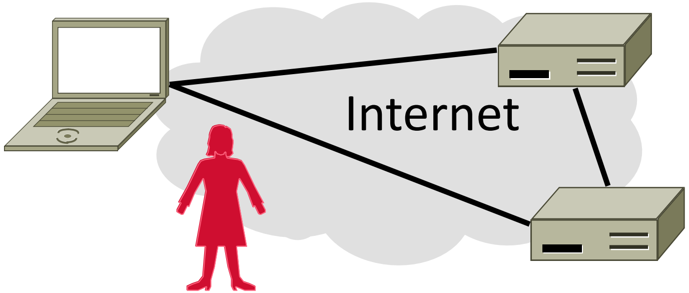
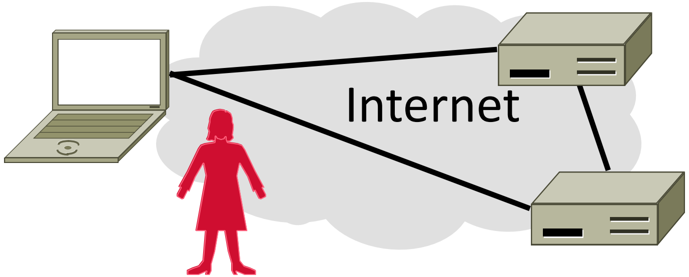
Topic

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



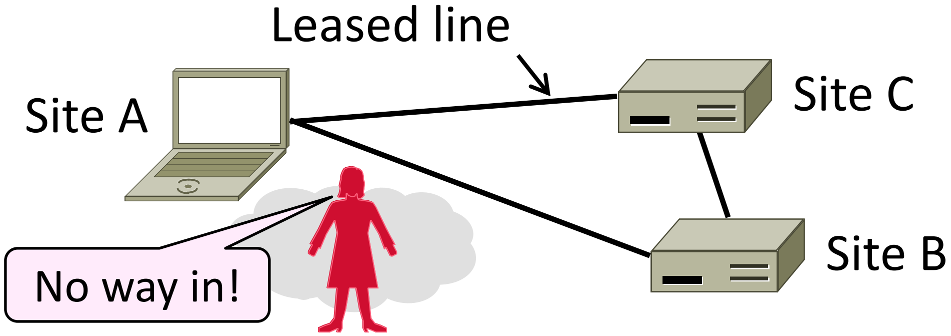
Motivation

- 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 …



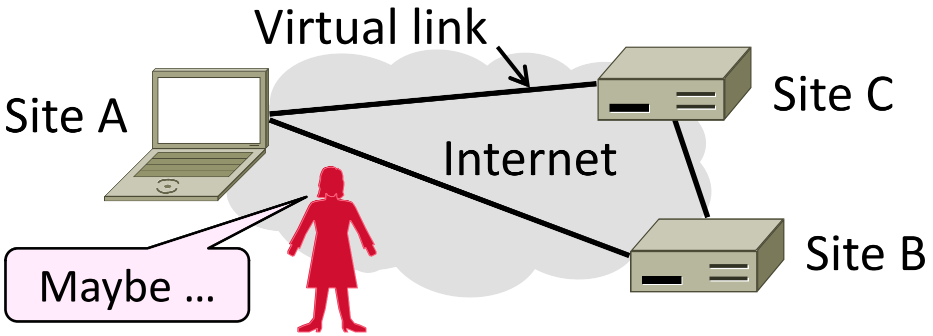
Motivation (2)

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



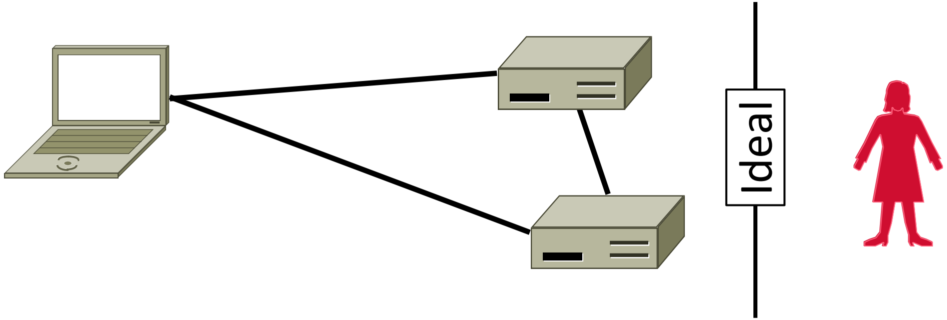
Motivation (3)

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



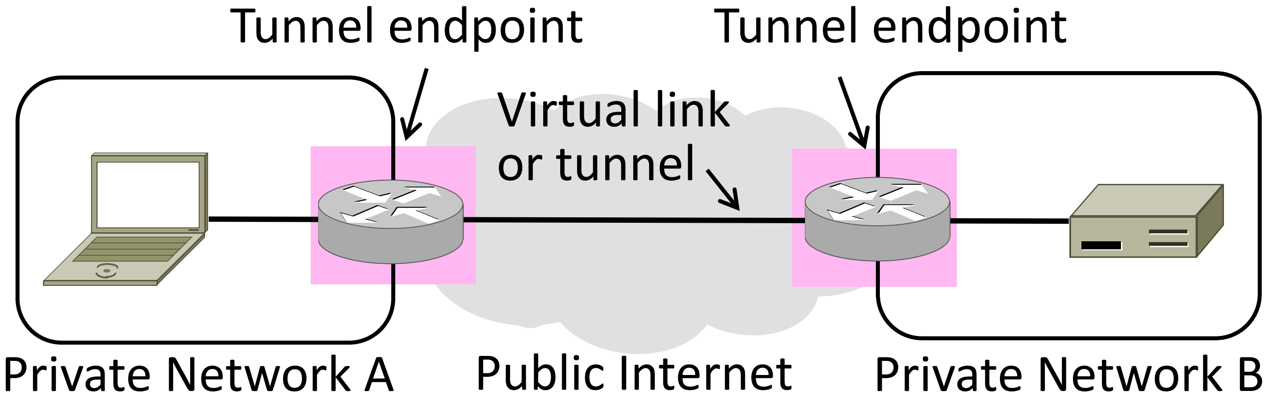
Goal and Threat Model

- 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



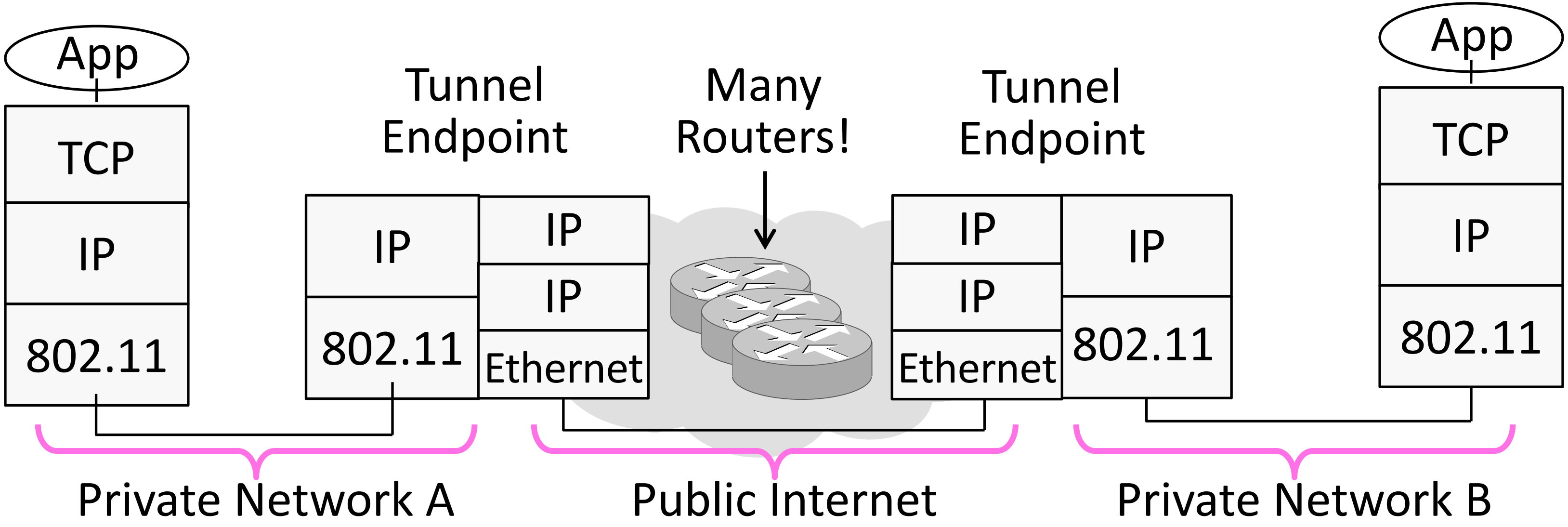
Tunneling

- 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



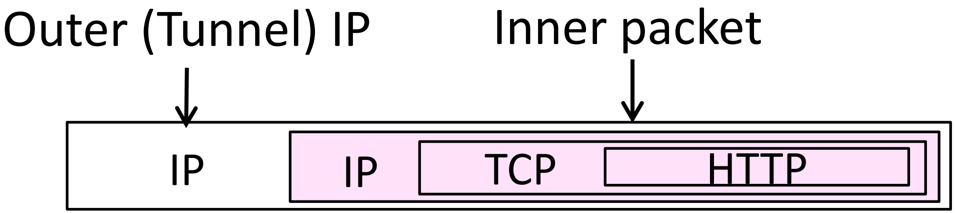
Tunneling (2)

- 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



Outer (Tunnel) IP

Inner packet

IP

IP

TCP

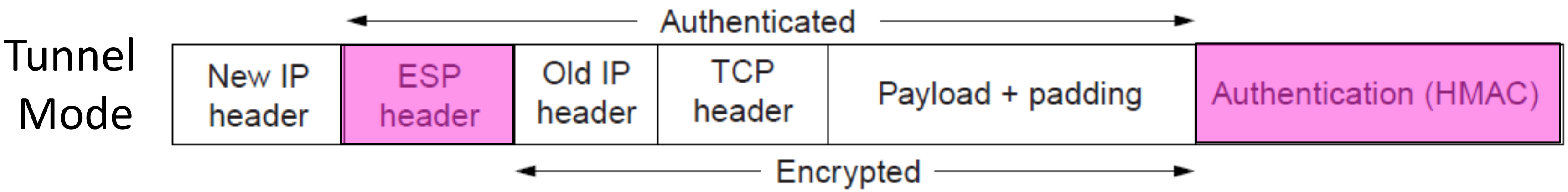
HTTP

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
  - Communication becomes more connection-oriented
  - Header and trailer added to protect IP packets
  - Encapsulating Security Payloads (ESP) provide confidentiality, data integrity, authenticatiion, and anti-replay service

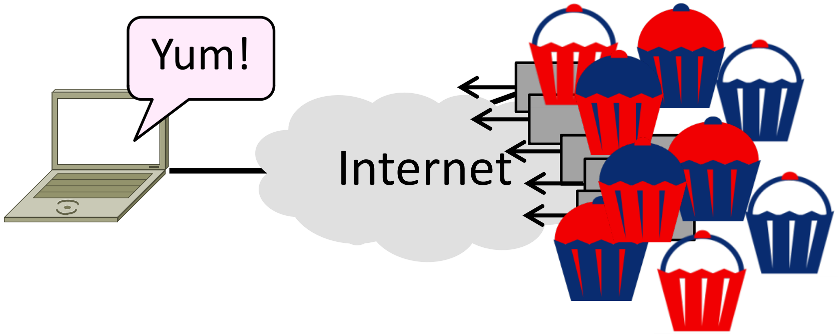


Takeaways

- 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

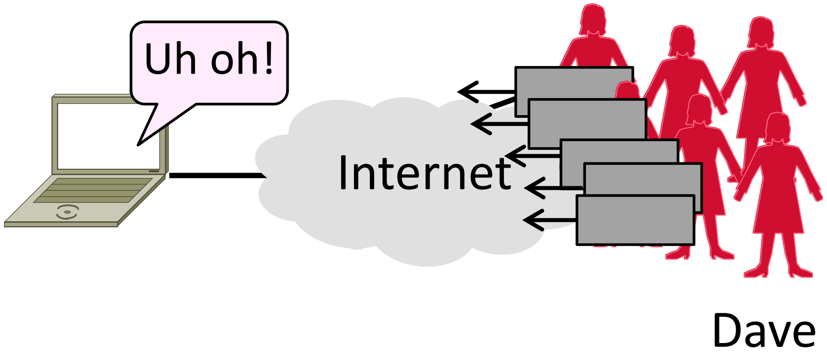
Topic

- Distributed Denial-of-Service (DDOS)
  - An attack on network availability



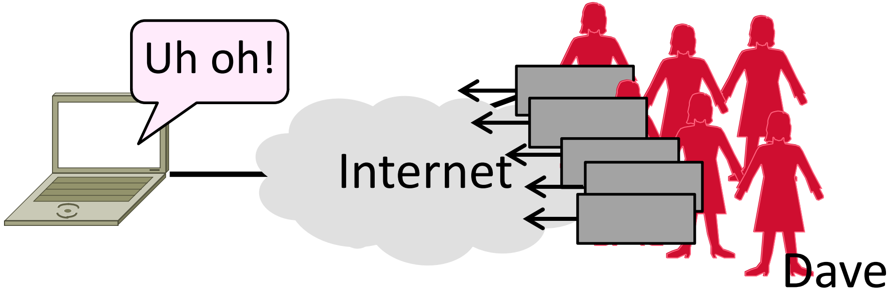
Topic

- Distributed Denial-of-Service (DDOS)
  - An attack on network availability



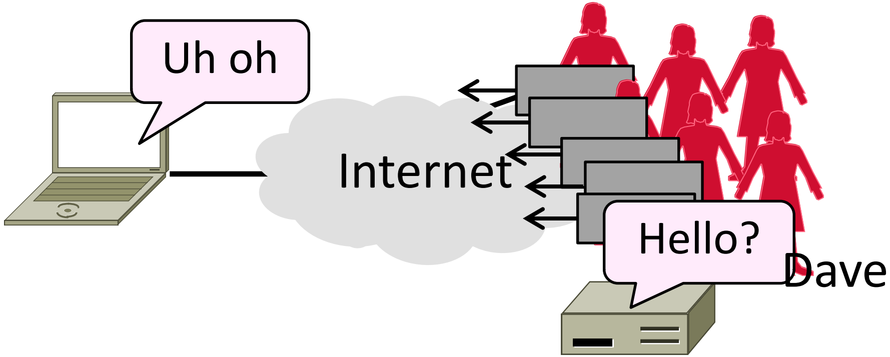
Motivation

- 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!



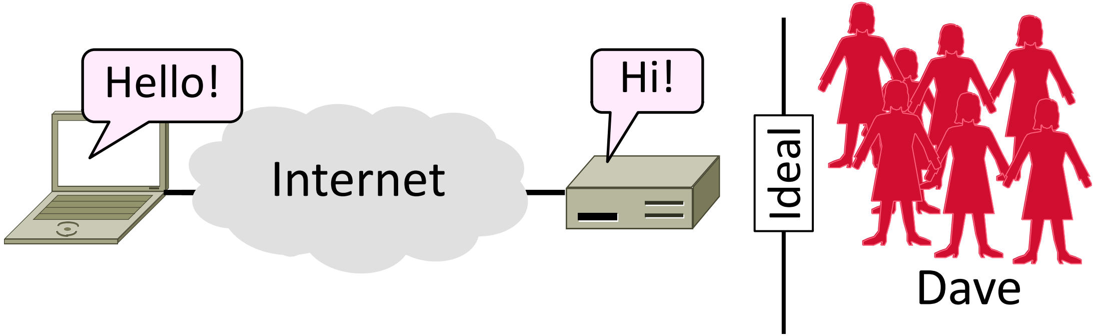
Motivation (2)

- Flooding a host with many packets can interfere with its IP connectivity
  - Host may become unresponsive
  - This is a form of denial-of-service



Goal and Threat Model

- Goal is for host to keep network connectivity for desired services
  - Threat is Dave may overwhelm host with undesired traffic



Internet Reality

- Distributed Denial-of-Service is a huge problem!
  - Akamai Q3-12 reports DDOS against US banks peaking at 65 Gbps …
- There are no great solutions
  - CDNs, network traffic filtering, and best practices all help

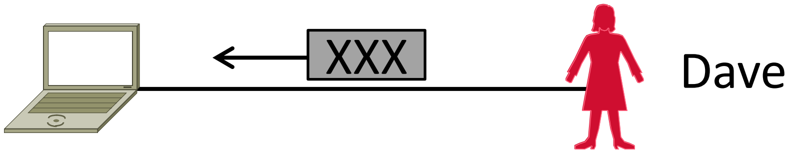
Denial-of-Service

- Denial-of-service means a system is made unavailable to intended users
  - Typically because its resources are consumed by attackers instead

- In the network context:
  - "System" means server
  - "Resources" mean bandwidth (network) or CPU/memory (host)

Host Denial-of-Service

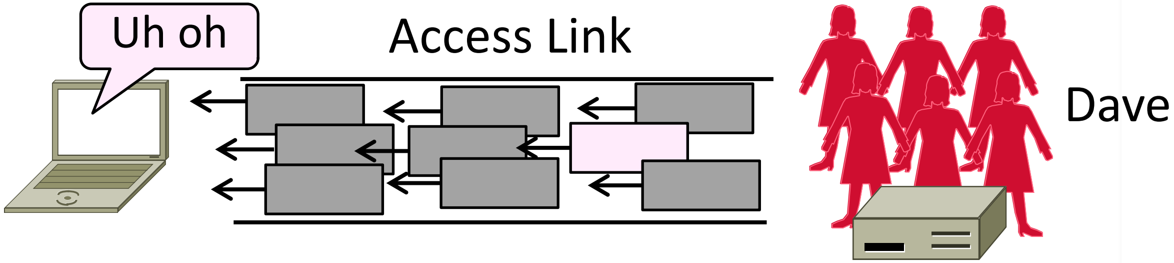
- Strange packets can sap host resources!
  - “Ping of Death” malformed packet
  - “SYN flood” sends many TCP connect requests and never follows up
  - Few bad packets can overwhelm host



- Patches exist for these vulnerabilities
  - Read about “SYN cookies” for interest

Network Denial-of-Service

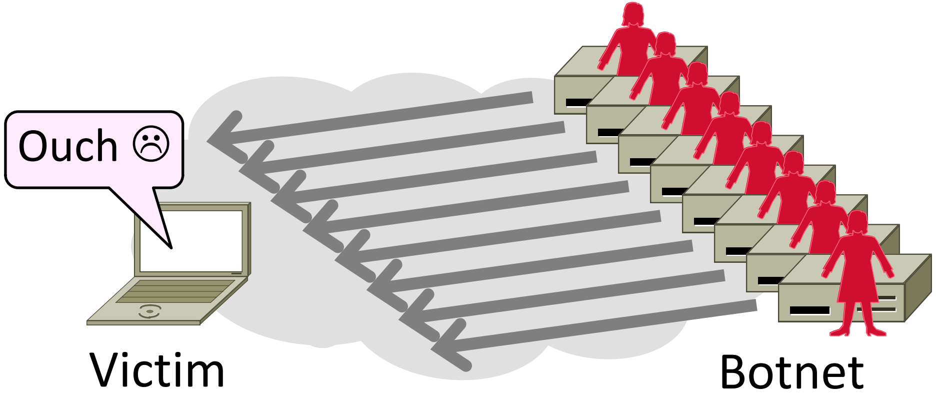
- Network DOS needs many packets
  - To saturate network links
  - Causes high congestion/loss



- Helpful to have many attackers … or <u>Distributed Denial-of-Service</u>

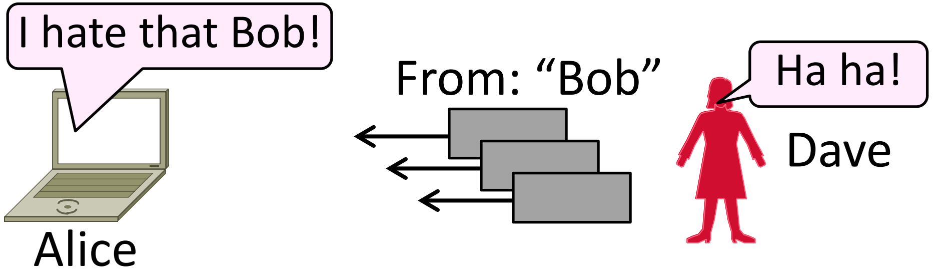
Distributed Denial-of-Service (DDOS)

- Botnet provides many attackers in the form of compromised hosts
  - Hosts send traffic flood to victim
  - Network saturates near victim



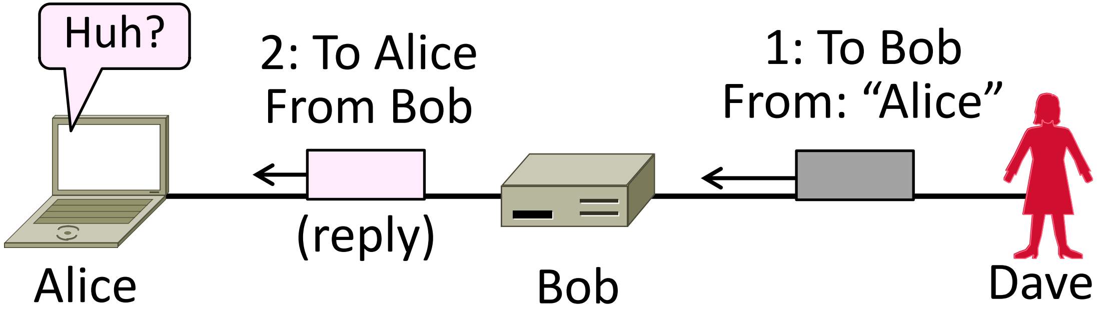
Complication: Spoofing

- Attackers can falsify their IP address
  - Put fake source address on packets
  - Historically network doesn’t check
  - Hides location of the attackers
  - Called IP address <u>spoofing</u>



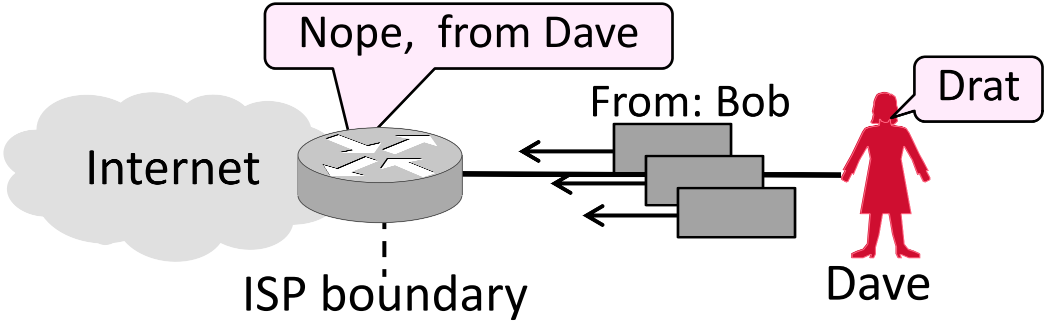
Spoofing (2)

- Actually, it’s worse than that
  - Dave can trick Bob into really sending packets to Alice
  - To do so, Dave spoofs Alice to Bob



Best Practice: Ingress Filtering

- Idea: Validate the IP source address of packets at ISP boundary (Duh!)
  - <u>Ingress filtering</u> is a best practice, but deployment has been slow



Flooding Defenses

1. Increase network capacity around the server; harder to cause loss
   - Use a CDN for high peak capacity

2. Filter out attack traffic within the network (at routers)
   - The earlier the filtering, the better
   - Ultimately what is needed, but ad hoc measures by ISPs today