哈爾濱工業大學
HARBIN INSTITUTE OF TECHNOLOGY
立足航天，服务国防，面向国民经济主战场

计算机网络之危机四伏

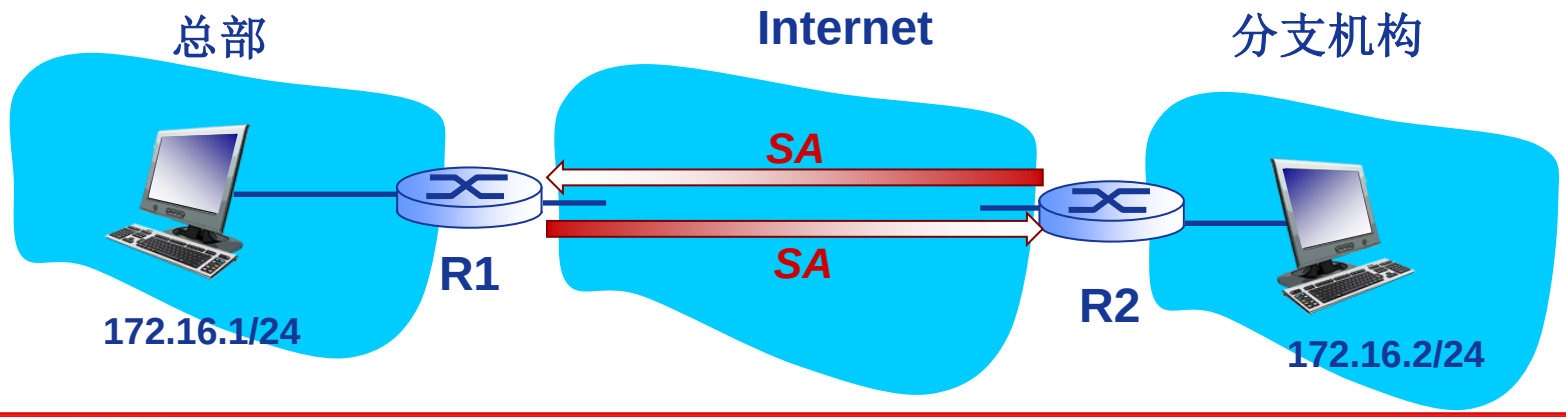
主讲人：李全龙

本讲主题

IP安全（IPsec）（2）

安全关联(SA)

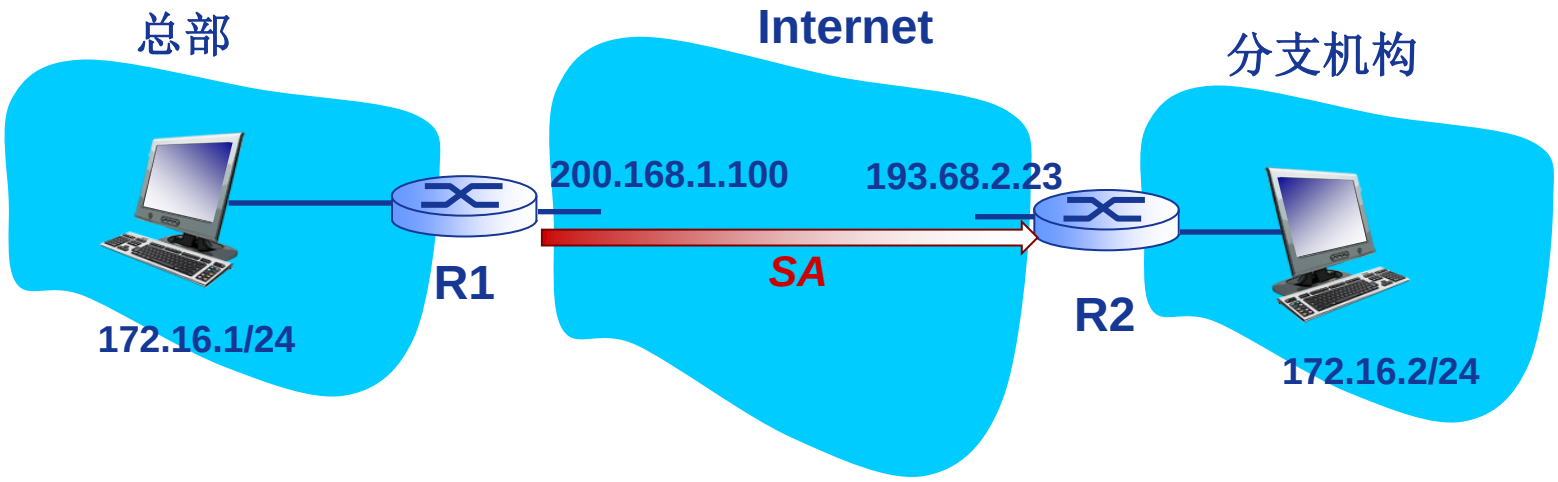
- 发送数据前，从发送实体到接收实体之间需要建立安全关联SA (security association)
  - SA是单工的: 单向
- 发送实体与接收实体均需维护SA的状态信息
  - 回顾: TCP连接的端点也需要维护状态信息
  - IP是无连接的；IPsec是面向连接的！
- 例如：



安全关联(SA)

- 安全关联主要参数：
  - 安全参数索引(SPI)：32位SA唯一标识(ID)
  - 加密密钥、认证密钥
  - 密码算法标识
  - 序列号(32位)
    - 抗重放攻击
  - 抗重播窗口
    - 接收方使用滑动窗口检测恶意主机重放数据报
  - 生存周期
    - 规定SA的有效使用周期
  - 运行模式：传输模式或隧道模式
  - IPSec隧道源、目的地址

SA举例



R1为SA存储:

- 32位SA标识(ID) : 安全参数索引SPI (Security Parameter Index)
- 起点(origin)SA接口(200.168.1.100)
- 终点(destination)SA接口(193.68.2.23)
- 加密类型(e.g., 3DES with CBC)
- 加密密钥
- 完整性检验类型(e.g., HMAC with MD5)
- 认证/鉴别密钥

安全关联数据库(SAD)

- IPsec端点将SA状态保存在安全关联数据库SAD (security association database)中
  - 在处理IPsec数据报时，定位这些信息
- 对于n个销售人员，1个分支机构的VPN，总部的路由器R1的SAD中存储2 + 2n条SAs
- 当发送IPsec数据报时，R1访问SAD，确定如何处理数据报
- 当IPsec数据报到达R2
  - R2检验IPsec数据报中的SPI
  - 利用SPI检索SAD
  - 处理数据报

安全策略数据库(SPD)

- Security Policy Database (SPD)
- 安全策略(SP):定义了对什么样的数据流实施什么样的安全处理
  - 应用IPSec、绕过、丢弃
- 安全策略组成了SPD，每个记录就是一条SP
  - 提取关键信息填充到一个称为“选择符”的结构
    - 包括目标IP、源IP、传输层协议、源和目标端口等
  - 利用选择符去搜索SPD，检索匹配的SP
- 安全处理需要的参数存储在SP指向的SA结构

哈爾濱工業大學
HARBIN INSTITUTE OF TECHNOLOGY

立足航天，服务国防，面向国民经济主战场

谢 谢！