上海交通大学
SHANGHAI JIAO TONG UNIVERSITY

SJTU

IPv6环境下的网络安全攻防对抗

上海交通大学
姜开达
2023/11/28

目 录

IPv6 发展现状

中国IPv6综合发展指数地图

依据《中国IPv6发展指标》，综合各省用户、流量、网络基础设施、应用基础设施、网站和应用的IPv6发展数据计算得出，港澳台数据来自APNIC

IPv6互联网活跃用户

7.712亿

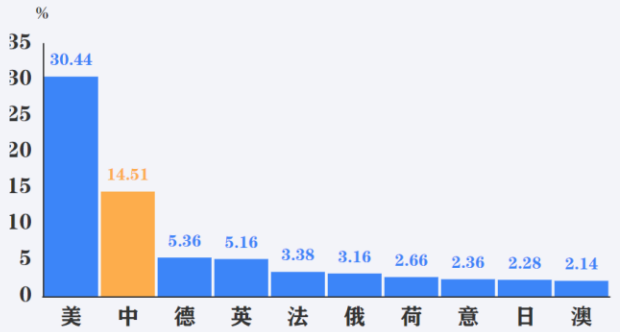
72.27%

IPv6流量

移动核心网入口IPv6流量占比 60.22%

移动核心网出口IPv6流量占比 56.9%

IPv6地址拥有量

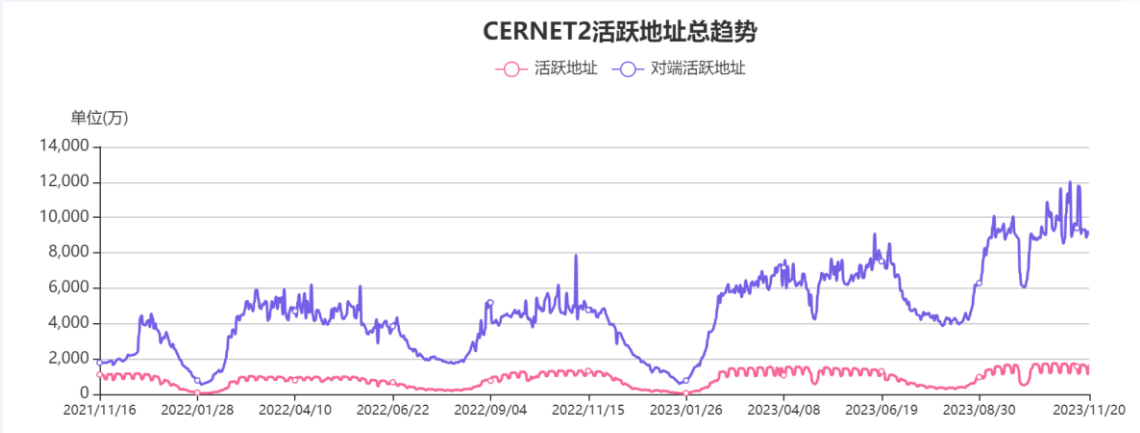


67427 块/32

IPv6地址数量

2

全球排名



数据来源：国家IPv6发展检测平台 https://m.china-ipv6.cn/complete/

与 IPv6 安全相关的政策文件

工业和信息化部等八部门关于推进IPv6技术演进和应用创新发展的实施意见

工信部联通信〔2023〕45号

- **13.强化IPv6网络安全防护。**加强基础电信企业、互联网企业等IPv6网络安全改造和防护管理，落实通信网络安全防护管理有关要求，持续开展IPv6网络和系统单元定级备案，定期开展风险评估和安全检测。强化IPv6环境下网络安全技术手段建设，扩大移动互联网、互联网数据中心等IPv6重要网络节点覆盖范围，强化IPv6网络安全威胁监测处置技术能力。
- **14.加快IPv6安全技术创新。**组织开展网络安全技术应用试点，遴选IPv6环境下网络安全解决方案，促进IPv6环境下网络安全技术创新。加快IPv6技术在安全领域的融合创新，促进IPv6与人工智能、区块链、大数据、数字身份证等新技术以及网络安全技术的深度融合，强化安全监测、安全编排等技术能力建设。
- **15.推动IPv6安全应用。**支持研究制定安全测评规范与评价准则，完善评估评价体系，提升安全能力。推动基于“IPv6+”的网络安全产品和服务在政府、电信、金融等重点行业普及应用。

与 IPv6 安全相关的政策文件

关于加快推进互联网协议第六版（IPv6）规模部署和应用工作的通知

中网办发文〔2021〕15号

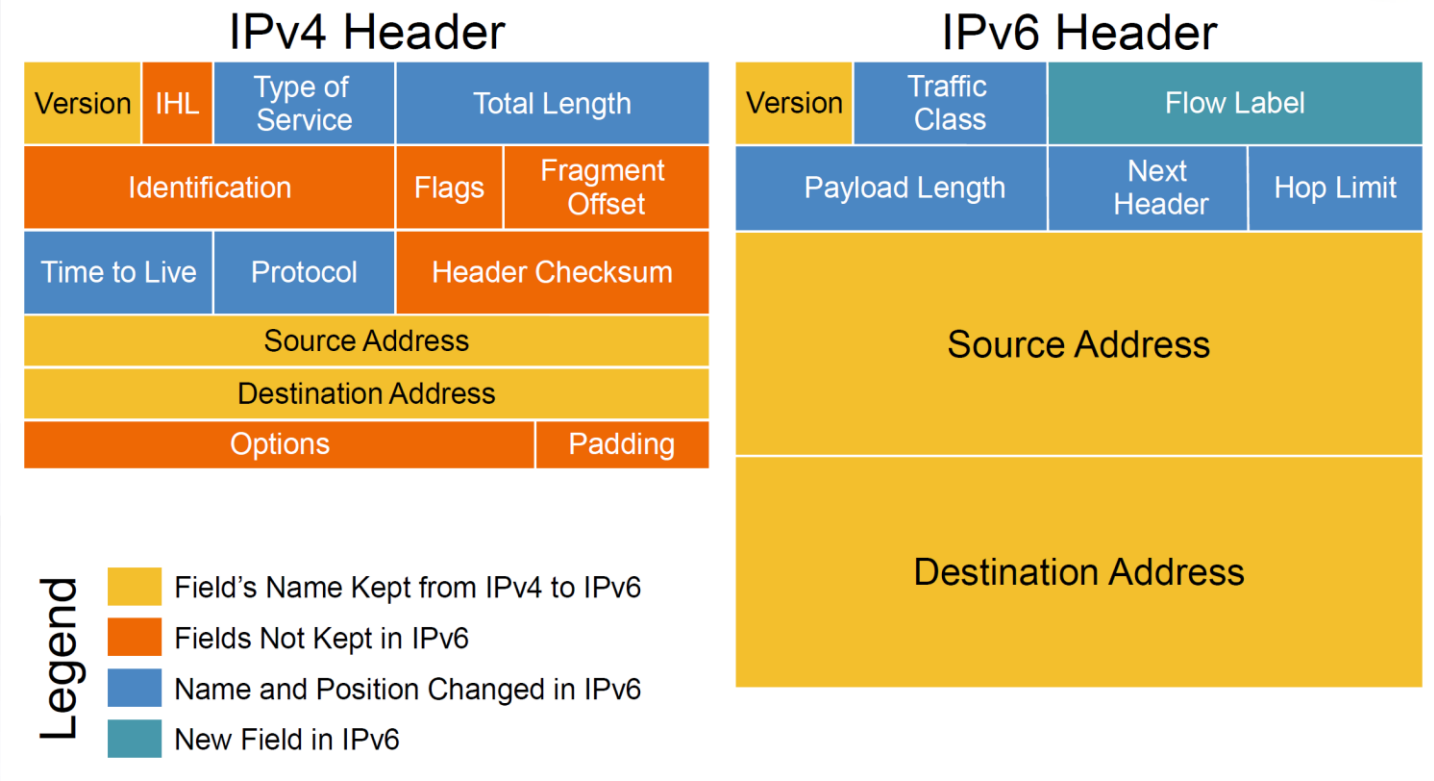
- **29.构筑IPv6网络安全防护体系。**落实网络安全等级保护制度，明确IPv6安全保护要求。加强重点领域IPv6安全防护体系建设，升级安全系统，强化复杂场景下IPv6安全保障能力。依托国家网络与信息安全信息通报机制，构建IPv6安全监测体系，提高IPv6安全态势感知、通报预警和应急响应能力。

- **30.提升新兴领域安全保障能力。**加强IPv6安全技术研究，开展IPv6核心安全技术攻关。加强IPv6环境下工业互联网、物联网、车联网、云计算、大数据、人工智能等新兴领域的安全技术、管理及机制研究。

目 录

IPv6 与 IPv4 的变化

- 变化不大
  - L2以下与L4以上
  - 路由协议
    - BGP、OSPF、RIP
- 主要改变
  - 地址空间增大 $2^{32} \rightarrow 2^{128}$
  - 单主机拥有多个地址
  - 报文头
  - 使用ND协议替代ARP
- 引入众多安全更新



IPv6 对安全性的提升

- IPv6的安全增强源于两个方面
  - 地址空间的显著增加对安全形成了增强
  - IPv6协议设计上增加了多项安全特性

✓ 反黑客扫描能力大大提高
- IPv6地址空间巨大，广泛的IPv6地址扫描困难
- 业务系统被互联网探测引擎扫描发现的可能性降低

✓ 信息的可溯源性显著提升
- IPv6可为每个网络设备分配唯一的地址
- 设备发出的数据包与设备地址对应，具备事后追查回溯能力

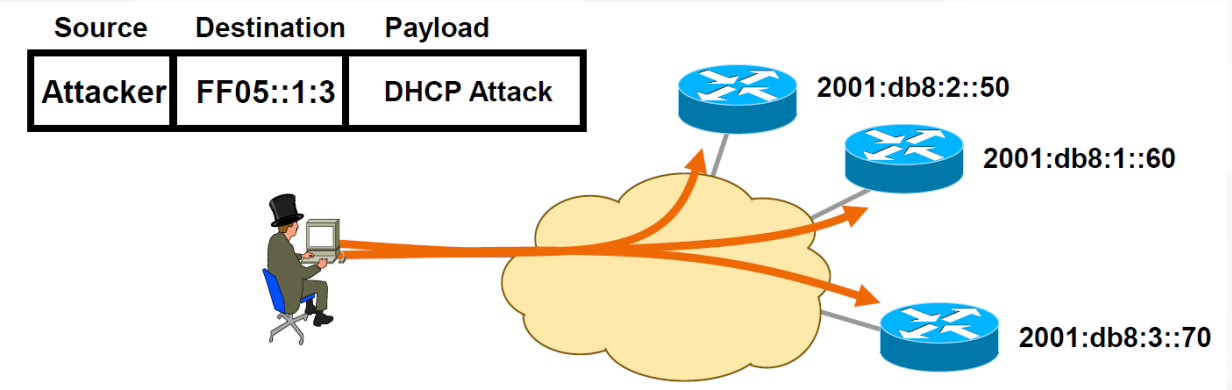
✓ 部分IPv4中常见的攻击风险得以避免或缓解
- IPv6中无广播机制
- IPv6不允许碎片重叠

IPv4 & IPv6 共有安全问题

- **IPv6只变更了网络层协议**
  - 应用层的攻击依然存在
  - 例如Web漏洞、各类弱口令、配置运维不当等
- **默认配置的IPv6依然会受到以下网络层攻击**
  - 嗅探
  - 恶意设备接入
  - 中间人攻击
  - 泛洪攻击
- **IPv6原生支持IPsec所以更安全?**
  - 错误的，AH与ESP报文头依然是可选项
  - 全设备通用的端到端安全部署仍有困难（PKI更新等）
  - IPsec 在 IPv6 下部署要求与 IPv4 差异不大

IPv4 & IPv6 共有安全问题 – 主机发现

- IPv6使用ICMPv6 ND协议替代了IPv4 ARP协议，移除了广播，但没有解决所有安全问题。
- 主机发现
  - IPv6组播地址
    - FF02::1 link-local 所有主机
    - FF02::2 link-local 所有路由
    - FF05::2 site-local 所有路由
    - FF05::1:3 site-local DHCP服务器
    - ……



- IPv6无法对地址空间进行枚举，但在 本地网络 内依然有主机发现能力。
- 在一些特定的攻击场景下，IPv6组播甚至提供了便利。

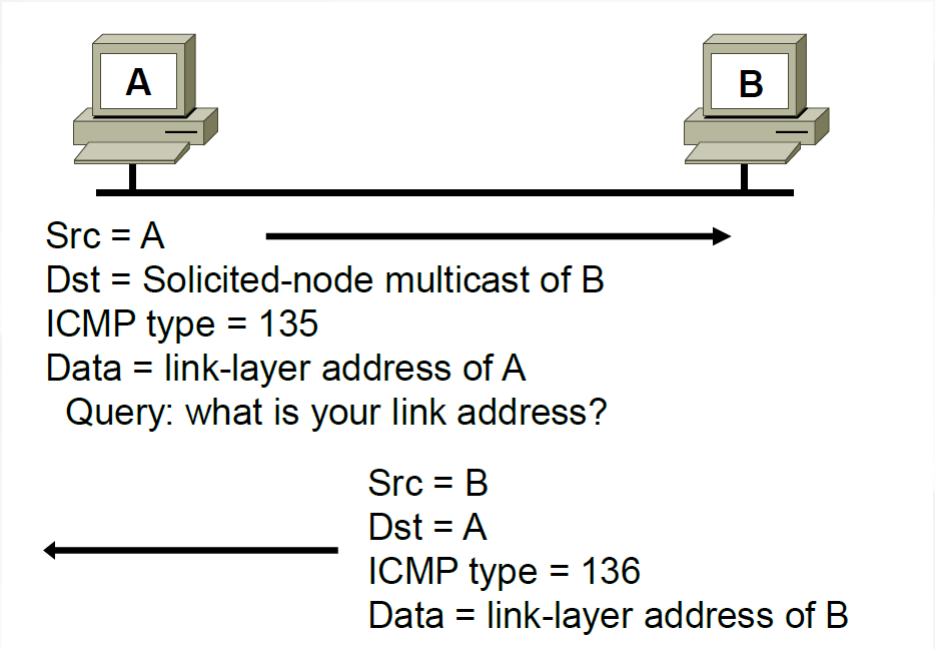
- 工具：ping -6 ff02::1%eth0

IPv4 & IPv6 共有安全问题 – 主机仿冒

- IPv6邻居发现请求 Neighbor Solicitation
  - 每个主机根据IPv6地址的主机段信息自动加入对应组播组，组播组对加入成员无约束机制
  - 主机A向主机B所在组播组发送二层地址查询请求
  - 无原生安全机制，与IPv4 ARP非常相似

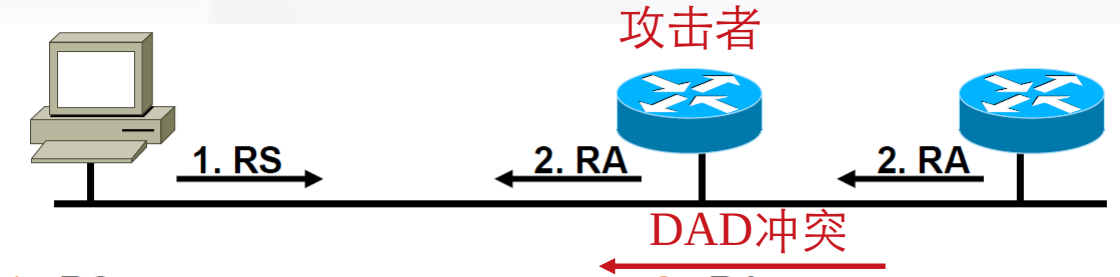
- 攻击者通过应答所有邻居发现请求，达成仿冒主机的目的。

- 工具： thc-ipv6/parasite6



IPv4 & IPv6 共有安全问题 – 路由劫持

- IPv6使用广泛的无状态地址自动配置(SLAAC)过程
  - 地址与路由配置使用
    - 路由宣告RA（Router Advertisement）
    - 路由请求RS（Router Solicitation）
  - 未配置鉴权的RA、RS与IPv4 ARP协议完全相同，没有任何安全保证。
- 攻击者
  - 与IPv4 ARP劫持效果相同
  - 伪造RA路由宣告消息
  - 地址冲突中断正常地址配置
  - 设置自己为高优先级默认路由
  - 成功劫持流量
- 工具：thc-ipv6/fake_router6

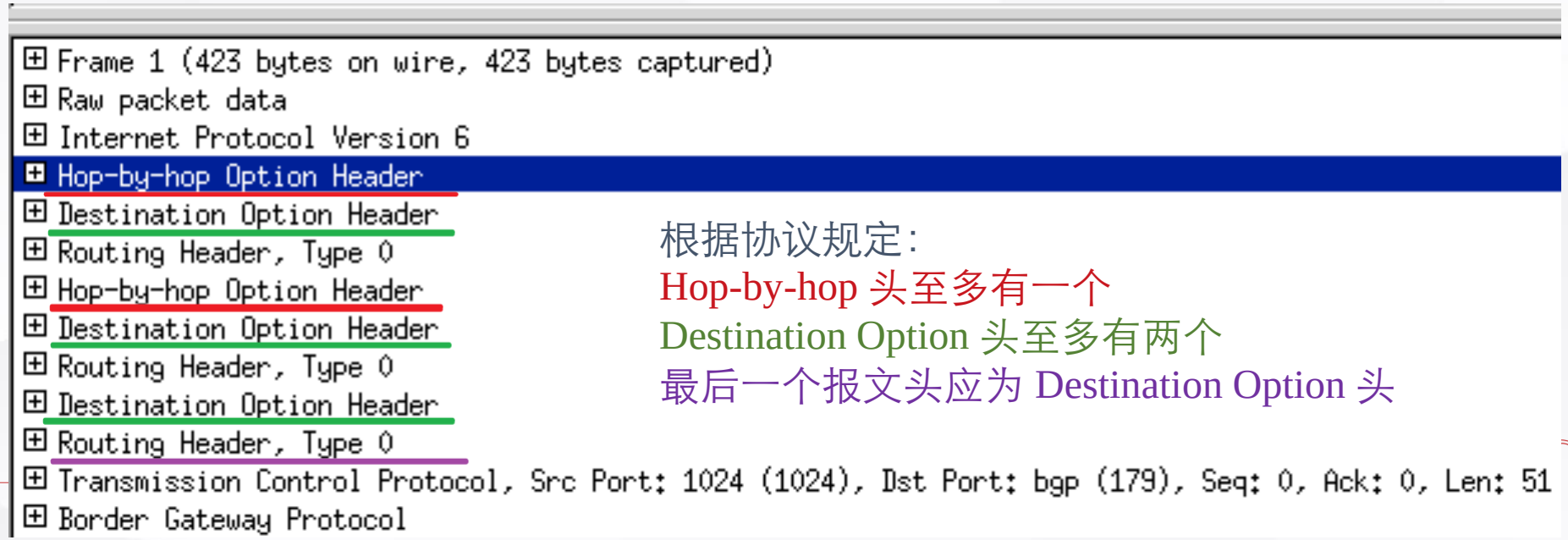


IPv4 & IPv6 共有安全问题 – 对抗方法

- 组播地址主机发现
  - 在互联边界的三层设备上阻止site-local地址组播包
- **RA伪造路由劫持**
  - 在交换机端口配置ACL或RA保护
  - 拒绝来自非信任端口的ICMPv6 RA路由宣告报文
- ND协议安全（主机伪造、DAD拒绝服务攻击）
  - Secure Neighbor Discovery（SEND）
  - 依赖PKI体系，部署困难，使用较少

IPv6 专有安全问题 – 灵活的报头

- **IPv6在协议层面允许任意大小与数量的报文头**
  - 大小上限与最大包大小相同
- **不健壮的协议栈实现存在风险**
  - 恶意构造的IPv6报文导致拒绝服务攻击
  - 对访问四层协议的内容需要首先解析所有的报头
  - 网络设备对报文处理相比IPv4占用更多资源



根据协议规定：
Hop-by-hop 头至多有一个
Destination Option 头至多有两个
最后一个报文头应为 Destination Option 头

DHCPv6 安全风险

- **与IPv4类似的，内网中也可以伪造DHCPv6服务器**
  - 达成流量劫持，DNS劫持等目的
  - 使用交换机端口ACL拒绝来自不信任端口的DHCPv6报文
- **DHCPv6不安全地址配置**
  - IPv6的关键安全改进之一，巨大地址空间使得互联网范围的扫描不可行。
  - DHCPv6有状态地址分配，如果图方便使用连续地址分配给主机，将严重破坏这一安全特性。
    - 2001:da8:yyyy::1
    - 2001:da8:yyyy::2
    - 2001:da8:yyyy::3

    DHCPv6**可能**分配的主机地址
    - ……
    - 2001:da8:zzzz::69ef:b922:182c:c30b

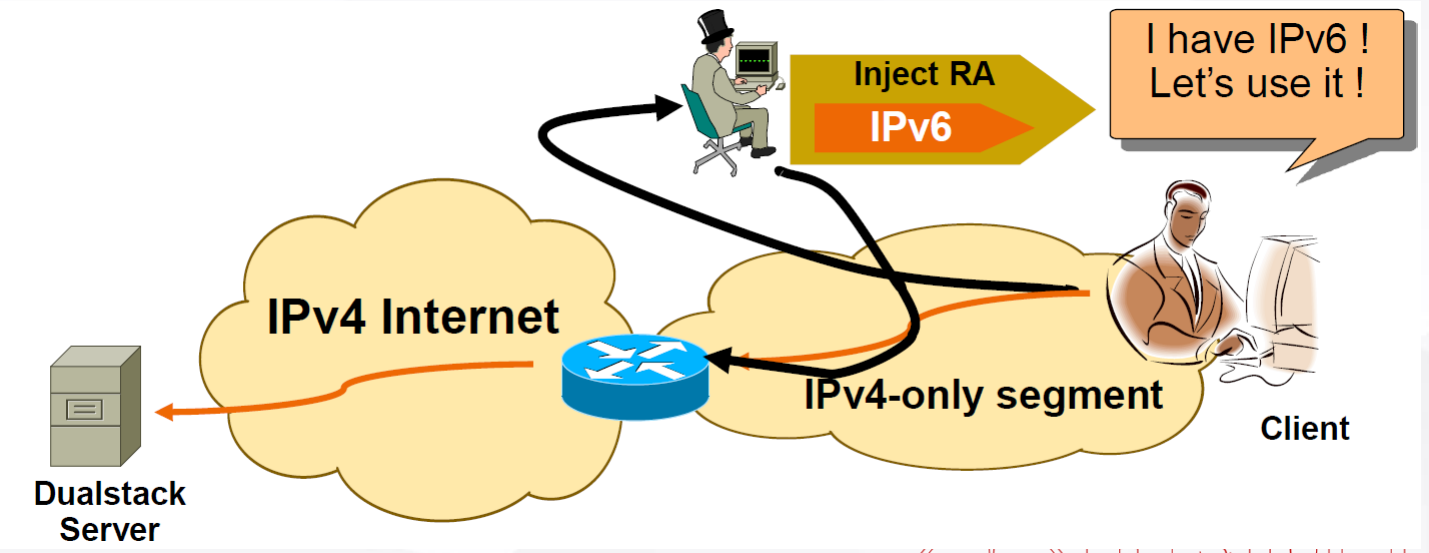
    SLAAC自动配置的主机地址

IPv4 Only 网络不会遇到 IPv6 安全问题?

- 终端设备
  - IPv4 网络受到保护
  - IPv6 操作系统默认启用
    - Windows、MacOS、Linux
    - iOS、Android
- 网络
  - 不提供原生 IPv6
- 认为
  - 只要保护IPv4，网络就是安全的

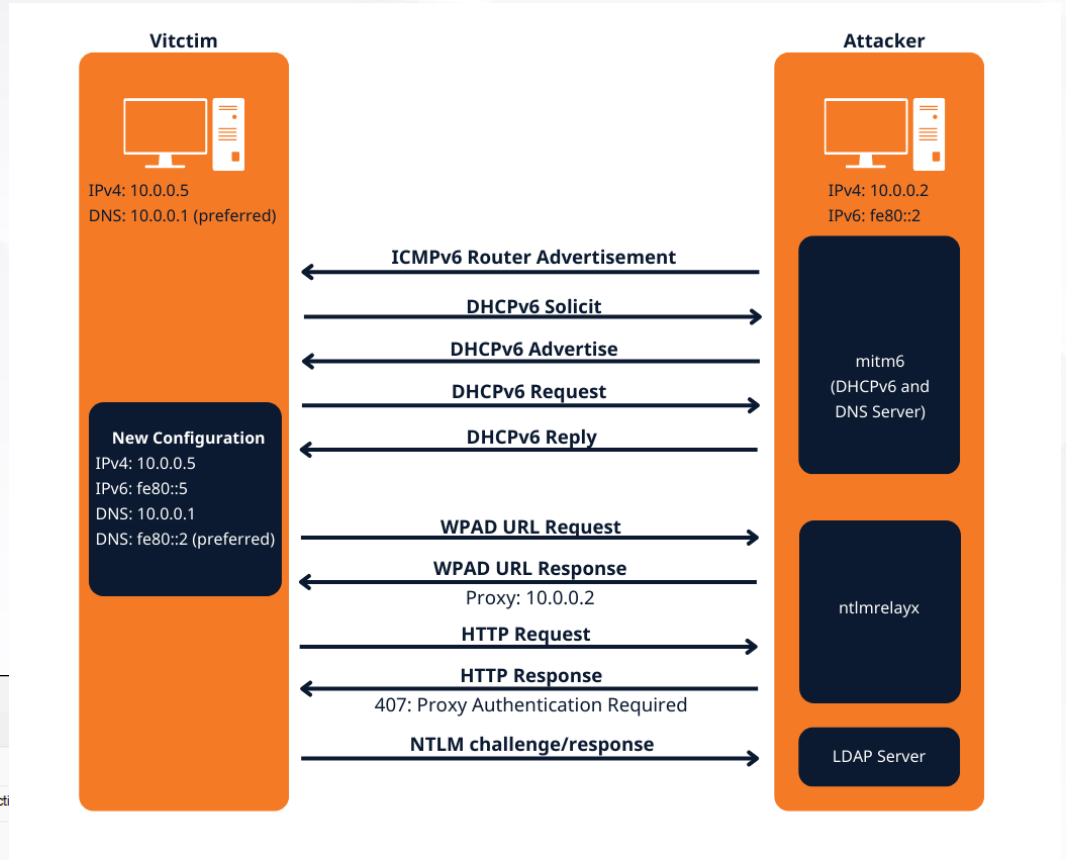
- 是时候考虑部署IPv6了！

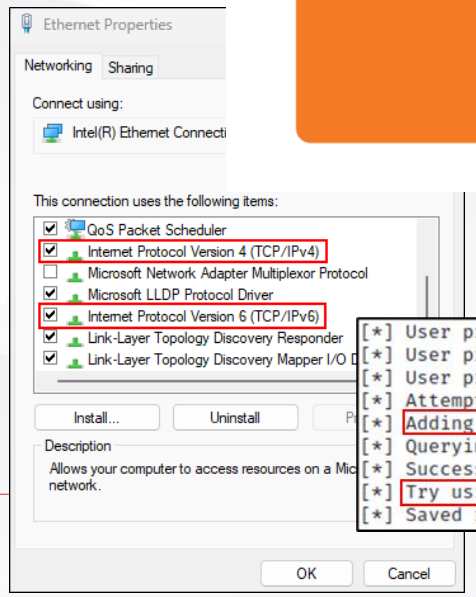
- 实际
  - 网络并不安全
  - 攻击者发送路由宣告RA
  - 终端设备自动配置IPv6
  - 设备优先选择IPv6
  - 暴露IPv6攻击面



案例 – IPv6 DNS Takeover 域渗透

- **攻击步骤**
  1. 攻击者伪造路由宣告RA
     - 发布DHCPv6配置信息
     - 发布IPv6 DNS配置信息
  2. 受害者主机
     - 默认启用IPv6，自动配置IPv6 DNS
  3. 受害者主机发送DNS查询
     - IPv6 DNS 优先
     - 查询域内WPAD解析信息
       - Windows自动发现代理
  4. 攻击者DNS应答WPAD DNS
  5. 受害者流量被劫持导致NTLMRelay攻击
  6. 域渗透成功

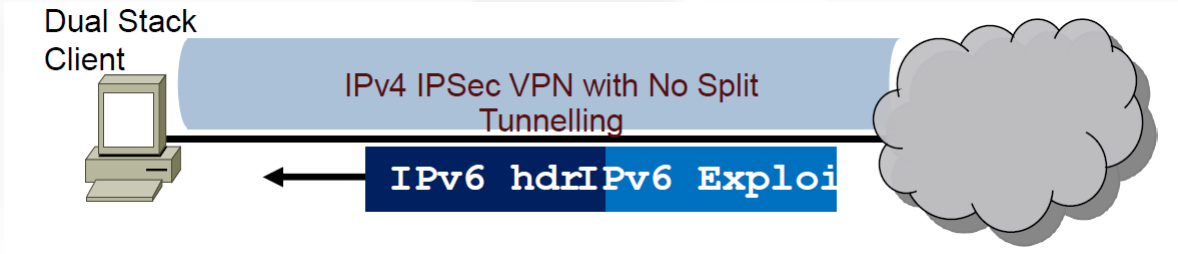





```
[*] User privileges found: Create user
[*] User privileges found: Adding user to a privileged group (Enterprise Admins)
[*] User privileges found: Modifying domain ACL
[*] Attempting to create user in: CN=Users,DC=adlab,DC=com
[*] Adding new user with username: NbuCuQKhZW and password: v(Zt<)J_Snii$uo result: OK
[*] Querying domain security descriptor
[*] Success! User NbuCuQKhZW now has Replication-Get-Changes-All privileges on the domain
[*] Try using DCSync with secretsdump.py and this user :)
[*] Saved restore state to aclpwn-20221221-101643.restore
```

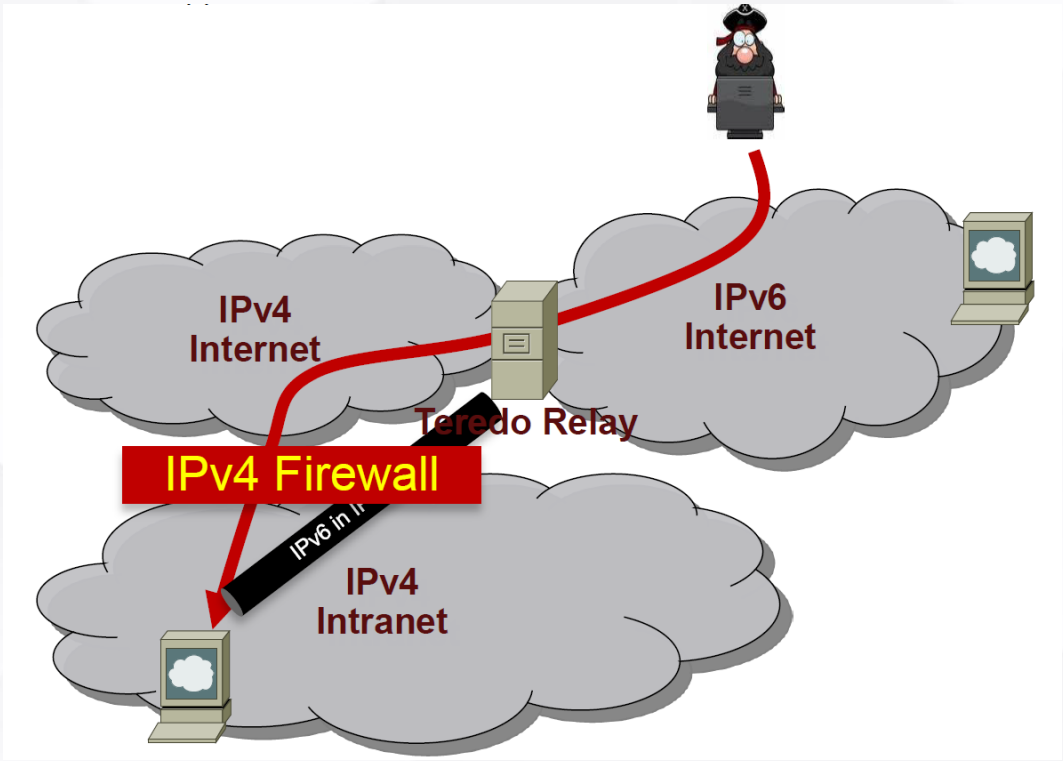
IPv4 & IPv6 演进 – 双栈安全风险

- 终端设备
  - 应用层服务同时暴露在IPv4与IPv6协议下
  - 木桶效应，最终的安全保护水平取决与双栈中最弱的一个
- 安全防护
  - 主机安全工具与网络访问控制工具需要同时检查双栈流量
  - 隧道工具需要考虑对另一栈的限制与保护，如工作VPN



IPv4 & IPv6 演进 – 隧道技术安全风险

- 通过IPv4与双栈网络服务器建立连接，通过远程的服务器处理IPv6流量收发，例如Teredo隧道。
- 出站保护绕过
  - IPv6流量从IPv4的隧道中通过
  - 绕过所有IPv4的审计设备
  - 绕过所有IPv4的防火墙安全规则
- 互联网入站
  - IPv6的网络特性，地址全球可达
  - 攻击者能够通过隧道内的IPv6链路直达内部主机
- 防护措施
  - 主机安全保护、部署原生IPv6网络



目 录

攻防演习中的突出问题

低级错误频发，安全管理能力不足

- 弱口令、通用口令、默认口令
- 历史老旧漏洞未修复，运维配置不当

供应链安全问题突出

- 数十家教育系统供应链厂商存在通用漏洞
- 易造成连片式安全事件
- 形成全国范围的影响

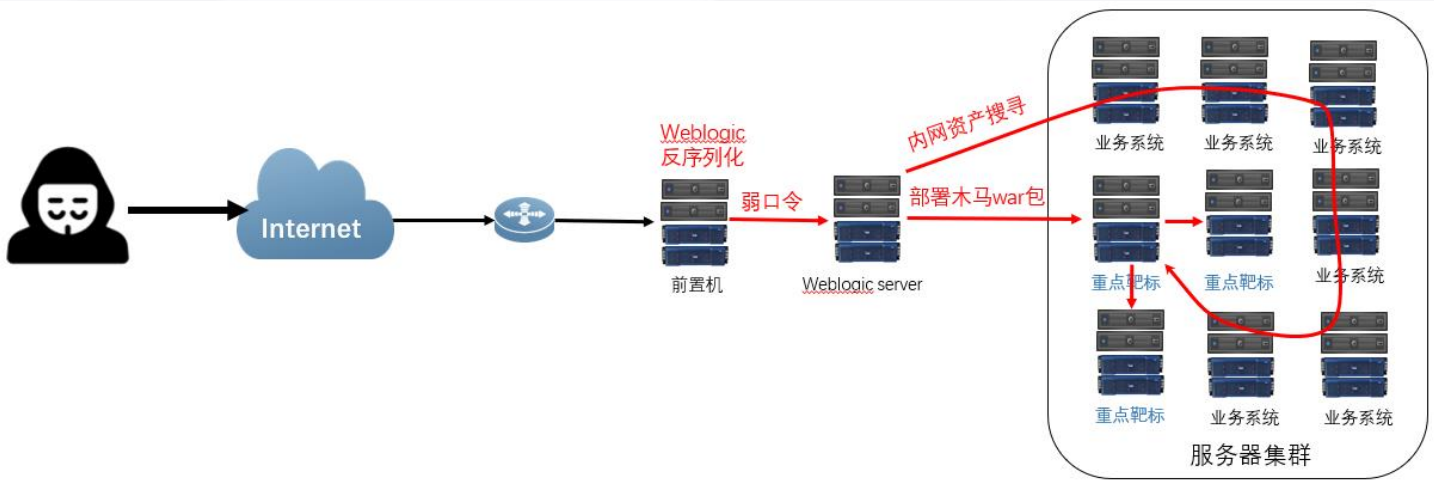
数据安全与内容安全防护措施缺乏

- 敏感个人信息未加密、脱敏
- 网页、视频内容篡改，造成违法不良信息传播

人员安全意识不到位

- 钓鱼邮件与社会工程学攻击频频得手
- 网络安全宣传欠缺

典型的攻防对抗场景



攻击成果

- 靶标系统权限：5个
- 数据库管理员权限：5个
- SMB文件共享服务权限：3个
- SSH登录凭证：8个
- 堡垒机1台，可管理数百台服务器

信息收集	确定突破口	获取权限	权限提升	横向漫游	达成目标
域名IP反查，发现源站地址；指纹匹配发现WebLogic组件；	WebLogic反序列化远程代码执行漏洞；	1.远程代码执行获取管理员口令；2.管理页面war包上传木马后门。	• MS7-010获取多个主机权限； • 弱口令获取多个数据库权限； • 内网SSH私钥泄露，直接访问多台服务器； • 弱口令登录堡垒机，接管数百台服务器； • 某靶标系统内网访问地址在浏览器中，存在Shrio反序列化漏洞，直接访问数据库获取百万数据； • 横向移动获取其余4个靶标内网访问地址，并获得访问权限		• 主机权限 • 特权设备权限 • 靶标系统权限 • 敏感数据

安全设备 – 网络层

- IPv6 环境下所有设备均可使用全球单播地址
  - 不需要使用NAT即可实现互通，缺少NAT设备形成的防护
- 网络层安全防护设备要求
  - 安全域划分与访问控制策略需要更加严格管理
  - 错误配置内网暴露，将会造成更大风险
  - 封禁IP的策略需要调整，封禁单个IP变为封禁前缀
- 在 IPv6 与 IPv4 混合网络中
  - 防火墙/安全网关等防护设备需要同时配置双栈策略保障安全性
  - 受到DDoS攻击时，易产生更大的连接数
  - IPv6报头解析对设备的性能要求更高

安全设备 – 网络层

- 校园网络出口存在 IPv4、IPv6 独立线路，可能出现
  - 安全设备部署不一致
  - 安全设备规则不同步
  - 人员配置疏忽，未配置IPv6相关策略
- IPv6 地址分配
  - SLAAC无状态无认证，与用户绑定的审计存在困难
  - 需要强审计的环境可以考虑使用 DHCPv6
    - 注意： Android 不支持有状态IPv6地址分配（DHCPv6）
    - DHCPv6分配的地址不应降低主机地址空间

安全设备 – 应用层

- 应用层安全防护设备（WAF、IPS）
  - 对设备提出更高的要求
  - 具有IPv6报文解析能力
  - 支持IPv6地址格式的配置（如黑白名单等）
- 网络扫描类设备要求
  - 开展漏洞扫描的策略需要调整
  - 主动扫描IP段不再可行
  - 可以通过流量发现活跃IPv6地址进行扫描
- 目前关于 IPv6 的安全威胁情报信息（IoC）相对缺乏

IPv6 业务安全 – 反代内容安全风险

- IPv4与IPv6过渡期间，为支持IPv6，反向代理被广泛使用。

  如反向代理存在错误配置，未对访问内容进行限制，则存在被黑产利用的风险。

IPv6 安全教育

- **IPv6 环境下网络安全专业人员正面临严峻挑战**
  - IPv6 环境下引入扩展头攻击、NDP 攻击等安全新威胁
  - 安全专业人员的IPv6 知识储备不足
    - 无法充分认识和理解IPv6 安全问题
    - 无法有效应对IPv6 安全防护需求等
- **运维人员缺乏IPv6 安全相关知识和经验**
  - 运维人员未能第一时间接触IPv6 业务运营、维护等实际业务环境
  - 现有IPv4安全知识和经验难以直接应用到IPv6 环境中
  - IPv6 相关业务的运维工作存在安全隐患
  - 不设防的IPv6 应用成为攻击者实施网络攻击的新突破口
- **IPv6 安全培训应成为提升安全防护不可或缺的内容**

最后的话

- 网络安全，因为无知，所以恐惧
- 攻防对抗中，早走别人的路，让别人无路可走
- 学习IPv6，未雨绸缪，早做准备，迎接新挑战

上海交通大學

SHANGHAI JIAO TONG UNIVERSITY

谢 谢!