标识该组播组。

永久分配的组播地址与该地址的有效范围是独立的。举例来说，如果“NTP服务器组”被分配了一个永久组播地址，并且其组标识为101，那么:

FF01:0:0:0:0:0:0:101 表示与发送者处在同一节点的所有 NTP 服务器；

FF02:0:0:0:0:0:0:101 表示与发送者处在同一链路的所有 NTP 服务器；

FF05:0:0:0:0:0:0:101 表示与发送者处在同一站点的所有 NTP 服务器。

FF0E:0:0:0:0:0:0:101 表示因特网上的所有 NTP 服务器。

非永久分配的组播地址只在指定范围内有意义。例如，在某个站点内的非永久组播地址FF15:0:0:0:0:0:0:101，与其他站点内的具有相同地址的组播地址组没有任何关系，与组标识相同的但有效范围不同的非永久组播地址组也没有关系，与组标识相同的永久组播地址组也没有关系。

组播地址不能用在IPv6数据包的源地址域中，也不能出现在任何路由头中。

4.8.1 预定义的组播地址

以下是预定义的知名组播地址。

预留的组播地址：

FF00:0:0:0:0:0:0:0

FF01:0:0:0:0:0:0:0

FF02:0:0:0:0:0:0:0

FF03:0:0:0:0:0:0:0

FF04:0:0:0:0:0:0:0

FF05:0:0:0:0:0:0:0

FF06:0:0:0:0:0:0:0

FF07:0:0:0:0:0:0:0

FF08:0:0:0:0:0:0:0

FF09:0:0:0:0:0:0:0

FF0A:0:0:0:0:0:0:0

FF0B:0:0:0:0:0:0:0

FF0C:0:0:0:0:0:0:0

FF0D:0:0:0:0:0:0:0

FF0E:0:0:0:0:0:0:0

FF0F:0:0:0:0:0:0:0

以上是预留的组播地址。这些地址不能分配给任何组播组。

所有节点地址：

FF01:0:0:0:0:0:0:1

FF02:0:0:0:0:0:0:1

以上组播地址标识所有IPv6节点组。有效范围分别为节点本地范围或链路本地范围。

所有路由器地址：

FF01:0:0:0:0:0:0:2

FF02:0:0:0:0:0:0:2

FF05:0:0:0:0:0:0:2

上述组播地址标识所有IPv6的路由器地址组，有效范围分别为节点本地范围、 链路本地范围和站点本地范围。

请求节点地址：

FF02:0:0:0:0:1:FFXX:XXXX

该组播地址作为节点的单播和泛播地址的功能而计算的。该地址由两部分组成：一部分是取该地址（单播或泛播）的低24比特，并拼接到前缀FF02:0:0:0:0:1:FF00::/104后面，一共128比特组成一个组播地址。该地址范围是从FF02:0:0:0:0:1:FF00:0000到FF02:0:0:0:0:1:FFFF:FFFF。例如，与地址4037::01:800:200E:8C6C相对应的请求节点组播地址为FF02::1:FF0E:8C6C。这样对那些由于不同地址聚合需要、只是高位不同的IPv6地址将会映射到相同的请求节点地址，从而减少了节点必须加入的组播地址。

节点必须针对其被分配的每个单播和泛播地址都计算并加入相应的请求节点组播地址。

4.8.2 新的 IPv6 组播地址分配

当前，以太网由IPv6组播地址映射到IEEE802 MAC地址的途径是取IPv6组播地址的低32比特，用其生成MAC地址。需要指出的是，令牌环网络采用不同的方法。组标识≤32比特的可以生成惟一的MAC地址。新的IPv6组播地址在分配时应该按图12所示，组标识总是在最低的32比特。

8比特	4比特	4比特	80比特	32比特
11111111	标志	范围	保留（0）	组标识

图12 新的 IPv6 组播地址的分配

由于一共只有2～32个永久的IPv6组播地址可以分配，因此将来可能出现不足。如果将来有必要突破该限制，组播地址仍会工作，但是处理会变慢。

其他的IPv6组播地址由IANA定义和登记。

4.9 一个节点应有的地址

一个主机要求能识别以下可以标识其自身的地址：

— 其每个接口的链路本地地址；

— 分配的单播地址；

— 环回地址；

— 所有节点组播地址；

— 对应每个被分配的单播和泛播地址的请求节点组播地址；

— 该主机所属的所有组播地址。

路由器除了需要识别主机能识别的地址外，还需要加上以下地址来标识自身：

— 在其被配置为路由器的接口上的子网路由器泛播地址；

— 该路由器被配置的其他泛播地址；

— 所有路由器组播地址；

— 该路由器属于的所有其他组播地址。

在实现中应预定义的合适地址前缀有：

— 未指明的地址；

— 环回地址；

— 组播前缀；

— 局部使用的前缀（链路本地和站点本地）；

— 预定义的组播地址；

— 与 IPv4 一致的地址。

实现时应假定其他所有地址为单播地址，特别指定时例外（如指定为泛播地址）。

4.10 IPv6 地址分配原则

— 全国范围互联网运营商建议采用/28 – /35 地址；

— 个人用户建议采用/64 地址；

— 中小型企业建议采用/48 地址；

— 大型企业用户以及地区性互联网运营商建议采用/40 地址；

— 企业网内部最小子网建议采用/80。

5 IPv4 向 IPv6 的过渡

5.1 过渡概述

由于因特网的规模以及目前网络中数量庞大的IPv4用户和设备，IPv4向IPv6的过渡不可能一次性实现。因此IPv4向IPv6的过渡必须是一个循序渐进的过程。能否顺利地实现从IPv4向IPv6的过渡也是IPv6能否取得成功的一个重要因素。

IPv6在设计过程中就已经考虑到IPv4向IPv6的过渡问题，并提供了一些特性使过渡过程简化。目前针对IPv4向IPv6过渡问题已经提出了许多机制，其实现原理和应用环境各有侧重。

在IPv4向IPv6过渡的过程中，必须遵循如下的原则和目标：

— 保证 IPv4 和 IPv6 主机之间的互通；

— 保证原有 IPv4 网络服务；

— 保护以往投资；

— 在更新过程中避免设备之间的依赖性；

— 过渡过程易于理解和实现；

— 过渡可以逐个进行；

— 充分考虑 IPv4 与 IPv6 长期共存情况；

— 用户、运营商可以自己决定何时过渡以及如何过渡。

新建网络可以采用双协议栈网络设备分别为IPv4用户提供IPv4网络服务，为IPv6用户提供IPv6服务。已建成IPv4网络对于IPv6专线接入用户提供透传服务可以采用配置隧道技术。新建纯IPv6网络建议支持以隧道方式传送IPv4分组。运营商可以设置网关采用协议转换等方式支持IPv4和IPv6相互翻译。

5.2 过渡策略与技术概述

过渡策略与技术主要分类如图13所示。

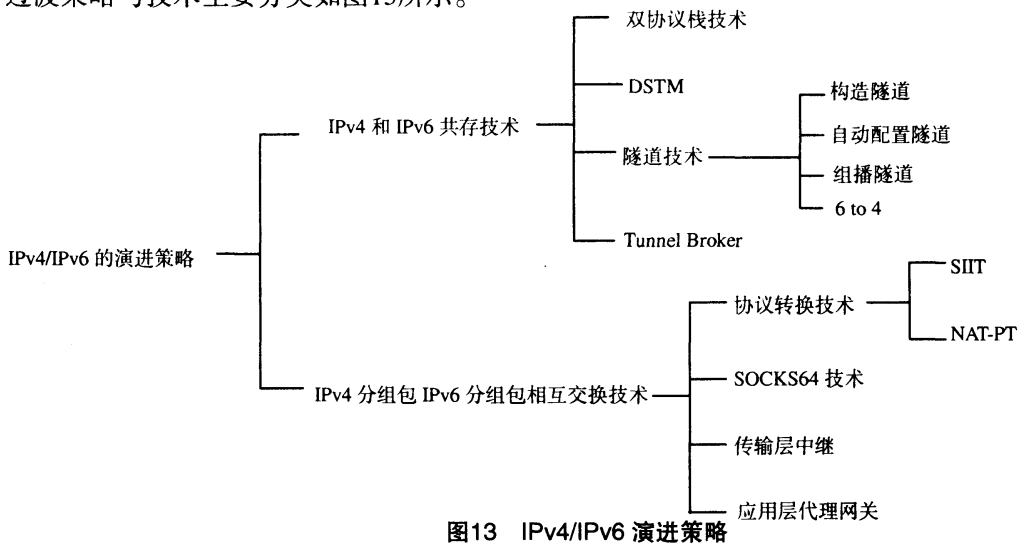


图13 IPv4/IPv6 演进策略

5.3 双栈策略

5.3.1 双栈策略概述

实现IPv6节点与IPv4节点互通最直接的方式是在终端设备和网络节点同时实现IPv4与IPv6协议栈。实现双栈的节点可以使用IPv4与IPv4节点互通，也可以直接使用IPv6与IPv6节点互通。

双栈方式的工作过程可以简单描述为：

— 若目的地址是一个 IPv4 地址，则使用 IPv4。

— 若目的地址是“IPv4 兼容”IPv6 地址，则将 IPv6 分组封装在 IPv4 报文里。

— 若目的地址是其他类型的兼容地址，则使用 IPv6。使用 IPv6 时有可能要进行封装。

5.3.2 双栈节点的地址配置

由于双栈节点同时支持IPv4/v6协议，因此必须配置IPv4和IPv6地址。节点分别使用IPv4机制（如DHCP）获取IPv4地址，使用IPv6协议机制（如无状态自动配置）获取IPv6地址。节点的IPv4和IPv6地址之间不必有关联，但是对于支持自动隧道的双栈节点，必须配置有与IPv4地址兼容的IPv6地址，地址格式是96比特0加IPv4地址。

5.3.3 通过 DNS 获取通信对端的地址

用户给应用层提供的只是通信对端的名字而不是地址，这就要求系统中提供名字与地址之间的映射。无论是在IPv4中还是在IPv6中，这个任务都是由DNS完成的。对于IPv6地址，定义了新的记录类型“A6”和“AAAA”。由于IPv4/IPv6节点要能够直接与IPv4和IPv6节点通信，因此必须提供对IPv4“A”、IPv6“A6/AAAA”类记录的解析库。

但是仅仅有解析库还不够，还必须对返回给应用层的地址类型做出决定。在查询到IP地址之后，解析库向应用层返回的IP地址可以有三个选择：

— 只返回 IPv6 地址；

— 只返回 IPv4 地址；

— 返回 IPv6 和 IPv4 地址。

对前两种情况，应用层将分别使用IPv6或IPv4与对端通信；对第三种情况，应用层必须做出选择使用哪个地址，即使用哪个IP协议。具体选择哪一个地址与应用的环境有关。

5.3.4 双栈技术附加要求

采用双栈策略除需要IPv4、IPv6协议栈外，还需要下列内容：

— IPv6、ICMPv6 和邻居发现等程序；

— 上层 TCP、UDP 对 IPv6 的处理软件；

— 高层应用程序接口的 Socket 库，以便支持 IPv6 地址和接口的扩充；

— 支持 IPv6 的 DNS。

5.4 隧道技术

5.4.1 隧道技术概述

在IPv6发展初期，必然有许多局部的纯IPv6网络，这些IPv6网络被IPv4骨干网络隔离开来。为了使这些孤立的“IPv6岛”互通，可以采取隧道技术的方式来解决，利用穿越现存IPv4因特网的隧道技术将许多个“IPv6孤岛”连接起来，逐步扩大IPv6的实现范围。

隧道技术是在IPv6网络与IPv4网络间的隧道入口处，由路由器将IPv6的数据分组封装入IPv4中。IPv4分组的源地址和目的地址分别是隧道入口和出口的IPv4地址。在隧道的出口处再将IPv6分组取出转发给目的节点。隧道技术在实践中有4种具体形式：构造隧道、自动配置隧道、组播隧道以及6to4隧道。

5.4.2 构造隧道（Configured Tunneling）

构造隧道的IPv6-in-IPv4隧道目的端IPv4地址是由封装IPv6分组的IPv4节点预先配置的，隧道可以是单向的，也可以是双向的。双向配置的隧道在实际运行中就像一个虚拟的点到点的连接。

5.4.3 自动配置隧道（Automatic Tunneling）

自动配置的IPv6-in-IPv4隧道目的端IPv4地址不需要事先配置，使用这种隧道机制的节点必须使用IPv4兼容的IPv6地址作为目的地址，隧道端口根据这个IPv4兼容地址直接产生隧道端口的IPv4目的地址，然后建立隧道。

5.4.4 组播隧道（Multicast Tunneling）

IPv4组播隧道使用的IPv4隧道目的端口IPv4地址是通过邻居发现机制来获得的。这种隧道配置技术要求IPv4网络支持组播。

5.4.5 6to4 隧道

提出6to4隧道的目的是为IPv4网络中的IPv6孤岛提供互通的手段，并且使手工配置隧道的工作量尽量少。这种方式要求每个IPv6孤岛至少有一个全网惟一的IPv4地址。6to4隧道的基本思路是，任何一个IPv6孤岛都使用其全网惟一的IPv4地址构造自己的IPv6地址前缀，因此前缀也是全网惟一的。每个孤岛的出口路由器从IPv6目的地址中提取出隧道末端的IPv4地址，因此隧道的构造过程可以自动进行。可见6to4隧道的关键是在IPv4地址和IPv6地址之间定义了一种映射，与“IPv4兼容”IPv6地址不同，在6to4隧道中，IPv4到IPv6地址的映射是把IPv4地址作为IPv6地址前缀的一部分。6to4中的地址构成方法如图14所示。

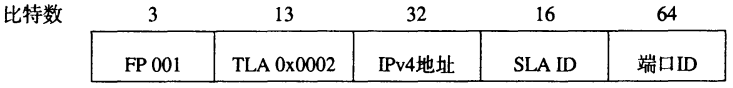


图14 6to4 隧道地址构成

5.4.6 隧道代理（TB，Tunnel Broker）

对于独立的IPv6用户，要通过现有的IPv4网络连接IPv6网络上，必须采用隧道技术。但是手工配置隧道的扩展性很差，TB的主要目的就是简化隧道的配置，提供自动的配置手段。对于已经建立起IPv6的ISP来说，使用TB技术为网络用户的扩展提供了一个方便的手段。从这个意义上说，TB可以看作是一个虚拟的IPv6 ISP，它为已经连接到IPv4网络上的用户提供连接到IPv6网络的手段，而连接到IPv4网络上的用户就是TB的客户。

TB的结构如图15所示。

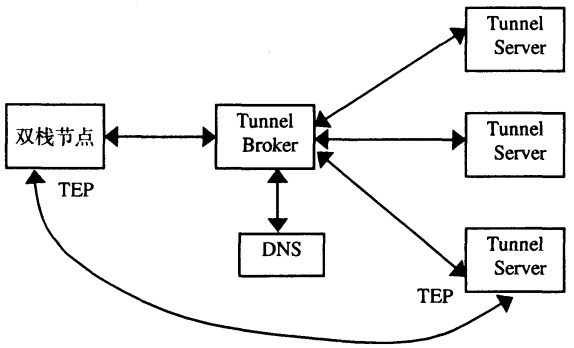


图15 TB 的结构

— 隧道代理：负责根据用户（双栈节点）的要求建立、更改和拆除隧道。为了均衡负载，TB 可以在多个隧道服务器中选择一个作为 TEP。TB 还负责将用户的 IPv6 地址和名字信息存放到 DNS 中。

— 隧道服务器：是一个双栈服务器，是连接到 IPv6 网络上的隧道末端。它从隧道代理处接收命令，对隧道进行必要的操作。

5.4.7 站内字段隧道寻址协议（ISATAP）

ISATAP 过渡技术使用一个内嵌公有或私有的 IPv4 地址的 IPv6 地址，可以在站点内应用 IPv6-in-IPv4 的自动隧道技术。ISATAP 地址格式可以使用站点单播 IPv6 地址前缀或全局单播 IPv6 地址前缀，支持站点和全局的 IPv6 路由。通过 ISATAP 过渡技术，可以使 IPv4 站点内的双栈节点通过自动隧道接入到 IPv6 路由器，并且允许双栈节点不必使用与 IPv6 路由器共享同一物理链路就可以通过 IPv4 自动隧道将数据包送达 IPv6 下一跳。ISATAP 过渡技术将 IPv4 网络作为 IPv6 的链路层，把其他网络节点作为潜在的 IPv6 主机或路由器，不需要使用 IPv6 路由器，或者网络中的所有成员重新做地址分配和规划，可以在 NAT 环境中运行。

5.5 协议转换技术

5.5.1 协议转换技术概述

其主要思想是在IPv6节点与IPv4节点通信时借助中间的协议转换服务器，此协议转换服务器的主要功能是把网络层协议头进行IPv6/IPv4间的转换，以适应对端的协议类型。

5.5.2 无状态 IP/ICMP 翻译（SIIT Stateless IP/ICMP Translation）

此技术单独对IP分组和ICMP分组报文进行协议转换，不记录一个流的状态，所以是“无状态”的。其工作机理如下：

1）IPv4到IPv6的头标转换

其工作机理如图16所示。

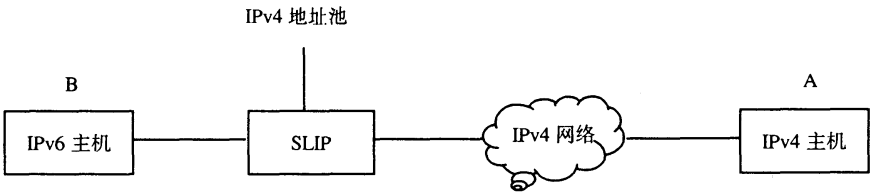


图16 IPv4 到 IPv6 的头标转换模型

IPv4主机要访问IPv6主机，IPv4地址是没有限定的全球IPv4地址，IPv6地址必须是形如::FFFF:0:a.b.c.d的IPv4翻译地址，且低32位是SIIT分配的全球IPv4地址。当IPv4主机发出的访问IPv6的分组到达SIIT时，分组中目的地址是IPv6的低32位地址，SIIT判断出此地址属于其管理的IPv6-Only节点的IPv4地址空间，因此做相应的IPv4－IPv6的协议分组头转换，把源地址转换成IPv4的映射地址，目的地址转换成IPv4的翻译地址，再把此IPv6分组传给主机B。

2）IPv6到IPv4的头标转换

IPv6访问IPv4，发出的分组中源地址是IPv6的翻译地址，目的地址是IPv4的映射地址，当IPv6的分组到达SIIT协议转换器时，SIIT判断出目的地是IPv4的映射地址，就要对该分组进行IPv6－IPv4的协议分组头转换，再把转换后的IPv4分组传给主机。

3）SIIT的局限

SIIT技术需要有一个备用的全局IPv4地址池来给与IPv4节点通信的IPv6节点分配IPv4地址，这个备用的全局IPv4地址池不能很大，因为IPv4地址空间优先。这样，当SIIT中备用的IPv4地址池分配完时，如果有新的IPv6节点需要同IPv4节点通信，就会因为没有剩余的IPv4地址空间而导致SIIT无法进行协议转换，造成通信失败。显然此技术应用的网络规模不能很大。

5.5.3 NAT-PT

NAT-PT是SIIT协议转换技术和IPv4网络中动态地址翻译技术（NAT）相结合的一种技术。它利用了SIIT技术的工作机制，同时又利用传统的IPv4下的NAT技术来动态地给访问IPv4节点的IPv6节点分配IPv4地址，很好地解决了SIIT技术中备用全局IPv4地址池规模有限的问题。

NAT-PT 处于IPv6和IPv4网络的交界处，可以实现IPv6主机与IPv4主机之间的互通。协议转换的目的是实现IPv4和IPv6协议头之间的转换；地址转换则是为了让IPv6和IPv4网络中的主机能够识别对方，也就是说，IPv4网络中的主机用一个IPv4地址标识IPv6网络中的一个主机，反过来，IPv6网络中的主机用一个IPv6地址标识IPv4网络中的一个主机。

当一台IPv4主机要与IPv6对端通信时，NAT-PT从IPv4地址池中分配一个IPv4池地址标识IPv6对端。在IPv4与IPv6主机通信的全过程中，由NAT-PT负责处理IPv4池地址与IPv6主机之间的映射关系。在NAT-PT中可以选择使用ALG（Application Level Gateway，应用层网关），因为NAT-PT只能对IP头中的地址进行转换，而有些应用在净荷中包含有IP地址，此时只能通过ALG对分组净荷中的IP地址进行格式转换。

5.6 SOCKS64

SOCKS网关机制如图17所示。

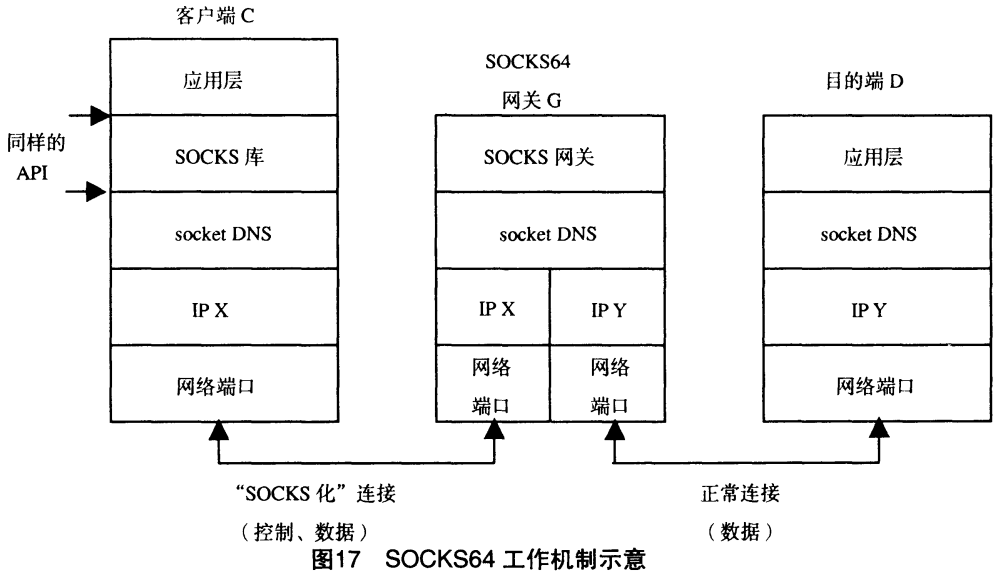


图17 SOCKS64 工作机制示意

在图17中增加了两个功能块实现SOCKS网关机制。一个是在客户端里引入SOCKS库，这个过程称为“SOCKS化”（socksifying），它处在应用层和socket之间，对应用层的socket API和DNS名字解析API进行替换。另一个是SOCKS网关，它安装在IPv6/IPv4双栈节点上，是一个增强型的SOCKS服务器，能实现客户端C和目的端D之间任何协议组合的中继。当C上的SOCKS库发起一个请求后，由网关产生一个相应的线程负责对连接进行中继。SOCKS库与网关之间通过SOCKS（SOCKSv5）协议通信，因此它们之间的连接是“SOCKS化”的连接，不仅包括业务数据也包括控制信息；而G和D之间的连接未做改动，属于正常连接。D上的应用程序并不知道C的存在，它认为通信对端是G。

SOCKS网关机制的关键是名字解析的实现。由于通信双方的地址格式不同，因此在名字解析的过程中必须进行一些处理。SOCKS网关机制中采用了DNS名字解析代理方法。

由SOCKET库将应用层发出的socket调用改为由SOCKS客户主机向SOCKS服务器发出的socket调用。SOCKS64机制的一个限制是连接必须由内部发起，因此是单向的。

SOCKS64网关是一个双栈主机，它可以同时和IPv4或IPv6节点进行通信，SOCKS64的客户只与SOCKS64网关直接通信，与IPv4或IPv6节点的通信实际上由SOCKS64网关来完成。

5.7 传输层中继（Transport Relay）

与SOCKS64的工作机理相似，只不过是在传输层中继器进行传输层的“协议翻译”，而SOCKS64是在网络层进行协议翻译。它相对于SOCKS64，可以避免“IP分组分片”和“ICMP报文转换”带来的问题，因为每个连接都是真正的IPv4或IPv6连接。但同样无法解决网络应用程序数据中含有网络地址信息所带来的地址无法转换的问题。

5.8 应用层代理网关（ALG）

ALG与SOCKS64、传输层中继等技术一样，都是在IPv4与IPv6间提供一个双栈网关，提供“协议翻译”的功能，只不过ALG是在应用层级进行协议翻译。这样可以有效解决应用程序中带有网络地址的问题，但ALG必须针对每个业务编写单独的ALG代理，同时还需要客户端应用也在不同程序上支持ALG代理，灵活性很差。显然，此技术必须与其他过渡技术综合使用才有推广意义。

6 IPv6 网络 QoS 机制

6.1 IPv6 QoS 机制概述

IP协议是无连接协议，IP网络基于数据报传输模式，因此最初的IP网络中没有服务质量（Quality of Service）的概念，IP网络不能保证足够的吞吐量和符合要求的传送时延，网络只是尽最大努力（Best-effort）来满足客户的需要。在Internet网络规模迅速扩展的同时，网络上开放的业务种类也在不断增加。在传统的非实时型的数据通信方式的基础上，网络业务正逐步向实时性要求很强的话音通信、传真通信和多媒体通信等方面发展。目前在Internet上已开通的实时型通信业务的典型例子是IP 电话（IP Phone）和IP 传真（IP FAX）。随着网络硬件环境的不断改善，电视会议、可视电话和点播电视（VOD）等多媒体和宽带通信业务也正在加入到Internet业务中。针对IP网络上传输实时数据的问题主要关系到它们需要的带宽以及必须满足的严格的最大延迟时间要求，Steve Deering在1992年秋提出的新因特网的协议IPv6草案中就考虑到了对QoS的支持。IPv6对QoS的支持主要反映在IPv6的包头中定义了两个重要参数：业务类别（traffic class）域和数据流标志（flow label）位。

目前，IETF有多个工作组在不同的领域从不同角度研究解决IP网服务质量的方案。有针对具体业务的要求，对业务进行分类和/或进行资源预留来实现服务质量要求的协议机制，如综合业务模型（IntServ）/资源预留协议（RSVP）、区别业务模型（DiffServ）。

6.2 综合业务模型（IntServ）

综合业务模型（IntServ）以标准的RSVP协议作为实现机制。通过IntServ，将可以实现IP网中的QoS传输以及对实时业务的支持，使得各种应用能够为其数据包选择服务等级。

6.2.1 IPv6 对流和资源预留的支持

流是特定源和目的地间的报文序列，源要求中间路由器对这些报文进行特殊处理。一般来说，路由器收到流中报文后，根据流标识符查找路由器中保存的流上下文，对流中的报文进行同样的处理，从而加快了报文的处理速度。

IPv6报头的格式里，有20比特的流标签（Flow Label）域。当主机发送报文时，如果需要把报文放到流中传输，只需在流标签里填入相应的流编号。如果在流标签里填0，就作为一般的报文处理。路由器收到流的第一个报文时，以流编号为索引建立处理上下文，流中的后续报文都按上下文处理。

IPv6的资源预留协议（RSVP）使用流标签来申请资源和相当的优先级，实现IP网中的QoS传输以及对实时业务的支持，使各种应用能够为其数据包选择服务等级。

IPv6流标签可以用在IPv6服务质量保证，流标签的具体使用在本标准范围之外。

6.2.2 IntServ

该模型是对于每一个需要进行QoS处理的数据流使用一定的信令机制，在其经由的每一个路由器上进行资源预留实现端到端的QoS业务。首先该模型定义了一个作用于整个网络的要求集合，整个网络中的每一个元素（子网或路由器）都将能够实现这一要求集合。随后，通过一定的信令机制，将特定应用的服务等级要求通知其传输路径上的所有网络元素，并在应用与各个网络元素之间进行管理信息的交换，网络元素将为该应用进行各种资源预留与处理策略的设置。这样，当整条路径建立起来之后，这一路径上的所有网络元素都已经做好了为相应的数据流提供QoS业务的准备。

目前，IntServ模型定义了三种业务类型，并且对这些业务类型对路由器的要求进行了描述：

1）保证型业务（Guaranteed Service）。该业务将提供时延、带宽与丢包率等参数的保证。该业务不

能控制固定延迟（传输延迟等，它们取决于由连接建立机制所选的路由），它所能保证的是排队延迟的大小（排队延迟是令牌桶大小和数据速率的函数）。网络采用加权公平排队（WFQ）算法。

2）控制负载型业务（Controlled load Service）。在轻载网络中，这种业务类似于 best-effort 业务。它能够提供最小的传输时延，对于排队算法没有特别的要求。在控制负载业务网络中，应用可以假设网络传输的包差错率近似于下层传输媒质的基本包差错率，包平均传输延迟与网络绝对延迟（包括光传输延迟加路由器转发延迟）差别不大。

3）尽力而为型业务（Best-effort Service）。实际就是传统的 Internet 所提供的业务，该业务不提供任何 QoS 保证。

IntServ的技术基础包括：先进的冲撞管理；限制延迟、抖动以及网络内带宽消耗的排队算法；资源预留协议（RSVP）。

6.3 区别业务模型（DiffServ）

区别业务模型（DiffServ）与IntServ的本质不同在于它将不是针对每一个业务流进行网络资源的分配与QoS参数的配置，而是将具有相似要求的一组业务归为一类，随后对这一类业务采取一致的处理方式。

Diffserv的基本机制是在网络的边缘路由器上，根据某一业务的服务质量要求将该业务映射到一定的业务类别之中，随后利用IP分组中的DS字段惟一地标记这一业务所需的服务类别。网络中的各个节点将依据该字段对各种业务类别采取预先设定好的服务策略，保证相应的延迟、传送速率、抖动等服务质量参数。这样，对于一次会话中特定的数据流，在每次连接的过程中，将无需传递各种QoS信息，从而避免了RSVP中高昂的建立成本；同时也使得这种技术具有较好的反应灵敏度，特别适合于因特网中大量存在的短时间的连接。

6.3.1 DiffServ 工作机制

DiffServ模型利用了IPv6的业务类型（Traffic Class）字段作为DS字段。当数据流进DiffServ网络时，边缘路由器通过标识DS字段，将IP包分为不同的服务类别，而网络中的其他传送路由器在收到该IP包时，则根据该字段所标识的服务类别将其放入不同的队列，并由作用于输出队列的流量管理机制控制每个队列，即给予不同的每一跳行为（PHB）。其中最主要的就是对每个队列的出带宽分配、以及发生拥塞时如何丢包这些资源的分配规则都是预先设定好的。

6.3.2 DS 字段描述

DS字段共8比特，其中6比特可供目前使用，称为DSCP字段，剩余2比特供将来使用。DS字段的具体格式如图18所示。

0	1	2	3	4	5	6	7
DSCP						CU	

CU： 目前未使用。

图18 DS 字段格式

DSCP称为DiffServ编码点，如前所说，它将是分组所享受的服务质量的惟一标志。

DiffServ充分考虑了IP网络本身灵活、可扩展性很强的特点，将复杂的服务质量保证通过DS字段转换为先进的单跳行为，从而大大减少信令的工作。因此，DiffServ不但适合在运营商网络环境中使用，而且大大加快了IP QoS在实际网络中应用的进程。

6.3.3 PHB 定义

在DiffServ域的路由器中，将对属于某一服务类别的业务流进行一致的处理。这种处理包括队列选择、排队、丢弃等。对属于同一服务类别的业务流进行的标准化处理的组合就构成了每一跳行为（PHB）组。这一节将介绍现有的PHB组以及它们与DSCP编码点的关系。PHB中还包括了该PHB组与其他PHB组之间的互操作问题。

PHB是对路由器服务质量处理的总体描述，它并不对实现PHB的具体技术加以规定。这样，不同的厂商将可以采用自己的实现方式，只要结果能够满足标准PHB的要求就可以了。另外，通过对标准PHB的组合，各个厂商将可以实现自己所专有的业务。

目前定义了4种PHB，它们是尽力而为PHB（默认PHB，DS PHB）、加速转发PHB（EF PHB）、可靠转发PHB（AF PHB）和类别选择PHB（Class Selector PHB）。

1）尽力而为PHB（默认PHB，DS PHB）

即使 DiffServ 获得了广泛的应用，尽力而为型业务仍将是 Internet 的主要业务。这样，在 DiffServ 模型中也必须能够支持这种传统的业务。RFC2474 规定，当 DSCP 为全零（编码点为“000000”）时，对应的 PHB 就是尽力而为 PHB，也称为默认 PHB。当路由器收到 DSCP 为全零或者是无法识别的 DSCP 值时，都将使用尽力而为 PHB 对分组进行转发。但在后一种情况下，应当保持分组中的 DSCP 值不变。也就是说，尽力而为 PHB 是一种默认的服务质量。

2）类别选择PHB（Class Selector PHB）

为了与现在正在使用的 IP 优先级字段保持一定的后向兼容，在 DiffServ 中定义了类别选择 PHB。现有的 IP 优先级机制使用了 IPv4 TOS 字段的前三个比特，从而可以提供 8 个 IP 优先级。可见，这种方式与 DSCP 的用法是十分相似的，不同在于 DiffServ 使用了 TOS 字段中的前 6 个比特，另外现有的路由器都能够理解 TOS 域的意义。所以只要将 DiffServ 的一部分编码分配给传统 IP 优先级业务，就可以很容易地实现上述的后向兼容。同时，DiffServ 的业务等级可以与传统的 IP 优先级同时并存于网络之中。类别选择编码点的分配为“xxx000”，亦即“000000”~“111000”8 个编码点可见类别选择编码点的位置与传统 IP 中的 IP 优先级字段的位置是完全一样的。

3）加速转发PHB（EF PHB）

加速转发 PHB 描述的是一组用于实现低丢包率、低延迟、低抖动、具有带宽保证的以及在 DS 域中具有端到端服务质量的业务的服务策略。使用这一 PHB 组的业务流将获得 DiffServ 网络中最高服务质量，具有最高的优先级，在转发过程中所使用的队列将是节点上最短的。当网络发生拥塞时，这类业务将获得最先处理，这样可以使这类业务的时延最小，同时改善了该业务的其他服务质量参数。这一 PHB 对应的 DSCP 编码为“101110”。

4）可靠转发PHB（AF PHB）

可靠转发 PHB 所要达到的目标实际上主要是对相同业务中不同分组的丢失优先级进行一定的分级。

在业务开始转发之前，发送方与网络节点之间将对业务流的速率做出一定的约定，这种约定称为业务流的轮廓（profile）。在 AF PHB 中，网络节点将允许业务流的速率大于这一轮廓，但是网络节点将对超出轮廓的业务流分组采用较大的丢弃优先级。根据这一思想，RFC2597 对可靠转发 PHB 做出了定义。RFC2597 规定，AF PHB 组包括 4 个等级。网络中的节点将根据这些等级为相应的业务流分配网络资源并进行相应的转发处理。

在单跳行为之外，一个完整的 DiffServ 结构还包含边缘行为和带宽管理两个基本部件。

边缘行为是指数据包进入网络边缘时采取的一系列行为：通过分类器（classifier）对入局接口的业务进行分类（可以根据IP地址、协议类型以及TCP端口号区分不同服务级别），并对DS字段加以标记。对每个级别的业务加以监测，通过监管来对每个级别的业务监测，以确保符合SLA。

带宽管理。DiffServ为IP QoS提供一定支持，但还没有办法完全提供端到端的QoS。DiffServ需要大量网络单元的协同运作，才可能向用户提供端到端的服务质量。鉴于这些组件高度分散的特点和对它们进行集中管理的需要，必须要有一个全局的带宽管理来进行对全局资源的动态管理。解决这一问题的方法有两个：一是可以用功能强大的全局策略管理器来完成这一任务；另外一种就是利用MPLS将第三层的QoS转换为第二层的QoS，通过运营网中第二层的交换机来实现端到端的服务质量保证。尽管，这有可能不是一个真正意义上的IP QoS，但却是今天可以实现的一个切实可行的办法。

附 录 A
（资料性附录）
生成基于EUI-64接口标识符

根据一个特定的链路或节点的特征，有很多途径生成基于EUI-64的接口标识符。本附录描述这些途径的一部分。

— 有 EUI-64 标识地址的链路或节点

把一个EUI-64标识符转换到一接口标识符需要的惟一变化是转换全局/本地位（universal/local ）“u”。全球性惟一EUI-64标识符的格式如图A.1所示。

cccccc0gcccccccc	cccccccmmmmmmmm	mmmmmmmmmmmmmmmm	mmmmmmmmmmmmmmmm

图A.1 全球性惟一EUI-64标识符

其中“c”是给定的厂家标志位（company_id），“0”是表示全局范围的全局/本地位（universal/local）的值，“g”是个人/组织（individual/group）位，并且“m”是制造商选择的扩展标识符位。IPv6接口标识符将表示为图A.2格式。

cccccc1gcccccccc	cccccccmmmmmmmm	mmmmmmmmmmmmmmmm	mmmmmmmmmmmmmmmm

图A.2 IPv6接口标识符

惟一的变化是变换了全局/本地位的值。

— 有 IEEE 802 48 比特 MAC 地址的连接或节点

在EUI64 中定义了一个方法，用来从IEEE 48比特MAC标识符生成EUI-64标识符。就是把两个八进字（其值为十六进制0xFF和0xFE）插入到48比特MAC标识符的中间（在厂家标志位和制造商标志位之间）。具有全球范围的48比特MAC标识符如图A.3所示

cccccc0gcccccccc	cccccccmmmmmmmm	mmmmmmmmmmmmmmmm

图A.3 全球范围的48比特MAC标识符

其中“c”是给定的厂家标志位company_id，“0”是显示全球范围的全局/本地位的值，“g”是个人/组织位，“m”是制造商选择的扩展标识符位。接口标识符的格式如图A.4所示。

cccccc1gcccccccc	cccccccc11111111	11111110mmmmmmmm	mmmmmmmmmmmmmmmm

图A.4 接口标识符

当IEEE 802 48比特MAC 地址可用时（在一个接口或节点上），因为其可获取性和惟一性，IPv6的实现就应该使用这些MAC地址来生成接口标识符。

— 带非全球性标识符的链路

对有些类型的链路，当多接入时，没有全球性惟一的链路标识符。例如LocalTalk和Arcnet。生成一EUI-64格式标识符的方法是用链路标识符（例如 .....LocalTalk 8比特节点标识符）和在它左边填0。例如用LocalTalk十六进制值为0x4F的 8比特节点标识符可导出如图A.5接口标识符:

0000000000000000	0000000000000000	0000000000000000	0000000001001111

图A.5 接口标识符

注意在这个接口标识符全局/本地（universal/local）位被置为的“0”来显示本地范围。

— 没有标识符的链路

有很多链路没有任何类型的内建标识符。最常见的是串行链路和配置的隧道。接口标识符必须被选择为对该链路是惟一的。

当在一个链路上没有内建标识符可用的时候，推荐用该节点的另外一个接口的全球接口标识符或设定为节点自身的接口的全球接口标识符。使用这种方法时没有连到同一链路的相同节点的其他接口可以使用同一标识符。

如果在链路上没有可得到的全球接口标识符，则（IPv6）实现需要生成一个本地范围的接口标识符。仅有的要求是在该链路上是惟一的。有许多可能的方法来选择一个链路惟一的接口标识符。他们包括手工配置、产生随机数、节点串号（或其他的节点特定令牌）。

链路惟一的接口标识符应该按同一方式产生，它不致在某节点复位以后或者在节点上增加/删除接口后产生变化。

选择适当算法依赖于链路和实现的，建议将冲突检测算法作为任何自动算法的一部分来实现。

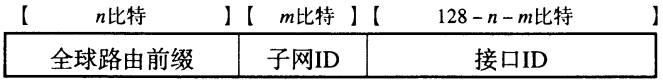
附 录 B
（规范性附录）
IPv6全球单播地址格式

B.1 概述

本附录规定用于因特网的IPv6全球单播地址格式。

B.2 地址格式

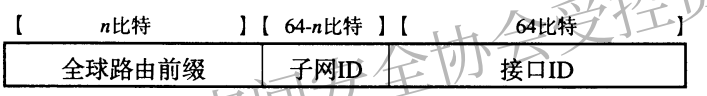
在IPv6地址结构定义的IPv6全球单播地址一般格式如图B.1所示。



图B.1 IPv6地址格式

全球可路由前缀（通常层次化结构）是一个分配给站点（一组子网和链路的集合）的值，子网ID是站点中子网的标识符，接口ID在第四章中描述。全球路由前缀被设计由RIR和ISP层次化构造使用。子网字段由站点管理员层次化构造使用。

IPv6地址结构规定除由二进制000开头以外的单播地址都应具有按照附录A构造的64比特长的接口标识。此时地址格式如图B.2所示。



图B.2 IPv6地址格式

路由前缀是标识站点的值，子网ID是站点中标识子网的值，接口ID是IPv6地址结构中规定的修改后的EUI - 64格式。

中华人民共和国
通信行业标准
IPv6 网络技术要求
——地址、过渡及服务质量
YD/T 1442-2006

*

人民邮电出版社出版发行
北京市崇文区夕照寺街 14 号 A 座
邮政编码：100061
北京新瑞铭印刷有限公司

*

开本：880 × 1230　1/16　　2006 年 9 月第 1 版
印张：2　　2006 年 9 月北京第 1 次印刷
字数：56 千字

ISBN 7 - 115 - 1297/06 - 118
定价：15 元