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

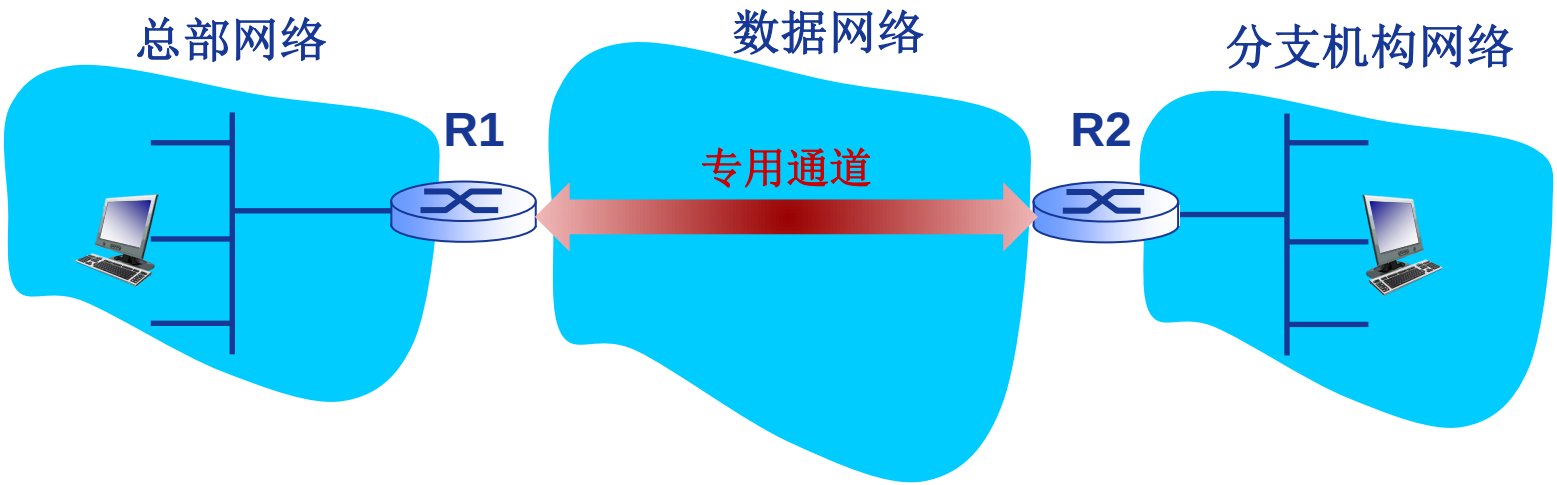
主讲人：李全龙

本讲主题

虚拟专用网（VPN）

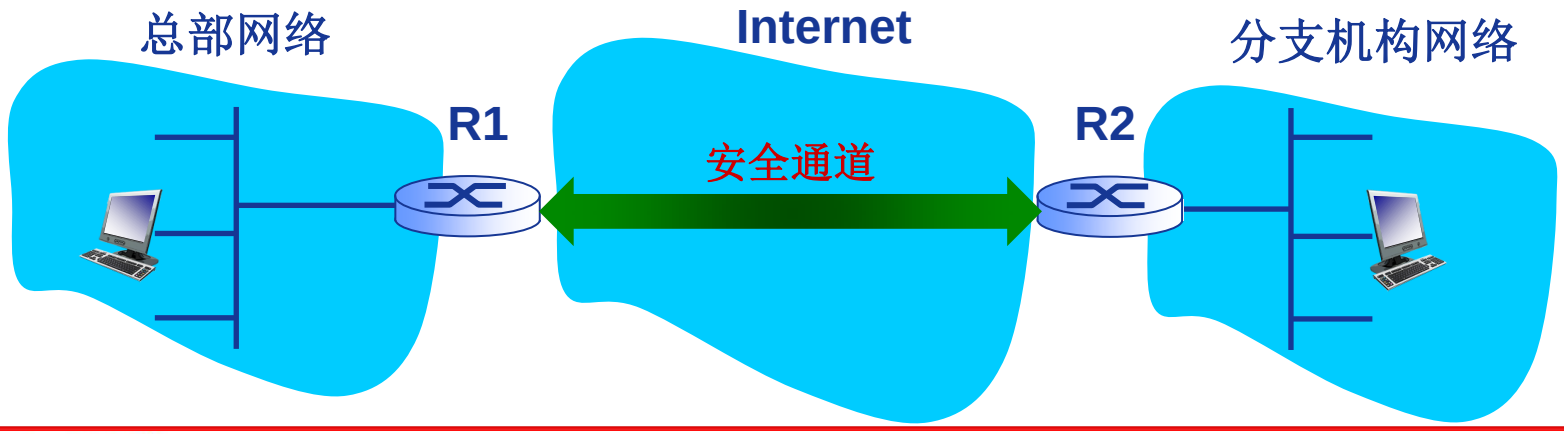
专用网(PN)

- 动机：安全
- 专用网络PN(Private Networks)：基于专属的网络设备、链路或协议等建设的专门服务于特定组织机构的网络。
  - 民航网络、铁路网络、银行网络、……
  - 成本问题：路由器、链路、DNS基础设施等

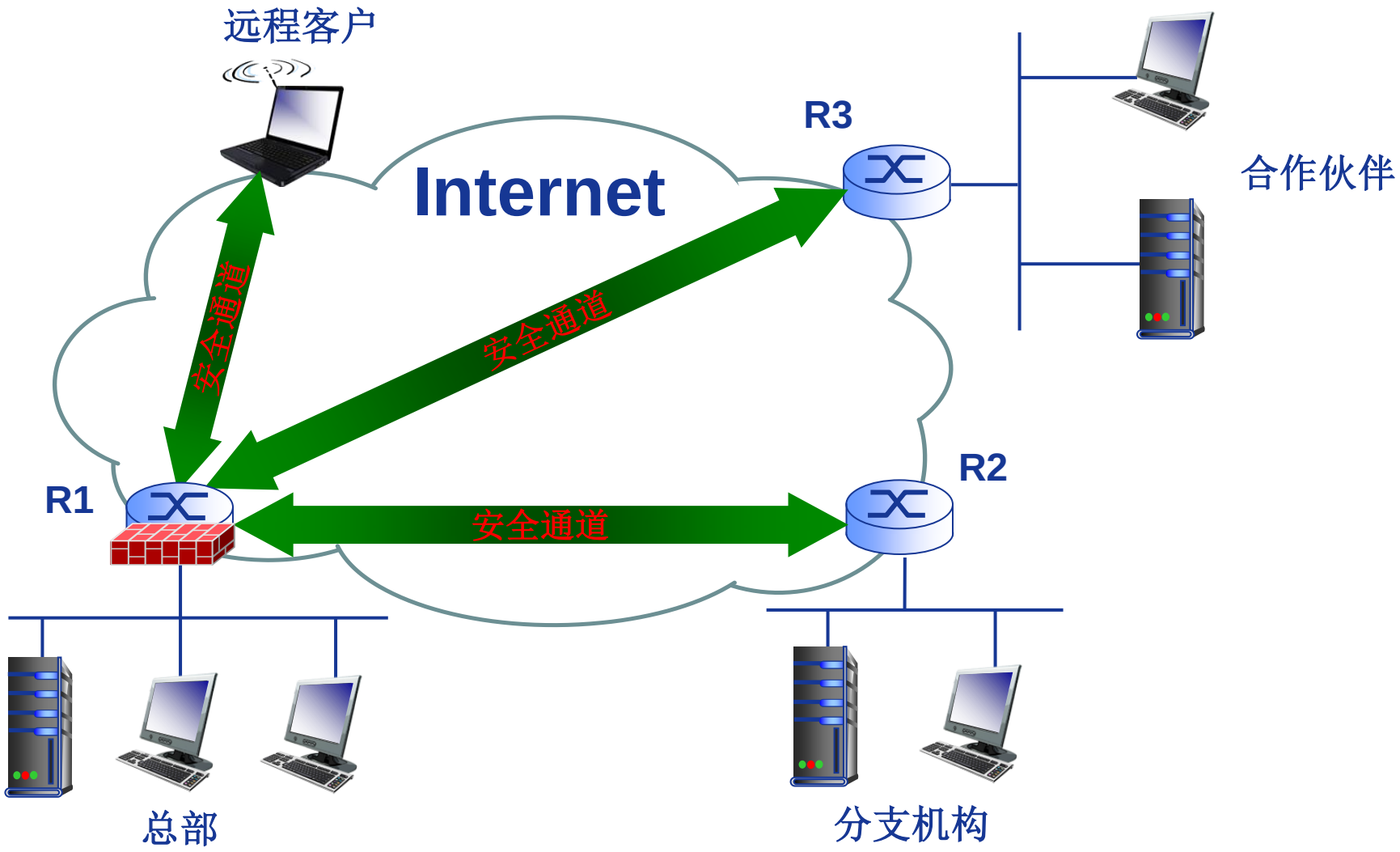


虚拟专用网(VPN)

- 动机：安全+成本
- 虚拟专用网VPN(Virtual Private Networks)：通过建立在公共网络(如Internet)上的安全通道，实现远程用户、分支机构、业务伙伴等与机构总部网络的安全连接，从而构建针对特定组织机构的专用网络。
  - 虚拟：“安全通道”不实际独占公共网络的资源，是一条逻辑的穿过公共网络的安全、稳定的隧道
  - 通过隧道技术、加密技术、密钥管理、认证和访问控制等，实现与专用网类似的安全性能



典型VPN应用



VPN的功能

- 数据机密性保护
- 数据完整性认证
- 数据源身份认证
- 防重放攻击
- 访问控制

VPN关键技术

- 隧道技术
- 数据加密
- 身份认证
- 密钥管理
- 访问控制
- 网络管理

隧道技术

- 构建VPN的核心技术
- 隧道：通过Internet提供安全的点到点(或端到端)的数据传输“安全通道”
  - 实质上是一种封装
- VPN隧道利用隧道协议对通过隧道传输的数据进行封装
  - 使数据安全穿越公共网络(通常是Internet)
  - 通过加密和认证以确保安全
  - 数据包进入隧道时，由VPN封装成IP数据报
  - 通过隧道在Internet上安全传输
  - 离开隧道后，进行解封装，数据便不再被保护

隧道协议

- 隧道协议内包括以下三种协议：
  - 乘客协议（Passenger Protocol）
  - 封装协议（Encapsulating Protocol）
  - 承载协议（Carrier Protocol）

- 常见VPN隧道协议：
  - 第二层隧道：PPTP、L2TP
    - 主要用于远程客户机访问局域网方案
  - 第三层隧道：IPSec
    - 主要用于网关到网关、或网关到主机方案
    - 不支持远程拨号访问

典型VPN实现技术

- IPSec：最安全、适用面最广
- SSL：具有高层安全协议的优势
- L2TP：最好的实现远程接入VPN的技术

- 典型VPN技术结合：IPSec与SSL、IPSec与L2TP

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！