IPv6相对于IPv4在安全方面的改进 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/251/2021_2022_IPv6_E7_9B_B8_E5_AF_B9_c101_251044.htm IP安全协议（IPSec） IPSec是IPv4的一个可选扩展协议，而在IPv6则是一个必备组成部分。IPSec协议可以“ 无缝 ”地为IP提供安全特性，如提供访问控制、数据源的身份验证、数据完整性检查、机密性保证，以及抗重播（Replay）攻击等。新版路由协议OSPFv3 和RIPng采用IPSec来对路由信息进行加密和认证，提高抗路由攻击的性能。 需要指出的是，虽然IPSec能够防止多种攻击，但无法抵御Sniffer、DoS攻击、洪水（Flood）攻击和应用层攻击。IPSec作为一个网络层协议，只能负责其下层的网络安全，不能对其上层如Web、E-mail及FTP等应用的安全负责。 端到端的安全保证 IPv6最大的优势在于保证端到端的安全，可以满足用户对端到端安全和移动性的要求。IPv6限制使用NAT，允许所有的网络节点使用其全球惟一的地址进行通信。每当建立一个IPv6的连接，都会在两端主机上对数据包进行IPSec封装，中间路由器实现对有IPSec扩展头的IPv6数据包进行透明传输，通过对通信端的验证和对数据的加密保护，使得敏感数据可以在IPv6 网络上安全地传递，因此，无需针对特别的网络应用部署ALG（应用层网关），就可保证端到端的网络透明性，有利于提高网络服务速度。 地址分配与源地址检查在IPv6的地址概念中，有了本地子网（Link- local）地址和本地网络（Site-local）地址的概念。从安全角度来说，这样的地址分配为网络管理员强化网络安全管理提供了方便。若某主机仅需要和一个子网内的其他主机建立联系，网络管

理员可以只给该主机分配一个本地子网地址；若某服务器只为内部网用户提供访问服务，那么就可以只给这台服务器分配一个本地网络地址，而企业网外部的任何人都无法访问这些主机。 由于IPv6地址构造是可会聚的（aggregate-able）、层次化的地址结构，因此，在IPv6接入路由器对用户进入时进行源地址检查，使得ISP可以验证其客户地址的合法性。 源路由检查出于安全性和多业务的考虑，许多核心路由器可根据需要，开启反向路由检测功能，防止源路由篡改和攻击。 防止未授权访问 IPv6固有的对身份验证的支持，以及对数据完整性和数据机密性的支持和改进，使得IPv6增强了防止未授权访问的能力，更加适合于那些对敏感信息和资源有特别处理要求的应用。 域名系统DNS 基于IPv6的DNS系统作为公共密钥基础设施（PKI）系统的基础，有助于抵御网上的身份伪装与偷窃，而采用可以提供认证和完整性安全特性的DNS安全扩展 （DNS Security Extensions）协议，能进一步增强目前针对DNS新的攻击方式的防护，例如“ 网络钓鱼（Phishing）”攻击、“ DNS中毒（DNS poisoning）”攻击等，这些攻击会控制DNS服务器，将合法网站的IP地址篡改为假冒、恶意网站的IP地址等。此外，专家认为，如果能争取在我国建立IPv6域名系统根服务器，则对于我国的信息安全很有必要和十分重要。 灵活的扩展报头 一个完整的IPv6的数据包可包括多种扩展报头，例如逐个路程段选项报头、目的选项报头、路由报头、分段报头、身份认证报头、有效载荷安全封装报头、最终目的报头等。这些扩展报头不仅为IPv6扩展应用领域奠定了基础，同时也为安全性提供了保障。 防止网络扫描与病毒蠕虫传播当病毒和蠕虫在感染了一台主机之后，就

开始对其他主机进行随机扫描，在扫描到其他有漏洞的主机后，会把病毒传染给该主机。这种传播方式的传播速度在IPv4环境下非常迅速（如Nimdar病毒在4～5分钟内可以感染上百万台计算机）。但这种传播方式因为IPv6的地址空间的巨大变得不适用了，病毒及网络蠕虫在IPv6的网络中传播将会变得很困难。 防止网络放大攻击（Broadcast Amplication Attacks） ICMPv6在设计上不会响应组播地址和广播地址的消息，不存在广播，所以，只需要在网络边缘过滤组播数据包，即可阻止由攻击者向广播网段发送数据包而引起的网络放大攻击。 防止碎片（Fragment）攻击 IPv6认为MTU小于1280字节的数据包是非法的，处理时会丢弃MTU小于1280字节的数据包（除非它是最后一个包），这有助于防止碎片攻击。