安全数字世界

预建未来
PLAN UP

作者版权所有
请勿转载

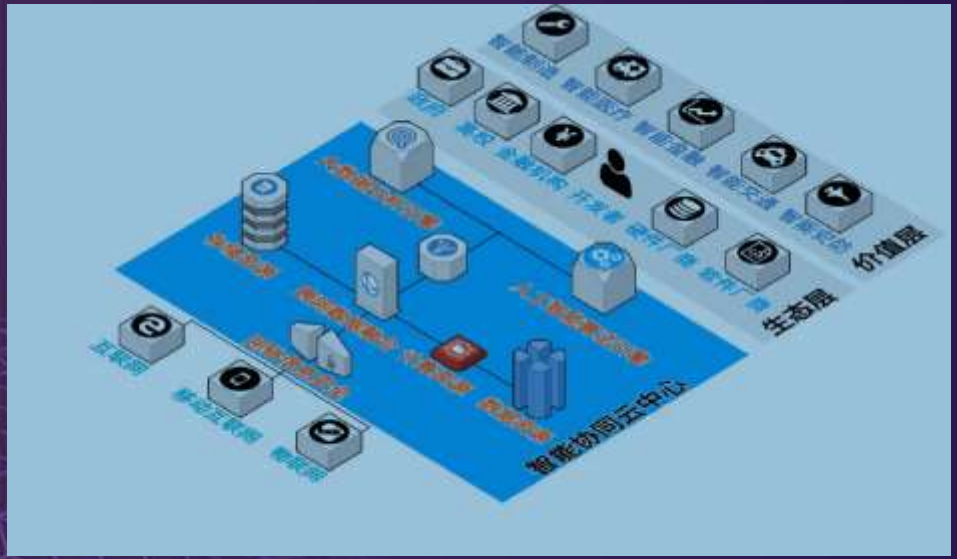
万网融合，IPV6规模部署下的网络安全挑战

王鸿志
中国航天科工集团有限公司
科技委及网信部

作者版权所有
请勿转载

目录

万网融合，万物互联的航天科工智能协同云



智能协同云以智能、协同、云化为核心特征，以万网融合和万物互联为基础，以人工智能为手段，以数据和知识为核心，以信息安全为基石，采用全新的网络信息架构体系，实现网络信息技术与实体经济的深度融合，为数字经济提供全方位、全领域、全纵深、全要素的安全、可靠、实用、快捷、廉价、方便的信息服务，打造一种万网融合型的“中国方案”。

IPv6是万网融合的网络基础

传统互联网时代

90年代初至2010年

- PC机互联
- 20年间共产生了21亿台的设备
- TCP协议全面替换NCP协议，面向可靠连接的互联网横空出世

移动互联网时代

2010年至今

- 移动端（人与人）互联
- 数年时间，设备量增长到了60亿以上
- 3G/4G网络的出现，使互联网走到了移动端

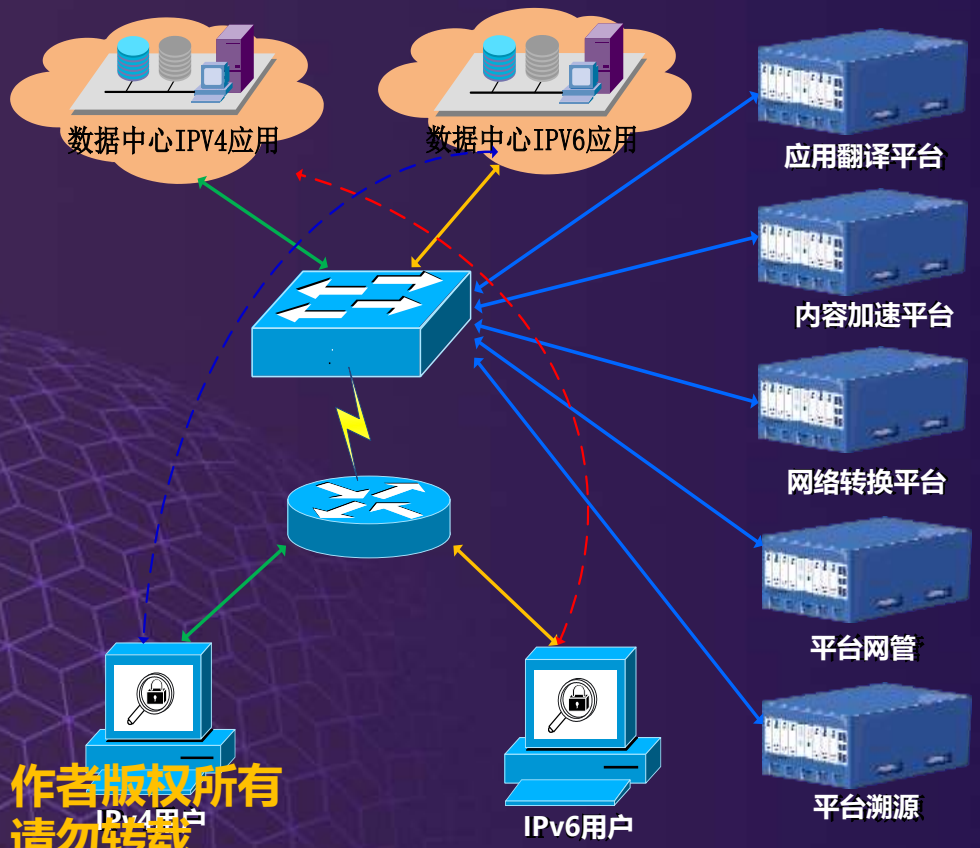
万网融合时代

未来10年

- 物与物互联
- 网网互联
- 设备量预计将增长到500亿台
- 物联网按60万亿终端规划
- 万物互联承载—IPv6

万网融合需要海量的IP地址，IPv4地址已近枯竭无法满足需要，必须采用IPv6地址

IPv6规模部署方案-IPv4/IPv6网间网协议交换平台



翻译平台：融合应用层和网络层协议翻译技术，实现IPv4和IPv6的内容互通（优于NAT64）

加速平台：通过静态数据智能缓存与内容加速，为用户提供更优的体验。

转换平台：基于云平台架构实现的DSLITE隧道与GREv6遂道，实现4in6 隧道传输，并具备NAT64+DNS64功能及NAT ALG扩展功能。

网管平台：服务状态，故障告警、性能管理，CPE管理，可视化业务开通等功能。

溯源平台：应用层翻译日志信息、网络转换日志、日志统计溯源等功能。

目录

作者版权所有
请勿转载

IPv6相对于IPv4具备明显的安全优势

IPv4	IPv6
采用了32bit的地址结构，以二进制或十进制格式表示，对网络发展速度估计不足，IPv4未分配地址很快会被耗尽。	**采用了128bit的地址结构**，以二进制或16进制格式表示，可以提供2^128地址，几乎可以不受限制地提供地址。

IPv6优势

- ✓ **反扫描**：提供了巨大的地址空间，地址空间扫描不再可行，基于网络扫描的传播方式不再可行，网络蠕虫攻击将变得困难。
- ✓ **可溯源**：建立了源地址验证机制，可用于攻击事件溯源；
- ✓ **数据认证和加密**：集成IPSec，采用邻居发现协议（NDP）取代IPv4中ARP及部分ICMP控制功能，提供了端到端通信防篡改和加密能力；
- ✓ **防碎片攻击**：IPv6数据包头固定长度，不允许分片，防止了针对报头的碎片攻击；分片ID不能被攻击者预测，发送伪造的碎片报文以发动攻击的方法不再有效。

网络安全挑战：IPv6没有完全解决IPv4的安全问题

- **传输数据报文**的基本机制没有发生改变，IP层以上的其他四层中的安全问题并没有解决。

- 应用层业务系统的**漏洞问题**没有改善；
  - ✓ **应用层欺骗攻击；**
  - ✓ **恶意用户发起的攻击；**
  - ✓ **木马间谍类攻击；**
  - ✓ **漏洞或误用类攻击；**

- **源地址伪造**等问题方面没有得到改善；

作者版权所有
请勿转载

网络安全挑战：IPv6协议脆弱性带来新的安全威胁

- **扩展报头攻击**

攻击者可能利用IPv6报文的扩展报头（可选且有多种扩展报头），通过自制畸形或者特定格式的恶意数据包来攻击路由器和主机。

- **拒绝服务攻击**

攻击者可能利用邻居发现协议发送错误的路由器宣告和重定向消息等让IP数据流向不确定的方向，进而达到拒绝服务、拦截和修改数据的目的。

- **非授权用户**

IPv6支持无状态地址自动分配可能使非授权用户可以更容易的接入和使用网络。无状态地址自动分配可能使非授权用户可以更容易的接入和使用网络。

- **组播维护协议隐患**

IPv6组播所需的MLD等组播维护协议不能满足安全的需要，存在机密数据被窃听、对处理MLD报文的路由转发设备发起拒绝服务攻击（DoS）的安全隐患。

作者版权所有
请勿转载

网络安全挑战：IPv4/IPv6过渡期间的安全威胁

当前，IPv4还是网络的主流，可以预见很长一段时间内，IPv4和IPv6将共存。过渡期间安全防护将面临更为复杂的安全威胁。

- **双栈技术**

许多操作系统都支持双栈，IPv6默认是激活的，但并没有像IPv4一样加强部署IPv6的安全策略，支持自动配置，即使在没有部署IPv6的网络中，这种双栈主机也可能受到IPv6协议攻击。

- **隧道技术**

几乎所有的隧道机制都不对IPv 4和IPv6地址的关系做严格检查，没有内置认证、完整性和加密等安全功能，攻击者可以随意截取隧道报文，通过伪造外层和内层地址伪装成合法用户向隧道中注入攻击流量，存在仿冒以及篡改泛洪攻击安全威胁。

- **翻译技术**

涉及载荷转换，无法实现端到端IPsec，存在受到NAT设备常见的地址池耗尽等DDoS攻击安全威胁。

作者版权所有
请勿转载

网络安全挑战：IPv6协议族安全威胁

- **ICMP v6报文控制协议**
  - ✓ 消息伪造
  - ✓ 恶意篡改
  - ✓ DoS攻击
  - ✓ 对上层协议的攻击
- **DHCP v6动态主机设置协议**
  - ✓ DoS攻击
  - ✓ 信息窃取
- **NDP邻居发现协议**
  - ✓ DoS攻击
  - ✓ 信息窃取
  - ✓ 中间人攻击

作者版权所有
请勿转载

网络安全挑战：网络安全设备升级支持IPv6的问题

- 市场上网络安全产品IPv6的支持度普遍较低，根据全球IPv6测试中心网站统计，国内共14个公司，110款安全产品通过IPv6 Ready Logo认证。

厂商名称	蓝盾	绿盟	华为	网神	亚信安全	安恒	启明星辰	天融信
数量	33	10	12	15	3	8	9	12

摘自全球IPv6测试中心网站2019.4.29

作者版权所有
请勿转载

网络安全挑战：万网融合数据安全更加挑战

跨网数据访问很难做到同样粒度的数据**访问权限控制**，容易出现木桶效应问题；数据的访问还要满足**安全审计**的要求。

不同密级/安全等级的数据跨网交换，既要保证数据的**机密性**，又要保证数据的**完整性**。

数据加密是最有效的手段，但是因为处理能力和功耗问题，加密强度不够。

敏感数据的共享需要提供**数据脱敏**安全能力。

无论是个人还是企业**隐私数据**，从法律遵从的角度（GDPR等），需要保证数据不被泄露和合法使用。

作者版权所有
请勿转载

目录

作者版权所有
请勿转载

IPv6安全防护建设思考

积极投入IPv6安全防护技术研究

- ✓ 防火墙技术
- ✓ 安全扫描技术
- ✓ 入侵检测技术
- ✓ 主机防护技术
- ✓ 安全调查取证
- ✓ 安全审计技术
- ✓ 态势感知技术

加大自主可控IPv6安全设备研发

- ✓ 防火墙
- ✓ 入侵检测系统
- ✓ 防病毒系统
- ✓ 安全管理系统
- ✓ 安全防护系统
- ✓ 安全监测系统
- ✓ 安全态势感知系统

建立IPv6安全制度、人才等安全保障

- ✓ 安全管理制度
- ✓ 安全人才队伍培训培养
- ✓ 安全应急演练
- ✓ 安全配置加固

制定IPv6网络安全相关技术、评测和产品认证标准

- ✓ 安全设备标准
- ✓ 安全运维标准
- ✓ 安全评估标准
- ✓ 安全评估工具
- ✓ 网络安全架构标准
- ✓ IPv6设备成熟度认证

Thank You

作者版权所有
请勿转载