计算机与网络安全综合实验

时间：2024年

本次实验任务——互联网安全实验

- OSPF路由项欺骗攻击和防御实验
- 策略路由项实验

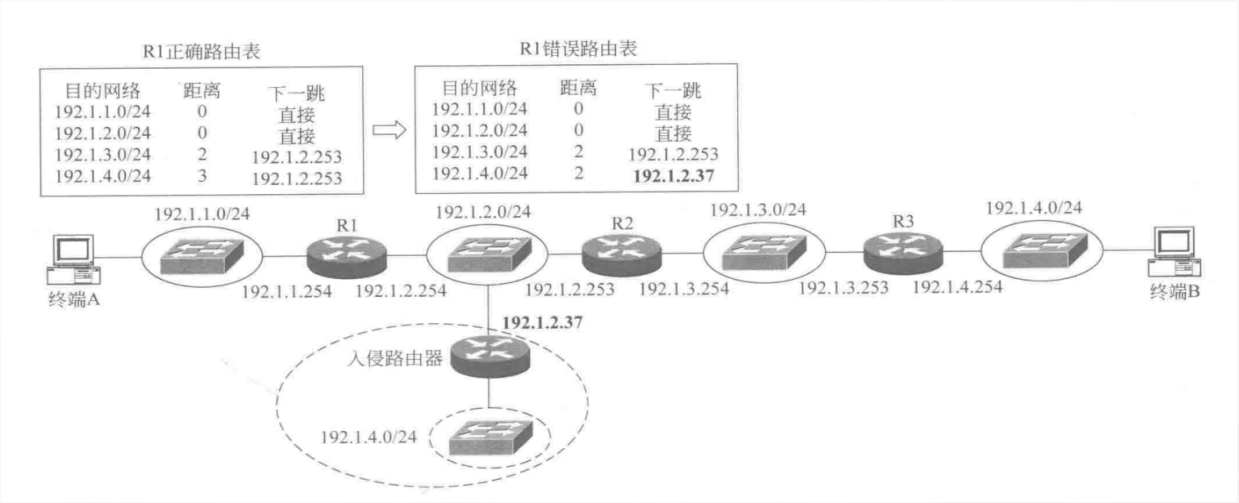
OSPF路由项欺骗攻击和防御实验

- 防御路由项欺骗攻击的方法是实现路由消息源端鉴别，使每一台路由器只能接收和处理授权路由器发送的路由信息。
- 确定路由消息是否是授权路由器发送的依据是：发送路由消息的路由器是否和接收路由消息的路由器拥有相同的共享秘钥。

OSPF路由项欺骗攻击和防御实验

- Packet Tracer不支持路由信息协议（Routing Information Protocol，RIP）的路由消息源端鉴别功能，但支持路由信息开放最短路径优先（Open Shortest Path First，OSPF）的路由信息源端鉴别功能。
- 所以，通过完成“OSPF路由项欺骗攻击和防御实验”验证路由器防路由项欺骗攻击功能的实现过程。

实验内容



- 构建如图所示的由3台路由器互连4个网络的互联网。
  - 通过OSPF生成终端A至终端B的IP传输路径，实现IP分组终端A至终端B的传输过程。
  - 然后在网络地址为192.1.2.0/24的以太网上接入入侵路由器，由入侵路由器伪造与网络192.1.4.0/24直接连接的路由项，用伪造的路由项改变终端A至终端B的IP传输路径，使终端A传输给终端B的IP分组被路由器R1错误地转发给入侵路由器。

实验内容——防御

- 启动路由器R1、R2和R3的路由消息源端鉴别功能，要求路由器R1、R2和R3发送的路由消息携带消息鉴别码(Message Authentication Code,MAC)，配置相应路由器接口之间的共享密钥。
- 使路由器R1不再接收和处理入侵路由器发送的路由消息，从而使路由器R1的路由表恢复正常。

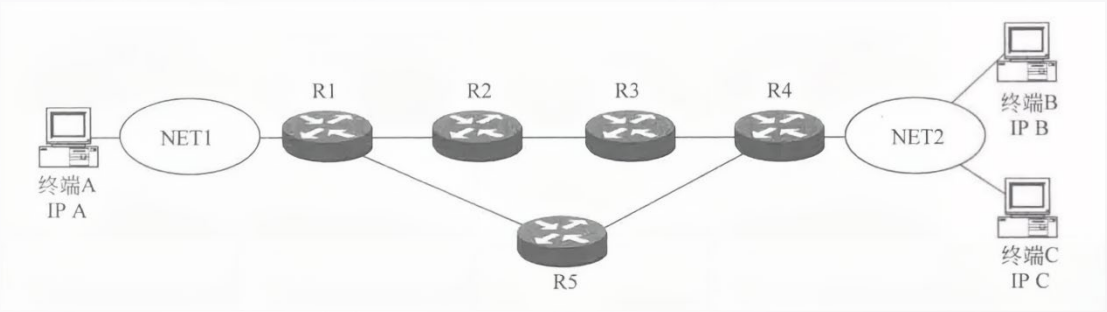
实验目的

- 验证路由器OSPF配置过程。
- 验证OSPF建立动态路由项过程。
- 验证OSPF路由项欺骗攻击过程。
- 验证OSPF源端鉴别功能的配置过程。
- 验证OSPF防路由项欺骗攻击功能的实现过程。

策略路由项实验

- 防路由项欺骗攻击和策略路由是保证IP分组沿着正确和安全的传输路径传输的安全技术。
- 流量管制是防止拒绝服务攻击的有效手段。
- 端口地址转换和网络地址转换使内部网络对于外部网络是不可见的。
- 热备份路由器协议用于实现默认网关的容错和负载均衡。

实验内容



- 互联网结构如图所示，根据最短路径原则，RIP生成的路由器R1通往网络NET2的传输路径是R1→R5→R4→NET2。
- 如果基于安全原因，不允许目的终端是终端C的IP分组经过路由器R5，需要在路由器R1中配置静态路由项，静态路由项将通往终端C的传输路径上的下一跳设置成路由器R2，由于静态路由项的优先级高于RIP生成的动态路由项，因此，路由器R1将目的IP地址为IP C的IP分组转发给路由器R2。
- 由于Packet Tracer中的路由器不支持策略路由功能，因此，用静态路由项仿真策略路由过程。

实验目的

- 验证RIP生成动态路由项的过程。
- 验证最长前缀匹配过程。
- 验证静态路由项改变IP分组传输路径的过程。
- 验证基于安全理由规避特定路由器的过程。