

下一代互联网IPv6能力的开发

Development of IPv6 Capabilities for Next Generation Internet

凌苗/LING Miao

秦浩/QIN Hao

(中兴通讯股份有限公司 数据事业部, 江苏
南京 210012)
(Data division of ZTE Corporation, Nanjing
210012, China)

摘要: 文章介绍了以IPv6为核心技术的下一代互联网在IPv6的地址管理、服务质量扩展、集成的安全特性、对移动性的支持等方面的功能特点,并针对现在电信运营中万兴未艾的虚拟专用网(VPN)业务,探讨了IPv6技术下VPN的实现。文章认为采用IPv6技术不仅会促进数据通信市场发展,还会促进以话音通信为主的固定通信和移动通信市场,产生新的以娱乐和教育为主的视频通信服务市场以及信息家电连网服务市场,IPv6技术会为电信运营带来广阔的市场前景。

关键词: 服务质量;流标签;差分服务;集中服务;流分类

Abstract: The paper analyzes the improved functionalities of IPv6 that is the core of Next Generation Internet (NGI), in respects of IP address management, QoS extension, integrated security property, and mobility support. Concerning the rising Virtual Private Network (VPN) services favored by carriers, it discusses how to implement VPN on the basis of IPv6. It is concluded that IPv6 will promote not only the data communications market but also the voice-service-dominant fixed-line and mobile markets, thus creating markets for new kinds of video services aiming at entertainment and education as well as markets of household electric appliance networking services. The IPv6 technology will certainly bring telecom carriers a prosperous future market.

Key words: quality of service; flow label; DiffServ; IntServ; traffic class

中图分类号:

TN393.4

文献标识码:

A

文章编号:

1009-6868 (2005) 03-0039-04

大量增加的上网设备使得互联网的规模不断扩大,基于32位地址的IPv4协议逐渐显得力不从心。尽管出现了诸如网络地址转换(NAT)、无类域间路由(CIDR)以及混合地址等技术,在一定程度上缓解了IPv4地址短缺的压力,但是同时也带来了许多负面作用(如破坏了网络层的端到端架构等)。

相对于IPv4,IPv6协议的显著特点有:地址充足,报头简单,易于扩展,层次区划,实现安全,组播完善,QoS有保证,即插即用,移动便捷。

一些国内外著名的通信设备制造商和软硬件生产商都已经在它们

的路由器产品和操作系统当中实现了对IPv6的支持,一些著名的开放系统平台如FreeBSD、Linux等也加入了支持IPv6的软件包。各国还建立了若干针对IPv6的实验网络如6Bone、6Init,中国也建立了实验网络6TNET,并在实施全新的IPv6网络CNGI的建设。IPv6地址已经开始分配,一些国外网络运营商,如日本的IIJ和KDDI等,开始提供商用的IPv6接入服务。

目前IPv6基本协议以及路由协议等已经形成标准,可以提供IPv4协议所具有的所有功能。2000年5月,第3代移动通信合作计划(3GPP)在其R5版本的3G标准中明确要求将IPv6作

为下一代移动通信系统中的标准IP协议。IPv6作为取代IPv4的唯一的新一代互联网网际协议已经在世界范围内取得了共识。^[1-5]

1 服务质量管理

和IPv4相比,IPv6的QoS在目前还没有突破IPv4的局限性,但是,IPv6力图在体系架构上实现真正的QoS,并且在多个方面做出了重大的改进,这就是在IPv6包头中增加了新的流标签字段。

IPv6在IP头中引入了两个字段:

(1) Traffic Class字段

Traffic Class字段紧跟版本字段后

面,共8比特,指明为数据包提供的某种“区分服务”。与IPv4的服务类型(ToS)字段功能相同,位置比IPv4的ToS字段靠前,且是一开始就在IPv6中支持。

(2)Flow Label字段

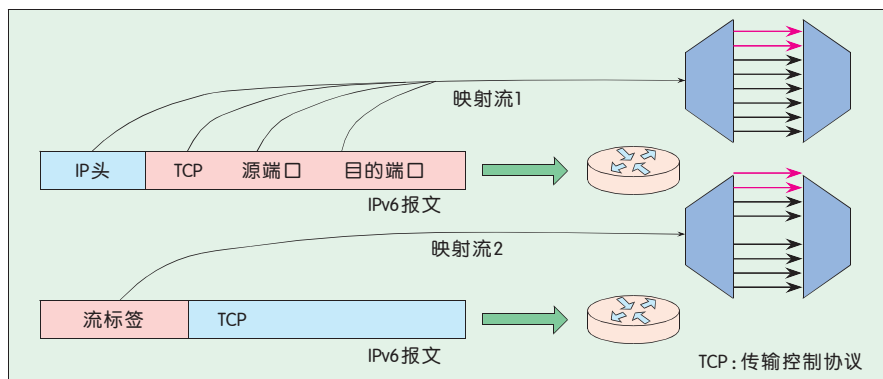
Flow Label字段跟在Traffic Class字段后面,共20比特,用于标识属于同一业务流的包。流标签和源节点地址唯一标识了一个业务流。同一个流中的所有包具有相同的流标签。可以对有同样服务质量要求的流作快速、相同的处理。

IPv6在报头中保留了类似IPv4的ToS域,称为传输级别域,可以继续为IP提供差分QoS服务,同时IPv6报头中增加了20比特流标签域,流标签可以更好地支持综合QoS服务,可以直接标识流,并配合资源预留协议(RSVP)实现资源预留,这是IPv6设计中对QoS能力增强的考虑。

IPv4的流分类器是根据信源地址、信宿地址、信源端口号、信宿端口号和传输协议类型的5元组确定,由于分组的拆分或加密,有些域往往难以获得高层协议的访问,也可能会阻碍新协议的引入。在拥有流标签的IPv6中,一个流可以由源IPv6地址和非空的流标签唯一地标识,源可以通过逐跳扩展头或控制协议RSVP等向转发路径的中间节点建立流状态。IPv6节点接收到一个有标记的IPv6分组时,可以用流标记、信源地址将分组分类到某个流。根据在一系列IPv6节点上建立的流状态可以对分组提供一些流特殊处理。IPv6和IPv4的不同可由图1简单说明。

除此之外,其他的QoS机制两者基本相同,不同点主要是多域(MF)分类和差分服务编码点(DSCP)标注:

(1)IPv4的MF分类主要基于源地址、目的地址、源端口、目的端口、协议号以及ToS,其中地址为32比特IP地址。而IPv6的MF分类主要基于Flow Label、源地址、目的地址、源端口、目的端口、协议号以及Traffic Class,其中



▲图1 IPv6和IPv4的流映射区别

地址为128比特IPv6地址。

(2)IPv4的DSCP标注在ToS字段中,而IPv6的DSCP标注在Traffic Class字段中。

2 集成的安全特性

IPv6将网络安全协议(IPSec)集成到协议内部,从此IPSec将不单独存在,而是作为IPv6协议固有的一部分贯穿于IPv6的各个部分。具体如下:

(1)IPv6针对网络安全做出的最大举措就是集成了IPSec,这对IPv6网络实现全网的安全认证和加密封装提供了协议上的保证。

(2)地址解析放在互联网控制协议(ICMP)的协议层使得ICMP协议与地址解析协议(ARP)相比与介质的耦合性更小,而且可以使用标准的IP认证机制。

(3)除了IPSec和IPv6本身对安全所作的举措之外,其他的安全防护机制在IPv6上仍然有效。

IPv6网络的安全性主要体现在3个层面,即协议安全、网络安全和安全加密的硬件实现。在协议安全层面上,IPv6的认证头(AH)和封装安全载荷(ESP)信息安全封装扩展头结合多样的加密算法可以满足协议层面的安全需求。在AH认证方面,加密算法可采用hmac_md5_96、hmac_sha_1_96等认证加密算法,在ESP封装方面经常采用的算法有DES_CBC、3DES_CBC以及Null等3种。

在网络安全实现方面,通过IPSec

的隧道和传输模式的各种应用组合,可以满足各个网络层面的安全需要,诸如端到端的安全保证、对内部网络的保密、通过安全隧道构建安全的VPN、以及通过嵌套隧道实现不同级别的网络安全等。

大量使用IPSec在提高网络安全的同时不可避免地导致路由器转发和处理性能的劣化,为了消除这些影响,通常是使用专用集成电路(ASIC)实现加密处理,或者通过网络处理器来实现加密处理和转发。

IPSec提供了网络数据和信息内容的有效性、一致性以及完整性的保证,但是对数据网络的安全威胁是多层面的,它们分布在物理层、数据链路层、网络层、传输层和应用层等各个部分。

通常物理层的威胁来自于设备的不可靠性,诸如板卡的损坏、物理接口的电器特性和电磁兼容环境的劣化等等,对这样的安全隐患可以通过配置冗余设备、冗余线路、安全供电、保障电磁兼容环境以及加强安全管理来防护。

对于物理层以上层面的安全隐患除了来自于针对各种协议的安全隐患以外,还有非法占用网络资源或者耗尽网络资源等隐患,诸如双802.1Q封装攻击、广播包攻击、媒体访问控制(MAC)洪泛、生成树攻击等二层攻击以及虚假的Internet控制消息协议(ICMP)报文、ICMP洪泛、源地址欺骗、路由振荡等来自针对三层协

议的攻击。在应用层还有针对HTTP、FTP/TFTP、TELNET以及通过电子邮件传播病毒的攻击手段。对于这些攻击,可以采用的防护手段如下:

(1) 通过诸如TACACS+、RADIUS、AAA等安全访问控制协议控制用户对网络的访问权限来防患针对应用层的攻击。

(2) 通过MAC地址和IP地址绑定、限制每端口的MAC地址使用数量、设立每端口广播包流量门限、使用基于端口和VLAN的ACL、建立安全用户隧道等来防范针对二层的攻击。

(3) 通过进行路由过滤、对路由信息的加密和认证、定向组播控制、提高路由收敛速度、减轻路由振荡的影响等措施来加强三层网络的安全性。

完善的IPv6的IPSec机制提供了网络数据和信息内容的有效性、一致性以及完整性的保证,并且为网络安全提供了诸多的解决办法。为了构建安全网络还可以结合AAA认证,NAT-PT,二、三层多协议标记交换(MPLS)VPN、ACL的标准访问列表和扩展访问列表、防分片包攻击来实现安全预防;通过路由过滤、静态路由、策略路由和路由负荷分担来实现安全路由;通过SSHv2、SNMPV3、EXC提供进程访问安全、线路访问安全;通过分级管理、定制特权级管理等手段来实现网络的安全管理;最后通过完善的告警、日志和审计功能实现网络时钟的安全,同时提供访问列表和关键事件的日志、路由协议事件和错误记录等供网络管理人员进行故障分析、定位和统计。

3 地址管理

IPv6采用128比特地址结构解决IPv4地址空间不足的问题,一个较大的地址空间可以在地址空间内使用多层等级结构,严格的层次性编址有助于实现路由聚合,不仅可以使路由条目大大减少,利于提高网络性能,而且提高了路由选择的效率和可扩展性。具有严格路由聚合的特性使

IPv6多点接入站点能够从数千个上游提供商那里配置地址,使多点接入成为可能,IPv6支持地址的自动配置。由于具有比较大的地址空间,IPv6能够在保持全球唯一性的同时自动配置设备上的地址。自动地址配置机制通过将自身的链路层地址(如以太网MAC地址)以EUI-64的格式附加在子网上公告的全球唯一单播IPv6前缀后面,保证自动配置的128比特地址是全球唯一的。IPv6允许网络中的节点自动配置它们自己的IPv6地址的特性,为将来移动设备的接入和热插拔的应用提供良好的保障。

IPv6的重新编址机制使在IPv6提供商之间的转换对最终用户是透明的。IPv6可以为公告的子网前缀赋予一个生存期的值,在当前的前缀到期后允许节点使用最新的前缀,这样主机和服务器的可以自动选用新的全球单播IPv6前缀,使用新的地址。

IPv6使用多播取代了IPv4中的广播,当在本地链路上使用多播组的多播地址发送数据包的时候,数据包只被这个组的成员处理。通过对不同的功能使用不同的多播组,有效地利用了网络,防止了IPv4中的广播风暴。

4 移动性支持

下一代网络基于IPv6构建IP核心骨干网,数十亿的3G蜂窝设备具有IPv6协议栈,IPv6的移动性是必须的。相比移动IPv4是IPv4协议的附加物来说,在IPv6中移动性是协议内置的,任何支持IPv6的节点在需要时都能够使用移动性支持。移动IPv6的主要目标就是使得移动节点总是通过家乡地址寻址,不管是连接在家乡链路还是移动到外地网络。移动IPv6对于IP层以上的协议层是完全透明的,这使得移动节点在不同子网间移动时,运行在该节点上的应用程序不需要修改或配置就仍然可用。

相比移动IPv4来说,移动IPv6没有外地代理,因为每个移动IPv6节点都能处理移动性,但是在IPv6中家乡

代理仍是必须的。移动IPv6主要使用两个IPv6扩展包头:目的地址扩展包头(注册时使用)和路由选择扩展包头(用于在移动节点和通信节点之间传输数据报)。

移动IPv6技术充分利用了IPv6协议对移动性的内在支持。移动节点根据路由器的广播报文宣称代理指示,向任意一个本地代理注册。本地代理中保存有移动节点的家乡地址和转交地址的对照表,家乡代理可以根据对照表把报文转发给移动节点。每当移动节点收到其他主机发来的报文后,在响应报文中以转交地址作为源地址,并要附上移动节点的家乡地址,当主机的后续报文以移动节点的转交地址为目的地址时,需要附带源路由选择扩展包头,包头内容为移动节点的家乡地址。使用这种机制的目的是保证移动节点在移动过程中也不会丢失报文。当移动节点在小区切换时,移动节点重新登记成功后,基站应该向原来的基站发重定向报文,使切换过程中路由有偏差的报文重新找到移动节点。移动IPv6协议目前还有一些问题需要解决,包括IPv6无缝越区切换技术和AAA问题等。

5 VPN业务实现

随着IPv6流量的迅速增长,下一代网络的骨干网将以集性能与可扩展性于一身的MPLS技术为主导,MPLS基于标记交换数据包,无需再在每个网络节点进行复杂的路由查找,带给硬件的负担更小。MPLS一般使用标记分配协议(LDP)或资源预留协议-流量工程(RSVP-TE)实现标签的分发。在IP骨干网上建立隧道,通过标签转发使数据快速地通过隧道,可以提供很好的服务质量保证和流量工程。

传统的二层VPN为点对点的直连链路,以L2TP为代表;下一代网络将以多点对多点二层MPLS VPN为主,按功能可以划分为虚拟专用线路服务(VPWS)和虚拟专用局域网子网段

(VPLS)两种。VPLS主要在MPLS/IP核心传输网络中提供以太网的仿真业务，而VPWS主要在MPLS/IP核心传输网络中提供对传统业务（如ATM、FR、HDLC或PPP等）的支持，很好地提供了Any Transport over MPLS的技术手段。二层MPLS VPN不用维护用户网络的路由信息，大大降低了对骨干网边缘（PE）路由器路由处理能力以及对用户网边缘（CE）路由器设备的要求。二层MPLS VPN在管理上比较简单，可以很好地降低运行维护成本。

传统的三层VPN以点对点的通用路由封装（GRE）和IPinIP为主，下一代网络的三层VPN将以BGP MPLS VPN为主导。BGP MPLS VPN允许多个用户站点通过一个公用的IP网络通信，好像所有的用户都处于同一个私有网络内。PE路由器必须为每个VPN用户分别维护一张虚拟路由/转发实例（VRF）表，记录有从CE学到的用户路由信息，用于VPN数据的转发。入口PE路由器为每个数据包加上两层标签，外层标签用于到达对端PE路由器，内层标签用于分发的标识用户网络的标签。包到达对端出口PE路由器时，出口PE路由器可以根据内层标签判断VPN，进行相应转发。

6PE功能是在MPLS的边缘路由器PE上支持IPv6的路由功能，实现私网为IPv6的BGP MPLS VPN，并通过MP-BGP技术和MPLS交换功能实现IPv6的网络互连。这种方式只需在PE路由器上增加软件配置即可以提供IPv6服务，作为MPLS骨干的设备和软件配置不需要做任何修改，从ISP的角度来看，整个骨干网的控制层面没有改变，也不需要添加任何的开销，包括运行管理和设备的添置，可以使因特网业务提供商（ISP）可平稳地过渡到IPv6通信服务。同时，ISP可最大限度地共享网络资源，节省网络的运行管理成本，减小技术投资风险。

6 结束语

由于IPv6具有的技术特点，基于

IPv6的网络有望支持大规模的、多种形式的、新型的网络应用，需要研制和开发大量的系统软件和应用软件。与网络建设与运营、设备制造产业相比，软件产业发展具有更大的自主性，更加贴近中国国情的发展需要，因此，IPv6技术将为中国的软件产业带来更大的发展空间，具有广阔的市场前景。

与互联网相关的设备包括通信设备、网络设备（路由器和交换机）、主机和终端设备、网络与信息安全设备（防火墙等）。采用IPv6技术建立互联网，中国有望成为世界上最大的互联网市场，为国内研制和生产上述设备的制造商提供了巨大商机，并可大大促进关键设备国产化的进程^[6,7]。同时，由于IPv6带来的网络可扩展性和可移动性，也为各种移动式终端、流媒体信息终端及其外部设备，以及信息家电的制造厂商提供重要发展机遇，因此，IPv6技术可为设备制造产业带来广阔的市场前景。

通过实验和验证IPv6技术的可行性，为电信运营商探索新型业务模式以及相应的运营模式，加速从传统电信到IP技术的过渡，支持多种形式的应用和服务，使电信运营商能够从下一代互联网中盈利。采用IPv6技术的互联网，不仅会覆盖以互联网为主的数据通信市场，还会覆盖以话音通信

为主的固定通信和移动通信市场，并会产生新的以娱乐和教育为主的视频通信服务市场，以及信息家电联网服务市场。因此，IPv6技术会为电信运营带来广阔的市场前景。

7 参考文献

- [1] IETF RFC2401 Security Architecture for the Internet Protocol [S].
- [2] IETF RFC2402 IP Authentication Header [S].
- [3] IETF RFC2406 IP Encapsulating Security Payload [S].
- [4] IETF RFC2474 Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers [S].
- [5] IETF RFC3697 IPv6 Flow Label Specification [S].
- [6] 中兴通讯. 宽带数据网络安全技术白皮书 [Z].
- [7] 中兴通讯. ZXR10 T128/64E QoS技术白皮书 [Z].

收稿日期：2005-04-07

作者简介



凌苗，中兴通讯数据事业部数据系统部系统工程师，从事ATM交换机、IP高端路由器、IPv4、IPv6路由协议栈平台的设计工作。



秦浩，中兴通讯数据事业部数据系统部系统工程师，从事IP高端路由器、IPv4、IPv6路由协议栈平台的设计工作。

中兴通讯获希腊电信DSL扩容项目合同

2005年5月10日，中兴通讯在全球多家知名厂商参与的竞标中一举胜出，获得希腊最大固网运营商希腊电信（OTE）DSL宽带网络扩容项目合同。据世界著名调查机构Gartner的最新市场报告，中兴通讯DSL产品全球应用规模已超1200万线，市场份额晋身全球三甲。

中兴通讯承建保加利亚DWDM项目

继2005年初与法国电信、葡萄牙电信等欧洲主流电信运营商签订网络设备供货合同之后，2005年5月9日，中兴通讯又与保加利亚主要固网运营商Cabletel签订了正式合同，独家承建全长500 km的保加利亚DWDM项目。目前，中兴通讯已成功进入亚洲、欧洲、独联体、南美、中东等地区的光网络市场，成为国际上成长最快的光网络设备供应商。