网络安全

海南大学网络空间安全学院

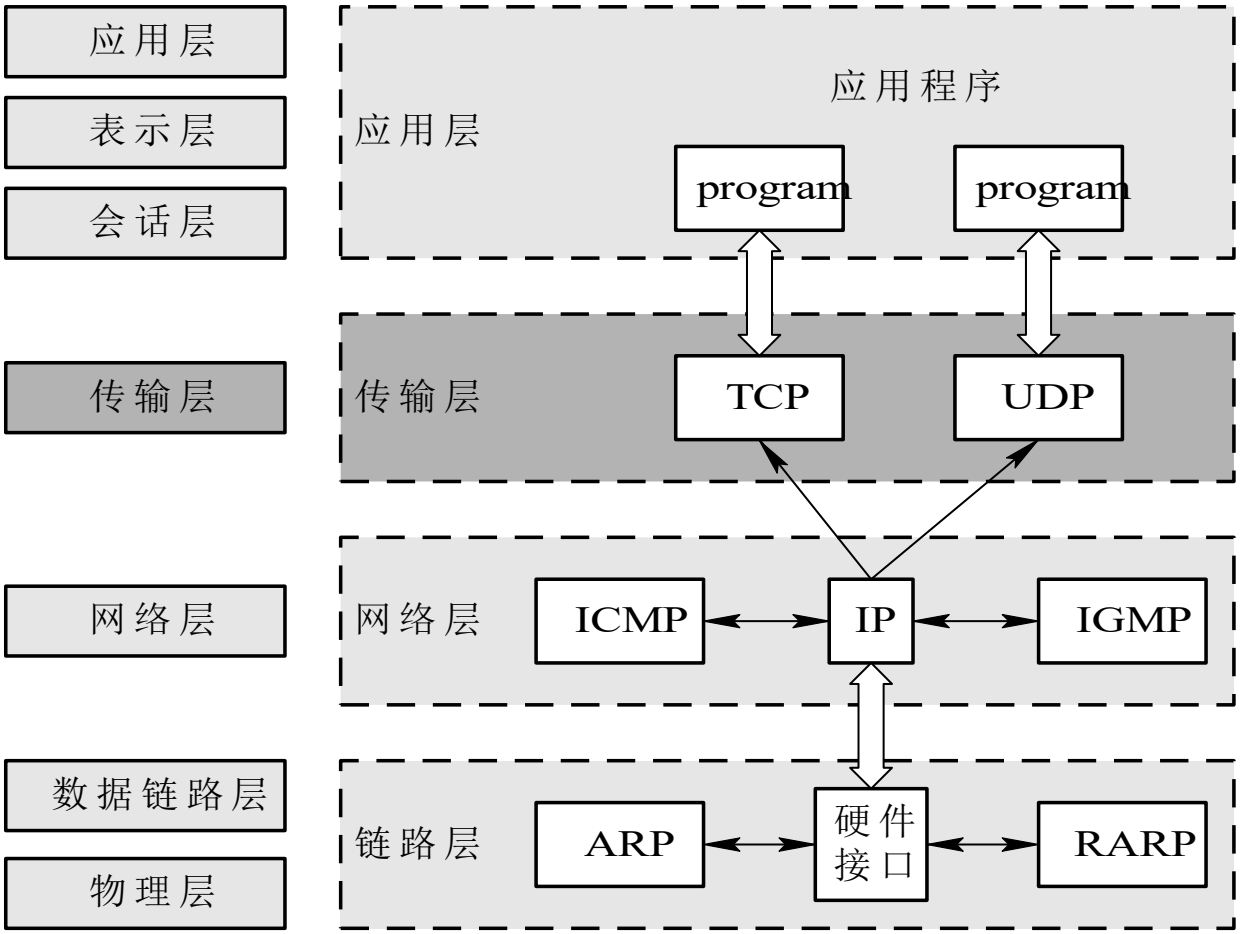
第五章 TCP-IP体系的协议安全

1. 概述
2. 物理层安全
3. 数据链路层安全
4. 网络层安全
5. 传输层安全

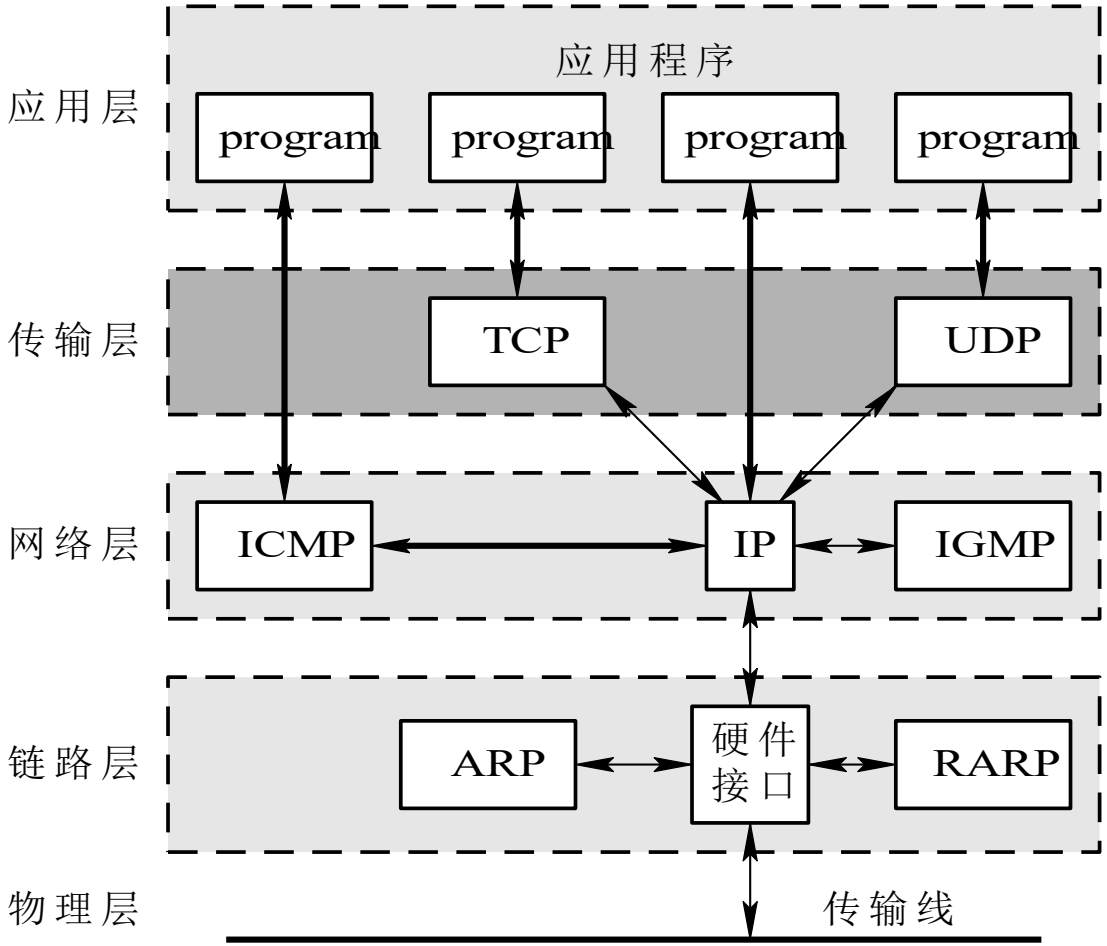
1.1 两种网络结构参考模型

- ISO/OSI 参考模型将网络设计划分为 7 个功能层，每层完成特定的功能。该模型只起到一个指导作用，并未被采纳为商业规范。
- TCP/IP 网络体系结构是许多支持 ISO/OSI 分层模型的协议栈的一种。TCP/IP 通常被认为是一个 4 层协议系统。

1.2 两种网络体系层次结构



1.3 广泛建议的参考模型



1.4 网络协议的安全风险

- 网络协议（Protocol）是为进行网络通信和数据交换而建立的规则、标准和约定的集合。
- 网络协议在其设计之初，主要注重解决不同结构网络的互联互通问题，而忽略了其安全性问题。
- 网络协议的安全风险主要包括：
  - 自身存在设计缺陷
  - 缺少有效认证机制
  - 没有保密传输机制

1.5 网络协议的安全缺陷

TCP/IP 协议栈层次	网络协议	存在安全缺陷	对应攻击技术	破坏安全属性
网络接口层	以太网协议	共享传输媒介并明文传输	网络嗅探与协议分析	机密性
	以太网协议	缺乏MAC身份认证机制	MAC欺骗攻击	真实性
	PPP协议	明文传输	网络嗅探与协议分析	机密性
互联层	IPv4	缺乏IP地址身份认证机制	IP地址欺骗	真实性
		处理IP分片时的逻辑错误	IP分片攻击	可用性
	ICMP	ICMP路由重定向缺乏身份认证	ICMP路由重定向	完整性, 真实性
		广播地址对Ping的放大器效应	Ping Flood, Smurf	可用性
	ARP	采用广播问询且无验证机制	ARP欺骗	真实性
	BGP等	缺乏较强的身份认证机制	路由欺骗攻击	完整性, 真实性
传输层	TCP	TCP三次握手存在连接队列瓶颈	TCP SYN Flood	可用性
		TCP会话对身份认证不够安全	TCP RST攻击	真实性, 可用性
		TCP会话对身份认证不够安全	TCP会话劫持	真实性, 可用性
	UDP	N/A	UDP Flood	可用性
应用层	DNS	DNS验证机制不够安全	DNS欺骗	完整性, 真实性
	SMB	SMB协议的NTLM认证机制存在安全缺陷	SMB中间人攻击	真实性, 可用性
	HTTP	URL明文, 缺乏完整性保护, 编码滥用等	钓鱼	完整性, 真实性
		内嵌链接滥用	网页木马攻击	完整性

第五章 TCP-IP体系的协议安全

1. 概述
2. 物理层安全
3. 数据链路层安全
4. 网络层安全
5. 传输层安全

2 物理层安全

- 物理层的作用是屏蔽掉计算机网络中硬件设备和通信手段的不同，在传输媒体上传输数据比特流，而不必考虑具体的传输媒体是什么。
- 物理层安全是指保护网络设备、设施等媒体以及媒体上的数据免受自然灾害和人为失误、和犯罪行为破坏的措施及过程。物理层安全是整个网络系统安全的重要基础和保障。

2.1 物理层安全威胁及防范

- 自然灾害
  - 水灾、火灾、损耗
  - 防火、防水、灾备
- 人为失误
  - 运行故障、管理疏漏
  - 提高安全知识和安全意识
- 犯罪行为
  - 偷窃、破坏电缆、电磁干扰、电磁泄露、搭线监听
  - 防盗、环境安全、电磁屏蔽、数据加密、流量填充

2.2 物理隔离技术

- 物理隔离的安全要求
  - 隔断内外网络传导
  - 隔断内外网络辐射
  - 隔断不同存储环境
- 物理隔离的技术手段
  - 物理隔离
  - 协议隔离
  - 网闸隔离

第五章 TCP-IP体系的协议安全

1. 概述
2. 物理层安全
3. 数据链路层安全
4. 网络层安全
5. 传输层安全

3 数据链路层安全

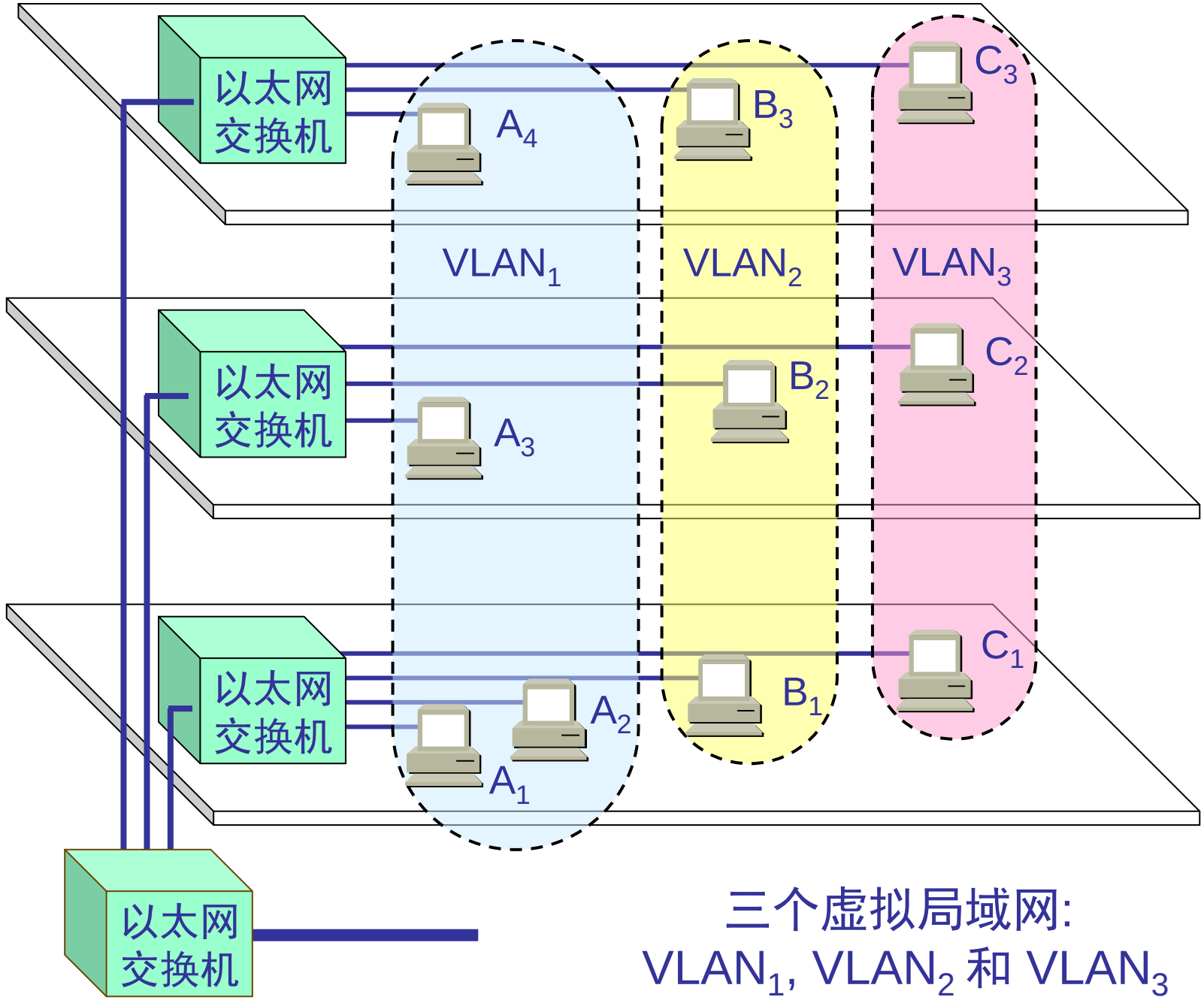
- 数据链路层也称作网络接口层，通常包括操作系统中的设备驱动程序和计算机中对应的网络接口卡。它们一起处理与传输媒介的物理接口细节，以及数据帧的组装。
- 数据链路层的安全威胁主要包括：
  - 网络嗅探
  - 负载攻击
  - MAC 欺骗
  - ARP 欺骗

3.1 网络嗅探与防范

- 将网络适配器设置为混杂模式，可以获取局域网内所有流量。
- 针对明文消息的数据监听
  - 数据加密。
- 针对密文消息的流量分析
  - 流量填充。

3.2 负载攻击与防范

- 负载攻击是指发送大量的广播包（如ARP广播），局域网内所有主机必须接收并处理，致使网络上的设备速度与真实流量降低，甚至造成网络瘫痪。
- 常用防范措施是使用 VLAN 细分网络拓扑。



三个虚拟局域网:
$VLAN_1$, $VLAN_2$ 和 $VLAN_3$

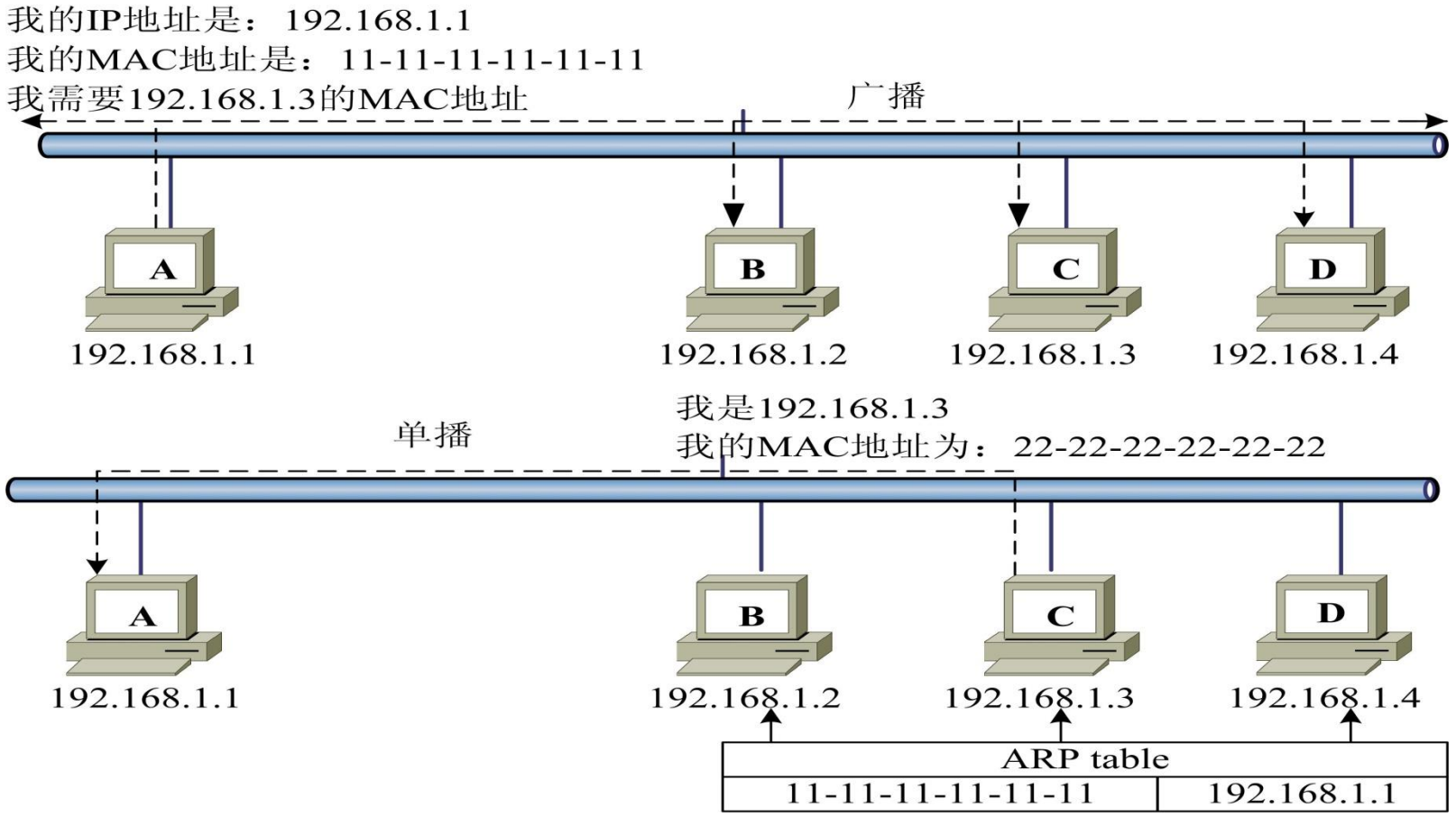
3.3 MAC 欺骗与防范

- 通过软件或编写批处理文件修改 MAC 地址，并在系统启动时写入硬件控制系统。
- 欺骗交换机
  - 故障：交换向接收报文接口以外的所有接口转发帧
  - 防范：转发接口与硬件地址的静态绑定
- 主机 MAC 地址冲突
  - 故障：网络没法区分设备，导致报文混乱、网络异常
  - 防范：修改MAC 地址

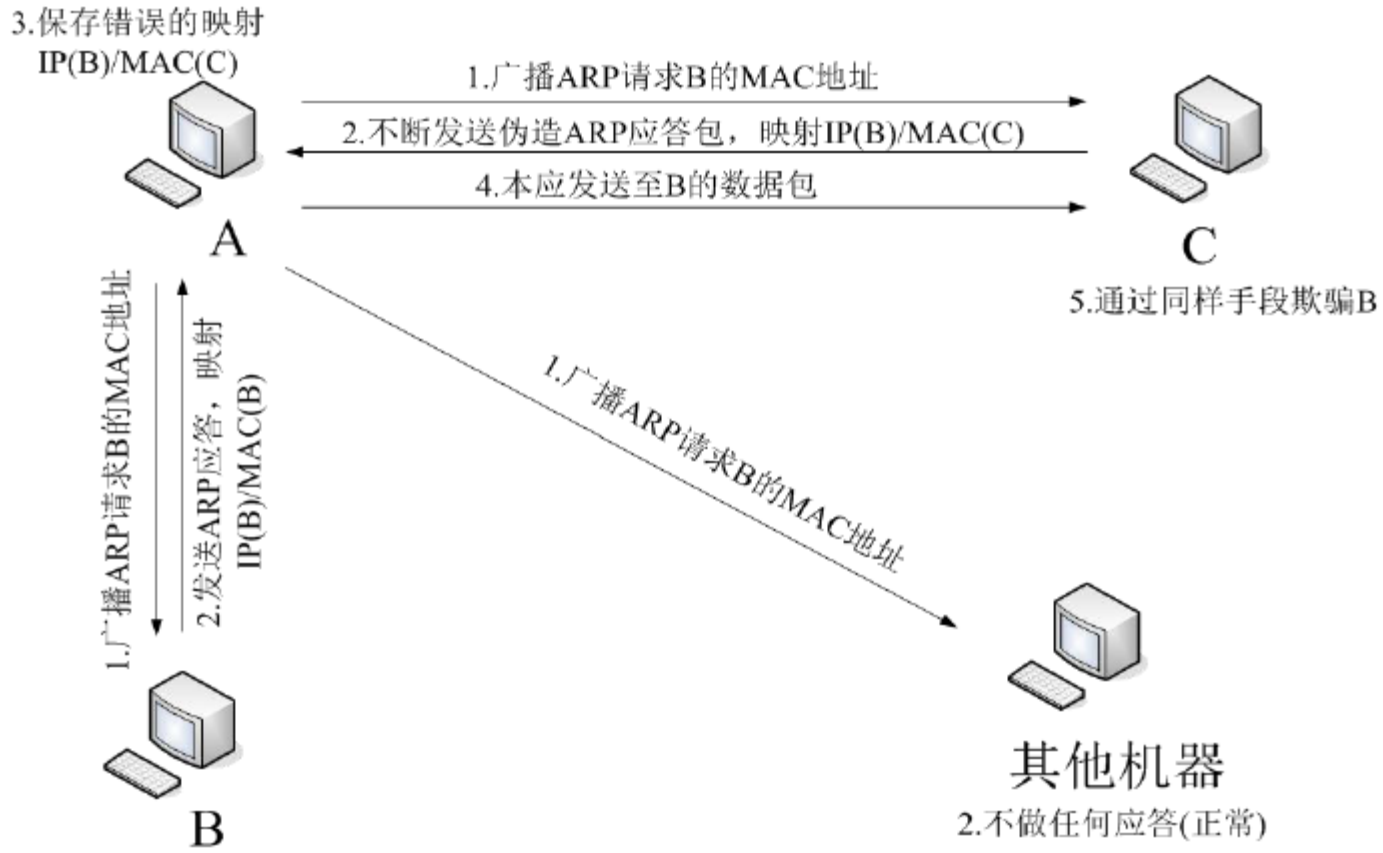
3.4 ARP 欺骗

- ARP 协议用于将网段内主机的 IP 地址解析成其 MAC 地址。
- ARP 欺骗是指通过构造虚假的 ARP 消息，向受害主机通告冒用 IP 地址与自身 MAC 地址的映射关系，从而达到假冒欺骗的恶意目的。

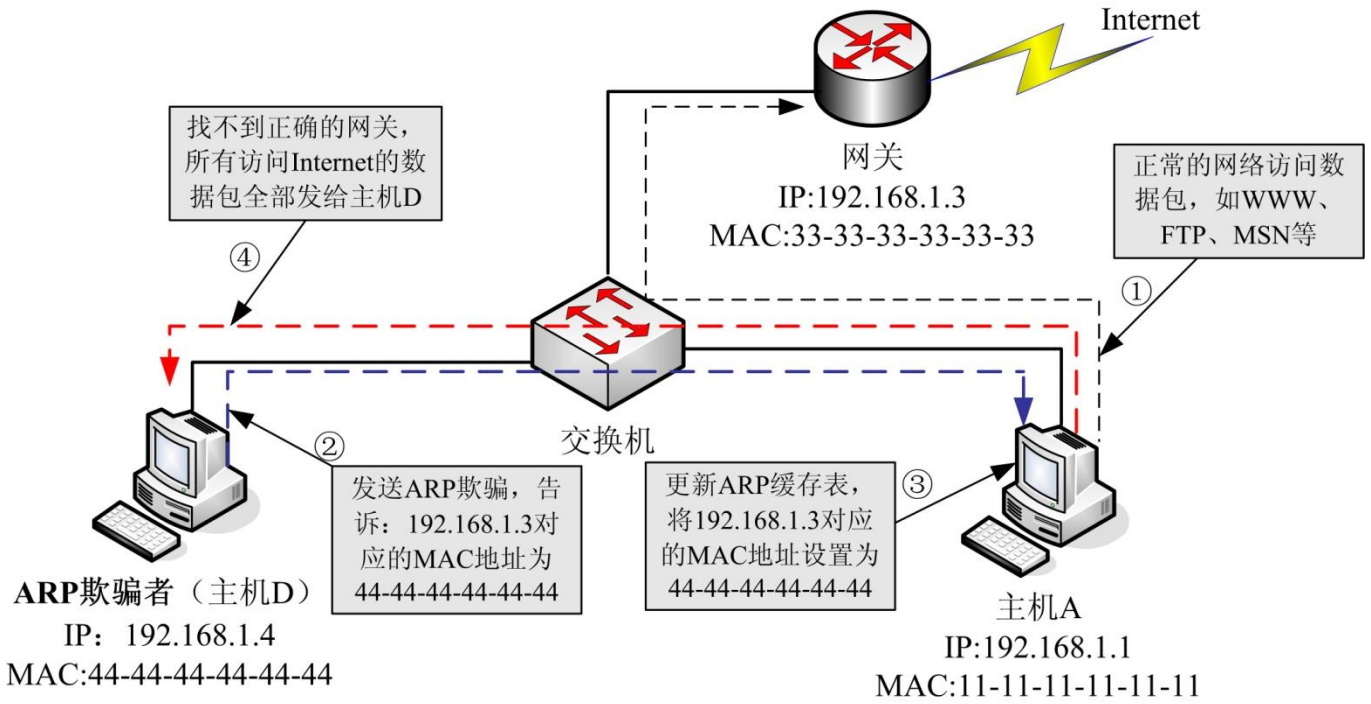
3.4.1 ARP 协议工作原理



3.4.2 假冒主机的 ARP 欺骗



3.4.3 假冒网关的 ARP 欺骗



注：①正常访问；②进行ARP欺骗；③被欺骗主机更新自己的ARP缓存表；④被欺骗主机无法正常访问Internet

3.4.4 ARP 欺骗的特点

- 可主动发送 ARP 请求。
- 接收主机对 ARP 请求不做真实性验证。
- 针对同一 IP 地址，新的映射覆盖旧的映射。
- 欺骗对象可以是特定主机或内网中全部节点。
- ARP 缓存为可能的虚假映射提供保活时间。
- ARP 欺骗需要周期性重复。
- 攻击主机必须与受害主机在同一网络。

3.4.5 ARP 欺骗的防范

- 静态绑定关键主机的映射关系。
- 使用 VLAN 以缩小范围。
- 加密数据以降低损失。

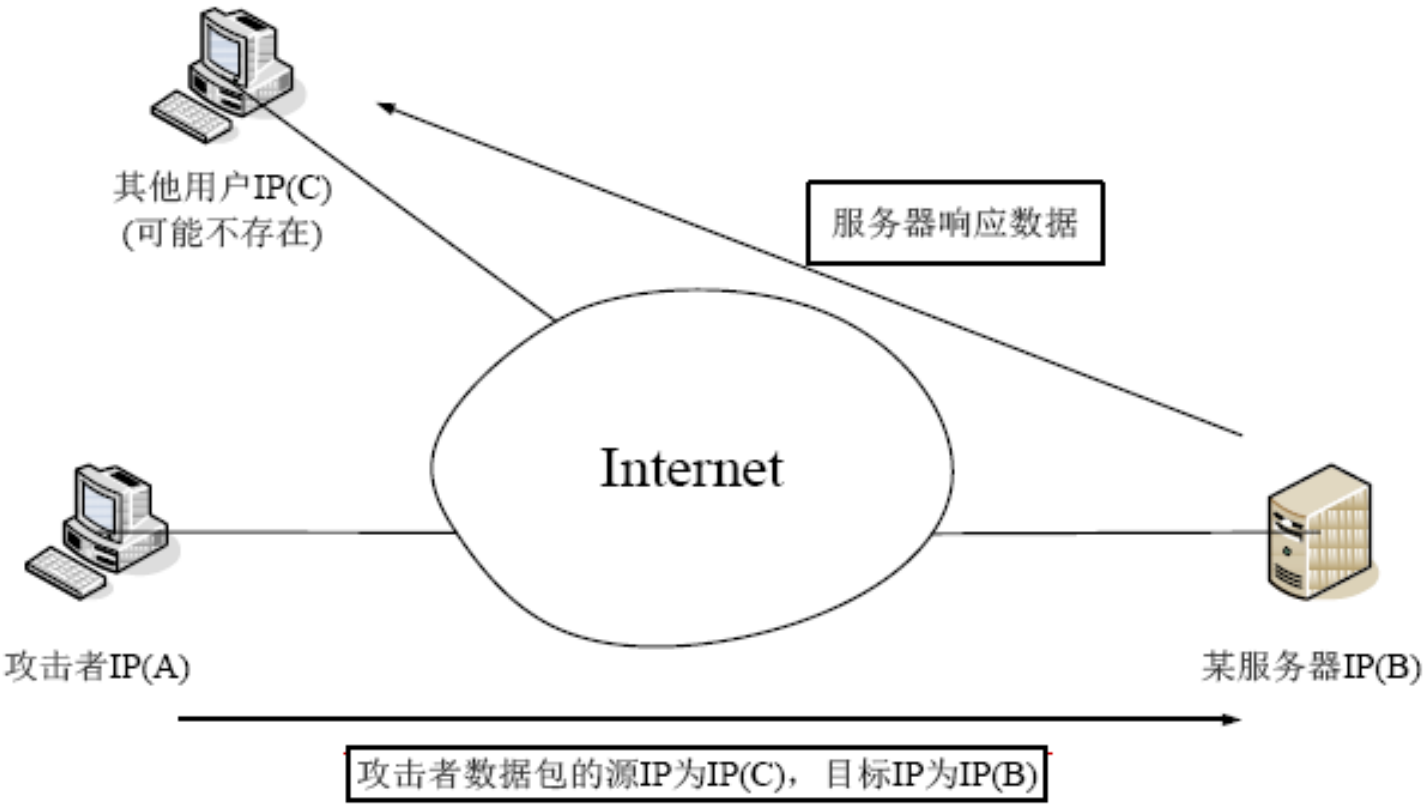
第五章 TCP-IP体系的协议安全

1. 概述
2. 物理层安全
3. 数据链路层安全
4. 网络层安全
5. 传输层安全

4 网络层安全

- 网络层提供无连接的、尽最大努力交付的数据报服务，即所传送的分组可能出错、丢失、重复和失序，也不保证分组传送的时限。
- 网络层的安全威胁主要包括：
  - IP 源地址欺骗
  - IP 源路径选项欺骗
  - IP 分片攻击
    - ✓ Ping of Death
    - ✓ Jolt2
    - ✓ TearDrop
  - ICMP 路由重定向攻击
  - Smurf 攻击

4.1.1 IP 源地址欺骗

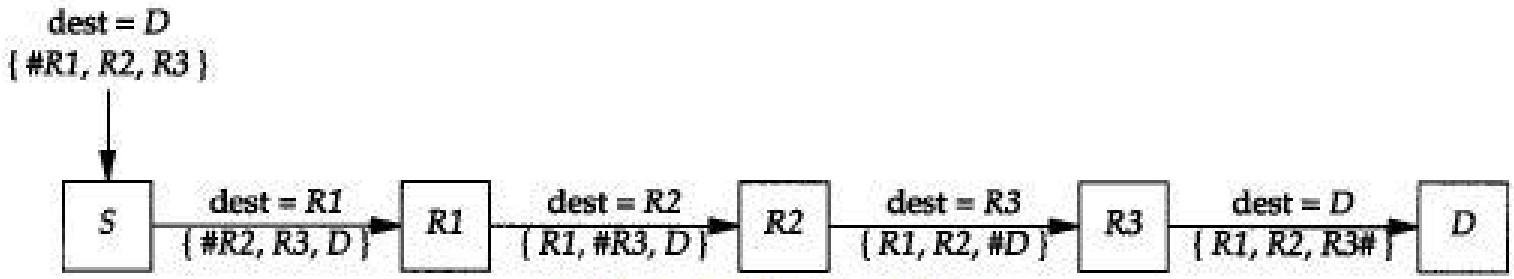

其他用户IP(C)
(可能不存在)
服务器响应数据
Internet
攻击者IP(A)
某服务器IP(B)
攻击者数据包的源IP为IP(C)，目标IP为IP(B)

4.1.2 IP 源地址欺骗与防范

- 伪造具有虚假源地址的 IP 数据包进行发送，以隐藏攻击者身份或假冒其他计算机。
- 路由转发只关注目标 IP，不对源 IP 做验证。
- 响应数据发往伪造 IP 地址，远程攻击主机通常无法获得响应包。
- 防范：
  - 不使用 IP 地址作为身份标识
  - 利用上层协议实现身份验证

4.2.1 IP 源路径选项

- IP 源路径选项允许 IP 数据报自已指定一条通往目的主机的传输路径。



4.2.2 IP 源路径选项欺骗与防范

- 攻击主机在请求报文中设置 IP 源路径选项，使得报文的其中一个目的地址指向防火墙，而最终地址是目标主机。当报文到达防火墙被允许接收，防火墙作为报文目的站处理该报文，并根据源路径域，转发给内网上的目标主机。
- 攻击主机使用目标主机地址发送源路径报文给防火墙，防火墙响应报文并根据逆向路径发回给内网目标主机。
- 防范：
  - 防火墙（路由器）禁止源路径选项。
  - 防火墙禁止来自外部的内部主机报文。

4.3 IP 分片攻击与防范

- 利用错误的 IP 分片进行攻击，达到受害主机因不能重组分片导致瘫痪的效果。
- 关注字段：
  - 首部长度
  - 总长度
  - 标识
  - 标志
  - 片偏移
- 攻击形式：
  - Ping of Death
  - Jolt2
  - TearDrop

4.3.1 Ping of Death 攻击与防范

- 利用 ICMP 协议发送一个长度超过 65535 字节的 Echo Request 数据包，目标主机在重组分片时会造成缓冲区溢出，导致系统崩溃。
  - Linux：65507；Windows：65500。
  - # ping -l 65535 192.168.0.1
    - ✓ Error：packet size 65535 is too large.
    - ✓ Maximum is 65507.
- 防范：
  - 操作系统禁止发送超长 ping 包。

4.3.2 Jolt2 攻击与防范

- 发送一个 偏移量 + 数据长度 > 65535 字节 的 ICMP 包，目标主机在接收分片时会造成缓冲区溢出，导致系统崩溃。
  - 192.168.0.1 -> 192.168.0.2 ICMP
  - IpLen:20 MF:0 DgmLen:29
  - ID:1109 Flag Offset: 0x1FFE
- 防范：
  - 利用算法安全的路由器先重组再转发，对不符合规则的数据包直接丢弃。

4.3.3 TearDrop 攻击与防范

- 构造 UDP 包，并进行错误分片。使第二分片的偏移量小于第一分片结束的位移，且加上第二分片载荷长度，仍未超过第一分片的尾部。
- 满足条件：
  - K < N 且 K + S < N
- 利用 UDP 包重组时重叠偏移的漏洞对系统主机发动拒绝服务攻击，因主机内核无法处理重叠偏移问题而最终导致主机宕机。
- 防范：
  - 及时为操作系统安装补丁

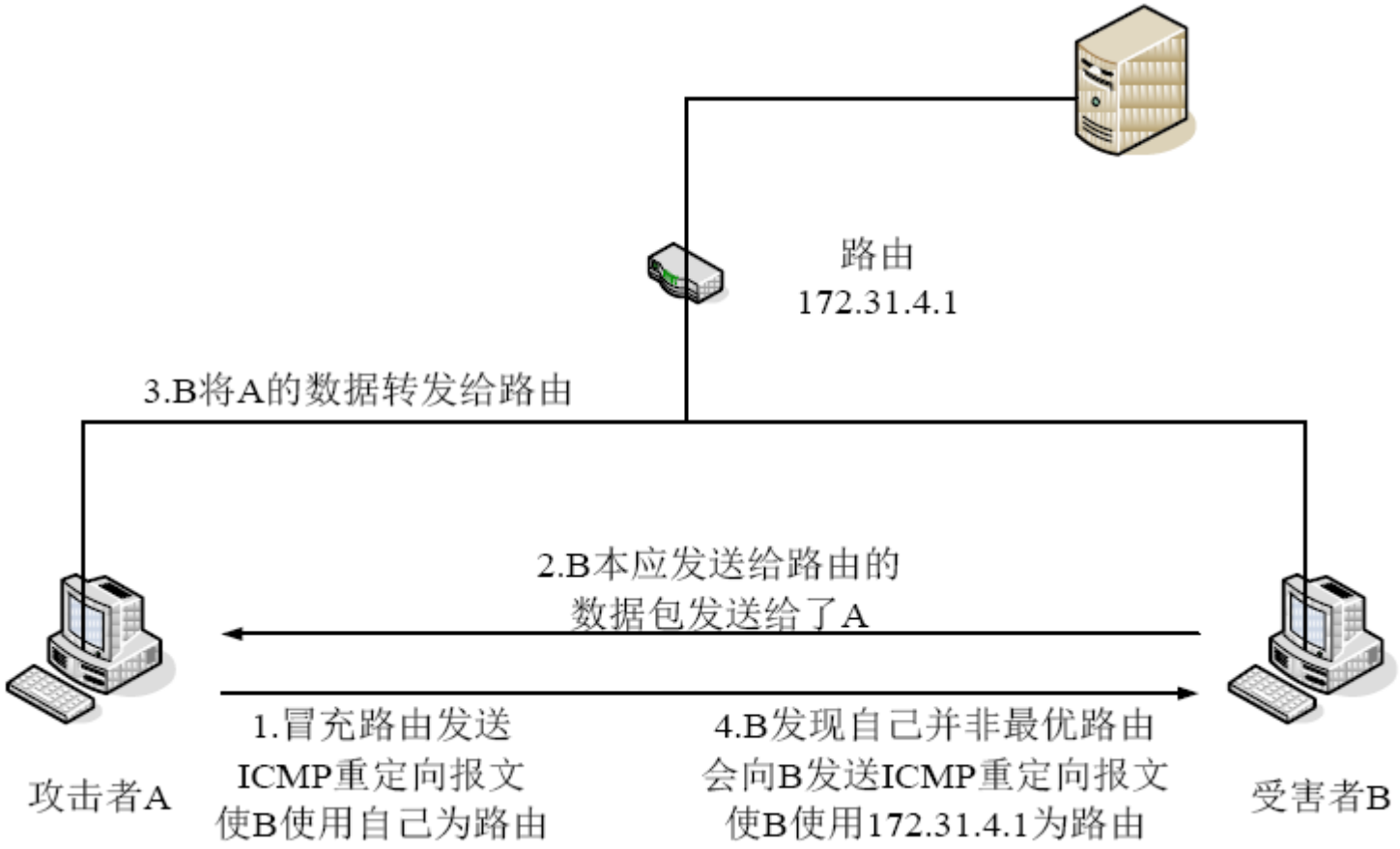
4.4 ICMP 协议

- 为了提高 IP 数据报交付成功的机会，在网际层使用了网际控制报文协议 （ICMP）。
- ICMP 报文作为 IP 层数据报的数据，加上数据报的首部，组成 IP 数据报发送出去。
- ICMP报文有两种
  - 差错报告报文 —— 改变路由（重定向）等
  - 询问报文 —— 回显请求和回答报文等

4.4.1 ICMP 路由重定向

- 默认网关可以通过 ICMP 重定向功能向报文发送者报告另一条到达特定主机的更短路由。除了路由器，主机必须服从 ICMP 重定向。

4.4.2 ICMP 路由重定向攻击

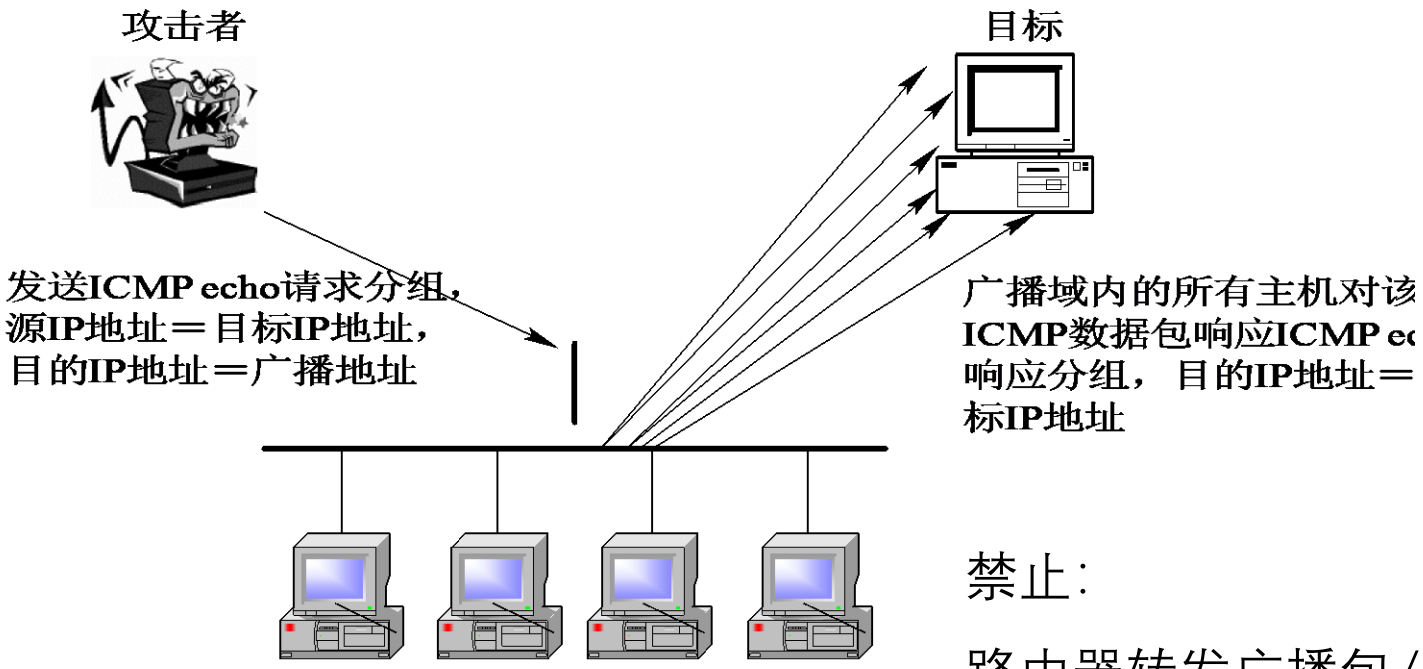


4.4.3 路由重定向攻击与防范

1. 攻击主机冒充网关 IP，向目标主机发送路由重定向报文，并将自身 IP 指定为新路由器。
2. 目标主机接受伪造的路由重定向报文，选择攻击主机作为其新路由器（即网关）。
3. 攻击主机开启路由转发功能，实施中间人攻击。
4. 转发过程中，攻击主机会发现更优路径，并通知目标主机，使路由恢复正常状态。

- 防范：
  - 检查重定向报文是否来自默认网关。

4.5 Smurf 攻击与防范



禁止：

路由器转发广播包/

特定类型ICMP包/

特定类型ICMP广播包

第五章 TCP-IP体系的协议安全

1. 概述
2. 物理层安全
3. 数据链路层安全
4. 网络层安全
5. 传输层安全

5 运输层

- 从通信和信息处理的角度看，运输层向上为应用层提供通信服务，它属于面向通信部分的最高层，同时也是用户功能中的最低层。
- 当网络的边缘部分中的两个主机使用网络核心部分的功能进行端到端的通信时，只有位于网络边缘部分主机的协议栈才有运输层，而网络核心部分的路由器在转发分组时只用到下三层的功能。
- 传输层提供了两种服务类型：TCP 和 UDP。

5.1.1 TCP 协议

- 是面向连接的运输层协议。
- 连接只能有两个端点，是点对点连接。
- 提供可靠交付的服务。
- 提供全双工通信。
- 面向字节流。

5.1.2 UDP 协议

- 无连接，即发送数据之前不需要建立连接。
- 尽最大努力交付，即不保证可靠交付。
- 是面向报文的，即没有拥塞控制。
- 支持一（多）对一（多） 的交互通信。
- 首部开销小，只有 8 个字节。

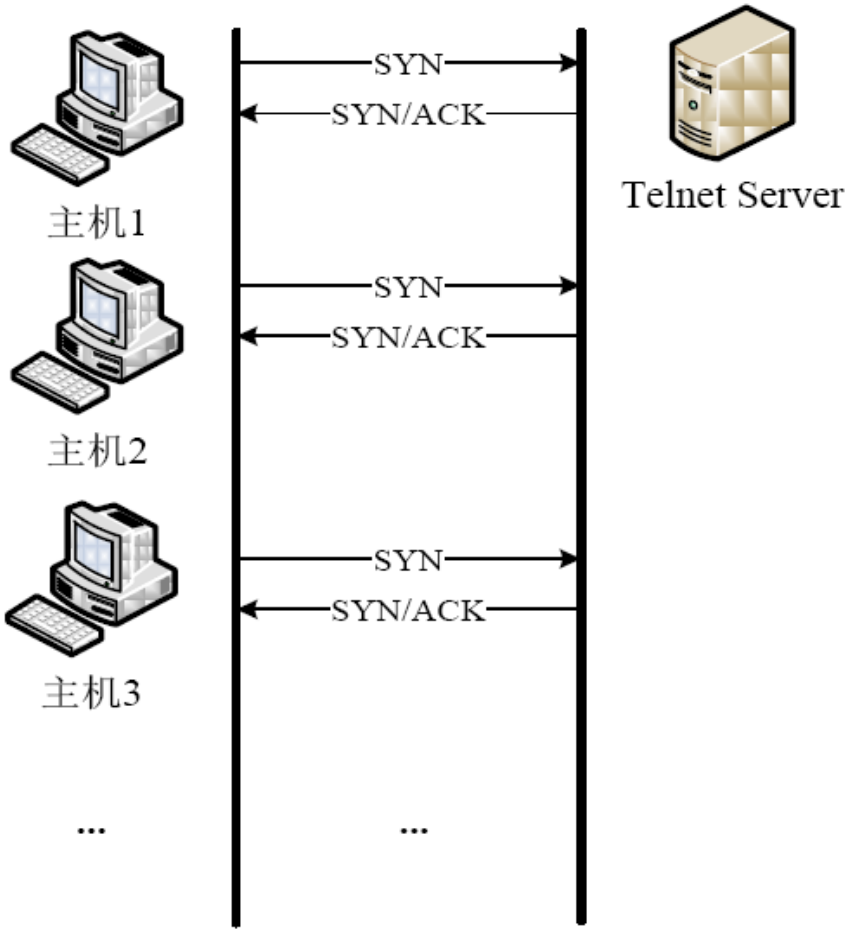
5.1.3 运输层威胁

- UDP Flood
- TCP SYN Flood
- TCP Land
- TCP 盲攻击
- TCP RST
- TCP 会话劫持

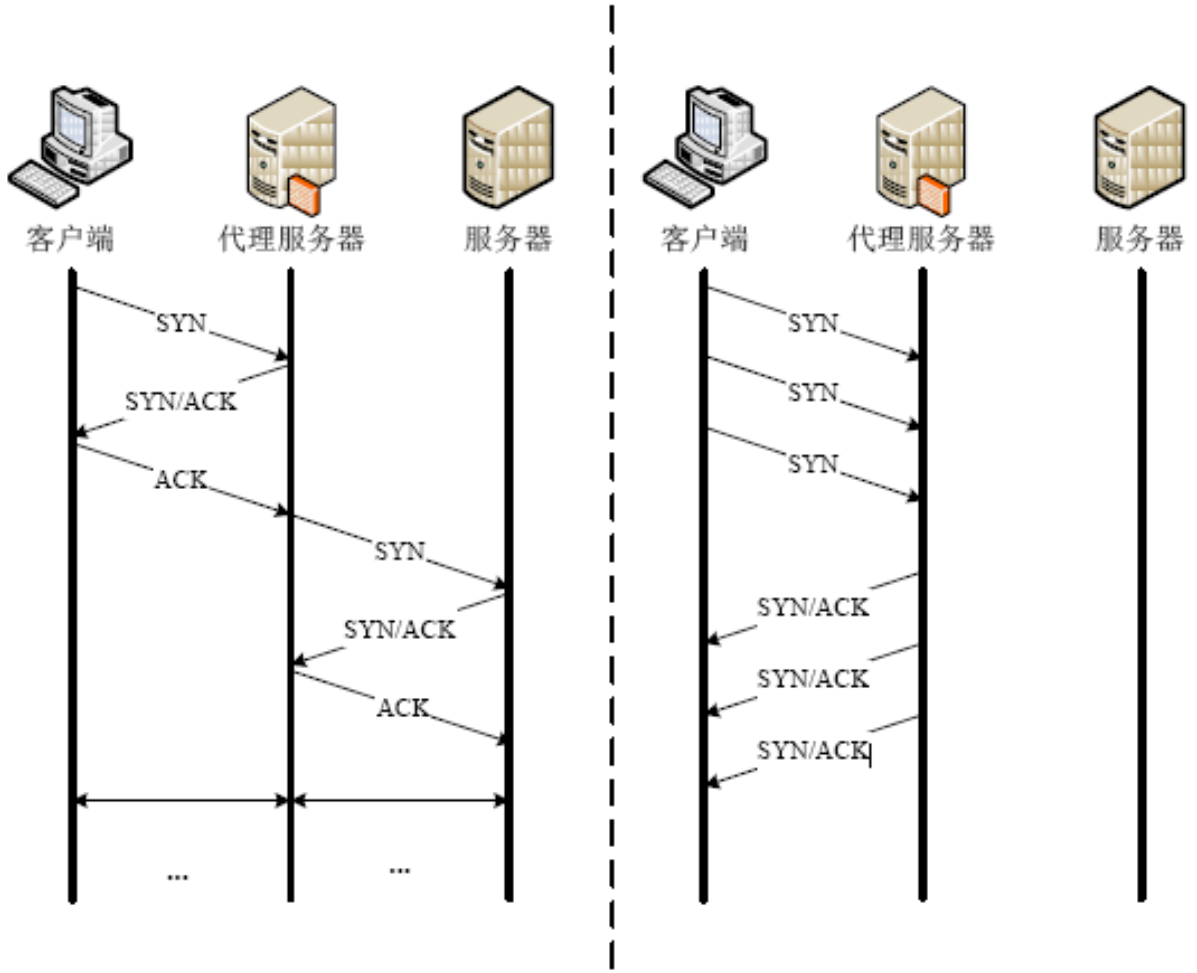
5.2.1 TCP SYN Flood

- 利用 TCP 三次握手协议的缺陷，发送大量伪造源 IP 的 SYN 连接请求，而不对服务器的请求响应做确认，最终耗尽目标主机的连接队列资源，使其不能够为正常用户提供服务。

5.2.2 TCP SYN Flood 图示



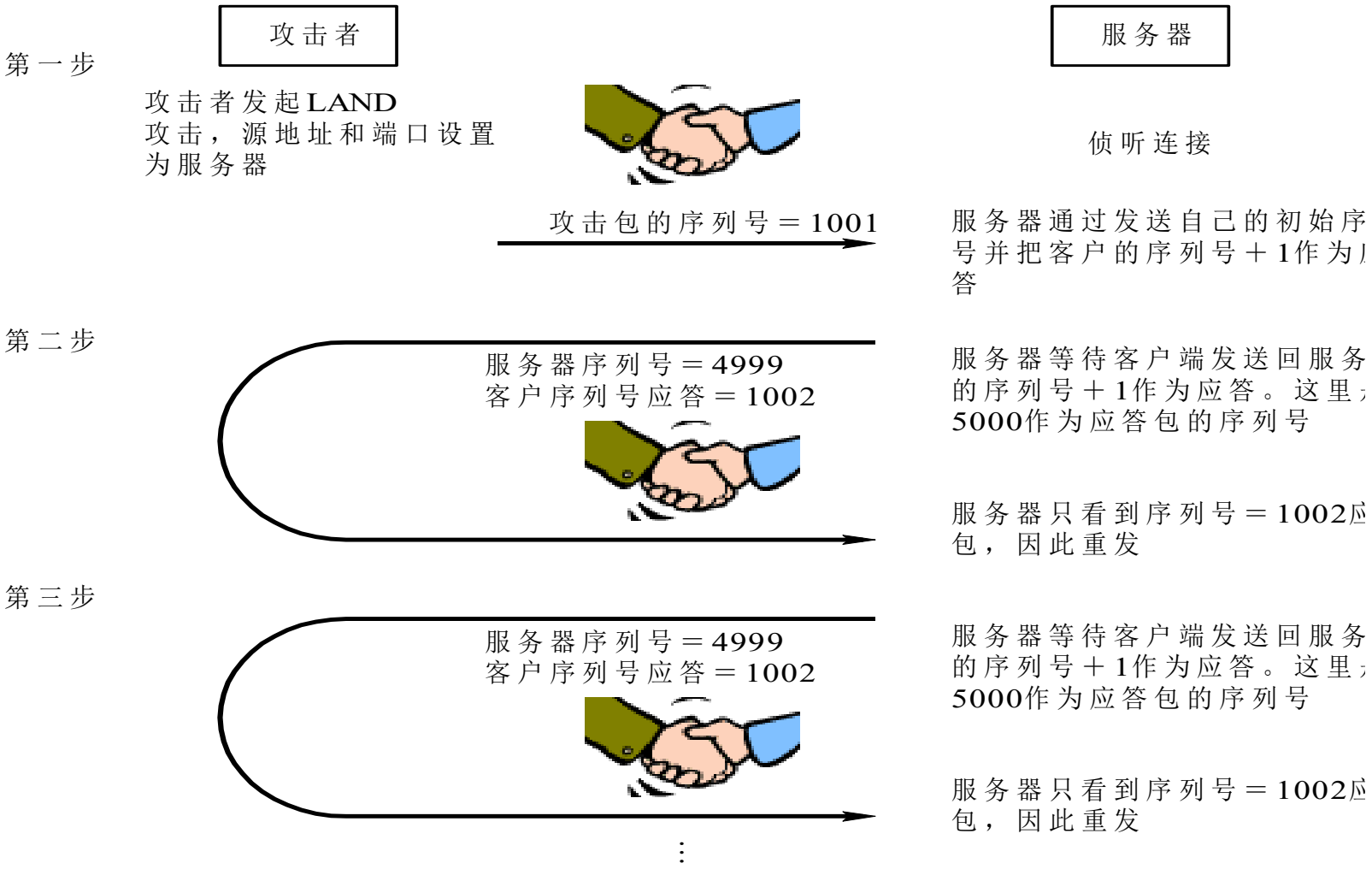
5.2.3 使用代理服务器防范（1）



5.2.4 使用代理服务器防范（2）

1. 使用防火墙对网络中的 TCP 连接进行状态监控和处理。
2. 为连接请求的源地址设定 NEW 状态。
3. 代替源地址为服务器的 SYN+ACK 响应 ACK。
4. 收到源地址 ACK，将其改为 GOOD 状态。
5. 源地址 ACK 超时，则代替源地址向服务器发送 RST，并将其改为 BAD 状态，以后拒绝其所有连接请求。

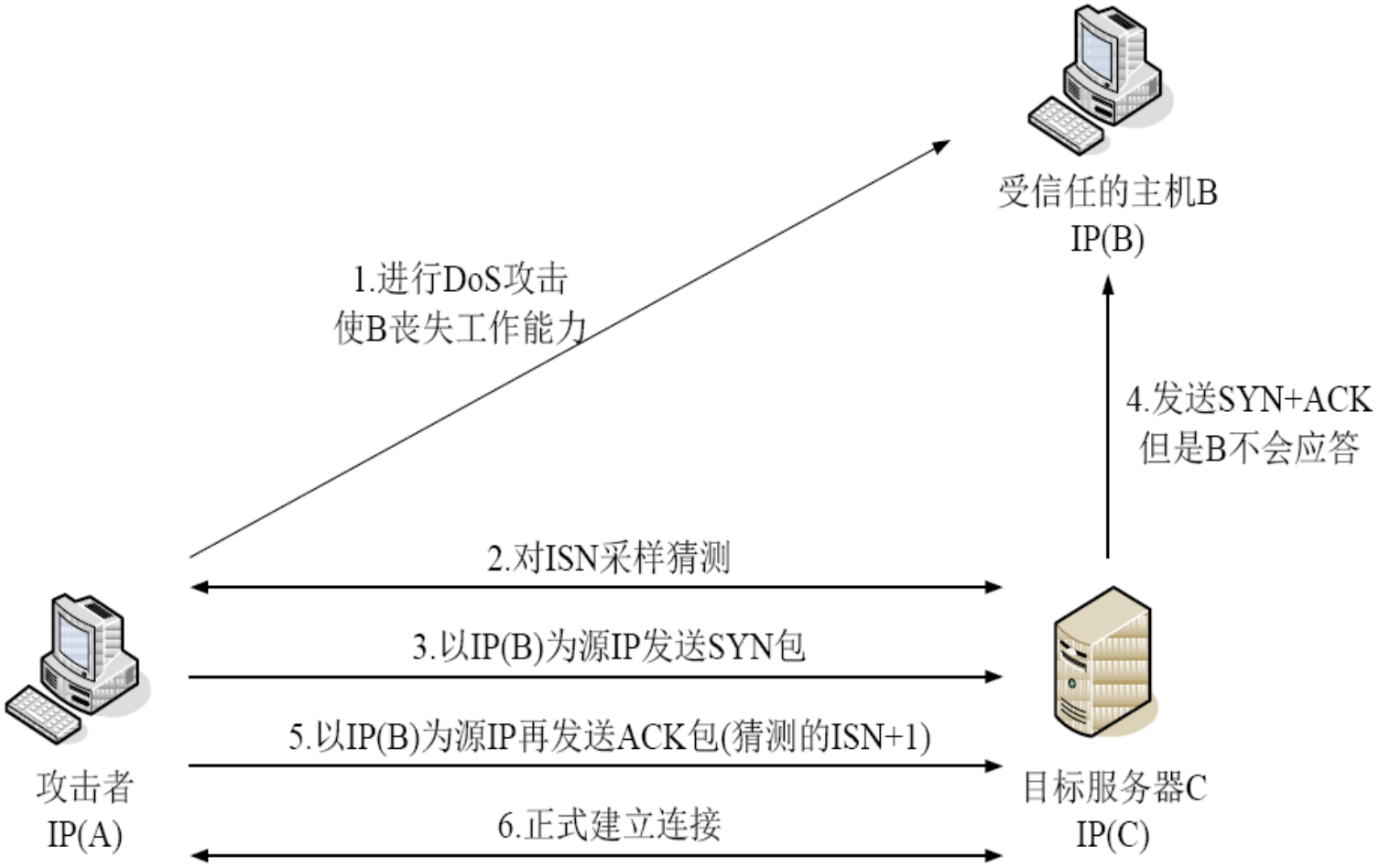
5.3.1 TCP Land 攻击图示



5.3.2 TCP Land 攻击与防范

- 构造 TCP 包，源端口和目的端口相同，源地址和目的地址同为目标主机地址。导致目标主机无限循环地给自己发送错误应答，并希望能够看到具有正确序列号的应答返回。能够有效的使目标主机宕机。
- 防范：
  - 防火墙拒绝源 IP 与目的 IP 相同的数据包；
  - 拒绝内网 IP 的数据包从外网接口进入。

5.4.1 TCP 盲攻击图示

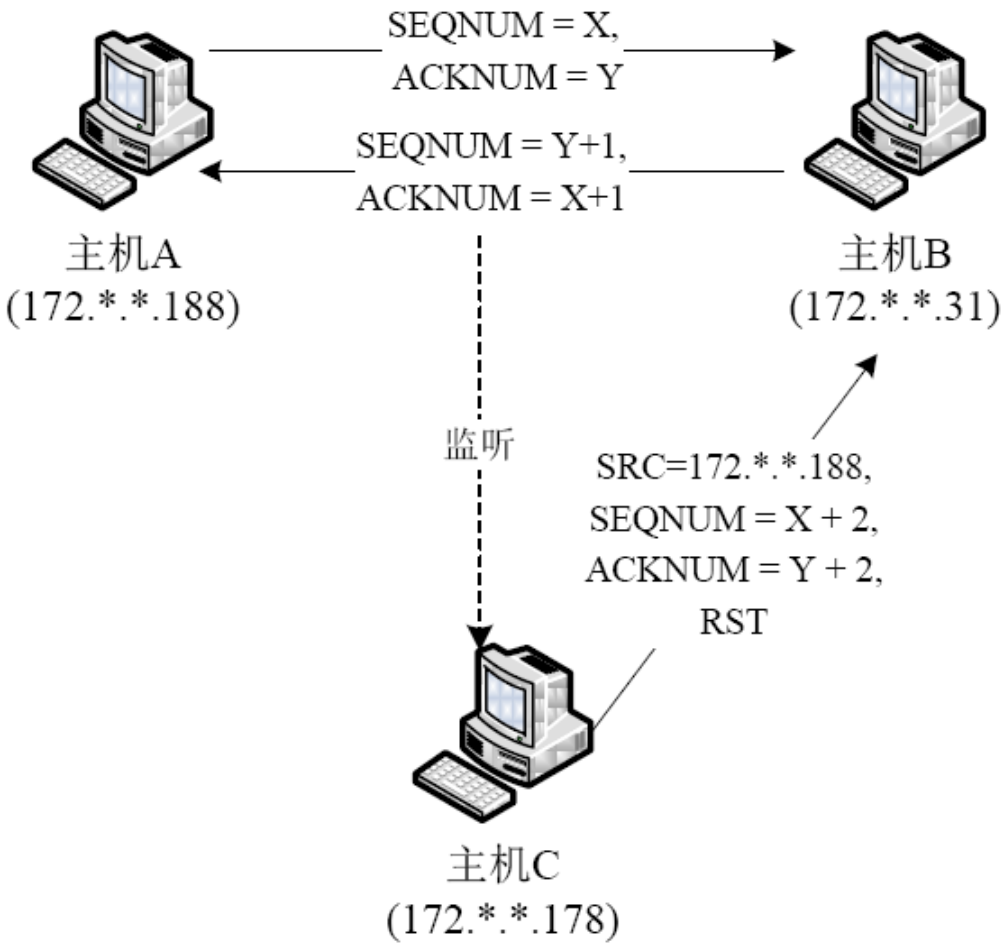


5.4.2 TCP 盲攻击与防范

1. A 对 B 实施 DOS 攻击。
2. A 冒充 B 请求 C 建立连接：
   - A → C： SYN(ISN_A)， SRC = B；
   - C → B： SYN(ISN_C)， ACK(ISN_A + 1)；
3. A 猜测 C 本次会话的 ISN_C， 完成三次握手：
   - A → C： ACK(ISN_C + 1)， SRC = B；
4. 连接建立， A 发送希望 C 接收并处理的数据。

- 防范：
  - 身份验证

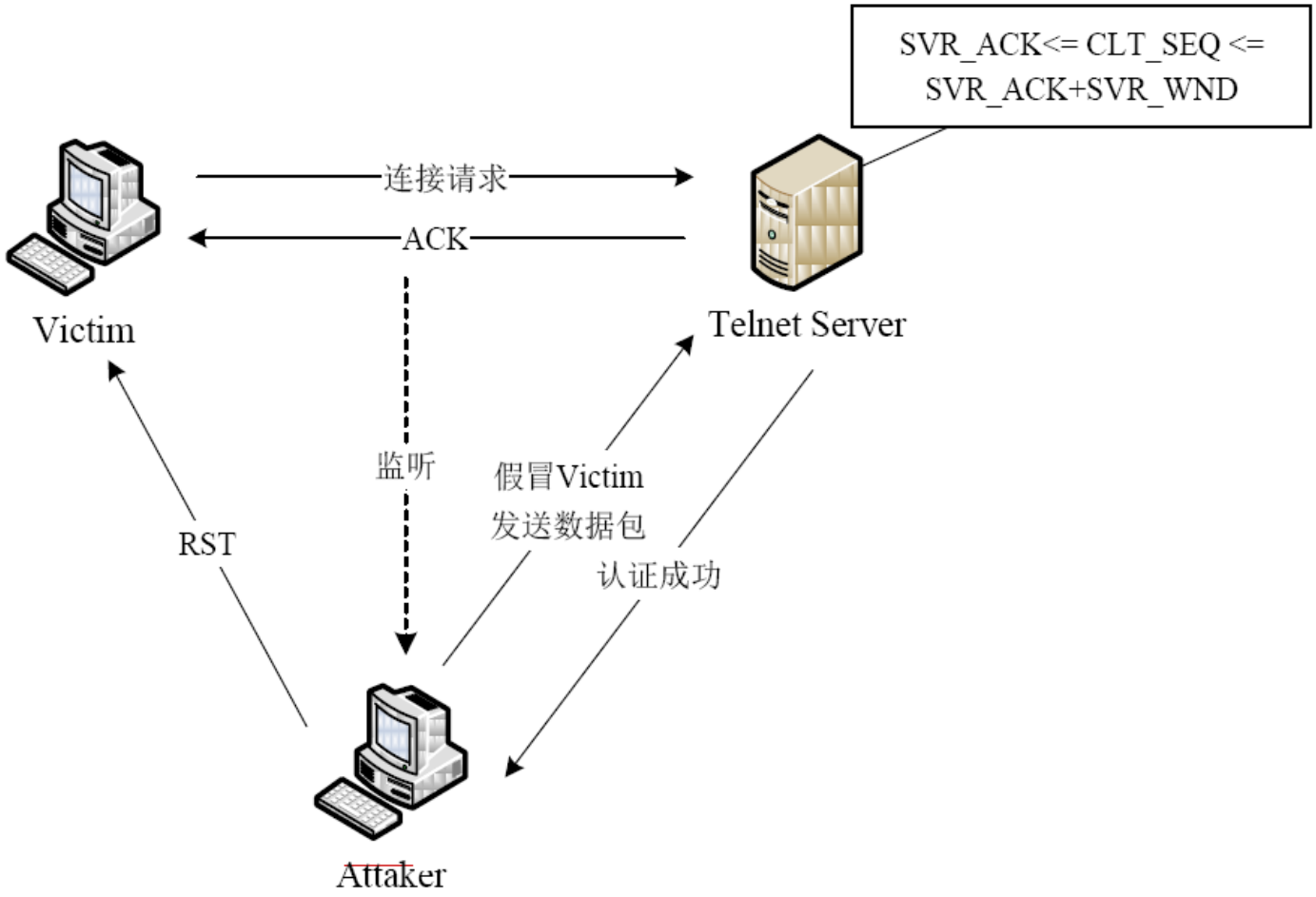
5.5.1 TCP RST 攻击图示



5.5.2 TCP RST 攻击与防范

- 攻击主机嗅探监视通信双方的 TCP 连接，获取源、目的 IP 地址及端口。伪装成通信一方发送 RST 报文给另一方，将直接关闭掉通信双方的 TCP 会话连接，完成拒绝服务攻击。
- 伪造 RST 报文要求：
  - 源 IP 地址及端口号一致；
  - 序列号落入 TCP 窗口之内。
- 防范：
  - 数据加密、包加密、对等实体验证。

5.6.1 TCP 会话劫持 图示



5.6.2 TCP 会话劫持攻击

1. C 与 S 建立TCP连接（可能经过身份验证）。
2. 若 A 与 C 在同一网络：可使信息流经自身，实现中间人攻击，并使用 IP_c 和正确的序列号接管会话。
3. 若 A 属于远程攻击：需要猜测序列号，并使用 IP_c 发送希望 S 接收并处理的数据。
4. 为防止 ACK 风暴，需要迫使 C 下线。

5.6.3 TCP会话劫持防范

- 禁用源路由选项
- 静态绑定 ARP 映射表
- 过滤 ICMP 重定向报文
- 包加密
- 对等实体认证
- VPN

作业

1. MAC 欺骗。
2. ARP 欺骗。
3. ICMP 路由重定向攻击。
4. Smurf 攻击。
5. TCP SYN Flood 攻击。
6. TCP 会话劫持。