Computer Networking and Network Security Problems

Jun Li

lijun@cs.uoregon.edu

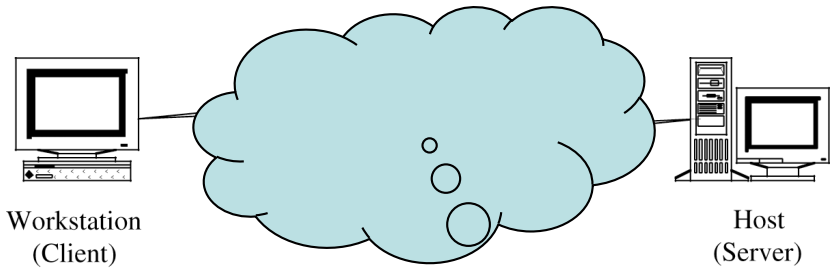
Learning Objectives

- Basic network concepts
- Threats in networks
- Network security controls
- Wireless security
- Denial of service

Network Concepts

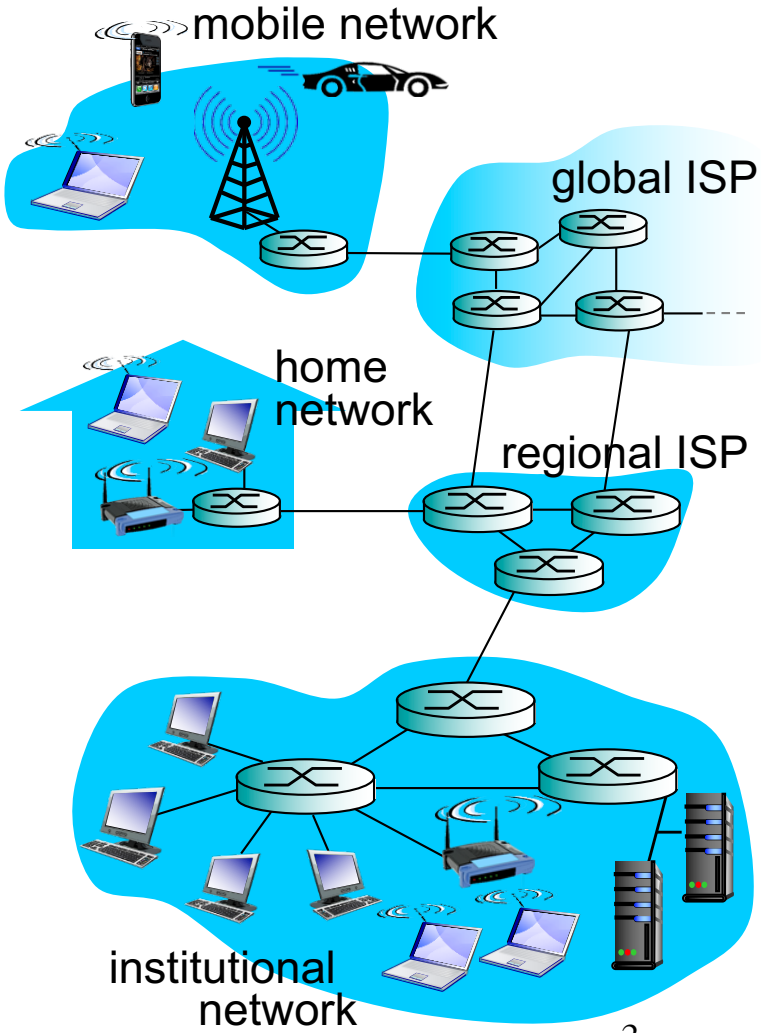
- Network is to support end-to-end communication

- Network can also be viewed as a cloud
  - What end hosts care is to receive service or retrieve content



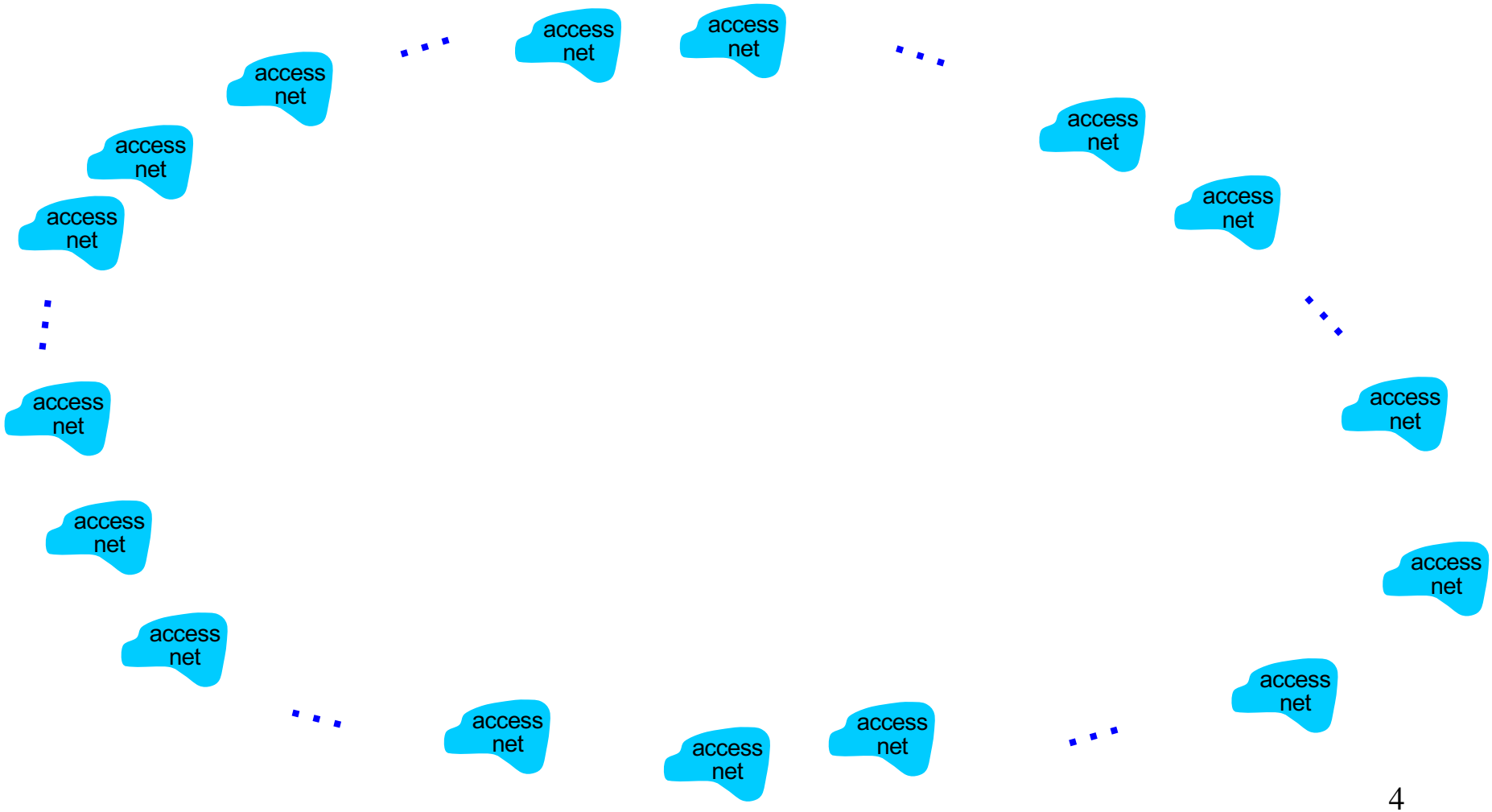
What is in the "Network"?

- Internet service providers, or ASes (autonomous systems)
- Local area networks (LAN)
- Wide area networks (WAN)
- Nodes
  - Routers
  - End hosts
- Links



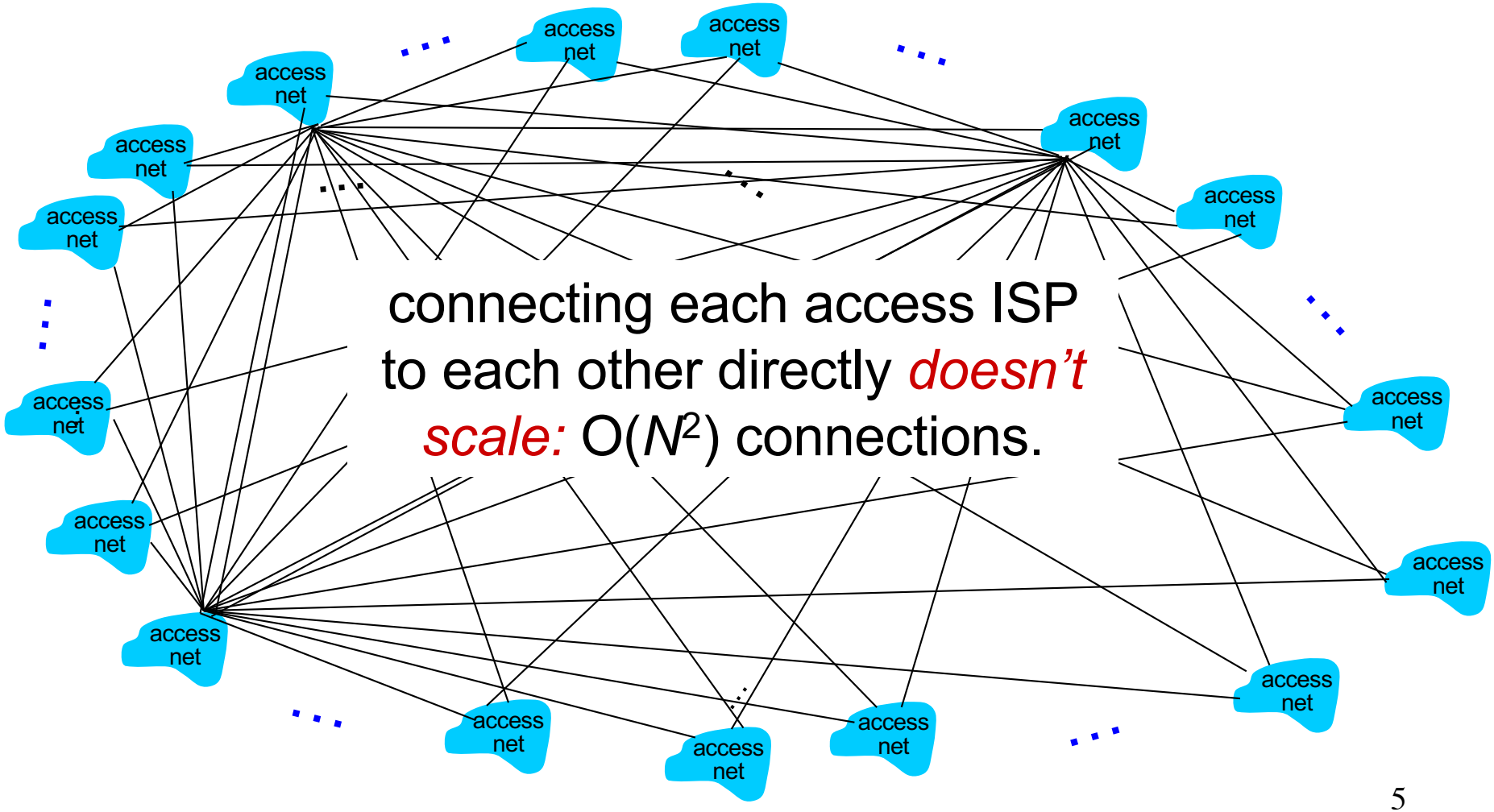
Internet structure: network of networks

Question: given *millions* of access ISPs, how to connect them together?



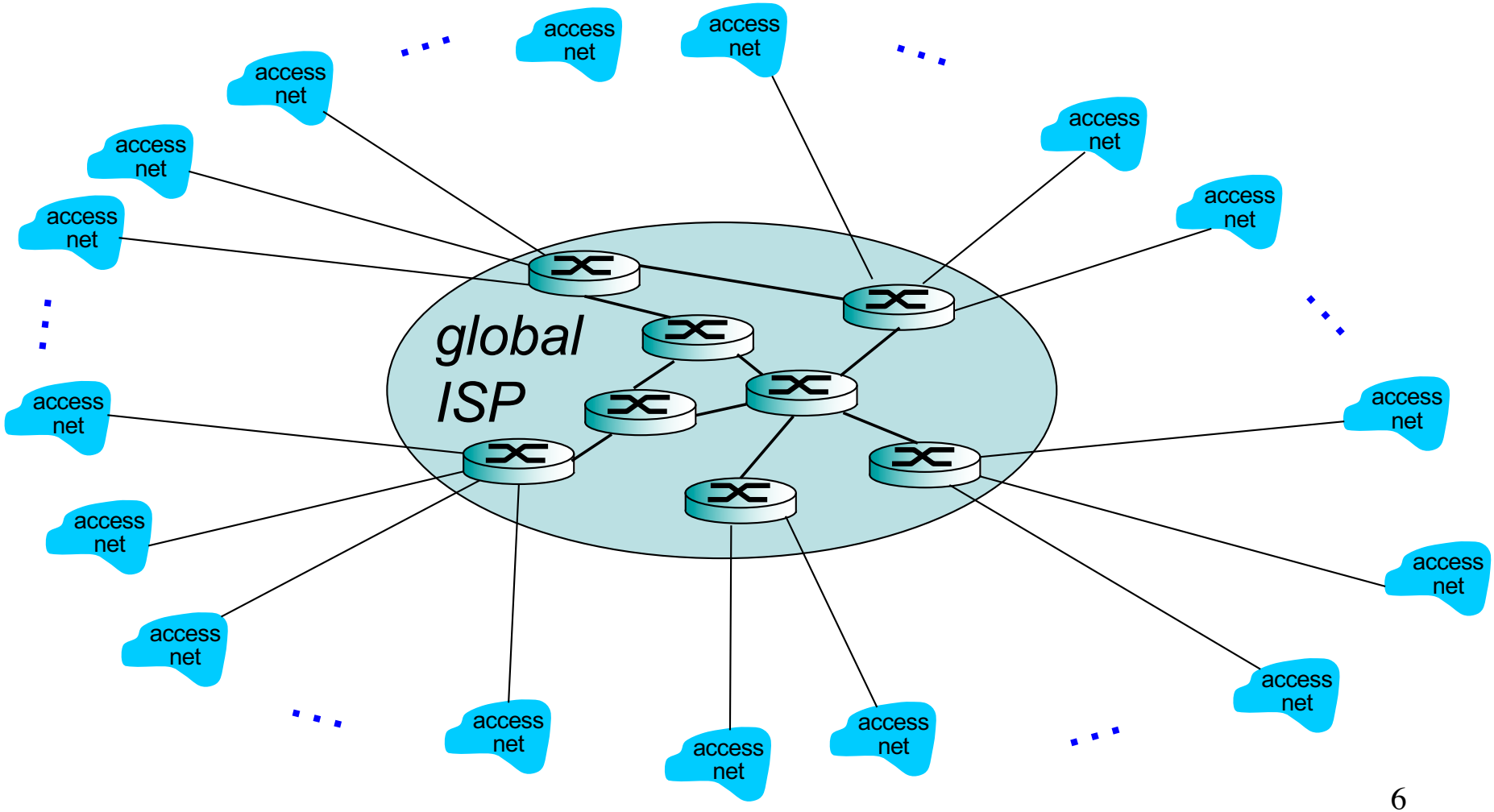
Internet structure: network of networks

Option: connect each access ISP to every other access ISP?



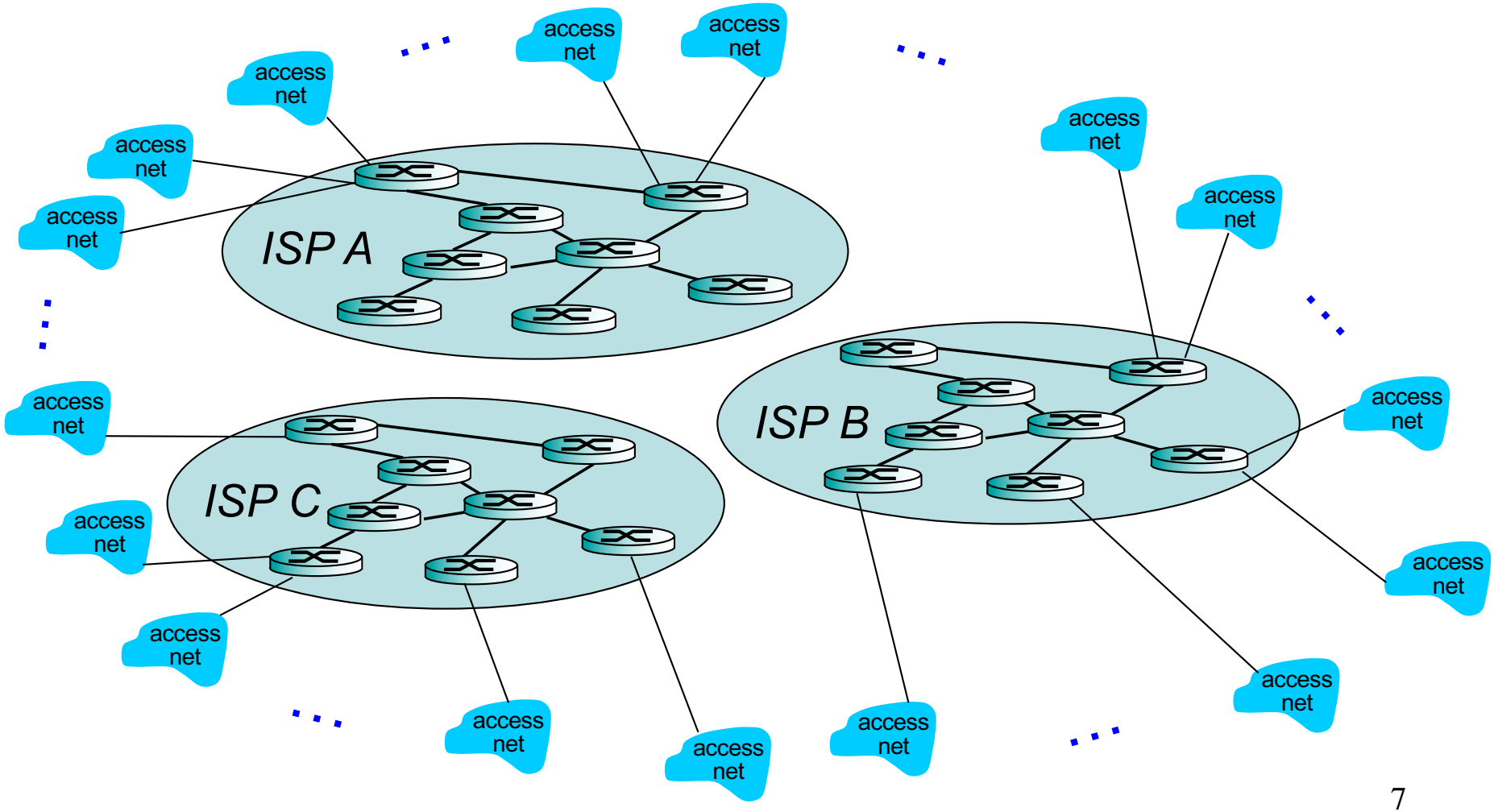
Internet structure: network of networks

Option: connect each access ISP to a global transit ISP?
Customer and provider ISPs have economic agreement.



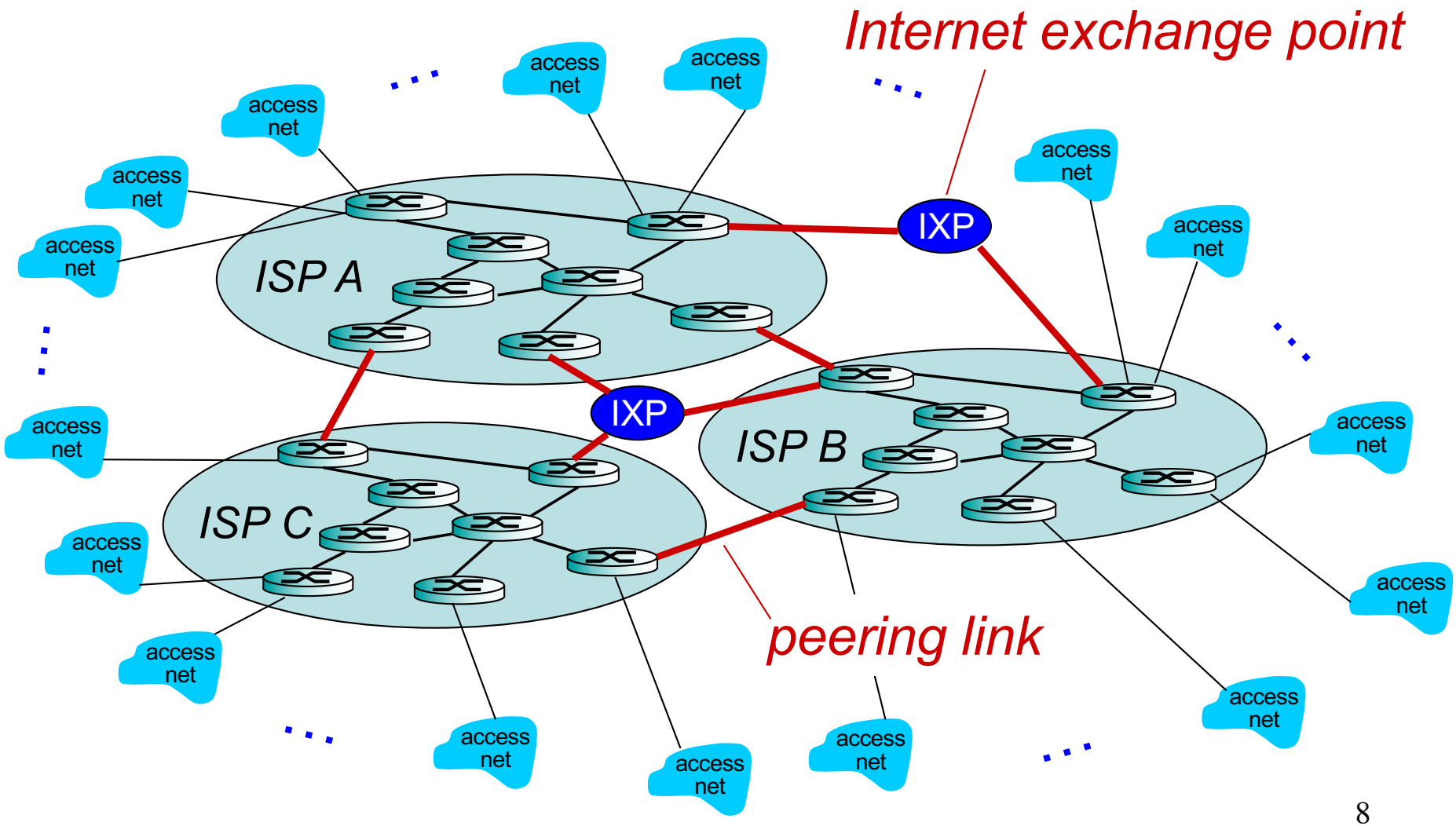
Internet structure: network of networks

But if one global ISP is viable business, there will be competitors ….



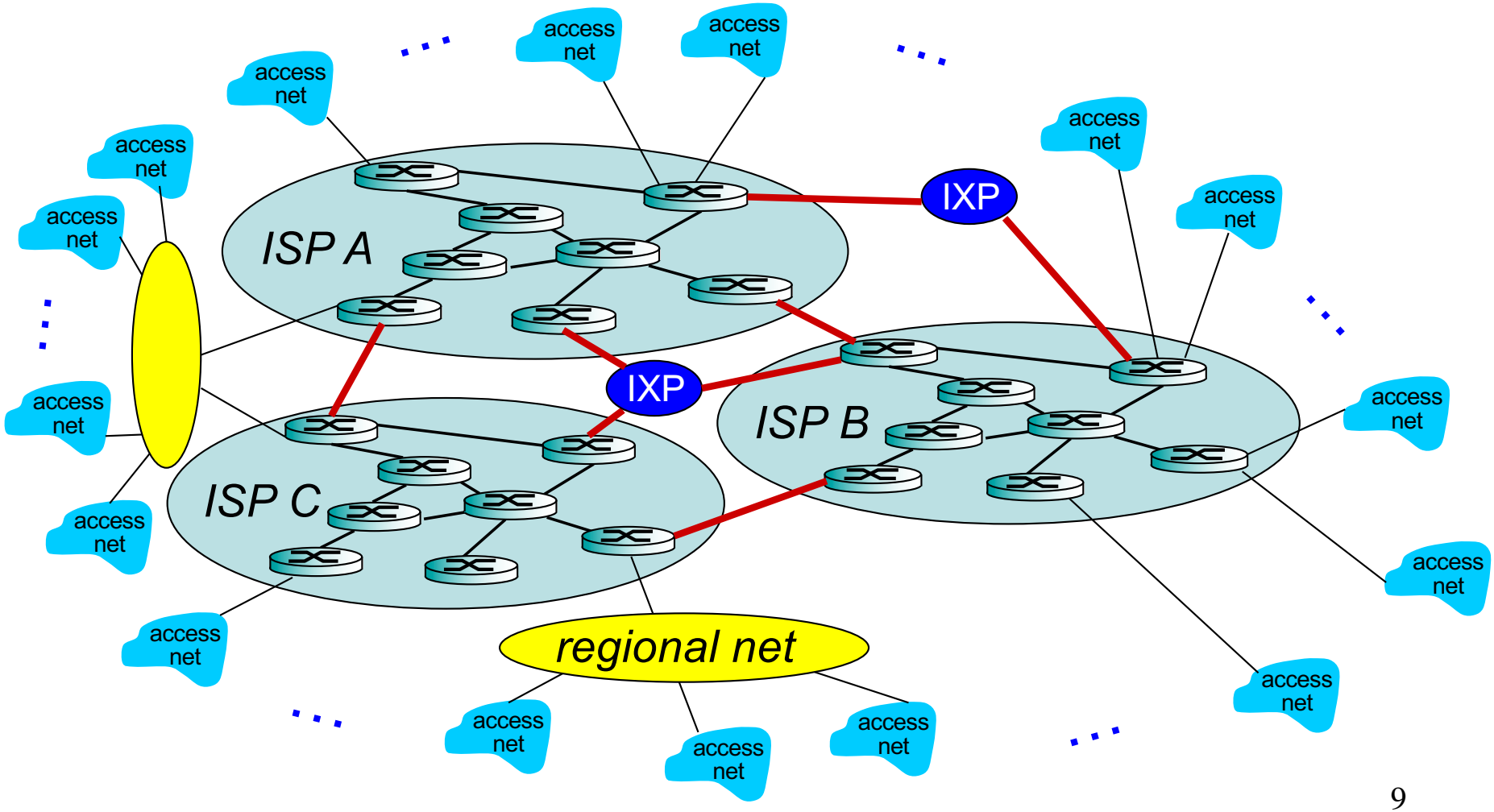
Internet structure: network of networks

But if one global ISP is viable business, there will be competitors …. which must be interconnected



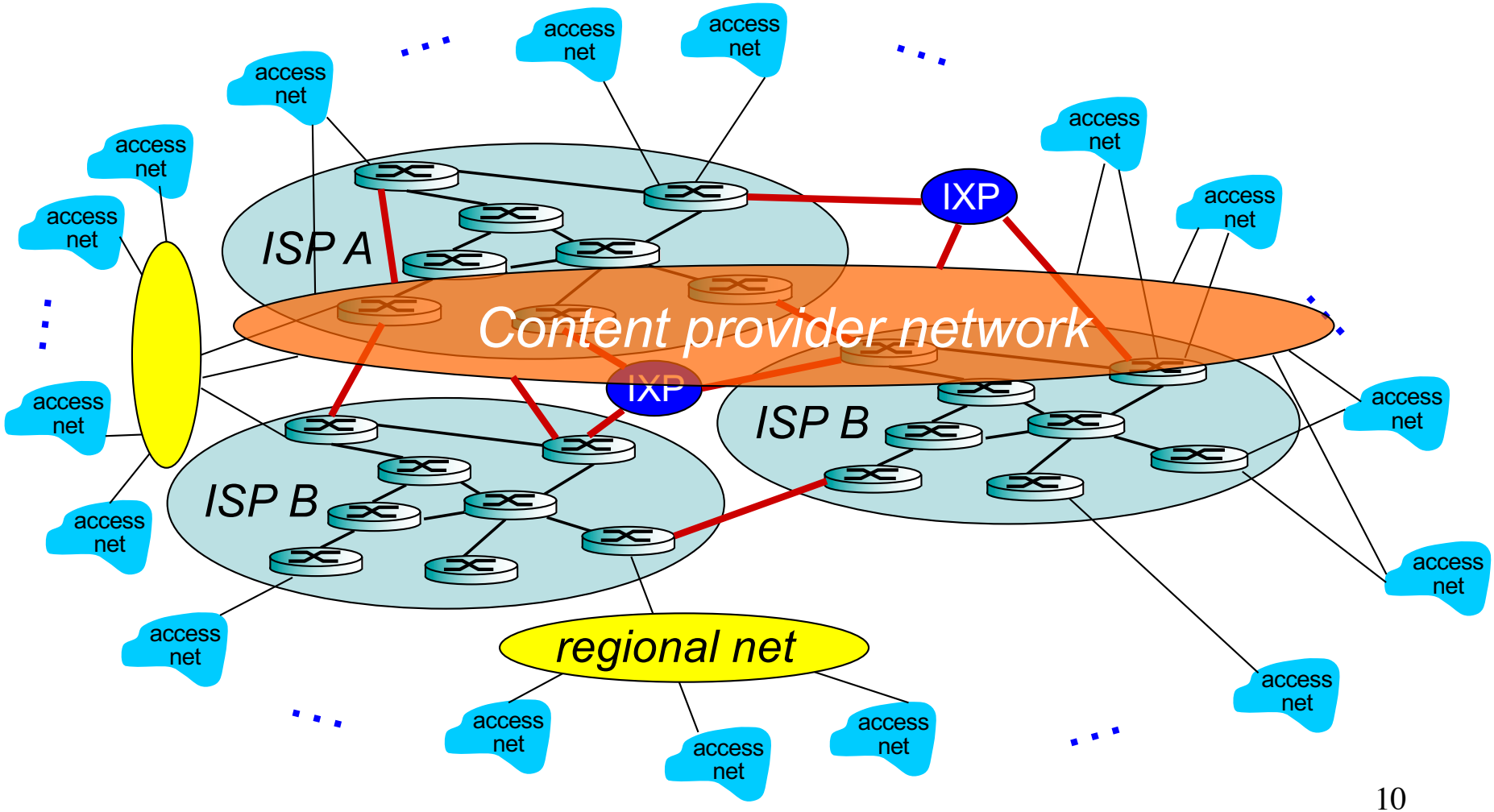
Internet structure: network of networks

… and regional networks may arise to connect access nets to ISPS

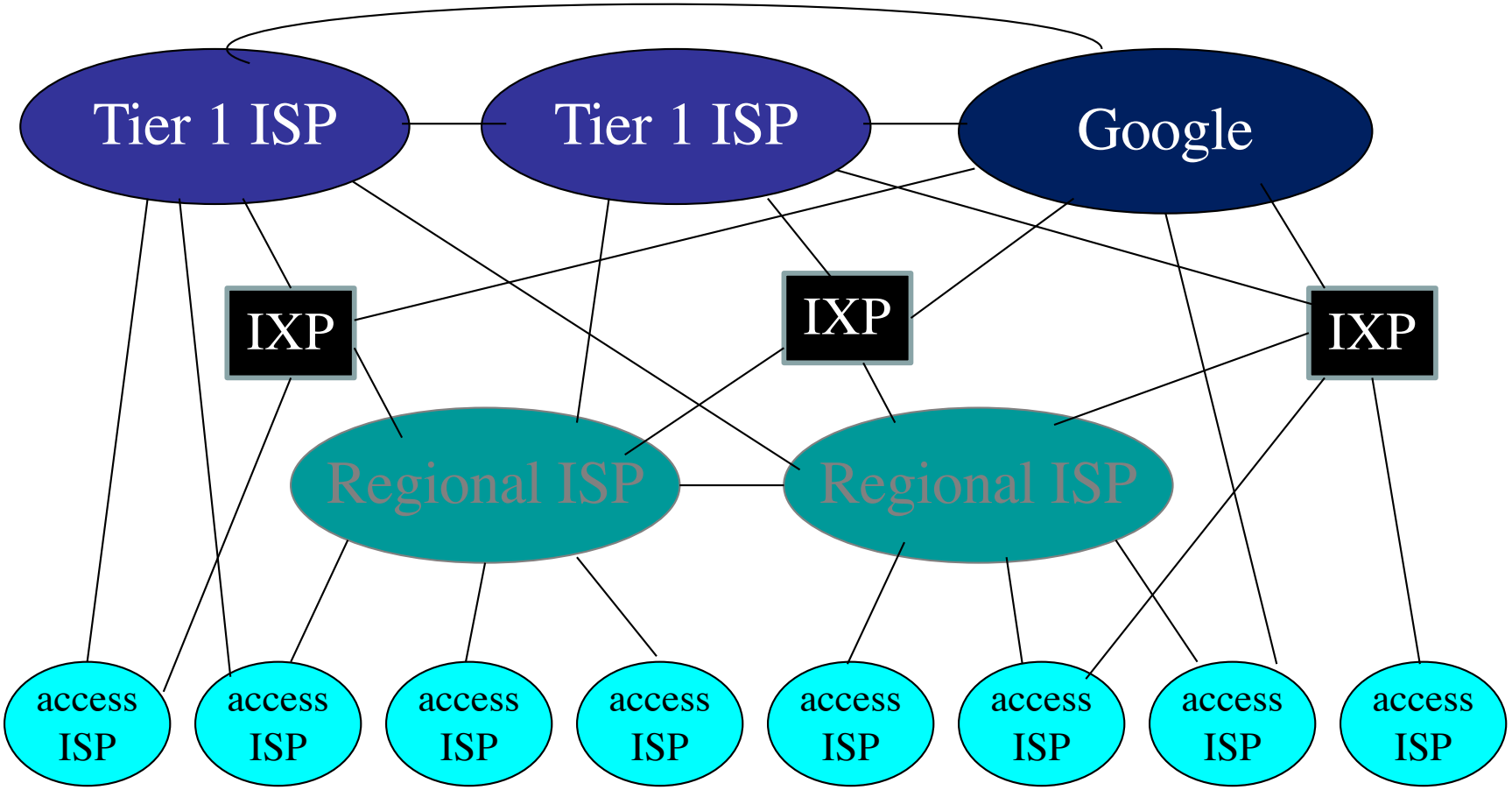


Internet structure: network of networks

… and content provider networks (e.g., Google, Microsoft, Akamai) may run their own network, to bring services, content close to end users

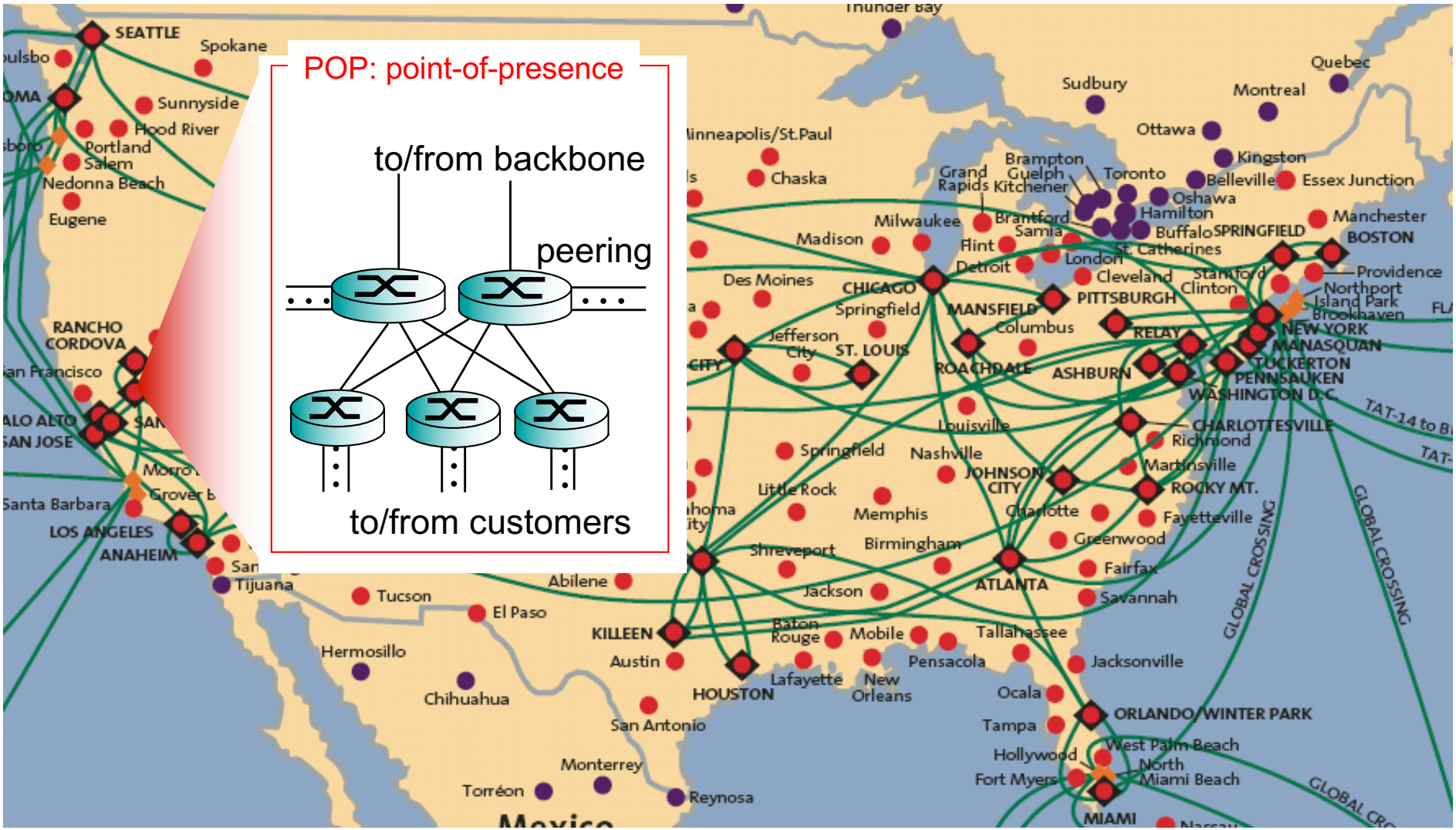


Internet structure: network of networks



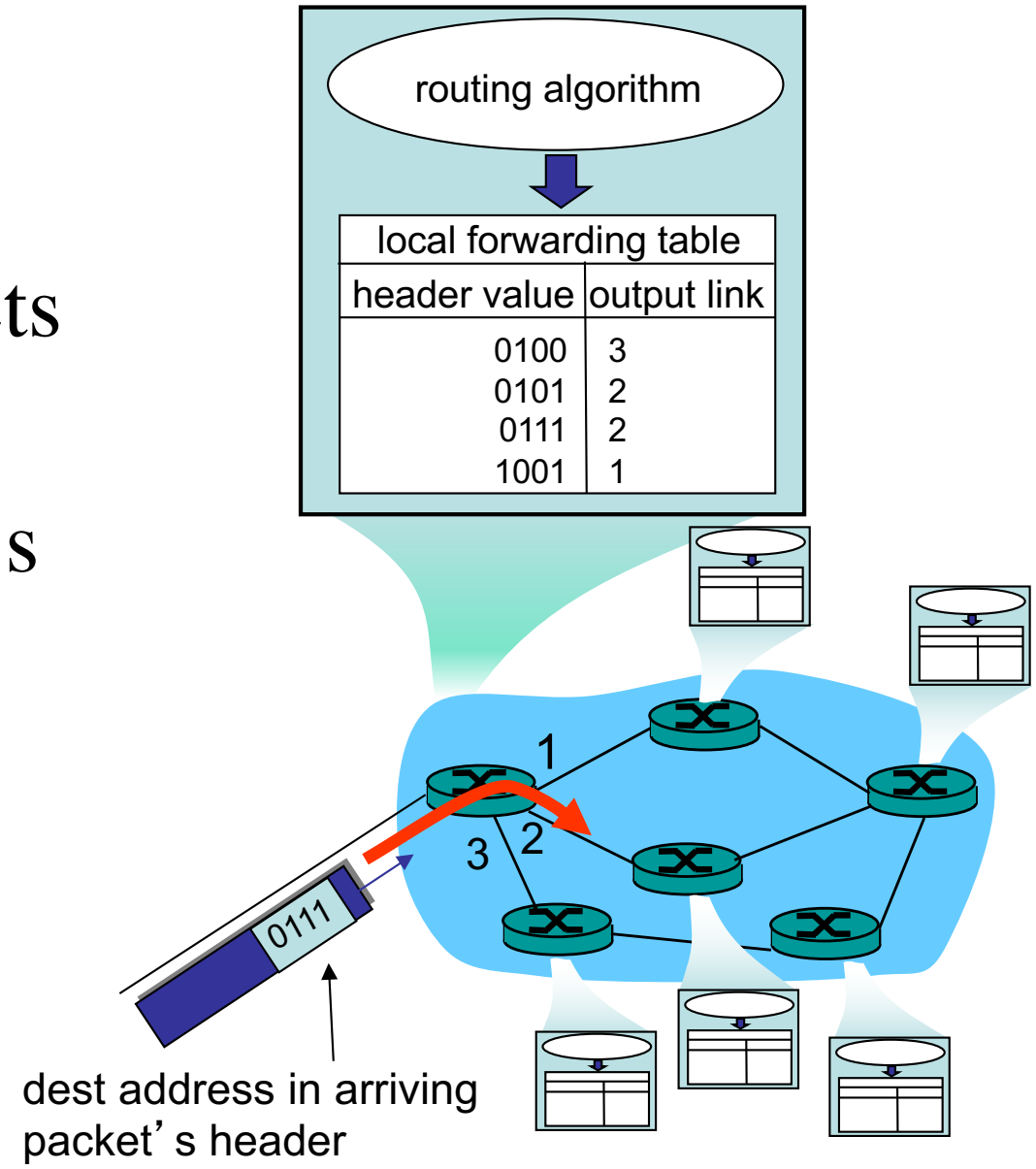
- at center: small # of well-connected large networks
  - "tier-1" commercial ISPs (e.g., Level 3, Sprint, AT&T, NTT), national & international coverage
  - content provider network (e.g, Google): private network that connects it data centers to Internet, often bypassing tier-1, regional ISPs

Tier-1 ISP: e.g., Sprint



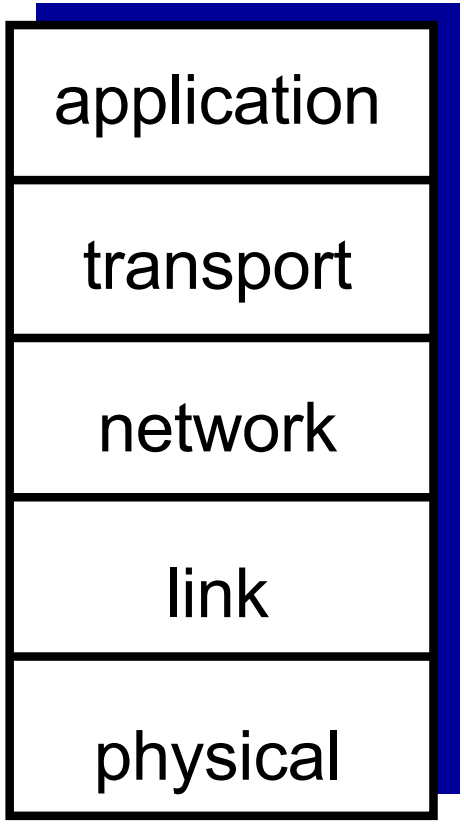
Two Key Network-Core Functions

- Routing: determines source-destination route taken by packets
- Forwarding: move packets from router's input to appropriate router output

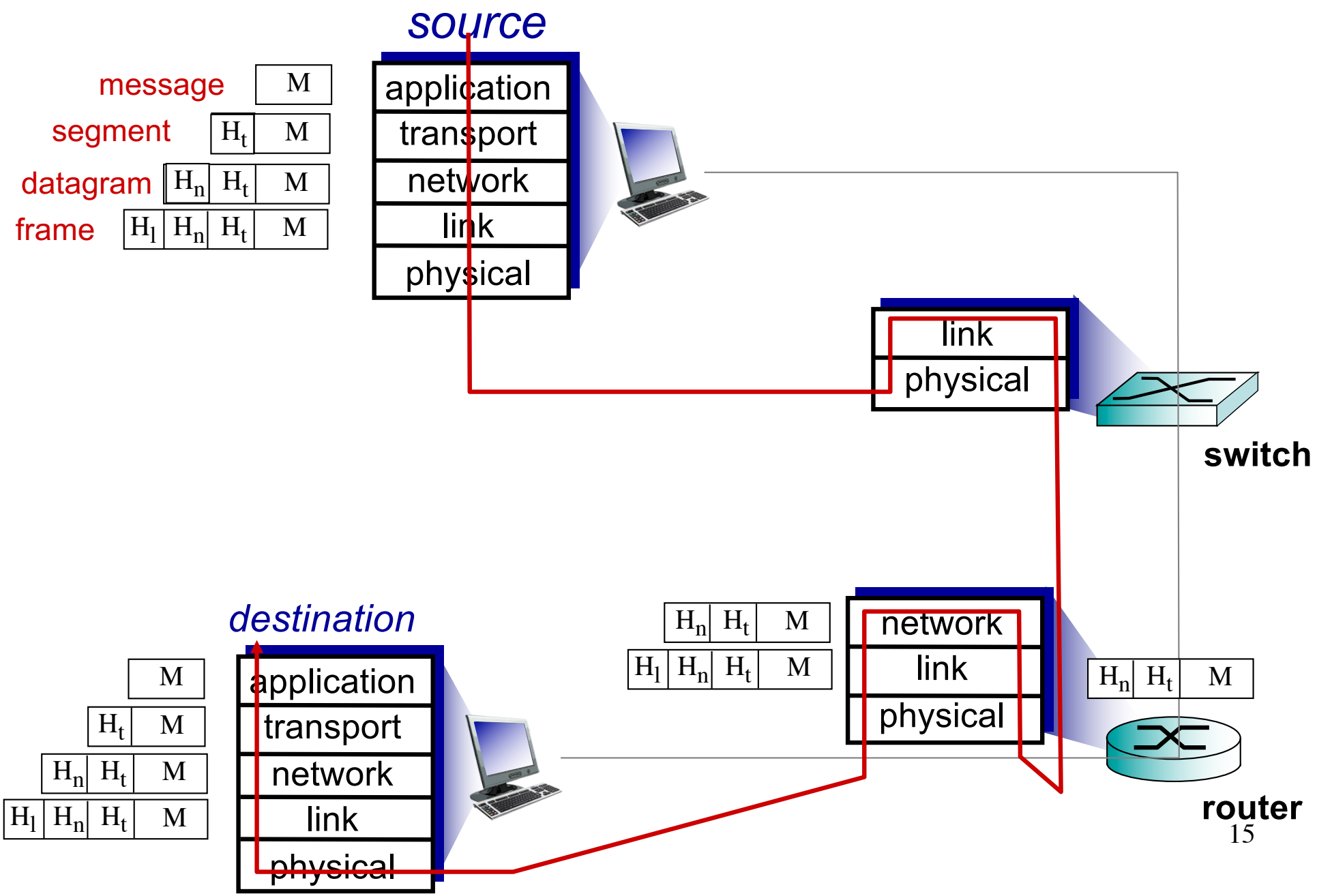


Internet protocol stack

- *application:* supporting network applications
  - FTP, SMTP, HTTP
- *transport:* process-process data transfer
  - TCP, UDP
- *network:* routing of datagrams from source to destination
  - IP, routing protocols
- *link:* data transfer between neighboring network elements
  - Ethernet, 802.111 (WiFi), PPP
- *physical:* bits "on the wire"



Message Delivery via Encapsulation



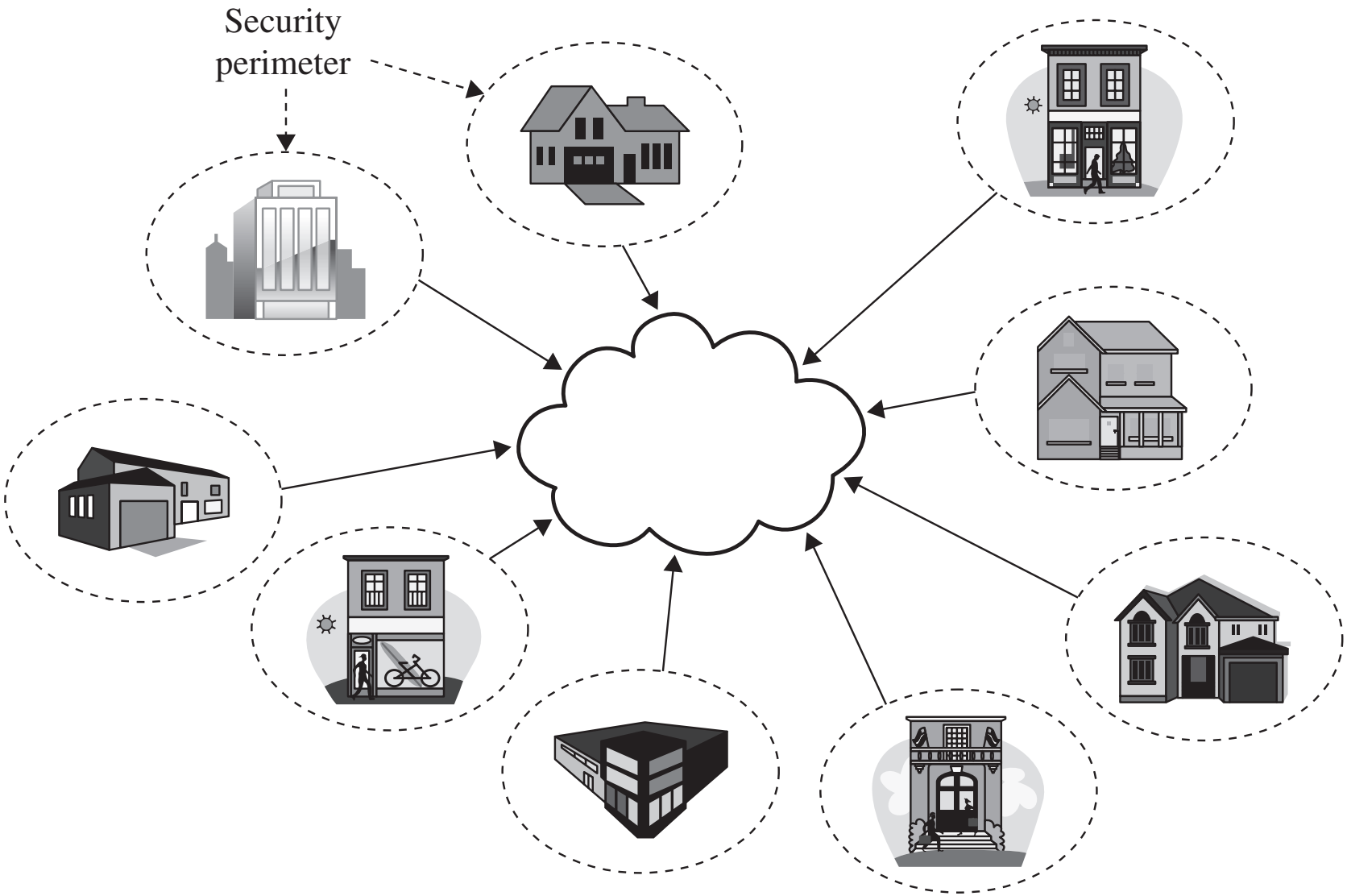
Threats to Network Communications

- *Interception*, or unauthorized viewing
- *Modification*, or unauthorized change
- *Fabrication*, or unauthorized creation
- *Interruption*, or preventing authorized access

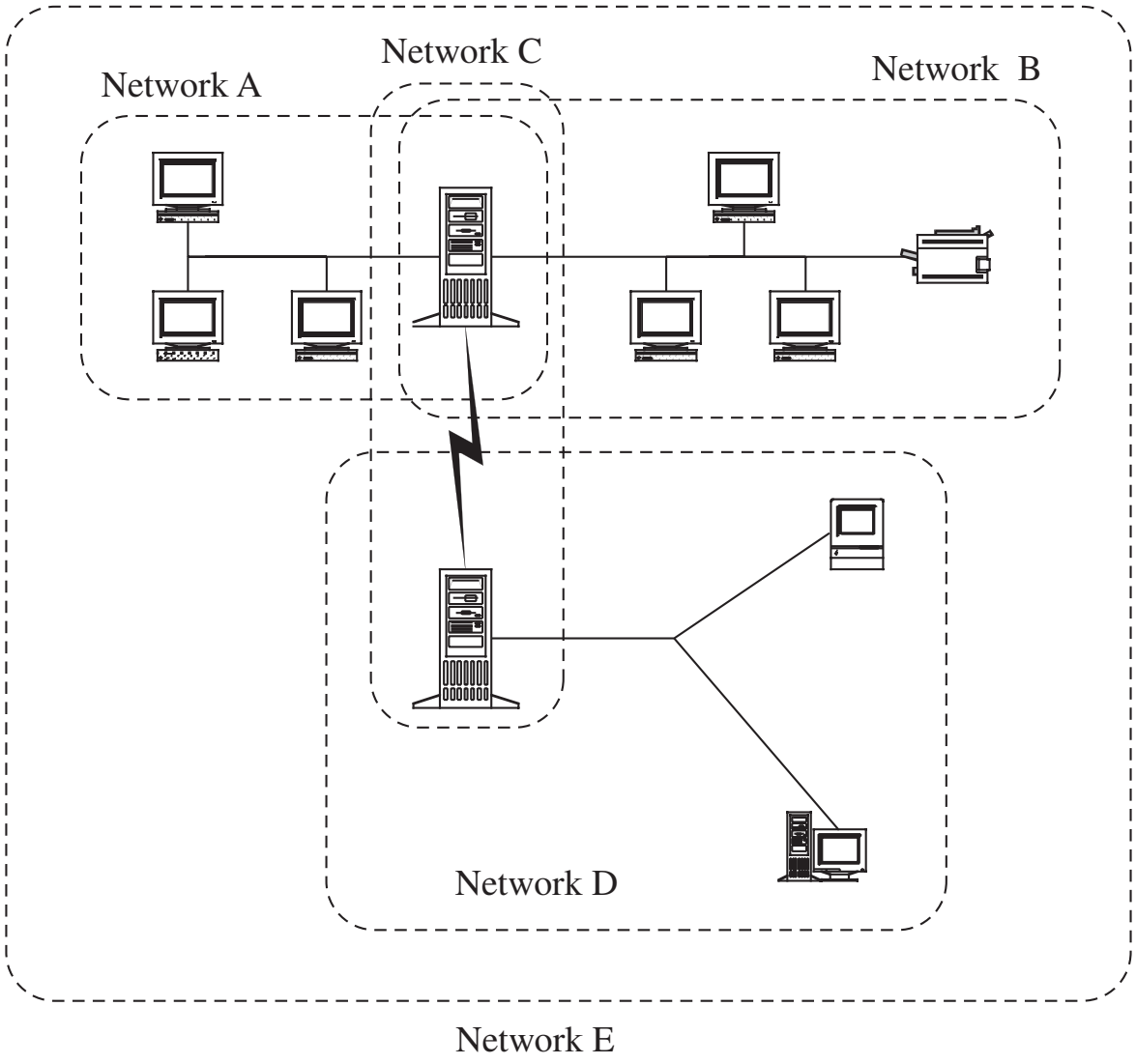
What Makes a Network Vulnerable to Interception?

- Anonymity
  - An attacker can attempt many attacks, anonymously, from thousands of miles away
- Many points of attack
  - Large networks mean many points of potential entry
- Sharing
  - Networked systems open up potential access to more users than do single computers
- System complexity
  - One system is very complex and hard to protect; networks of many different systems, with disparate OSs, vulnerabilities, and purposes are that much more complex
- Unknown perimeter
  - Networks, especially large ones, change all the time, so it can be hard to tell which systems belong and are behaving, and impossible to tell which systems bridge networks
- Unknown path
  - There may be many paths, including untrustworthy ones, from one host to another

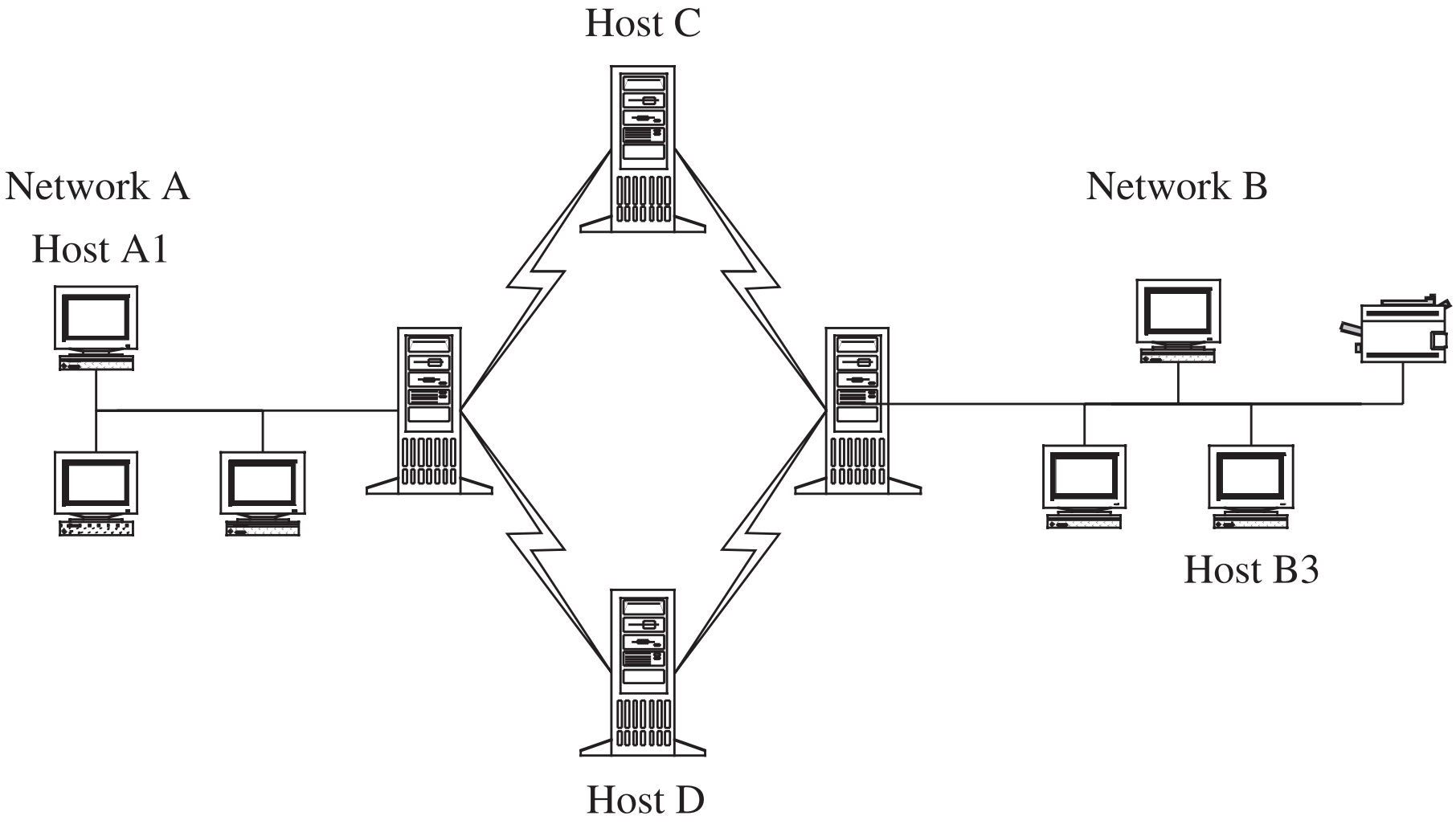
Security Perimeters



Unknown Perimeter



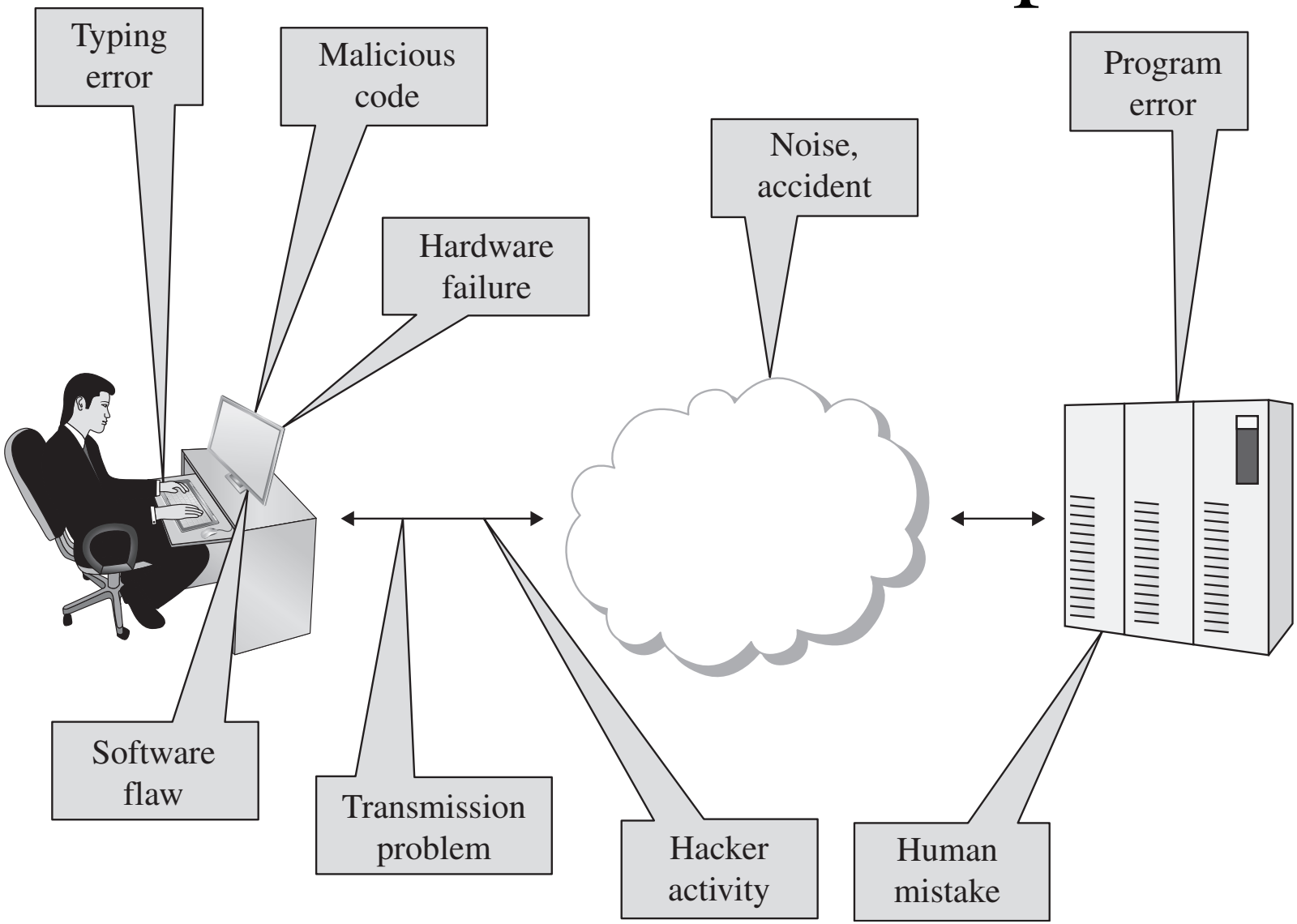
Unknown Path



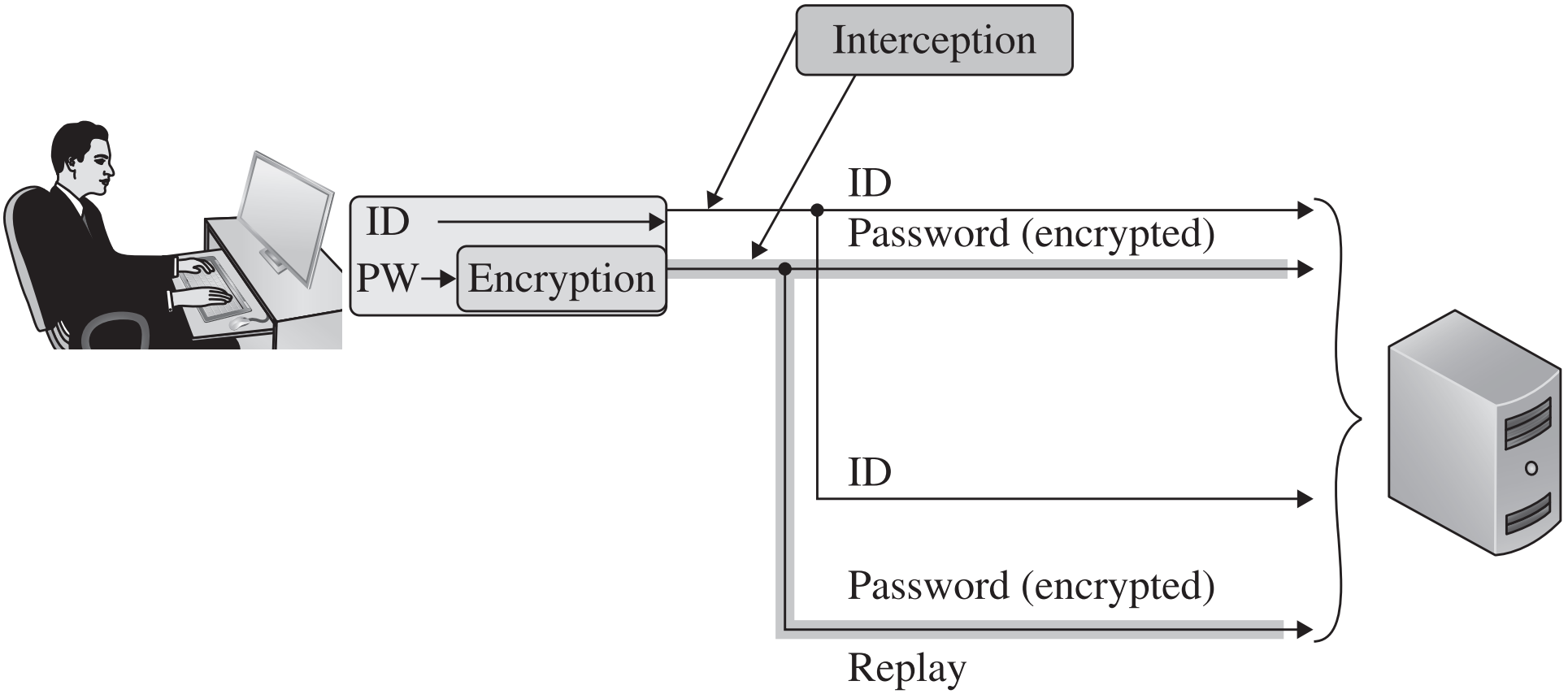
Modification and Fabrication

- Data corruption
  - May be intentional or unintentional, malicious or non-malicious, directed or random
- Sequencing
  - Permuting the order of data
- Substitution
  - Replacement of one piece of a data stream with another
- Insertion
  - A form of substitution in which data values are inserted into a stream
- Replay
  - Legitimate data are intercepted and reused

Sources of Data Corruption



Simple Replay Attack



Interruption: Loss of Service

- Routing
  - Internet routing protocols are complicated, and one misconfiguration can poison the data of many routers
- Excessive demand
  - Network capacity is finite and can be exhausted; an attacker can generate enough demand to overwhelm a critical part of a network
- Component failure
  - Component failures tend to be sporadic and unpredictable, and will cause loss of service if not planned for

Port Scanning

```
Nmap scan report
192.168.1.1 / somehost.com (online) ping results
address: 192.168.1.1 (ipv4)
hostnames: somehost.com (user)
The 83 ports scanned but not shown below are in state: closed
Port       State      Service Reason       Product  Version  Extra info
21   tcp   open       ftp     syn-ack      ProFTPD  1.3.1
22   tcp   filtered   ssh     no-response
25   tcp   filtered   smtp    no-response
80   tcp   open       http    syn-ack      Apache   2.2.3    (CentOS)
106  tcp   open       pop3pw  syn-ack      poppassd
110  tcp   open       pop3    syn-ack      Courier pop3d
111  tcp   filtered   rpcbind no-response
113  tcp   filtered   auth    no-response
143  tcp   open        imap    syn-ack      Courier Imapd       released
2004
443  tcp   open       http    syn-ack      Apache  2.2.3       (CentOS)
465  tcp   open       unknown syn-ack
646  tcp   filtered   ldp     no-response
993  tcp   open       imap    syn-ack      Courier Imapd       released
2004
995  tcp   open                syn-ack
2049 tcp   filtered   nfs     no-response
3306 tcp   open       mysql   syn-ack      MySQL   5.0.45
8443 tcp   open       unknown syn-ack
34 sec. scanned
1 host(s) scanned
1 host(s) online
0 host(s) offline
```

Vulnerabilities in Wireless Networks

- Confidentiality
- Integrity
- Availability
- Unauthorized WiFi access
- WiFi protocol weaknesses
  - Picking up the beacon
  - SSID in all frames
  - Association issues

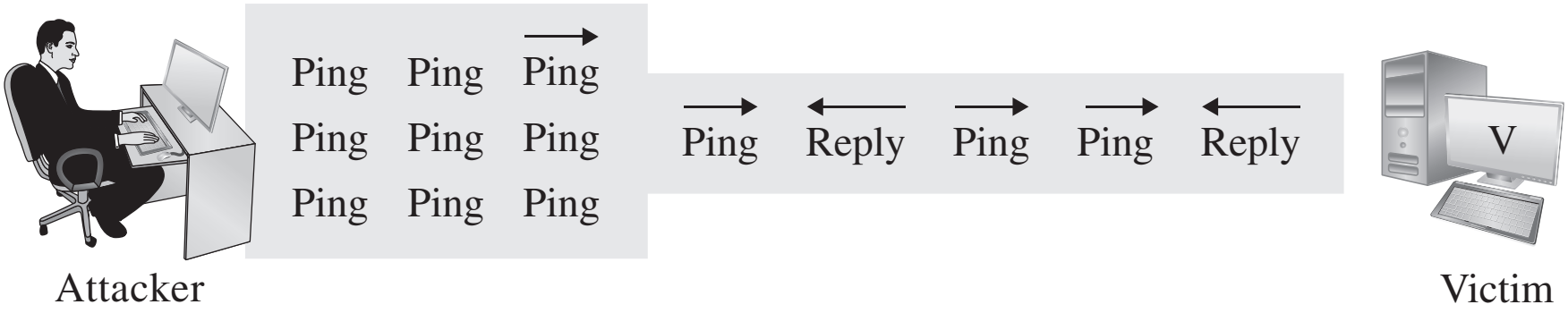
WEP, WPA, WPA2

- Wired equivalent privacy, or WEP, was designed at the same time as the original 802.11 WiFi standards as the mechanism for securing those communications
- Weaknesses in WEP were first identified in 2001, four years after release
- WPA (WiFi Protected Access) was designed in 2003 as a replacement for WEP and was quickly followed in 2004 by WPA2, the algorithm that remains the standard today

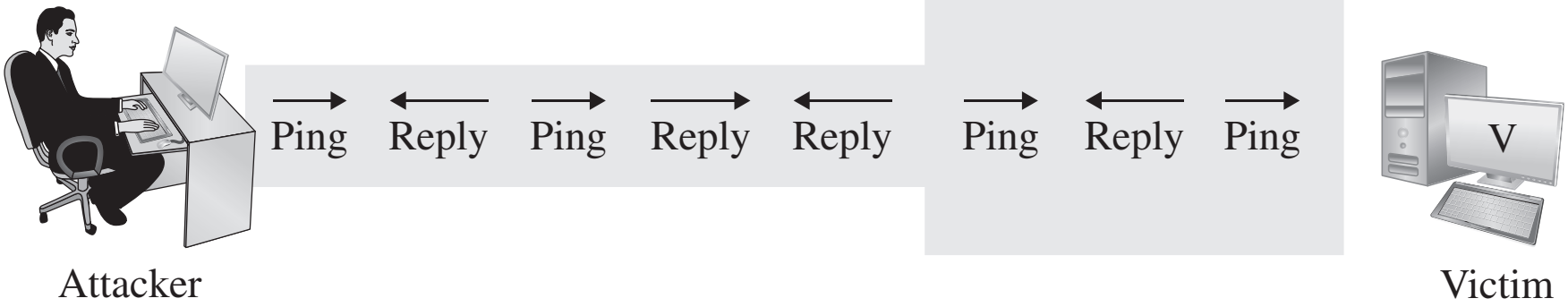
Denial of Service (DoS)

- DoS attacks are attempts to defeat a system's availability
- Volumetric attacks
- Application-based attacks
- Disabled communications
- Hardware or software failure

DoS Attack: Ping Flood

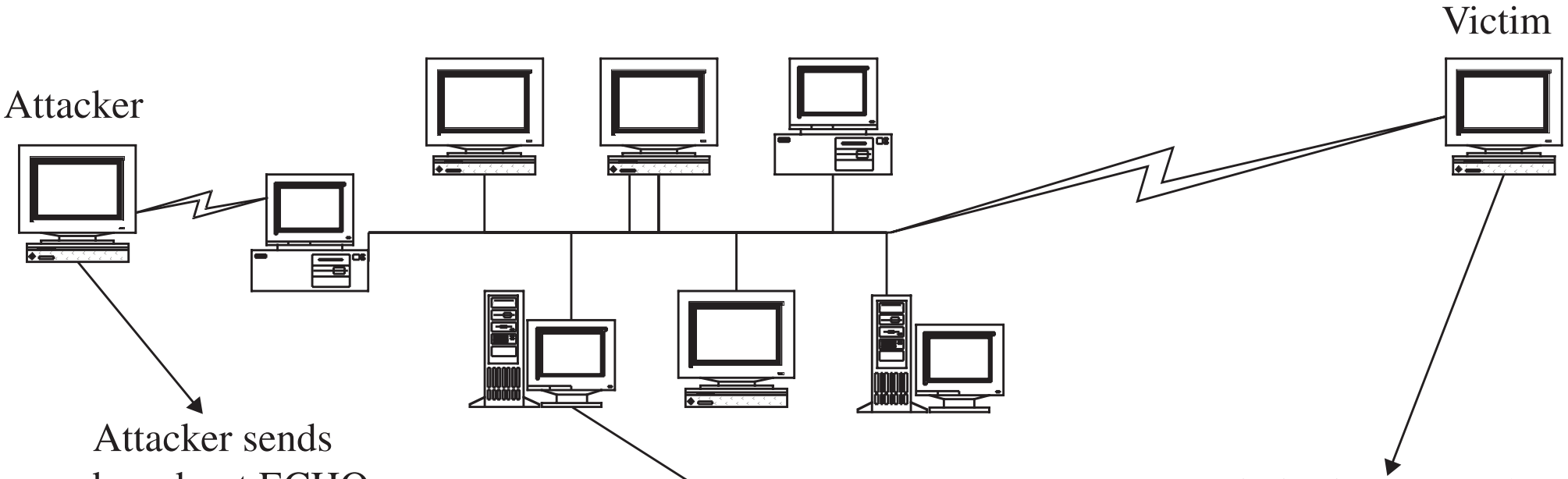


(a) Attacker has greater bandwidth

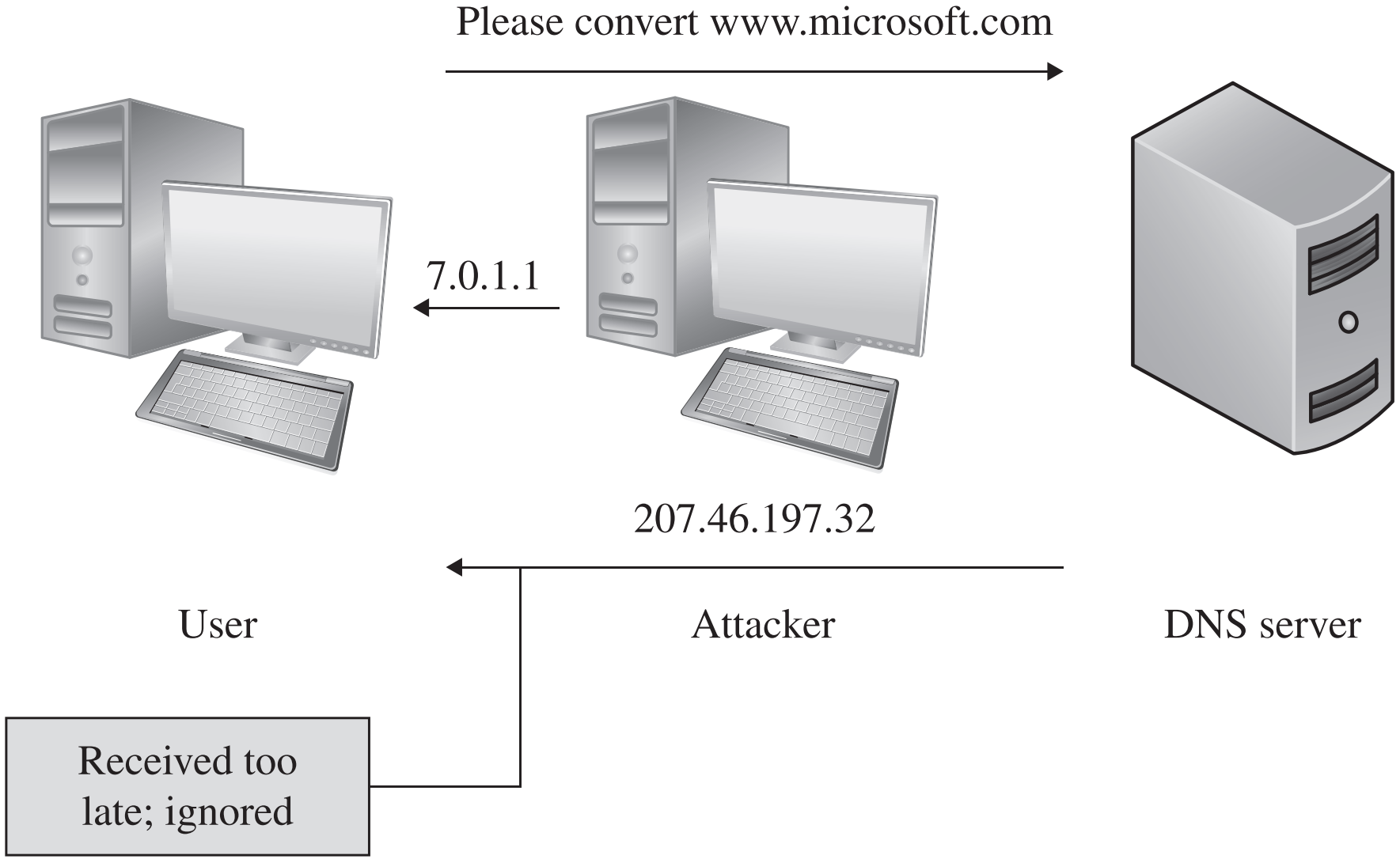


(b) Victim has greater bandwidth

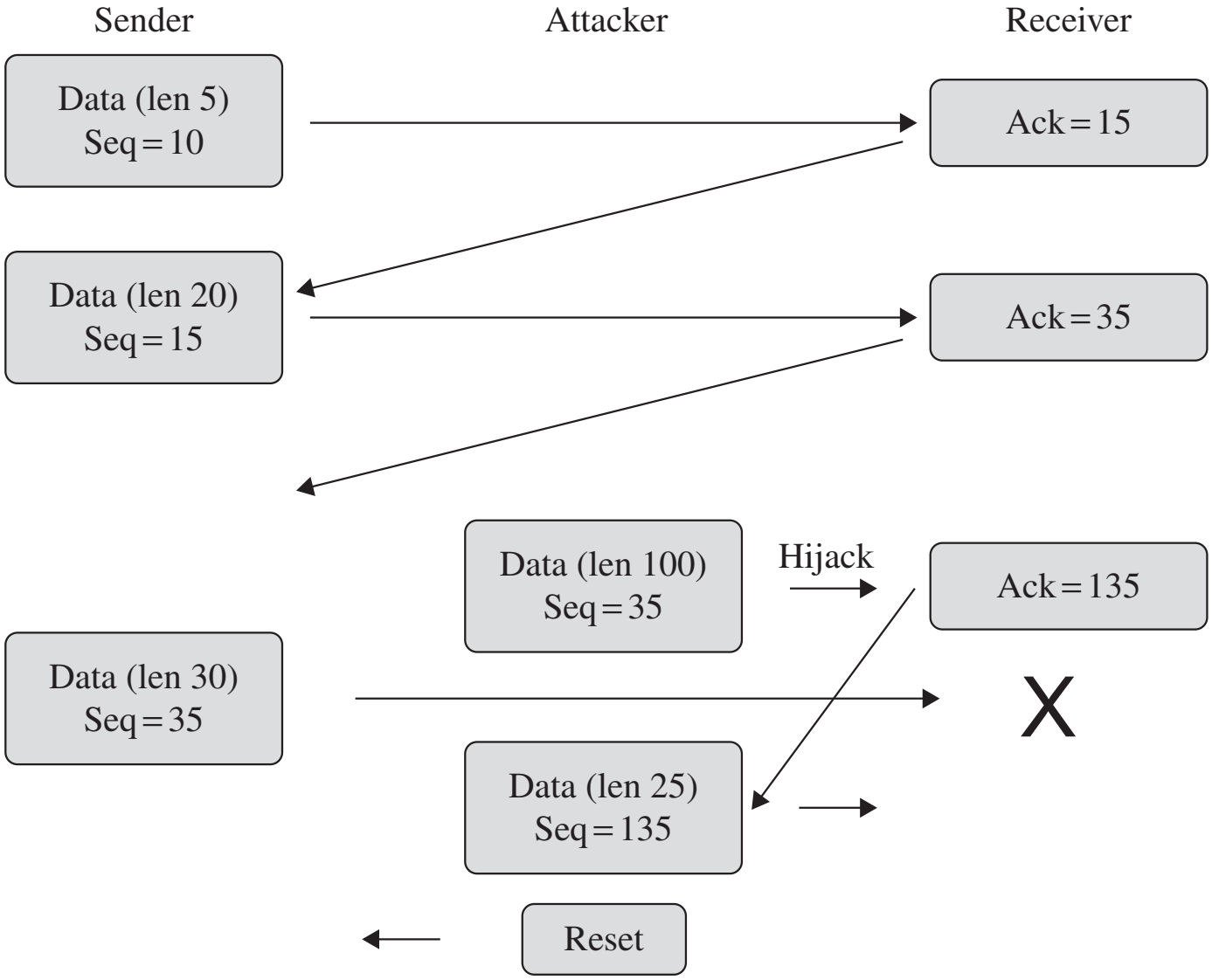
DoS Attack: Smurf Attack



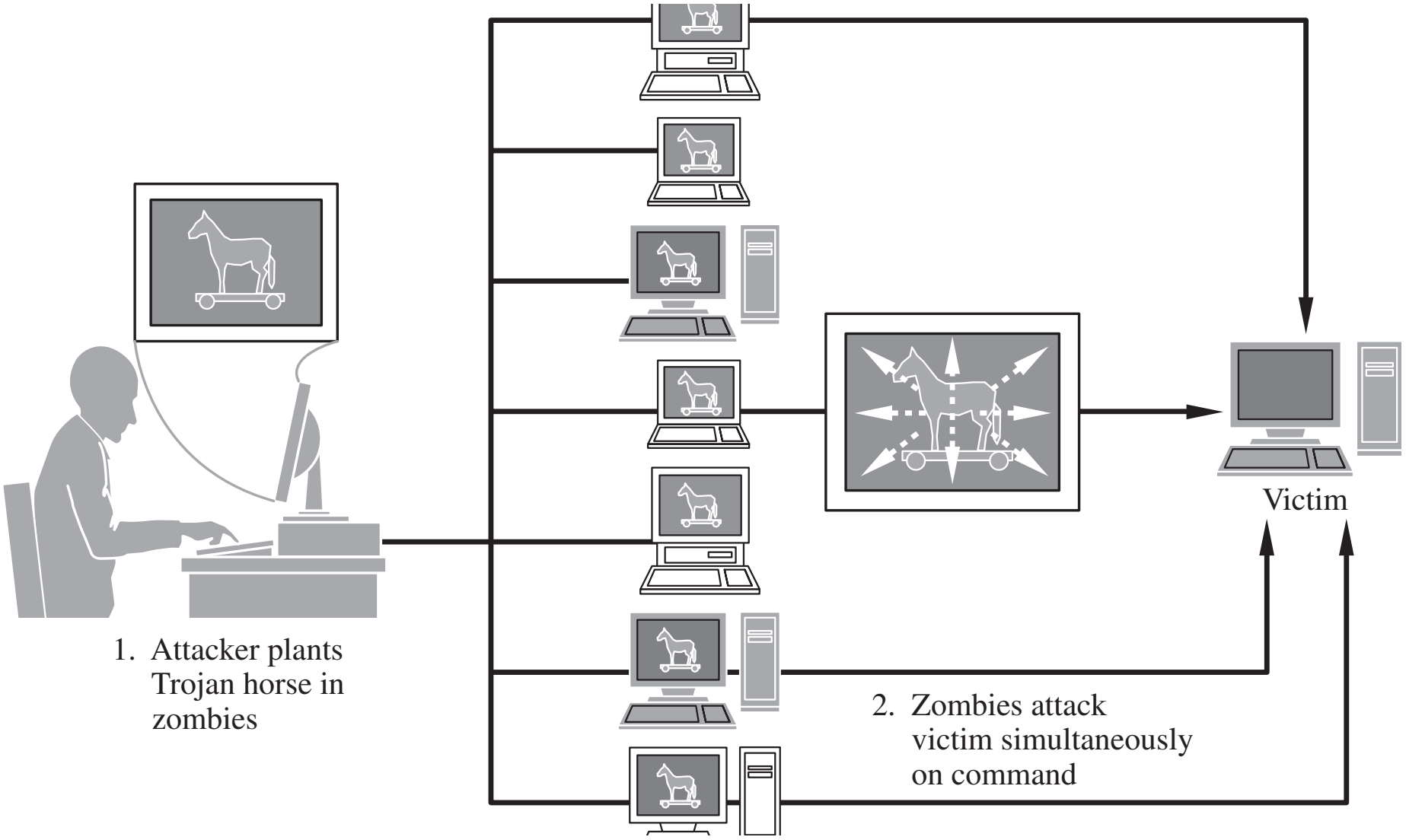
DoS Attack: DNS Spoofing



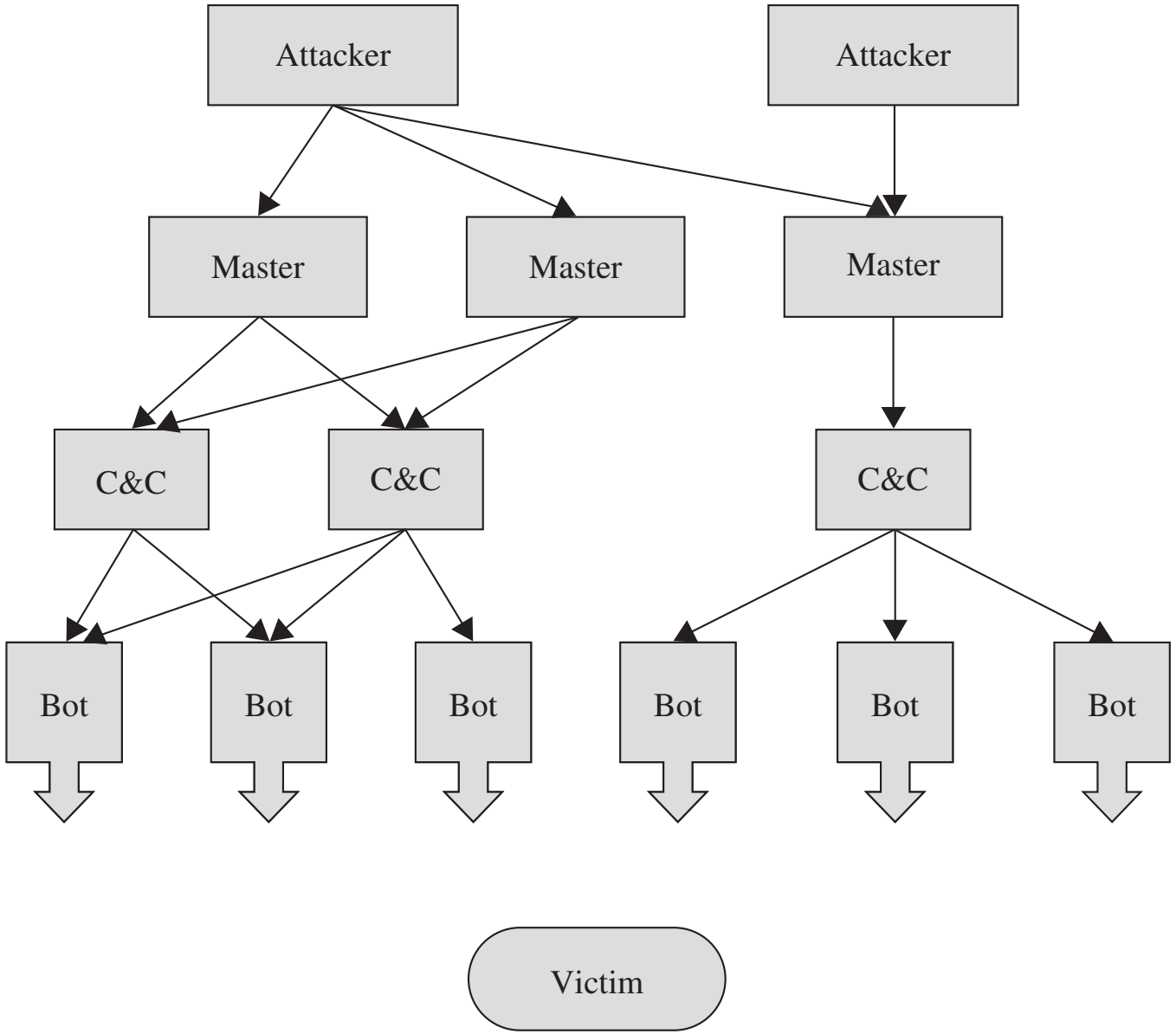
DoS Attack: Session Hijacking



Distributed Denial of Service (DDoS)



Botnets


Attacker
Attacker
Master
Master
Master
C&C
C&C
C&C
Bot
Bot
Bot
Bot
Bot
Bot
Victim