IPv6 互联网协议的特点分析

刘年生　郭东辉　吴伯僖　*Gerard Parr* *

关键词: 互联网 协议, 地址结构, 服务质量, 网络安全性

【摘要】为了具体阐述 IPv6 的具体内容和特点, 以及它与 IPv4 之间的主要差别, 本文将从地址机制、服务质量和网络安全性等方面对 IPv6 协议进行较深入的分析, 从中可以看到 IPv6 能较好地解决 IPv4 所面临的主要问题, 将进一步推动互联网的发展。

一、引　　言

现阶段的因特网是以 IPv4(Internet Protocol Version 4) [1] 为基础的国际互联网, 然而, 随着因特网规模和应用范围的迅速扩大, IPv4 互联网所面临的一些问题显得日益突出, 主要表现在:

(1) IP 地址耗尽和路由数据管理不堪重负;

(2) 通信链接没有带宽和流量控制功能, 服务质量(QoS) 没有保证;

(3) IPv4 的 Internet 安全性相当脆弱。

尽管目前人们采取了各种不同的技术措施来解决这些问题, 但是, 并不能彻底解决 IPv4 本身固有的缺陷[2], 因此, 人们希望通过制订新的互联网协议来实现能够满足各种通信业务要求的高质量的下一代国际互联网。

针对互联网所面临的问题, 在 IPv4 的基础上改进的 IPv6 (Internet Protocol Version 6) 已于 1994 年 11 月被认定为"the Next Generation Internet Protocol"即下一代 Internet 互联网的协议标准[3], 并建立了 IPv6 的实验平台——"6bone" 实验网[4]。目前世界上至少有 40 多个国家接入了"6bone" 实验网, 许多生产厂家已开始生产适应于 IPv6 的路由器、网卡等产品, 包括 IBM、HP、Sun、Cisco 等公司, 并开发适于 IPv6 操作系统, 如 Linux、Windows NT 等[5,6], 可见 IPv6 的实用日期就要到来了。为了详细了解 IPv6 的具体内容和特点, 以及它与 IPv4 之间的主要差别, 本文从地址机制、服务质量和网络安全性等方面对 IPv6 协议进行较深入的分析。

二、IPv6 的地址空间

IP 地址是因特网的基础, 与 IPv4 相比, IPv6 的地址空间有许多新的特点, 且其地址结构与路由选择、移动通信有着密切的关系。

1. IPv6 的地址结构与模型

IPv6 地址采用了 128 位二进制标识符(identifier, 简称为 ID), 既可用于单一接口, 也可用于一组接口。它包括 3 类: 单点广播地址(unicast address)、多点广播地址(multicast address) 和任意点广播地址(anycast address)。与现行的 IPv4 相比, 它的地址空间增大了 2^{96} 倍, 并且将多点广播地址作为一类基本地址结构, 新增了任意点广播地址。所谓任意点广播地址就是一组接口(典型情况的是属于不同的节点) 的一个标识符, 发向任意点广播地址的信息包被送到其中一个目标接口(通常是按路由选择协议所测得距离最近的一个接口)。

在 IPv6 中没有广播地址, 它的功能被多点广播地址所取代。为了方便简洁地表示所有的 IP 地址, 可采用 8 个 16 位的无符号整数表示, 每个整数用 4 个 16 进制的数字表示, 有如下几种特殊地址:

* 刘年生　厦门大学 博士研究生　厦门　361005
郭东辉　厦门大学 副教授　厦门　361005
吴伯僖　厦门大学 教授　厦门　361005
Gerard Parr　英国 Ulster 大学信息学院　N. Ireland, BT52 1SA

(1) 未指定地址(128 位全部为零);

(2) 回送地址(:: 1);

(3) 内嵌有 IPv4 地址的 IPv6 地址(在原 32 位 IPv4 地址前加 96 位零而成的);

(4) 站点本地地址(对不与因特网络连接的网络而言,带有二进制前缀 1111 1110 11);

(5) 链路本地地址(二进制前缀 1111 1110 10);

(6) 多点广播地址(前缀 1111 1111)。

所有的 IPv6 地址都是分配给接口的,而不是给节点的,如:一个 IPv6 单点广播地址只分配给唯一的接口,所有的接口都必须至少有个链路本地单点广播地址。一个接口可有多个 IPv6 地址,而不管其种类和作用域如何,但有一个例外,如果把一个并联的物理接口当作一个接口且出现在网络层时,就只能把一个单点广播地址或一组单点广播地址分配给这个并联的物理接口。

2. 地址与路由

在 IPv4 中地址分配是直接面向最终用户的,与网络的拓扑结构无关,当地址长度增了 4 倍为 IPv6 地址时,原来的路由表就可能出现爆炸性扩大而变得不堪重负,效率低下。在 IPv6 中为了解决这一问题,将地址分配方案从基于最终用户迁移到基于提供商(如表 1 所示),从构成了分层地址结构,使地址构造与网络拓相一致,相应地采用分层路由。

表 1 基于提供商的 IPv6 地址

位数	3 位	5 位	16 位	8 位	24 位	8 位	64 位
字段	FP (010)	注册表 ID	提供商 ID	保留	订户 ID	保留	接口 ID

在 IPv6 的扩展标题(header)选项中有一个路由标题,用于标示出由一个 IPv6 信源地址到目标地址之间要经过的一个或多个中间节点,并且能通过一个 ICMP(Internet Control Message Protocol)信息包告诉信源主机该链路本地路径的 MTU(Maximum Transmission Unit 最大传送单位),信源主机能根据最小的路径 MTU 进行分包发送,而数据包不再在路由器中进行进一步分段。

ICMPv6(Internet Control Message Protocol Version 6)可用于路由消息的广播,包括路由器请求消息、路由器宣告消息、邻居请求消息、邻居室宣告消息和路由器重定向消息等。由此建立起路由表,再根据路由协议来进行路由选择。原来的路由协议,包括内部路由协议和外部路由协议,均要进行一定的修改以适应 IPv6 的地址机制的要求。

在内部路由协议中,OSPF(Open Shortest Path First)是基于层次概念的链路态协议[7],已被首推为主要的 IPv6 的内部路由协议,原 OSPF 需作如下主要改变以适于 IPv6:

(1) 链路状态记录采用 128 位字段代替 32 位字段;

(2) 网络内的路由器应采用 IPv6 地址 ID 表示;

(3) 网络区间应采用 IPv6 地址 ID 或地址前缀来表示;

(4) 用表示地址前缀的整数代替子网掩码;

IDRP(Inter- Domain Routing Protocol)是基于路经矢量的外部路由协议[8],IDRPv6 比 BGP (Border Gateway Protocol, 即边界网关协议)[9] 更适于 IPv6,成为首选的 IPv6 外部路由协议。这主要为:

(1) 多数 BGP 设计者都参与了 IDRP 的设计;

(2) IDRP 是在 OSI(Open System Interconnect Reference Model)网络结构[10] 中定义的,但它本身并不依赖于 OSI 网络结构;

(3) 它的设计是基于多协议路由,并能计算不同地址类型的路由信息;

(4) 它跟 BGP 一样采用相同路径矢量方法,从技术上讲是安全的。在 IDRP 中将路由分为最终路由域(ERD)和传输路由域(TRD),每个路由器计算到达指定目的地的首选路由,并通过一路经矢量将传给 IDRP 邻接的路由器。

3. 地址与移动用户

在 IPv6 中能够有效地支持地址移动计算,满足移动用户的要求。移动用户通常经过公用移动无线网连接到 Internet,在移动通讯过程中会出现移动主机 IP 地址不断改变的问题。为了解决这问题,在 IPv6 中移动主机可有 2 个地址:一个是移动主机永久地址称为主地址(home address),是主机连接其默认网络时的地址,默认网络称为主网络(home network);另一个是移动主机在连接到外部网络时获得的地址,称为转发地址(care- of address)。移动主机通过其主网络中的一个被指定为主代理(home agent)的路由器来跟踪其移动情况,由主代理来负责管理主地址和转发地址,包括地址信息的接收、缓存、绑定、转发和更新。需要用来支持 IPv6 主机移动性的信息通过 4 个选项进行交换,这个选项由目的选项扩展标题内提供,包括绑定更新选项、绑定确

定选项、绑定请求选项和主地址选项, 进行地址的自动配置和信息交换。其通信过程如图 1 所示。

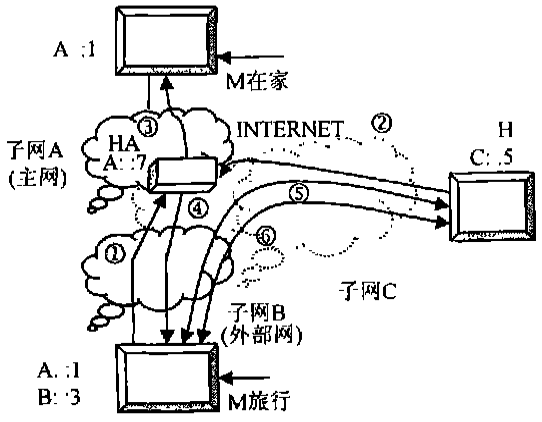

图 1 IPv6 中移动主机的通信过程示意图

主机 M 通常是连接到子网 A, A 是 M 的主网络, M 从 A 获得的地址为 A: : 1(注: 此地址的语法在形式上并不正确, 但这仅仅只是一个范例), 此为主机 M 的主地址。地址 A: : 1 在 DNS 层次上就转换为主机名 M。同样, H 连接到子网 C, 然后从 C 获得地址 C: : 5。当 H 向 M 发送信息包时, 它先询问 DNS 并获得地址 A: : 1, 然后 H 就会产生一个目的地址为 A: : 1、源地址为 C: : 5 的 IPv6 信息包 ②。这些信息包由 IPv6 路由来确定路由并到达目的子网 A。此时可能出现如下几种情况:

(1) 当节点 M 在家时, 信息包则通过经典的 IPv6 路由过程 ③传送到 M;

(2) 当节点 M 连接到子网 B 时, 它从 B 获得初级转发地址 B: : 3, 通过一个绑定更新信息 ①同其主代理(HA) 进行通信。主代理收到的信息包通过从 A: : 7 到 B: : 3 ④转发给 M。当 B: : 3 从信道中获取信息包时, 它会检查信息包是否发送给地址 A: : 1 的, 若是, 则 M 向 H 发送一条绑定更新信息 ⑤H 将此信息储存在其绑定缓存内, 此后就可进行路由优化, 通过路由报头强制信息源将目的路由改为 B: : 3 ⑥, 让 H 和 M 直接通信;

(3) 当 M 没有连接任何子网时, 则子网 A 的路由器就会利用 ICMP 将此故障发送回信息源。当 M 从子网 B 移动其它子网如: 子网 D, 将获得一个新的初级转发地址, 此新地址通过绑定更新信息同时发给 M 的主代理(HA) 及 H。

三、IPv6 的服务质量

在 IP 网络上进行多媒体通信已是 Internet 发展的必然, 而多媒体通信包括语音和图像信息处理和传输必须满足人们一定的感觉(如视觉和听觉等) 心理和实际应用的要求, 就必然提出相应的服务质量要求, 如实时通信、多点广播等。对带宽、流量、丢包率、时延和时延抖动等关系到传输质量的参数提出较严格的要求, 高质量的多媒体通信要求信息流量大而且分布均匀, 时延、时延抖动和丢包率应尽量地小, 至少是应降低到可接受的水平, 如延迟时间应低于 150 ms[11]。现有的 IPv4 Internet 没有带宽控制和流量控制功能, 服务质量没有保证, 而在 IPv6 中进行了较彻底的改进以支持多媒体通信。

1. IPQoS 的体系结构

到目前为止, 对于 IPQoS(IP Quality of Service) 的体系结构, 世界上主要有 2 种: IntServ(Integrated Services Architecture) 集成业务体系结构和 DiffServ(Differentiated Services Architecture) 区分业务体系结构。IntServ 是由 IETF(Internet Engineering Task Force) 的 IntServ 工作组于 1994 提出的[12], 它定义了 3 种服务类型:

(1) Guaranteed Services[13]: 对带宽、时延、丢包率提供定量的质量保证;

(2) Controlled- load services[14]: 给用户提供种类似在网络欠载情况下的服务, 是一种定性的指标;

(3) Bet- Effort: 是一种尽力而为的工作方式, 基本无任何质量保证。

而 DiffServ 也是由 IETF 提出的[15], 与 IntServ 相比, 它简化了信令, 而且更容易扩展。DiffServ 通过“aggregate”和 PHB(Per Hop Behavior) 的方式来提供一定程度上的 QoS 保证。“aggregate”(即聚集) 的意义在于允许路由器把 QoS 需求相近的各业务流看成一大类, 以减少调度法所处理的队列数; PHB 的意义在于逐跳的转发方式, 每个 PHB 对应一种转发方式或 QoS 要求。DiffServ 力图通过对业务流的分类、整形、标记和调度来实现对业务 QoS 一定的保证。目前, 在 DiffServ 上主要提出了“Expedited Services”和“Assured Services” 2 种服务业务[16,17]。

2. IP QoS 的实现

为了实现 IntServ 定义了 4 个功能部件: 资源预

备协议(Resource Reservation Protocol 简称 RSVP)、分类、访问控制和排队调度,网络中的路由器均需实现这4 个部件。主机执行的操作一般和路由器相同,但是多了应用程序的执行,如果对于通信量要求 QoS,则要求从本地预约(RSVP 代理)获得,可利用 IPv6 的流标签(flow label)标题字段来指定所需的资源保留,IPv6 路由器的接收和查看到这种给定流的信息包时可进行连续处理,减少中途时间延迟。

而 DiffServ 利用了 IPv6 Traffic Class 域中的 COS.(Class of service)作为 DSCP(DiffServ coding point)使用,每一种 DSCP 对应一种 PHB 方式。网络上的路由器通过查看信息包的 COS 字段中的 DSCP 值来进行分类,并提供相应的 PHB 转发方式。目前已定义的 DSCP 值有:000000 时为缺省(Best- effort) 101100 时为 Expedited Services 以及 12 个 Assured Services。IntServ 和 DiffServ 实际上都只提供了一种实施 QoS 的框架结构,但并没有指定实现 QoS 的某一具体机制,包括队列管理机制和队列调度机制。队列管理机制与信息包的时延、丢包率和链路有效利用率等 QoS 参数指标密切相关,常用算法有 PPD、EPD、RED、FRED、RIO、BLUE 等多种,其中以 RED 和 BLUE 算法效果较好。队列调度机制涉及路由器如何从多个队列中选择一个待转发的信息包,常用算法有先到先服务、循环处理、优先级服务、随机服务等,应根据不同通信质量要求来选择相应的调度算法[18]。

3. IPv6 的标题

原 IPv4 的包头标题域有 13 个,而 IPv6 只有 7 个域,这使得路由器可以更快的处理信息包,减少传送延时,以满足多媒体通信 QoS 要求。同时采用扩展标题供用户根据实际需要选择用,它顺次包括如下选项: IPv6 header、Hop by Hop header、Destination header、Routing header、Fragment header、Authentication header、Encapsulating Security payload header、Destination header、Upper layer header 等,扩展标题均含于 Next Header 字段域中,选项内容插在 IPv6 header 和上层协议头如 TCP header 之间。IPv6 格式如图 2 所示。

Version(4)	Traffic class (8)	Flow Label(20)
Payload Length(16)	Next Header(18)	Hop Limit(8)
Source Address (128)		
Destination Address (128)		

图 2 IPv6 的中帧头结构

图 2 中 Traffic class 域可用于源节点或路由器来验证和区分不同类或优先权的 IPv6 信息包。Flow Label 可用于标记需路由器作特别处理如非缺省 QoS 或实时服务 IPv6 信息包的顺序号。Next Header Hop Limit 取代 IPv4 中的包生存周期,每向前经过一个节点就减一,为零时丢弃该信息包。当然要取得到良好的效果,不仅仅考虑 IP 层协议,也应该系统考虑其它层或其它面向连接网络协议等,如 TCP 层协议,也应当进行相应修改以满足多媒体通讯 QoS 需要,又如 IP over ATM network 是目前现有 QoS 保证的网络通信协议之一。

四、IPv6 的安全性

IPv4 的 TCP/IP 网络常受到网络安全问题的困扰,易受信息包探测、IP 电子欺骗和连接截获等攻击。因此在设计 IPv6 协议时就考虑到在网络层次上设置一些安全机制,从 IP 层来保证的 Internet 的安全。

1. IPv6 的安全结构

IPSEC(IP security)是由 IETF 设计的[19],主要由 IP 的 AH(Authentication Header)和 ESP(Encapsulating Security Payload)组成实现[20,21]。IPv6 是通过 2 个专用的扩展标题将其列入的,AH 是用来确认 IP 信息包的可靠性和完整性,保护网络不受固定字段的非法修改和信息包电子欺骗的威胁,而 ESP 则提供数据加密封装确保只有目的接口才可阅读由 IP 信息包发送的有效数据,它们既可以分别单独使用,也可以一起使用,提供更高的保密强度。AH 和 ESP 标题的结构如图 3 所示。

下一个标题(8)	有效数据长度(11)	保留(16)
安全参数索引(32)		
顺序号字段(32)		
身份验证数据		

AH

安全参数索引(32)
顺序号(32)
加密数据

ESP

图 3 AH 和 ESP 标题的结构

2. IPSEC的算法

密码算法不仅直接关系到信息包的保密强度,而且也影响信息包的传输时间和流量,因此密码算法的选择是十分重要的,从逻辑上保证信息的安全。安全设置的对用户来说是可选择的,在IPSEC中支持多种密码算法,包括对称加密算法和非对称加密算法。IPv6中的AH和ESP标题均采用了SA(Security Association)的规则,保持发送方和接收方之间的安全算法和参数的一致性。其中AH既可采用对称加密码算法,如DES(Data Encryption Standard)算法[22]或单向赫序函数(MD5, SHA 等)[23,24]适用于点到点通信,也可采用对称加密算法和非对称加密算法相结合的方式,如对于多点广播通信则适于采用单向赫序函数与非对称签名算法相结合的密码体制,同时AH也支持其它算法。ESP的密码算法分为加密算法和身份验证算法,加密算法一般只采用对称加密算法,多数采用DES-CBC加密算法[25]。而身份验证算法则与AH中一样。

3. IPSEC的处理过程

信息包在发送前一般调用ESP处理程序进行处理,包括填补码、加密等,其结果作为AH包的一部分再作AH处理,生成一个IPSEC信息包进行发送,目的主机在收到一个IPSEC信息包后,将进行如下处理:

(1)查看包的协议标题,找到AH标题字段后调用AH处理程序,从中分设出SPI(Security Parameter Index即安全参数索引)信息,利用SPI从安全关联数据库中检出其共享密钥,使用共享密钥计算验证数据,并将计算结果与收到的验证数据作比较,如相同,则接着进行下一步处理,否则向发送方发一个错误信息包;

(2)再查看ESP标题字段,从中取出SPI,再次访问安全关联数据库,检出ESP解密密钥,对有效数据解密,并删去添加的尾部信息;

(3)将解密后的有效数据(明文)传送给上一层协议,如TCP协议层。

五、结　论

从以上协议分析可看到,与IPv4相比,IPv6在地址空间与结构、服务质量和安全性等方面均有显著的改进,随着因特网规模的不断增大和用户要求的不断提高,IPv6必将取代现有的IPv4,而成为互联网新的核心协议。在IPv4向IPv6过渡期间尽管能采用隧道(Tunnel)或双栈(Dual Stack)方式来使两者暂时兼存,但仍有许多问题难以解决,IPv4本身的不足难以弥补。另外,IPv6协议也是不断发展的,在设计IPv6时它为今后的各项改进提供了较大的余地。

参 考 文 献

[1] J. Postel, RFC791: Internet Protocol, September 1981.
[2] S. O. Bradner, A. Mankin, Ipng: Internet Protocol Next Generation, Addison-Wesley, 1995.
[3] S. Deering, R. Hinden, RFC1883: Internet Protocol, Version 6 (IPv6) Specification, December 1995.
[4] M. Mille, 兆雯. 从IPV4向IPV6转移的平稳之路. 今日电子. 97(4), 88-91.
[5] Silvano Gai. Internetworking IPv6 with Cisco Routers. 北京: 机械工业出版社. 1999年11月. P1-22
[6] Dee-Ann LeBlanc. Linux的Internet. 站点建立与维护. 北京: 清华大学出版社, 1997年7月, P69-156
[7] J. Moy, RFC1583: OSPF Version 2, March 1994.
[8] Y. Rekhter and Paul Traina, Inter-Domain Routing Protocol, Version 2, June 1996.
[9] Y. Rekhter and T. Li, RFC1771: A Border Gateway Protocol, March 1995.
[10] Tarek N. Saadawi, Mostafa H. Ammar and Ahmed El Hakeam. 远程通信网络基础. 北京: 电子工业出版社. 1996年5月, P9-22.
[11] ITU 标准, 一般延迟推荐值
[12] R. Braden, D. Clark and S. Senker, RFC1633: Integrated Services in the Internet Architecture: an overview, June 1994.
[13] S. Shenker, C. Partridge and R. Guerin, RFC2212: Specification of Guaranteed Quality of Service, September 1997.
[14] J. Wodawski, RFC2211: Specification of the Controlled-load Network Element Service, September 1997.
[15] S. Blake, D. Blake and M. Carlson, RFC2475: An Architecture for Differentiated Services, December 1998.
[16] V. Jacobson, K. Nichols and K. Podur, RFC2598: An expedited Forwarding PHB, June, 1999.
[17] J. Heinanen, F. Baker and W. Weiss, RFC2597: Assured Forwarding PHB Group, June 1999.
[18] 林闯. 多媒体信息网络QoS的控制. 软件学报. Vol. 10 (10), P1016-1024.
[19] R. Atkinson, RFC1825: Security Architecture for the Internet Protocol, August 1995.

[20] R. Atkinson, RFC1826: IP Authentication Header, August 1995.
[21] R. Atkinson, RFC1827: IP Encapsulating Security Payload, August 1995.
[22] 赖溪松,韩亮,张真诚.近代密码学及其应用.台湾:松岗.1995年,P63-91.
[23] P. Metzger and W. Simpson, RFC1828: IP Authentication Using Keyed MD5, August 1995.
[24] P. Metzger and W. Simpson, RFC1828: IP Authentication Using Keyed SHA, September 1995.
[25] P. Karn, P. Metzger and W. Simpson, RFC1829: the ESP DES-CBC Transform, August 1995.

The Characteristics of IPv6 and Protocol Analysis

Niansheng Liu Donghui Guo Boxi Wu

(Xia Men University)

Gerard Parr

(Ulster University UK)

Key words: IPv6, Address Architecture, Quality of Service, Network Security

Abstract: The characteristics of IPv6 in address mechanism, quality of service and network security are introduced in this paper. Compared with IPv4, there are so many improvements made in the IPv6. It resolves the main problems of IPv4 and pushes the Internet forward into the next generation.