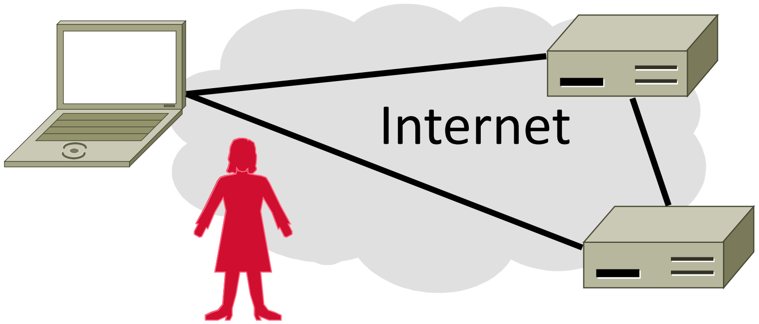
Computer Networks

Virtual Private Networks (VPNs)
(§8.6.3, §8.6.1)

David Wetherall (djw@uw.edu)
Professor of Computer Science & Engineering
UNIVERSITY *of* WASHINGTON

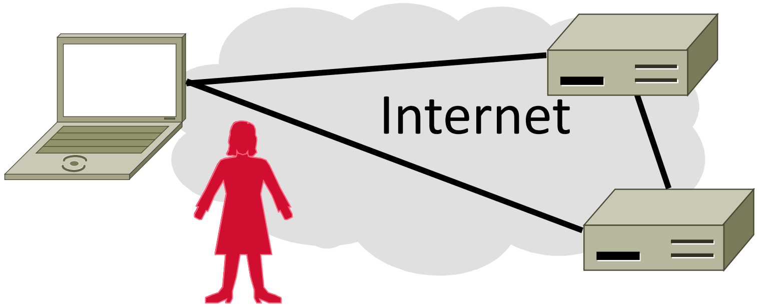
Topic

- Virtual Private Networks (VPNs)
  - Run as closed networks on Internet
  - Use IPSEC to secure messages



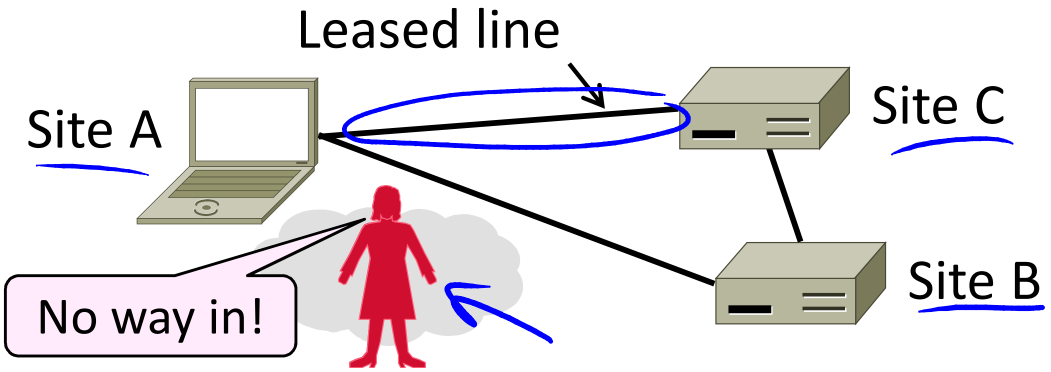
Motivation

- The best part of IP connectivity
  - You can send to any other host
- The worst part of IP connectivity
  - Any host can send packets to you!
  - There's nasty stuff out there …



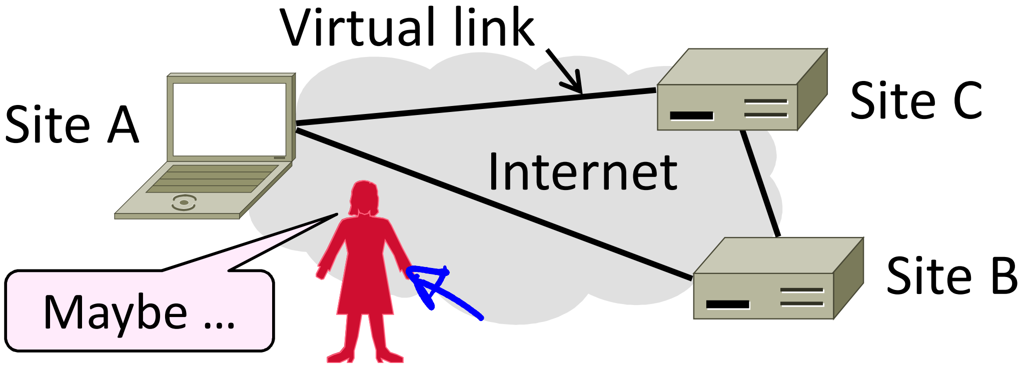
Motivation (2)

- Often desirable to separate network from the Internet, e.g., a company
  - Private network with leased lines
  - Physically separated from Internet



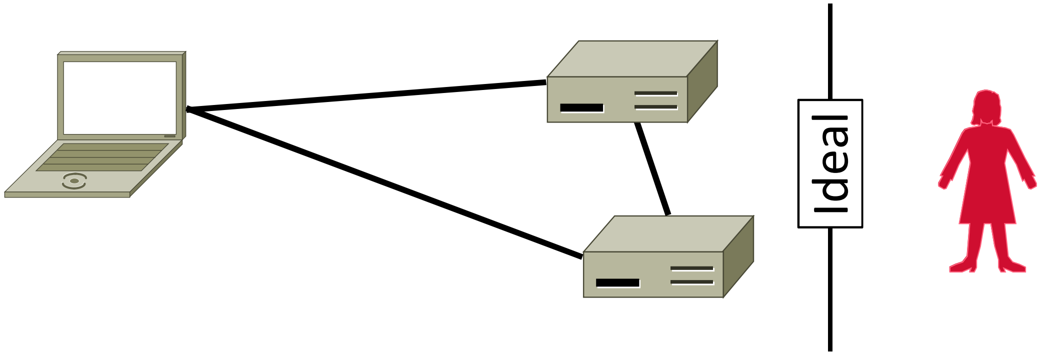
Motivation (3)

- Idea: Use the public Internet instead of leased lines – cheaper!
  - Logically separated from Internet …
  - This is a <u>Virtual Private Network</u> (VPN)



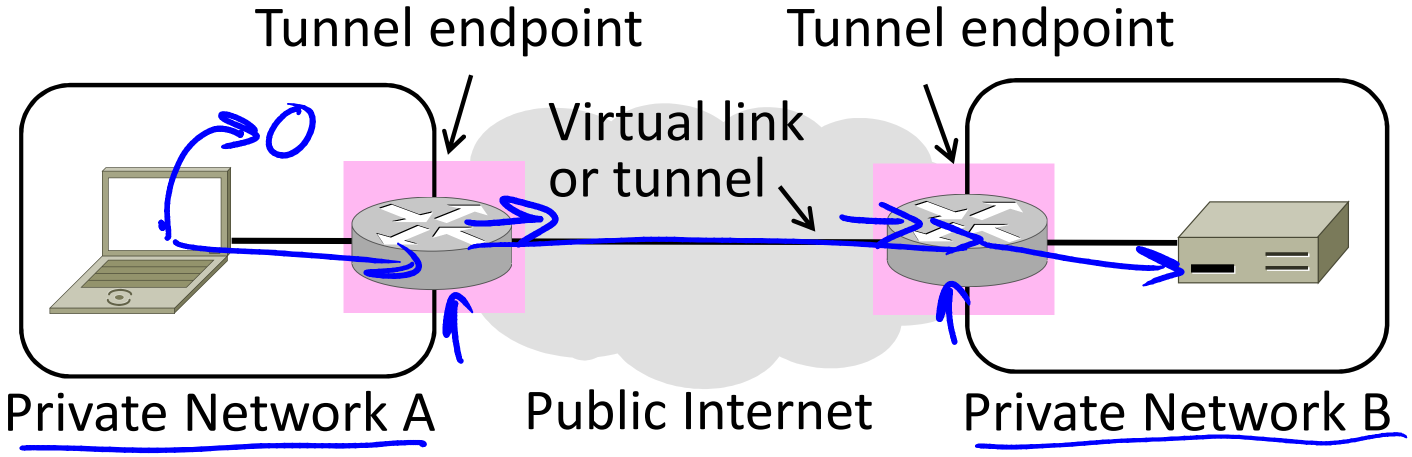
Goal and Threat Model

- Goal is to keep a logical network (VPN) separate from the Internet while using it for connectivity
  - Threat is Trudy may access VPN and intercept or tamper with messages



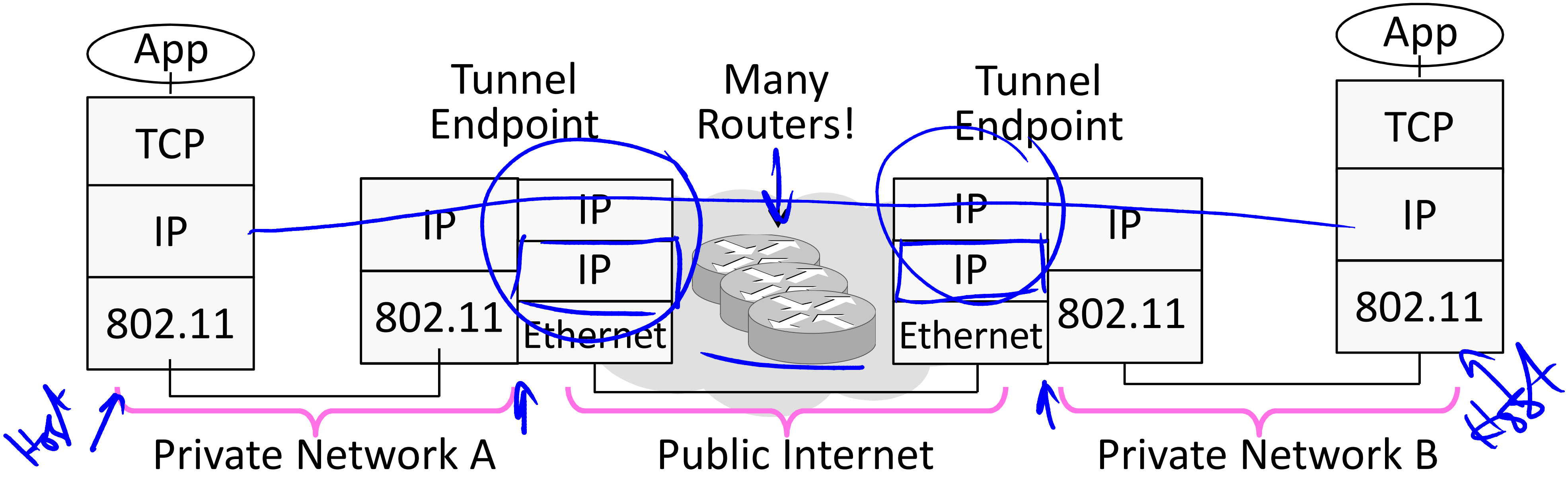
Tunneling

- How can we build a virtual link? With tunneling!
  - Hosts in private network send to each other normally
  - To cross virtual link (tunnel), endpoints encapsulate packet



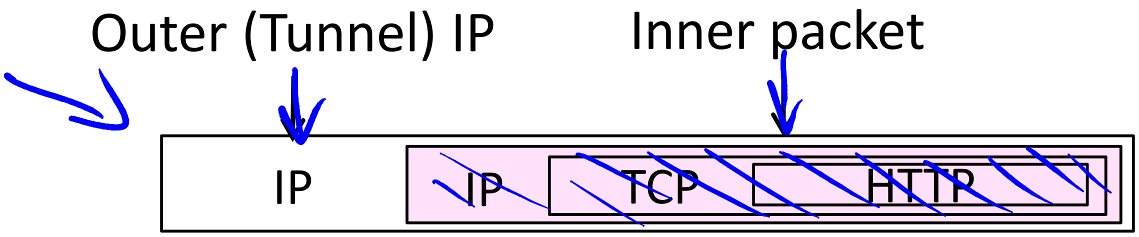
Tunneling (2)

- Tunnel endpoints encapsulate IP packets ("IP in IP")
  - Add/modify outer IP header for delivery to remote endpoint



Tunneling (3)

- Simplest encapsulation wraps packet with another IP header
  - Outer (tunnel) IP header has tunnel endpoints as source/destination
  - Inner packet has private network IP addresses as source/destination

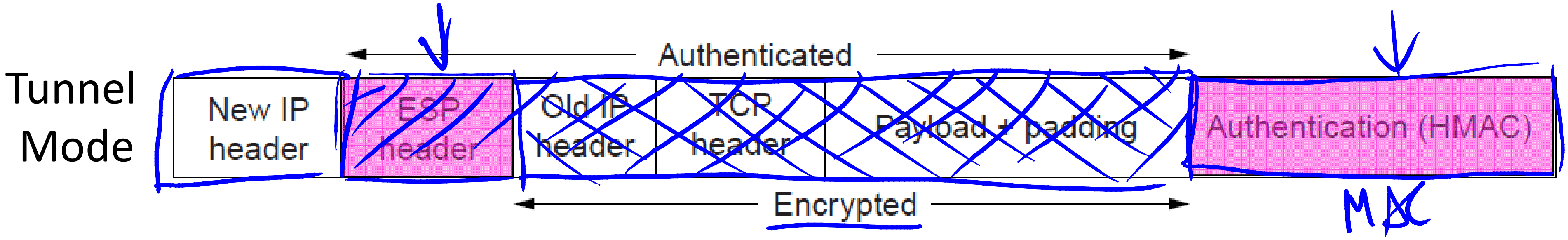


Tunneling (4)

- Tunneling alone is not secure …
  - No confidentiality, integrity/ authenticity
  - Trudy can read, inject her own messages
  - We require cryptographic protections!
- IPSEC (IP Security) is often used to secure VPN tunnels

IPSEC (IP Security)

- Longstanding effort to secure the IP layer
  - Adds confidentiality, integrity/authenticity
- IPSEC operation:
  - Keys are set up for communicating host pairs → tunnel end point
  - Communication becomes more connection-oriented
  - Header and trailer added to protect IP packets



Takeaways

- VPNs are useful for building networks on top of the Internet
  - Virtual links encapsulate packets
  - Alters IP connectivity for hosts
- VPNs need crypto to secure messages
  - Typically IPSEC is used for confidentiality, integrity/authenticity

END