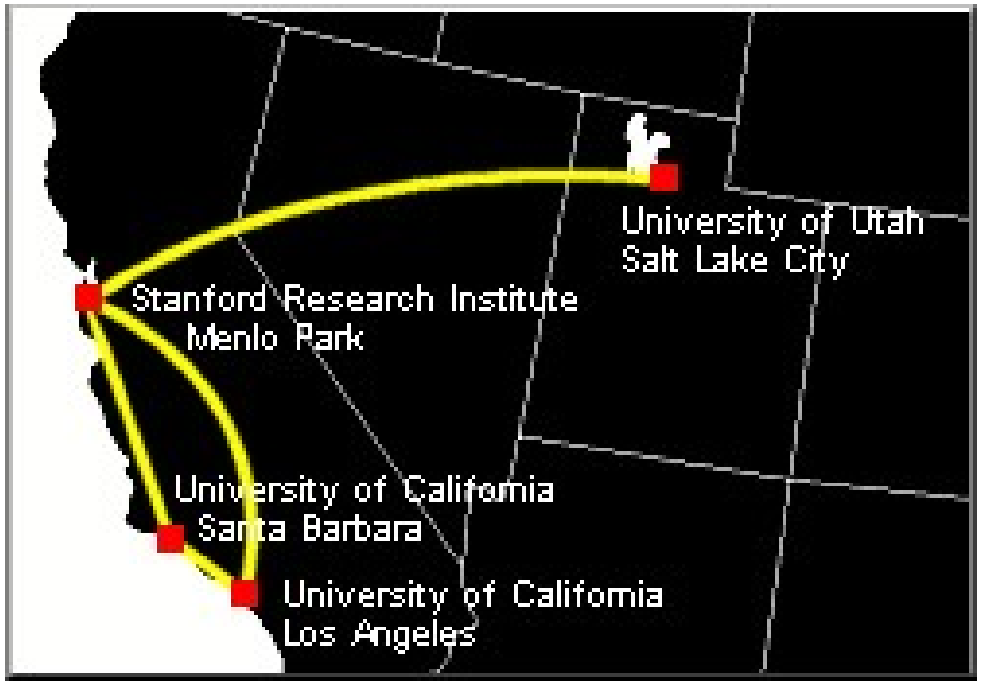
Chapter 15

Networks – Part 2



ARPANet in 1969

Internet Standards and RFCs

- **Internet Architecture Board** (IAB)
  - overall architecture
- **Internet Engineering Task Force** (IETF)
  - engineering and development
- **Internet Engineering Steering Group** (IESG)
  - manages the IETF and standards process

Request For Comments (RFC)

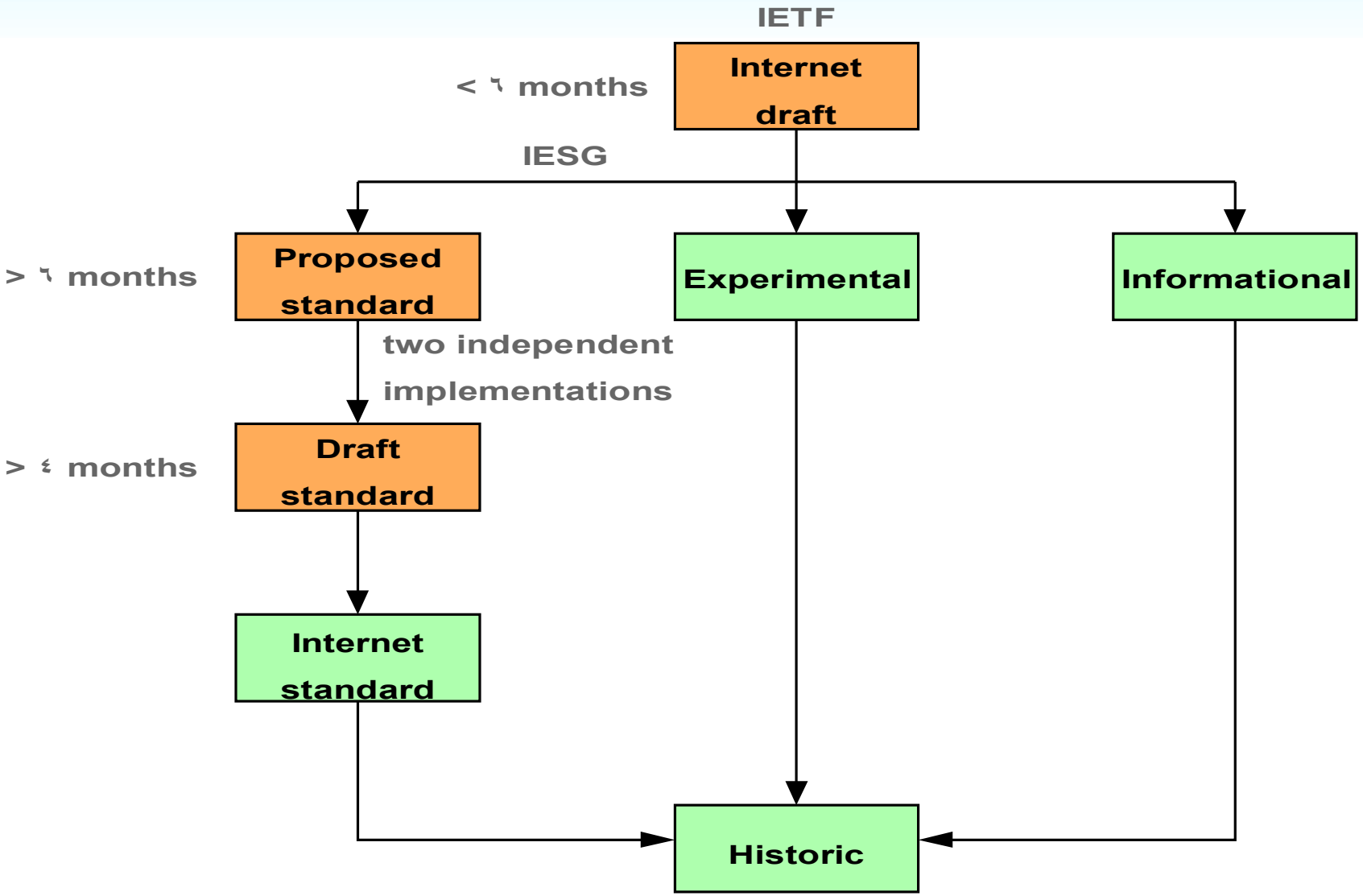
- **RFCs** are the working notes of the Internet research and development community

Standardization Process

- Stable and well understood
- Technically competent
- Substantial operational experience
- Significant public support
- Useful in some or all parts of Internet

Key difference from ISO: **operational experience**

RFC Publication Process



How To Find RFCs

- http://www.rfc-editor.org/rfcsearch.html
  - Search for RFCs
- Some Popular Ones:
-

Modern Life In Cyberspace…

- http://www.aclu.org/pizza/images/screer

…All I Wanted Was A Pizza!

Introduction to Network Security

Security Attacks

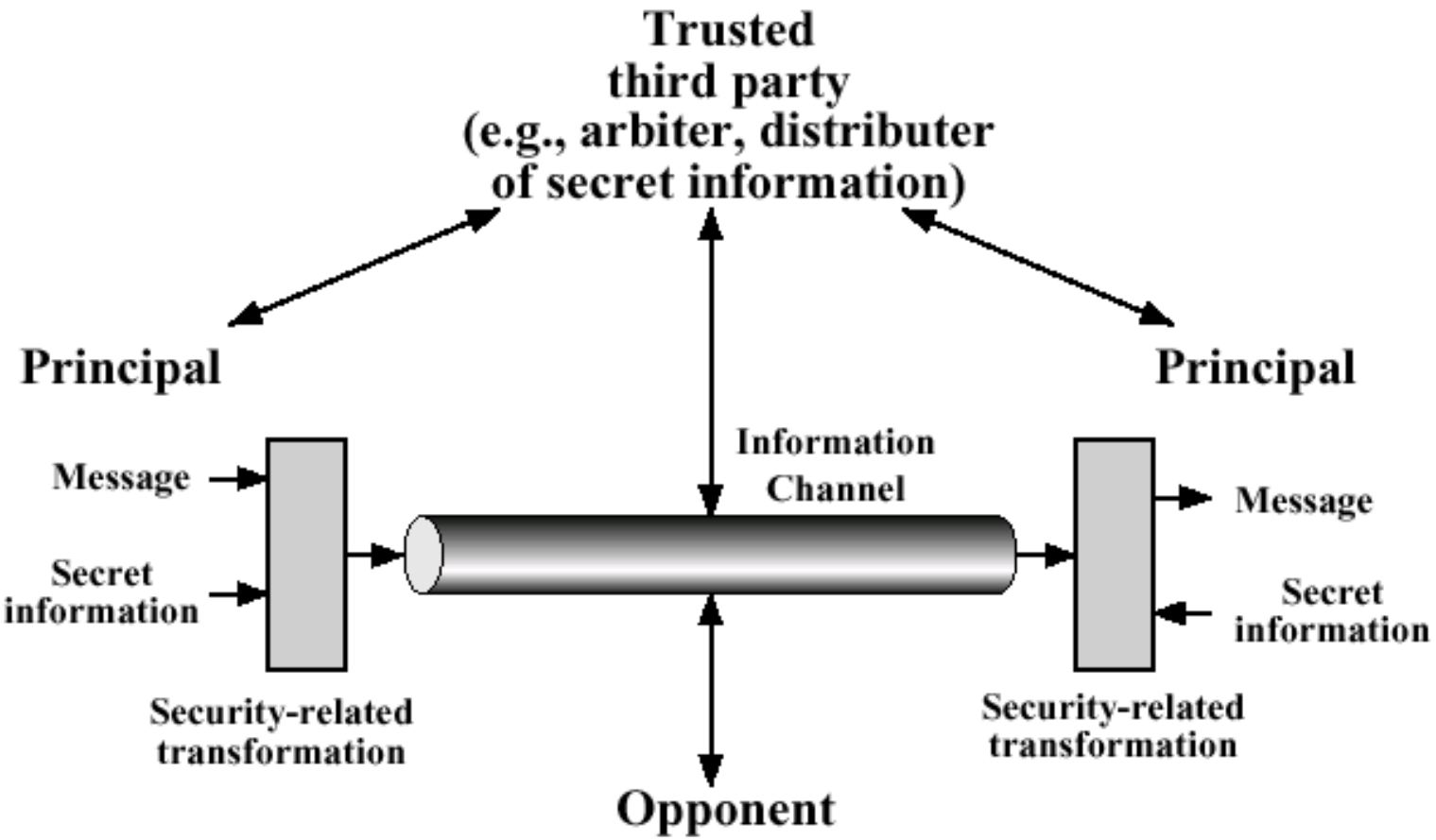
Security Services

- **Confidentiality** – protection from passive attacks
- **Authentication** – you are who you say you are
- **Integrity** – received as sent, no modifications, insertions, shuffling or replays

Security Services

- Nonrepudiation – can’t deny a message was sent or received
- Access Control – ability to limit and control access to host systems and apps
- Availability – attacks affecting loss or reduction on availability

Network Security Model



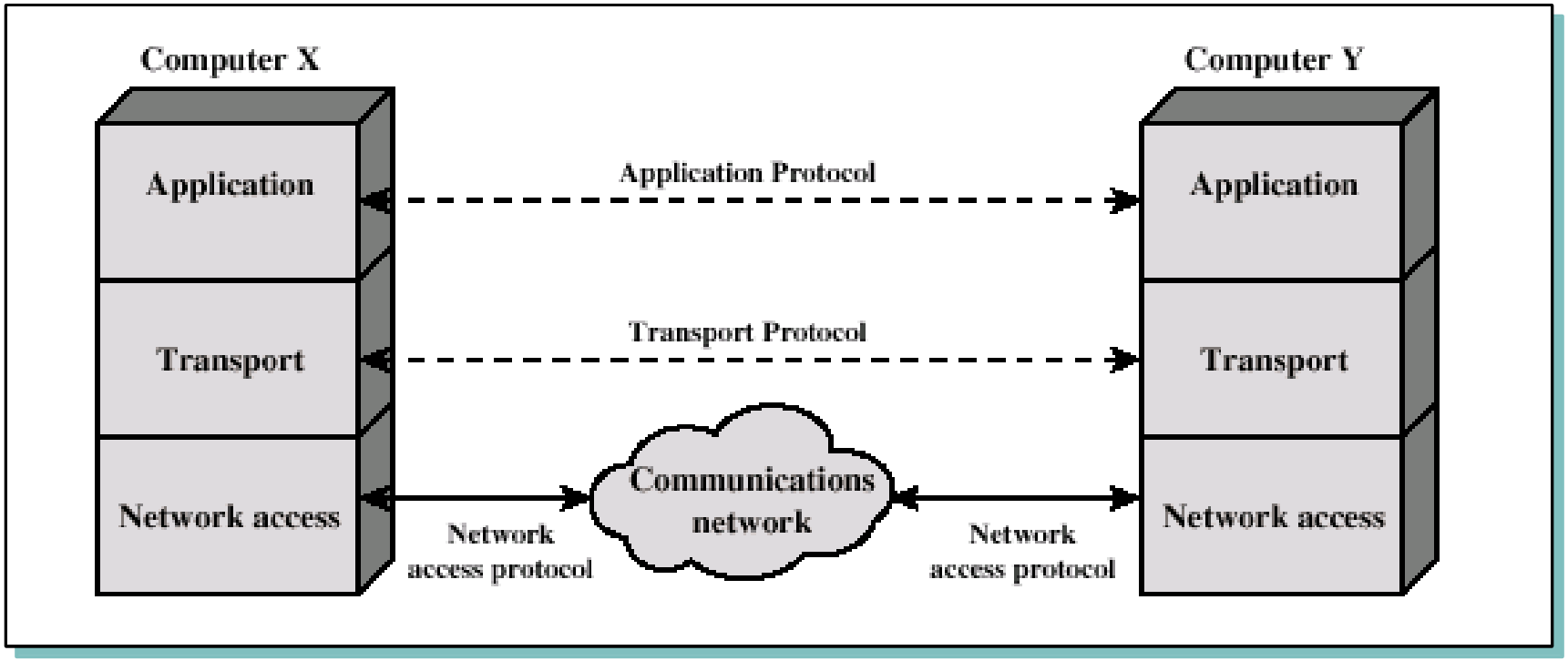
Network Security Model

Four basic tasks in designing a security service:

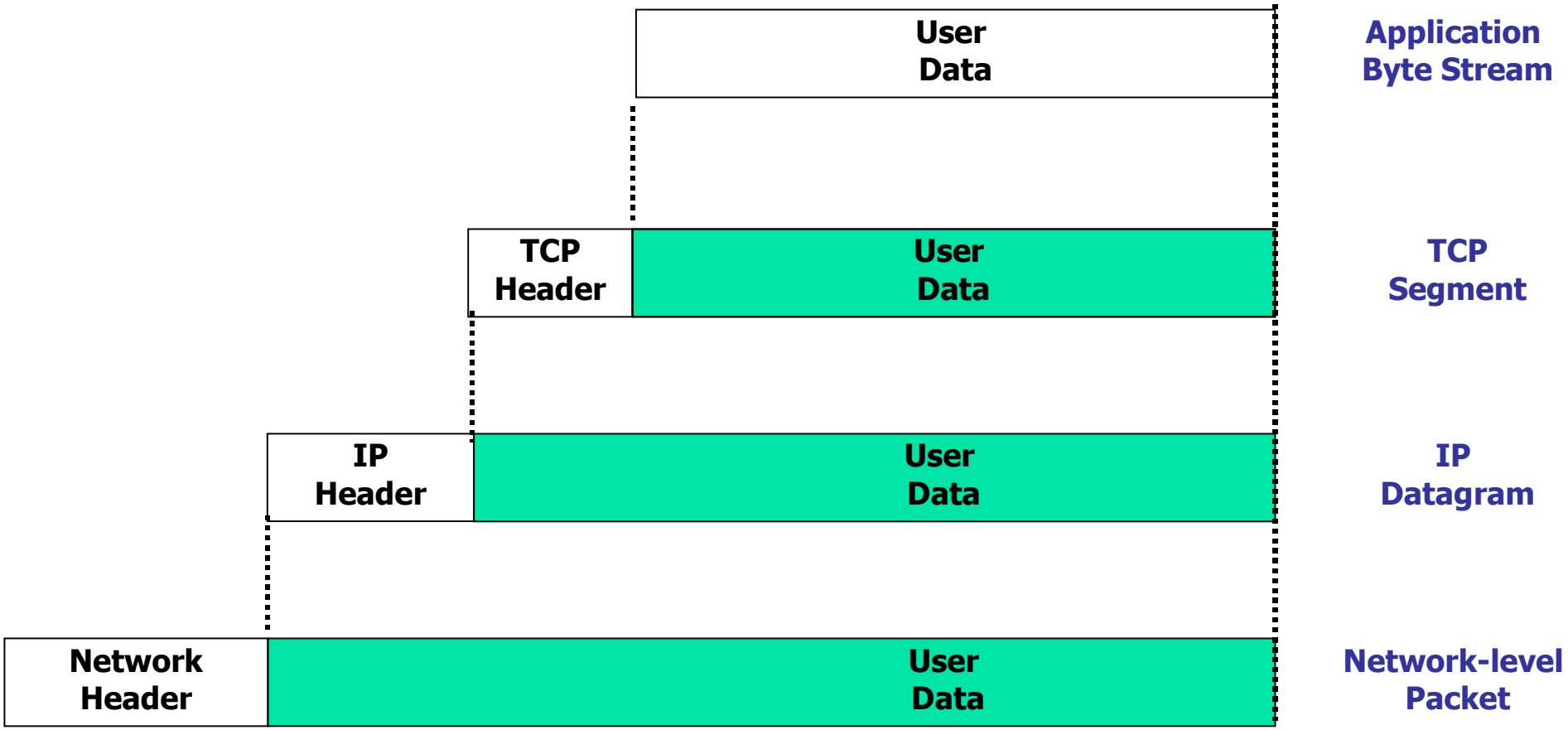
- **Design** algorithm
- **Generate** secret information to be used
- Develop methods to **distribute** and share info
- Specify a **protocol** to be used by the two principals

Protocols – Simple To Complex

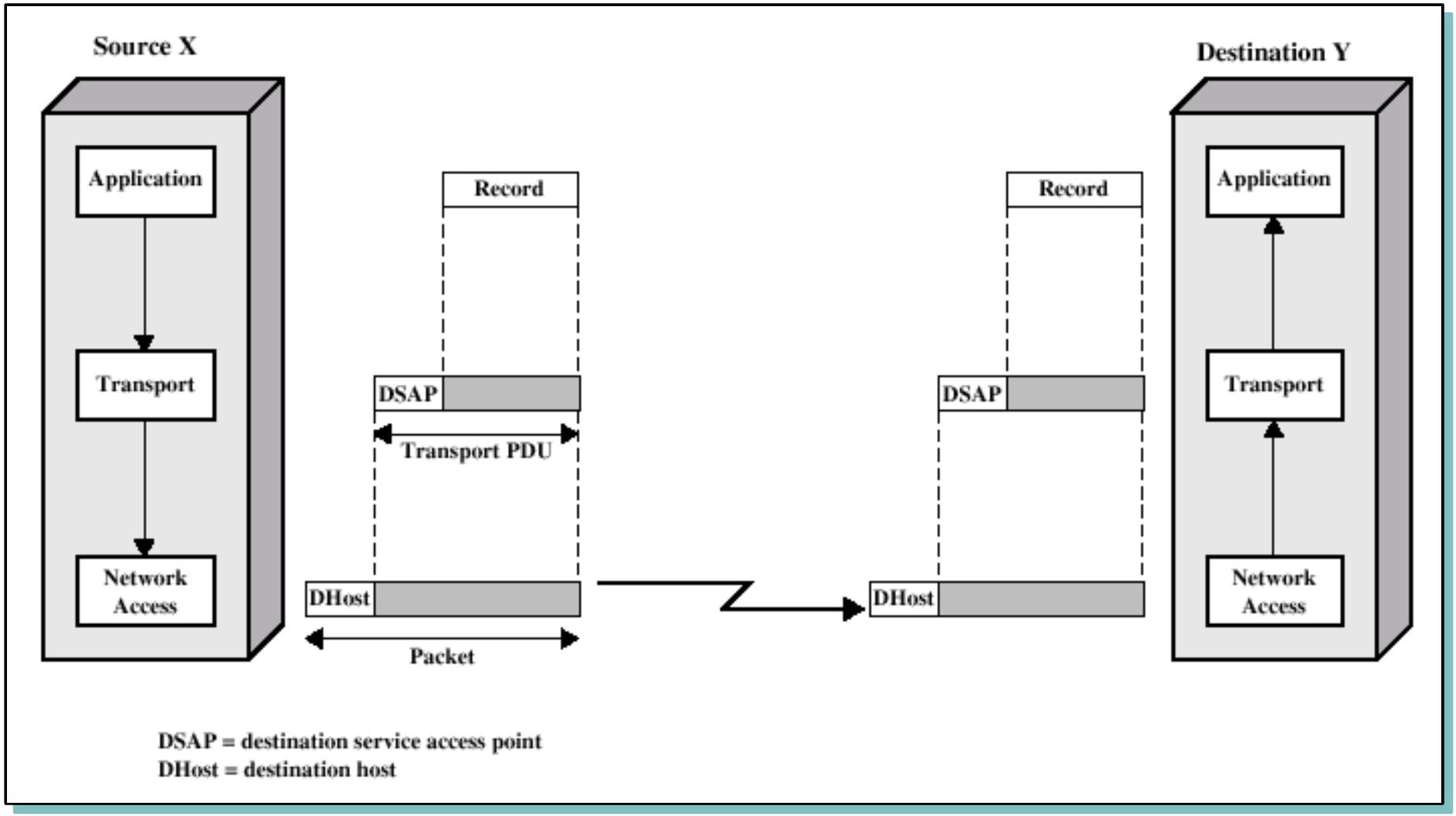
Protocols in a Simplified Architecture



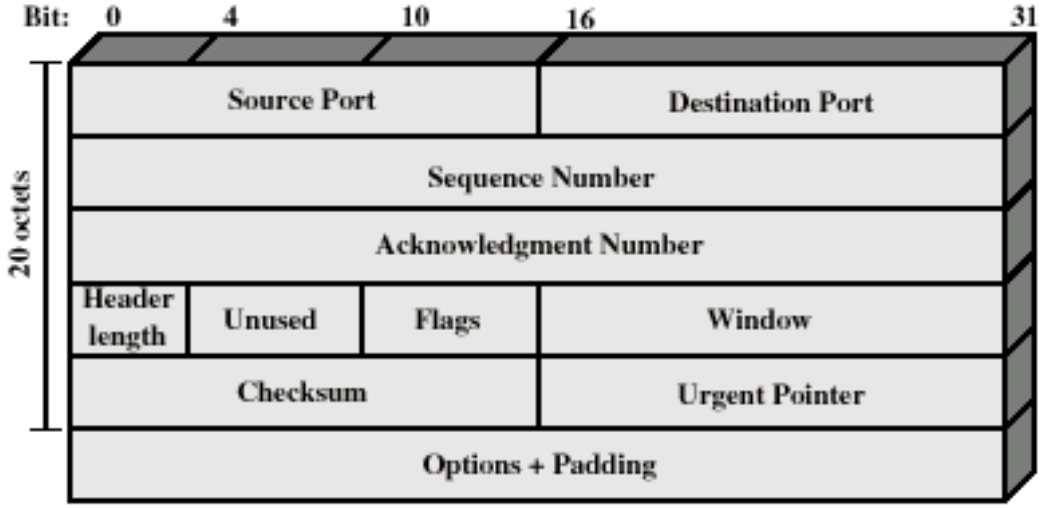
Protocol Data Units in TCP/IP



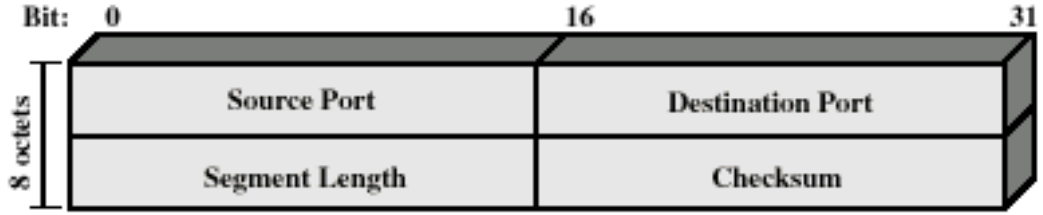
Operation of a Protocol Architecture



TCP and UDP Headers

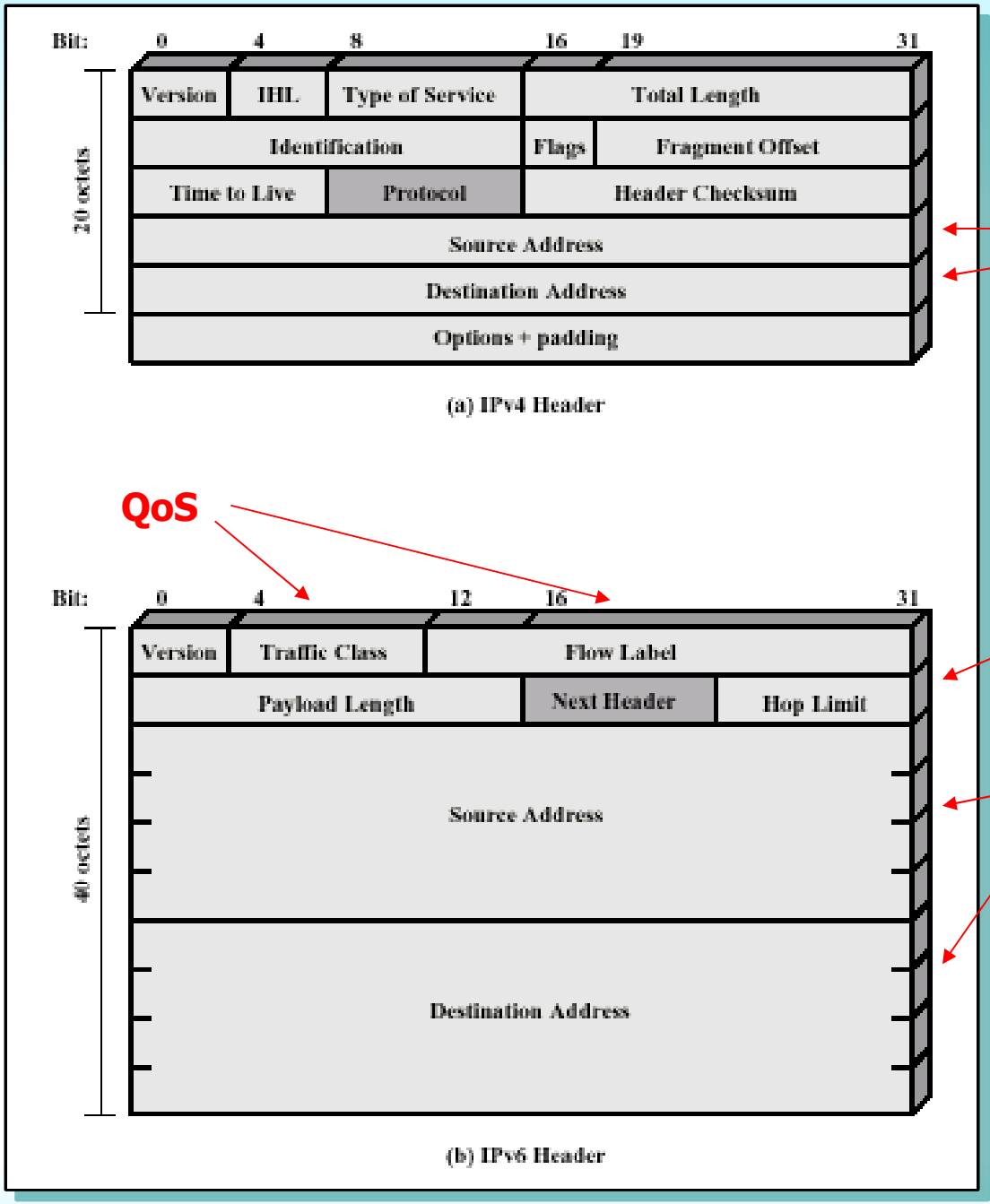


(a) TCP Header

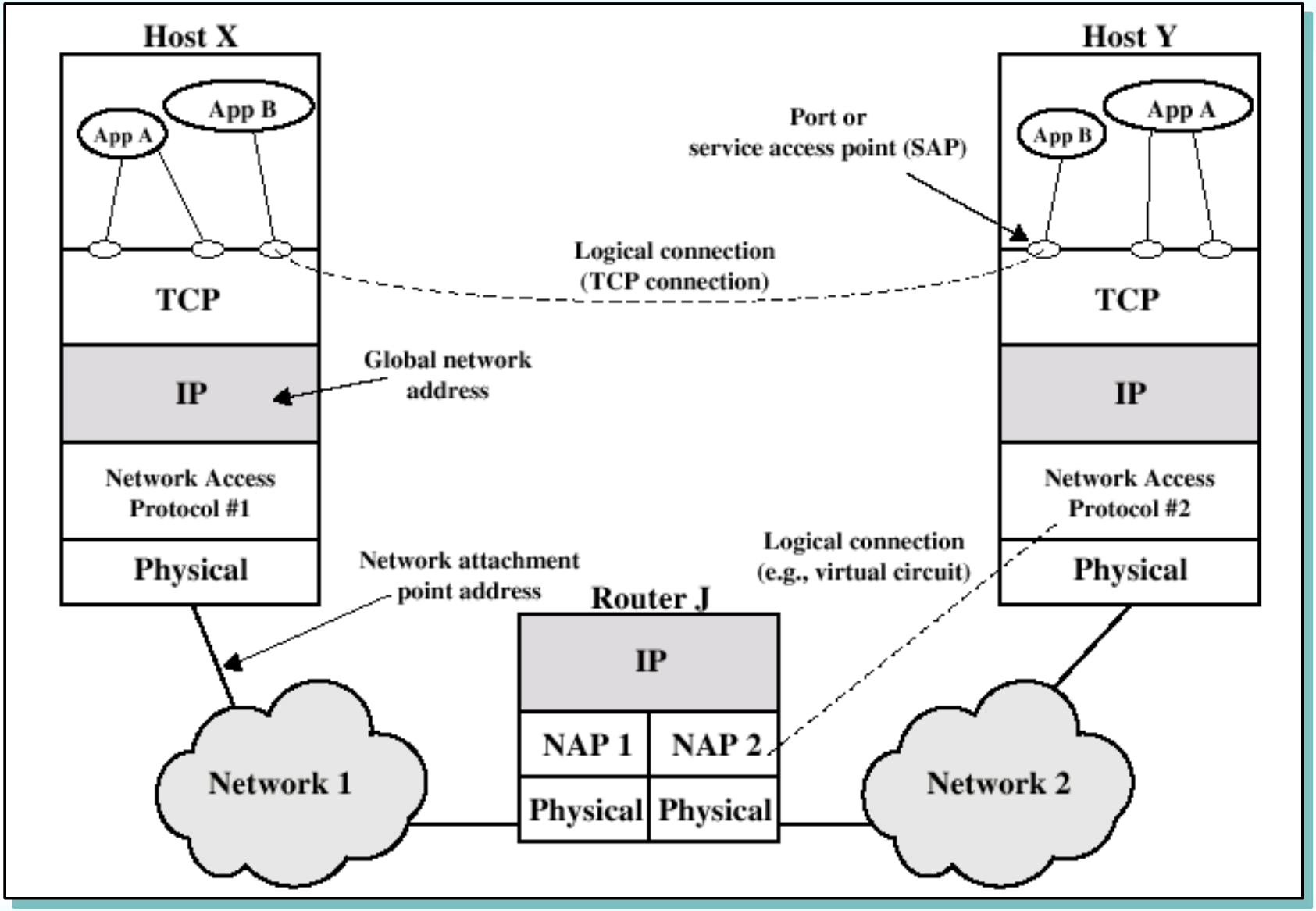


(b) UDP Header

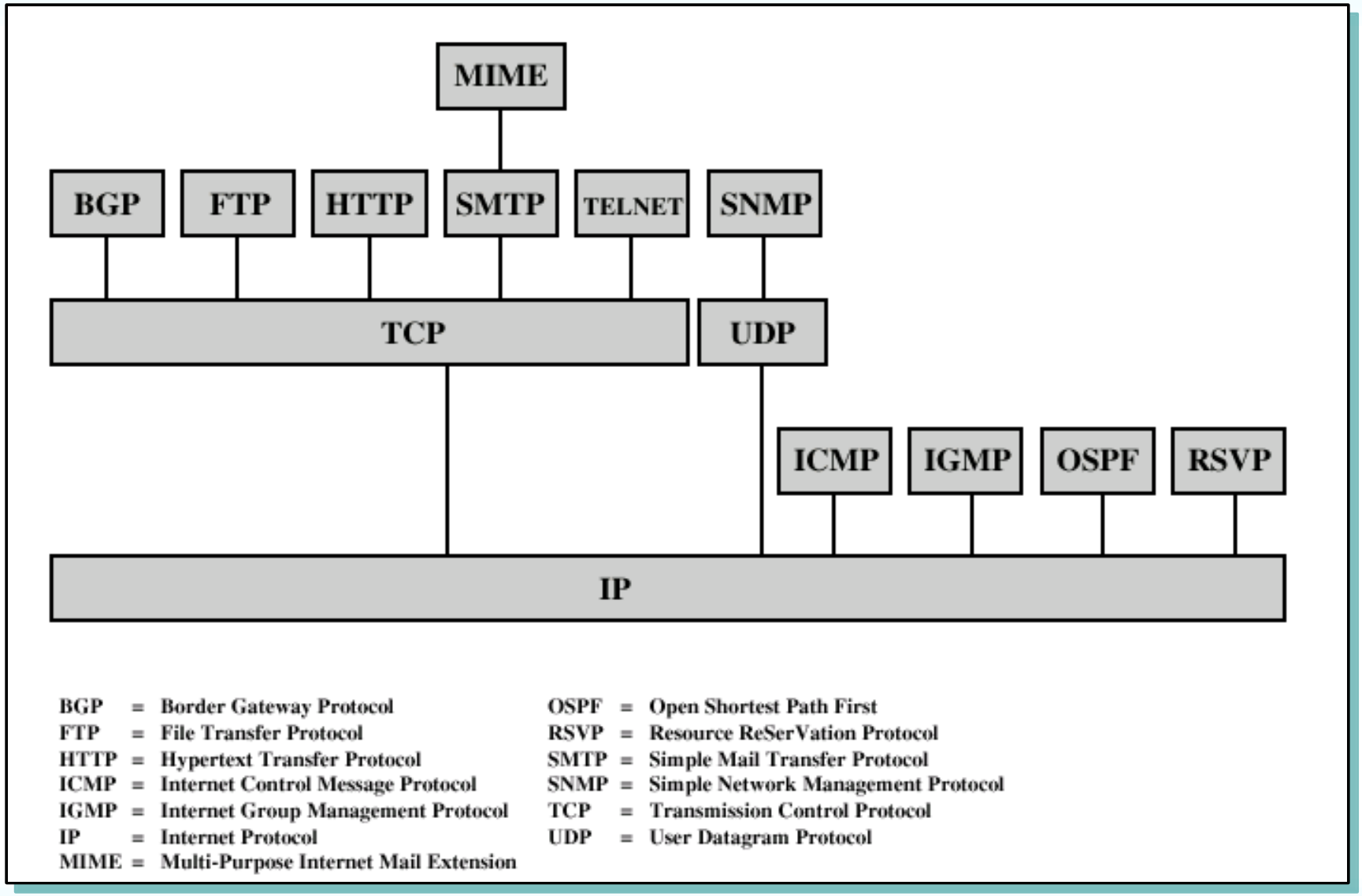
IP Headers


Bit:
0
4
8
16
19
31
Version
IHL
Type of Service
Total Length
Identification
Flags
Fragment Offset
Time to Live
Protocol
Header Checksum
Source Address
Destination Address
Options + padding
20 octets
(a) IPv4 Header
QoS
Bit:
0
4
12
16
31
Version
Traffic Class
Flow Label
Payload Length
Next Header
Hop Limit
Source Address
Destination Address
40 octets
(b) IPv6 Header
32-bit field
max # allowable hops
128-bit field

TP/IP Concepts



Some TCP/IP Protocols

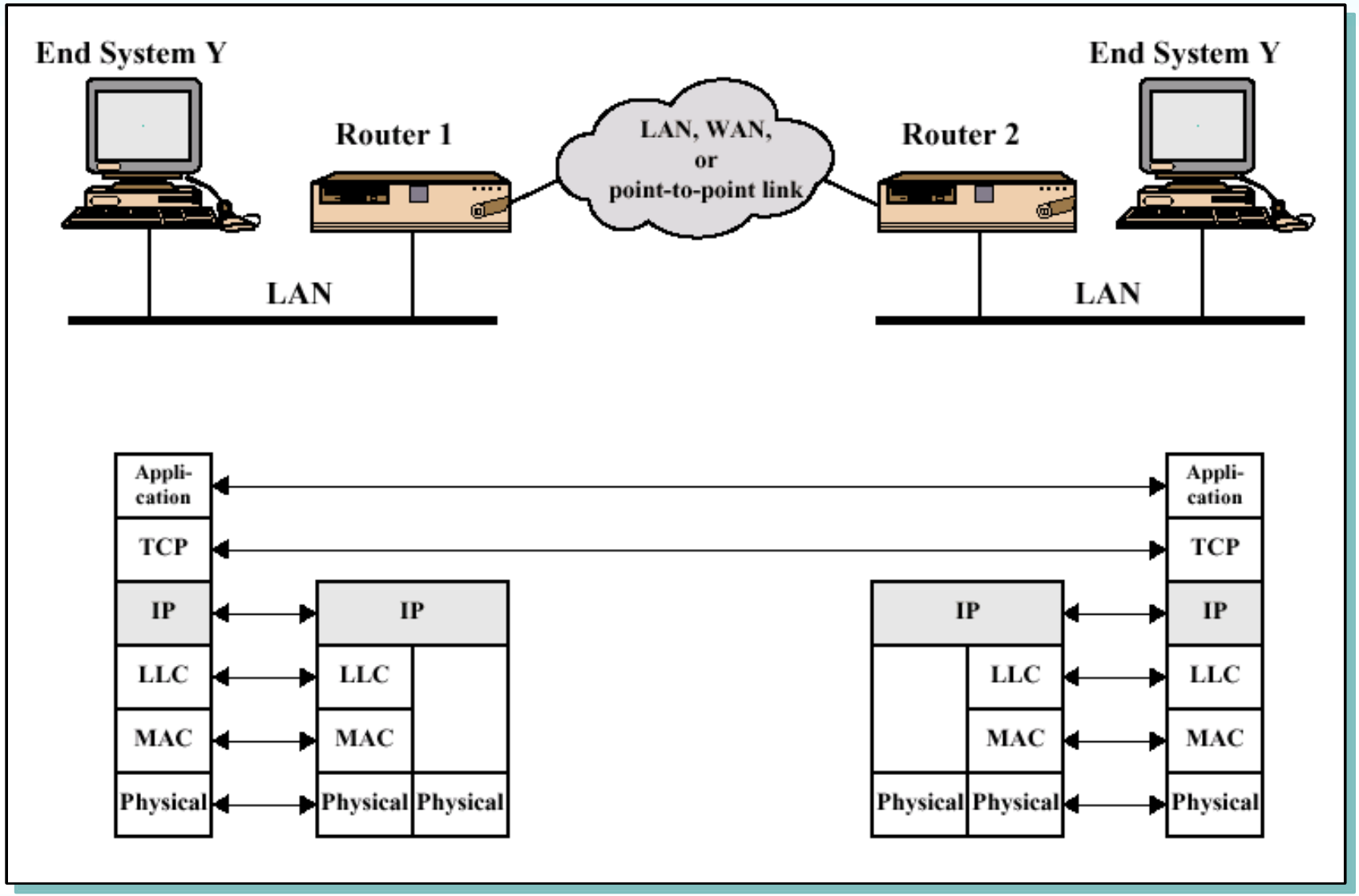


BGP = Border Gateway Protocol
FTP = File Transfer Protocol
HTTP = Hypertext Transfer Protocol
ICMP = Internet Control Message Protocol
IGMP = Internet Group Management Protocol
IP = Internet Protocol
MIME = Multi-Purpose Internet Mail Extension
OSPF = Open Shortest Path First
RSVP = Resource ReSerVation Protocol
SMTP = Simple Mail Transfer Protocol
SNMP = Simple Network Management Protocol
TCP = Transmission Control Protocol
UDP = User Datagram Protocol

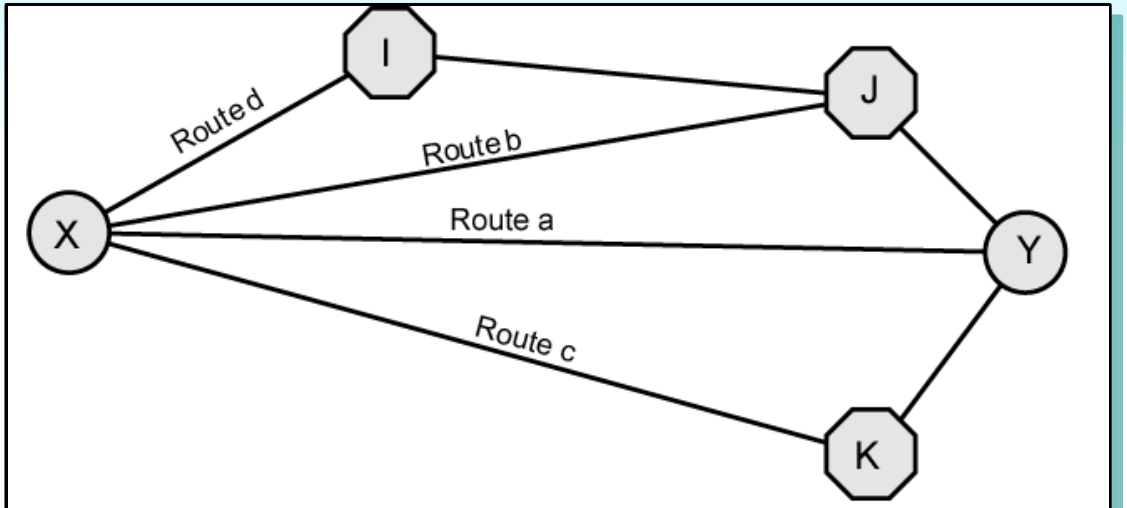
Assigned Port Numbers

Port	Service	Port	Service
7	echo	110	pop3
20	ftp-data	119	nntp
21	ftp	123	ntp
23	telnet	389	ldap
25	smtp	443	https
39	rip	500	isakmp
53	DNS	520	rip2
80	http	1812	radiusauth
88	kerberos	2049	Sun NFS

Configuration of TCP/IP



Alternate Routing Diagram



Route a: X® Y
Route b: X® J® Y
Route c: X® K® Y
Route d: X® I® J® Y

= end office

= intermediate switching node

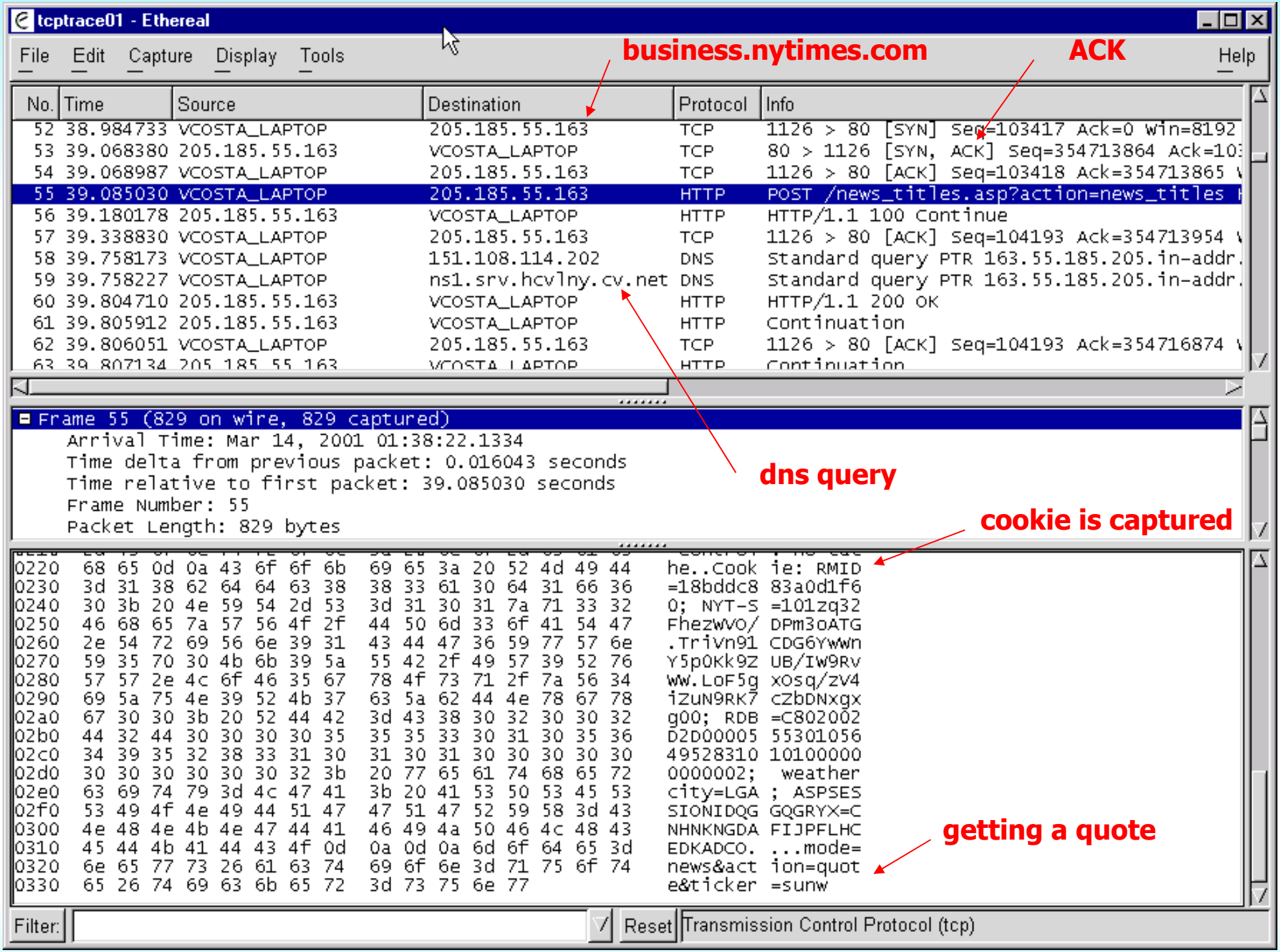
(a) Topology

Time Period	First route	Second route	Third route	Fourth and final route
Morning	a	b	c	d
Afternoon	a	d	b	c
Evening	a	d	c	b
Weekend	a	c	b	d

(b) Routing table

Ethereal

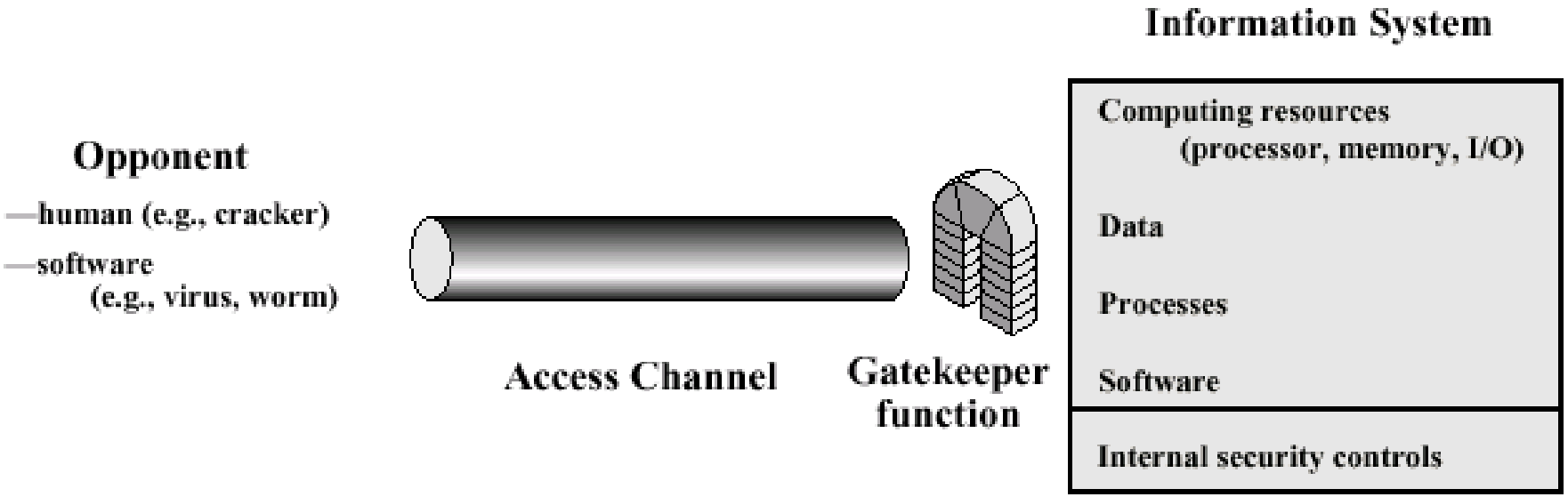
- Ethereal is a free network protocol analyzer for Unix and Windows
- Packet Sniffer - data can be captured "off the wire" from a live network connection
- www.ethereal.com - Everything you ever wanted to know about ethereal
- wiki.ethereal.com - This is the “User's Manual;” also has has a nice “References” section


tcptrace01 - Ethereal
File Edit Capture Display Tools Help
business.nytimes.com
ACK
No. Time Source Destination Protocol Info
52 38.984733 VCOSTA_LAPTOP 205.185.55.163 TCP 1126 > 80 [SYN] Seq=103417 Ack=0 Win=8192
53 39.068380 205.185.55.163 VCOSTA_LAPTOP TCP 80 > 1126 [SYN, ACK] Seq=354713864 Ack=103
54 39.068987 VCOSTA_LAPTOP 205.185.55.163 TCP 1126 > 80 [ACK] Seq=103418 Ack=354713865
55 39.085030 VCOSTA_LAPTOP 205.185.55.163 HTTP POST /news_titles.asp?action=news_titles
56 39.180178 205.185.55.163 VCOSTA_LAPTOP HTTP HTTP/1.1 100 Continue
57 39.338830 VCOSTA_LAPTOP 205.185.55.163 TCP 1126 > 80 [ACK] Seq=104193 Ack=354713954
58 39.758173 VCOSTA_LAPTOP 151.108.114.202 DNS Standard query PTR 163.55.185.205.in-addr.
59 39.758227 VCOSTA_LAPTOP ns1.srv.hcvlny.cv.net DNS Standard query PTR 163.55.185.205.in-addr.
60 39.804710 205.185.55.163 VCOSTA_LAPTOP HTTP HTTP/1.1 200 OK
61 39.805912 205.185.55.163 VCOSTA_LAPTOP HTTP Continuation
62 39.806051 VCOSTA_LAPTOP 205.185.55.163 TCP 1126 > 80 [ACK] Seq=104193 Ack=354716874
Frame 55 (829 on wire, 829 captured)
Arrival Time: Mar 14, 2001 01:38:22.1334
Time delta from previous packet: 0.016043 seconds
Time relative to first packet: 39.085030 seconds
Frame Number: 55
Packet Length: 829 bytes
dns query
cookie is captured
0220 68 65 0d 0a 43 6f 6f 6b 69 65 3a 20 52 4d 49 44 he..Cook ie: RMID
0230 3d 31 38 62 64 64 63 38 38 33 61 30 64 31 66 36 =18bddc8 83a0d1f6
0240 30 3b 20 4e 59 54 2d 53 3d 31 30 31 7a 71 33 32 0; NYT-S =101zq32
0250 46 68 65 7a 57 56 4f 2f 44 50 6d 33 6f 41 54 47 FhezWVO/ DPm3oATG
0260 2e 54 72 69 56 6e 39 31 43 44 47 36 59 77 57 6e .TriVn91 CDG6YwWn
0270 59 35 70 30 4b 6b 39 5a 55 42 2f 49 57 39 52 76 Y5p0Kk9Z UB/IW9Rv
0280 57 57 2e 4c 6f 46 35 67 78 4f 73 71 2f 7a 56 34 WW.LoF5g xOsq/zV4
0290 69 5a 75 4e 39 52 4b 37 63 5a 62 44 4e 78 67 78 iZuN9RK7 cZbDNxgx
02a0 67 30 30 3b 20 52 44 42 3d 43 38 30 32 30 30 32 g00; RDB =C802002
02b0 44 32 44 30 30 30 30 35 35 35 33 30 31 30 35 36 D2D00005 55301056
02c0 34 39 35 32 38 33 31 30 31 30 31 30 30 30 30 30 49528310 10100000
02d0 30 30 30 30 30 30 32 3b 20 77 65 61 74 68 65 72 0000002; weather
02e0 63 69 74 79 3d 4c 47 41 3b 20 41 53 50 53 45 53 city=LGA ; ASPSES
02f0 53 49 4f 4e 49 44 51 47 47 51 47 52 59 58 3d 43 SIONIDQG GQGRYX=C
0300 4e 48 4e 4b 4e 47 44 41 46 49 4a 50 46 4c 48 43 NHNKNGDA FIJPFLHC
0310 45 44 4b 41 44 43 4f 0d 0a 0d 0a 6d 6f 64 65 3d EDKADCO. ...mode=
0320 6e 65 77 73 26 61 63 74 69 6f 6e 3d 71 75 6f 74 news&act ion=quot
0330 65 26 74 69 63 6b 65 72 3d 73 75 6e 77 e&ticker =sunw
getting a quote
Filter: Reset Transmission Control Protocol (tcp)

Ethereal Etiquette

- Be careful when and where you use this tool
- It makes people nervous
- Use prudence with the information you collect
- **When in doubt, seek permission!**

Network Access Security Model



Information Security

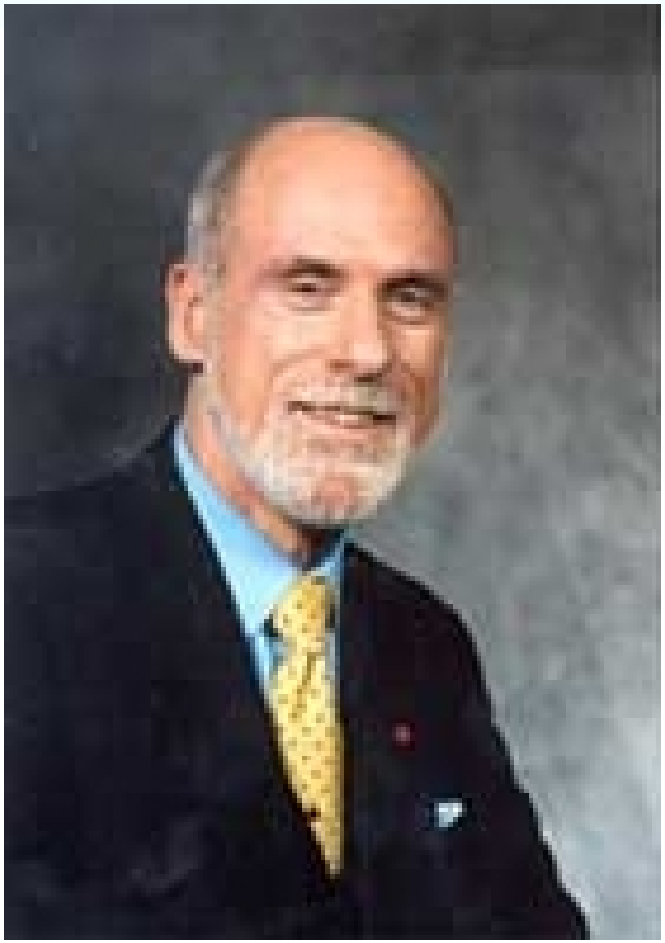
- Physical
- Administrative
- “Lockup the file cabinet”

Private Networks

- Isolated to individual organizations
- Emergence of **computer security**
- Sharing a system
- Protecting data

Networking

- Networks start talking to each other
- Gateways
- Arpanet
- TCP/IP Everywhere
- Vinton Cerf, “IP On Everything!”

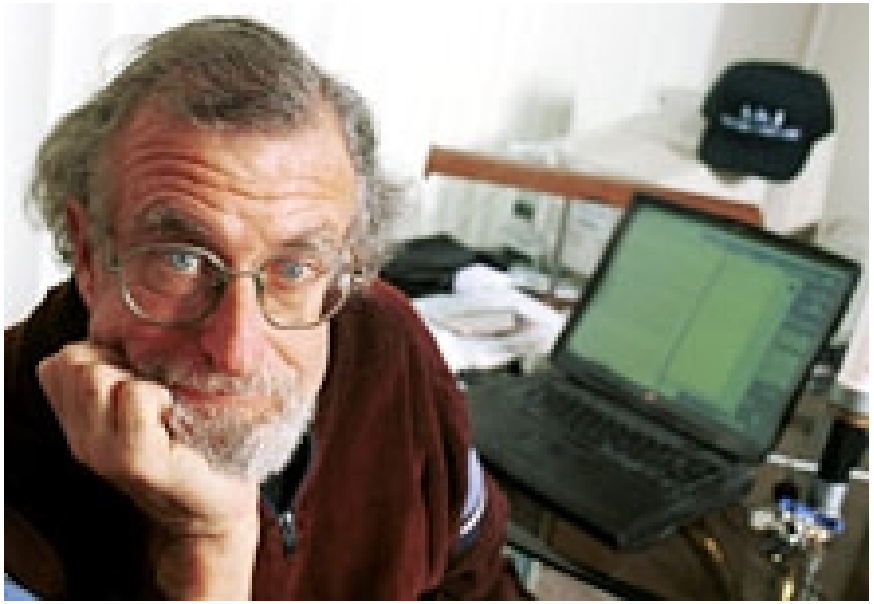


Maturing of the Internet

- Telephones used by 50% of worlds population
- Internet attains similar level of growth by 2010 – max growth
- Connecting computers and programmable devices
- More **devices** than people

Early Hacking

- Cap'n Crunch cereal prize
- Giveaway **whistle** produces 2600 MHz tone
- Blow into receiver – free phone calls
- "Phreaking" encouraged by Abbie Hoffman
- Doesn't hurt anybody



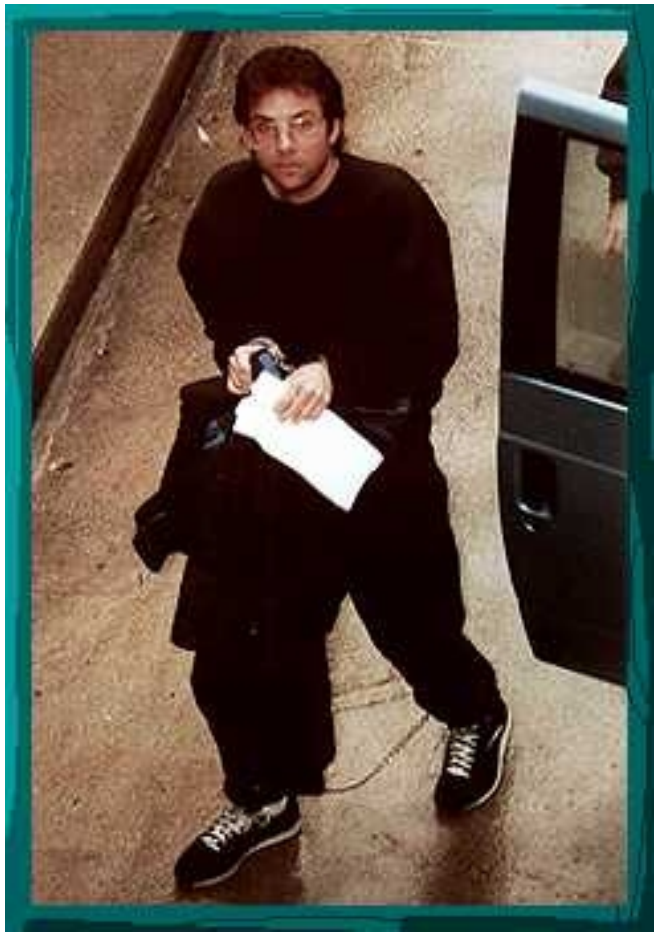
Captain Crunch

- **John Draper**
- `71: **Bluebox** built by many
- Jobs and Wozniak were early implementers
- Developed “EasyWriter” for first IBM PC
- High-tech hobo
- White-hat hacker

The Eighties

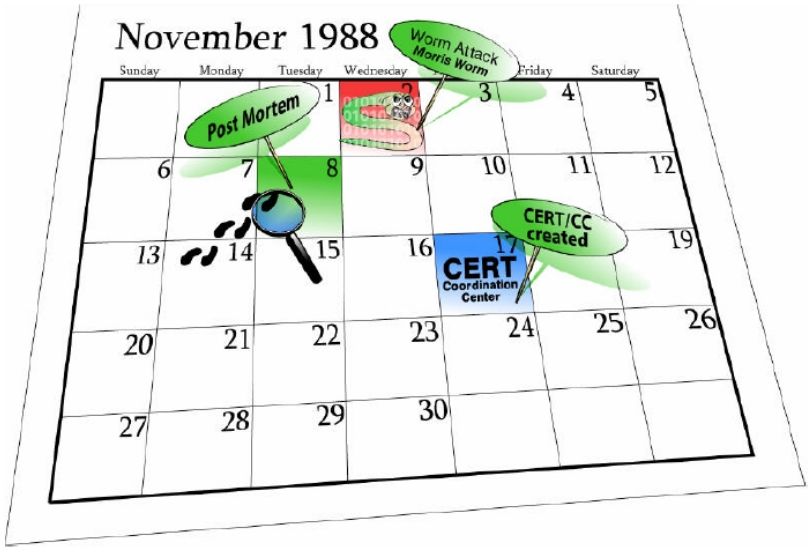
- 1983 – “War Games” movie
- Federal Computer Fraud and Abuse Act - 1986
- Robert Morris – Internet **worm** -1988
- Brings over 6000 computers to a halt
- $10,000 fine
- His Dad worked for the NSA!!!

It Got Worse

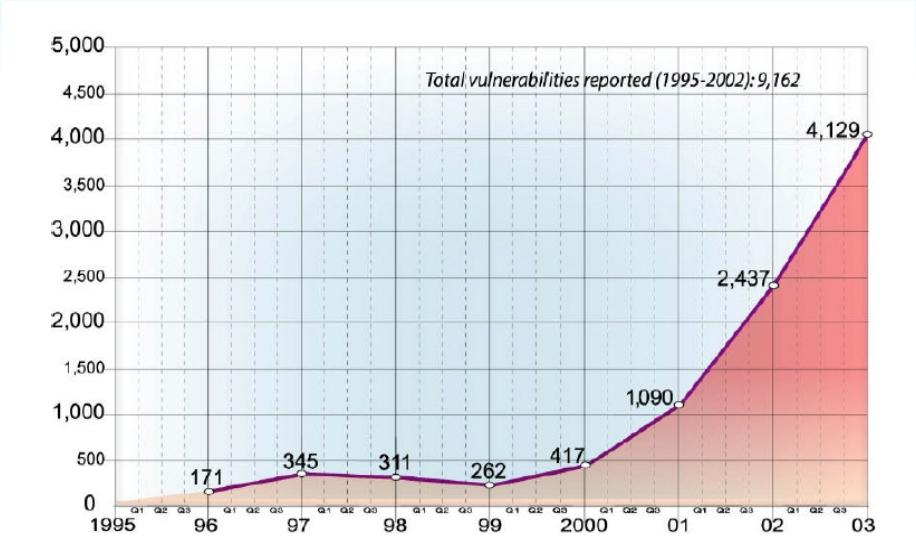


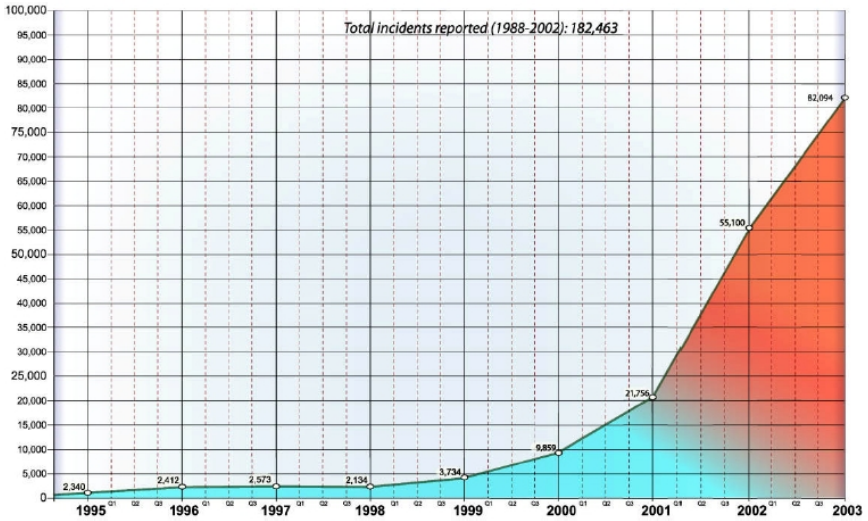
- 1995 – Kevin Mitnick arrested for the 2nd time
- Stole 20,000 credit card numbers
- First hacker on FBI's *Most Wanted* poster
- Tools: password sniffers, spoofing
- http://www.2600.com

Tracking Attacks



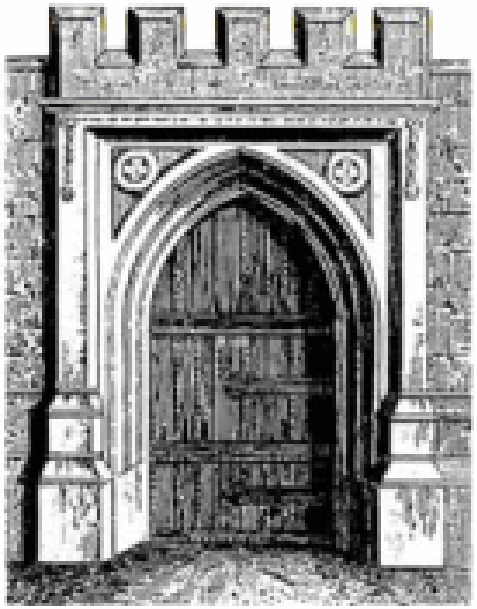
http://www.cert.org





Just because you're paranoid, doesn't mean they're not out to get you!

- Anonymous



Firewalls

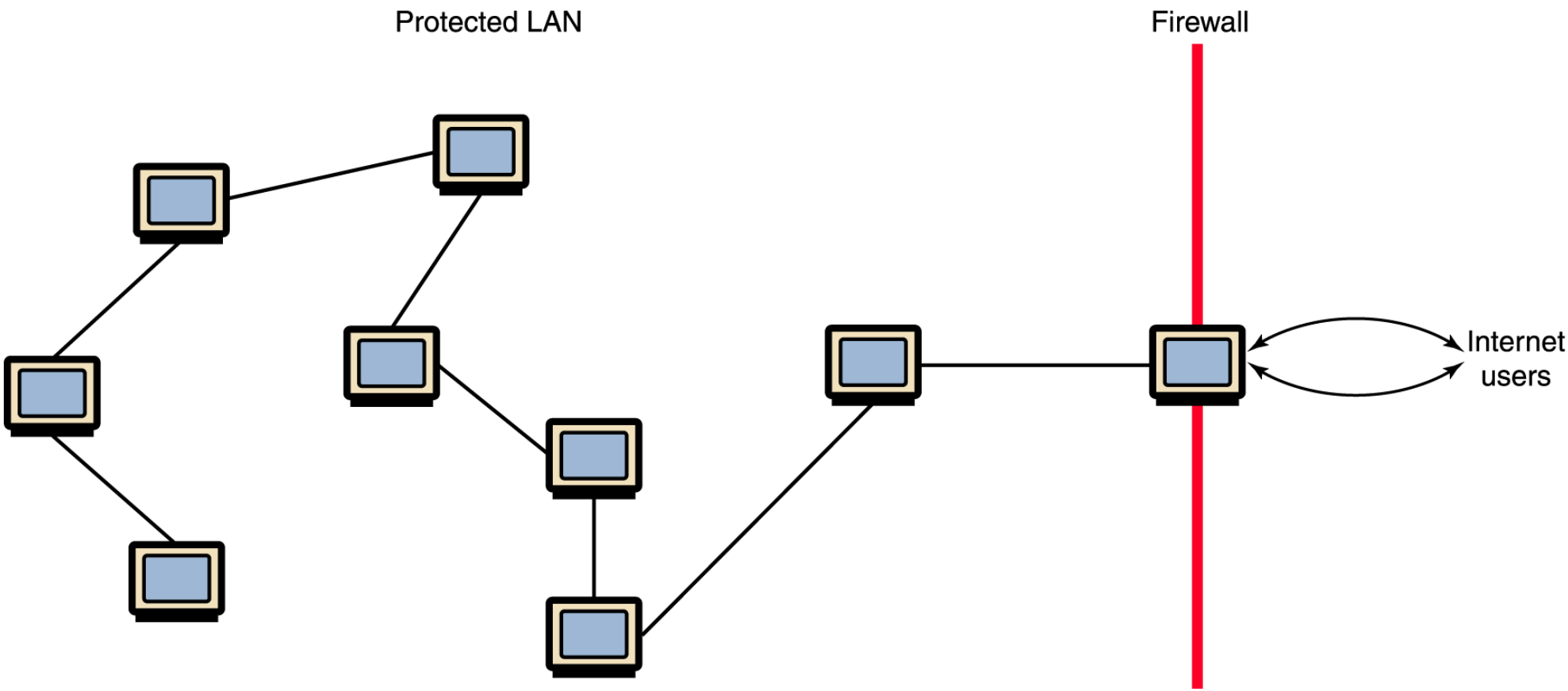


Figure 15.8 **A firewall protecting a LAN**

Firewalls Make It To The Movies

Why Firewalls?

- Internet connectivity is no longer an option for most corporations
- The Internet allows you access to worldwide resources, but...
  ...the Internet also allows the *world* to try and access your resources
- This is a grave risk to most organizations

Why Firewalls?

- A firewall is inserted between the premises network and the Internet
- Establishes a perimeter
- Provides a choke point where security and audits can be imposed
- Single computer system or a set of systems can perform the firewall function

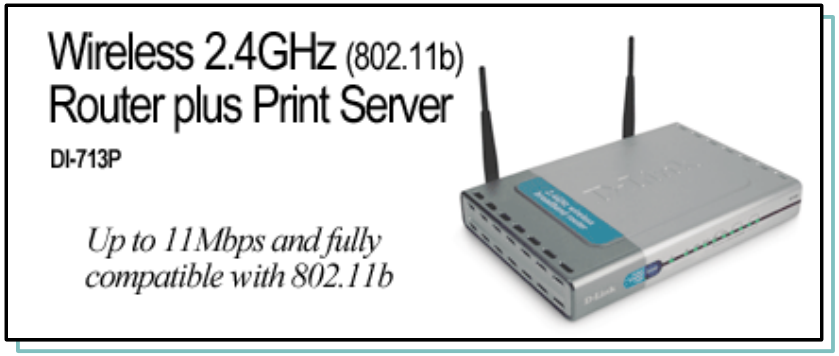
Good Fences Make Good Neighbors – Robert Frost, “Mending Wall”

Design Goals

- All traffic, from inside to outside and vice versa, must pass through the firewall
- Only authorized traffic (defined by the security policy) is allowed to flow
- Firewall is immune to penetration – uses a trusted system

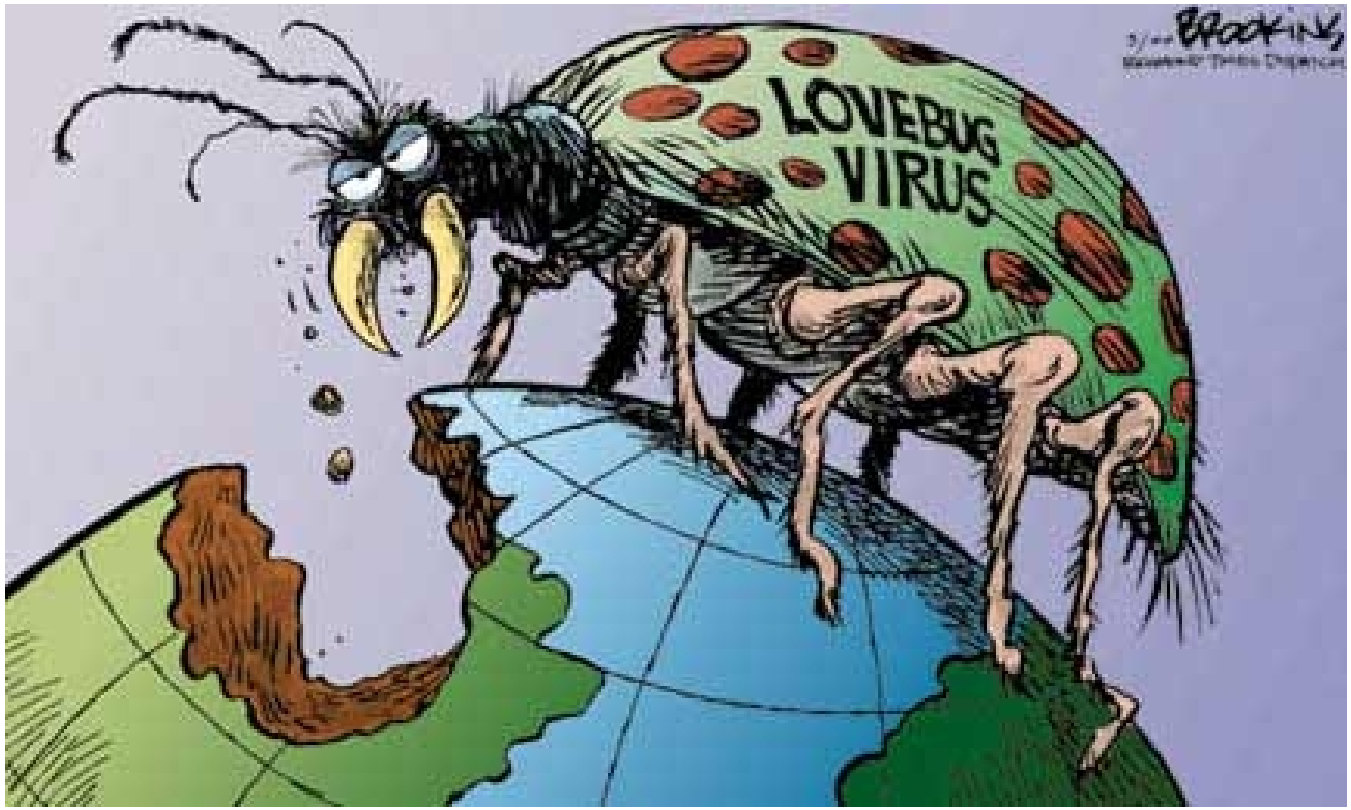
Other Types Of Firewalls

- Personal Firewalls Appliances – personal firewall appliances are designed to protect small networks such as networks that might be found in home offices
- Provide: print server, shared broadband use, firewall, DHCP server and NAT



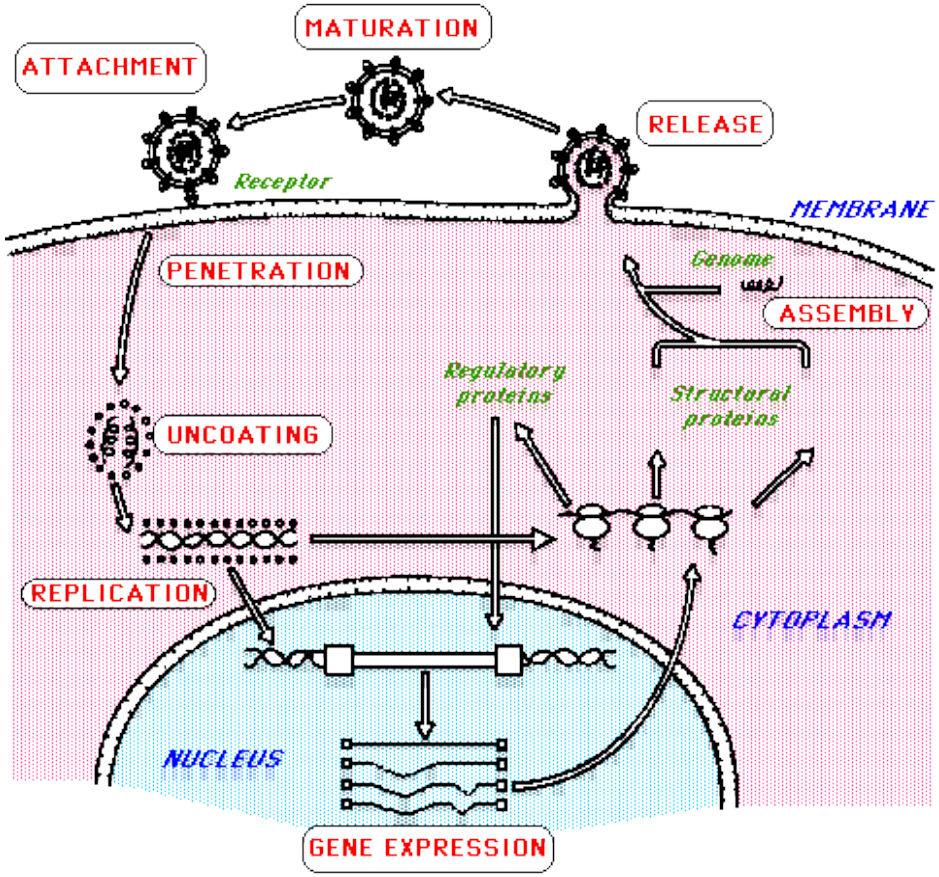
(NB: This is not an endorsement of any product)

Viruses



Viruses

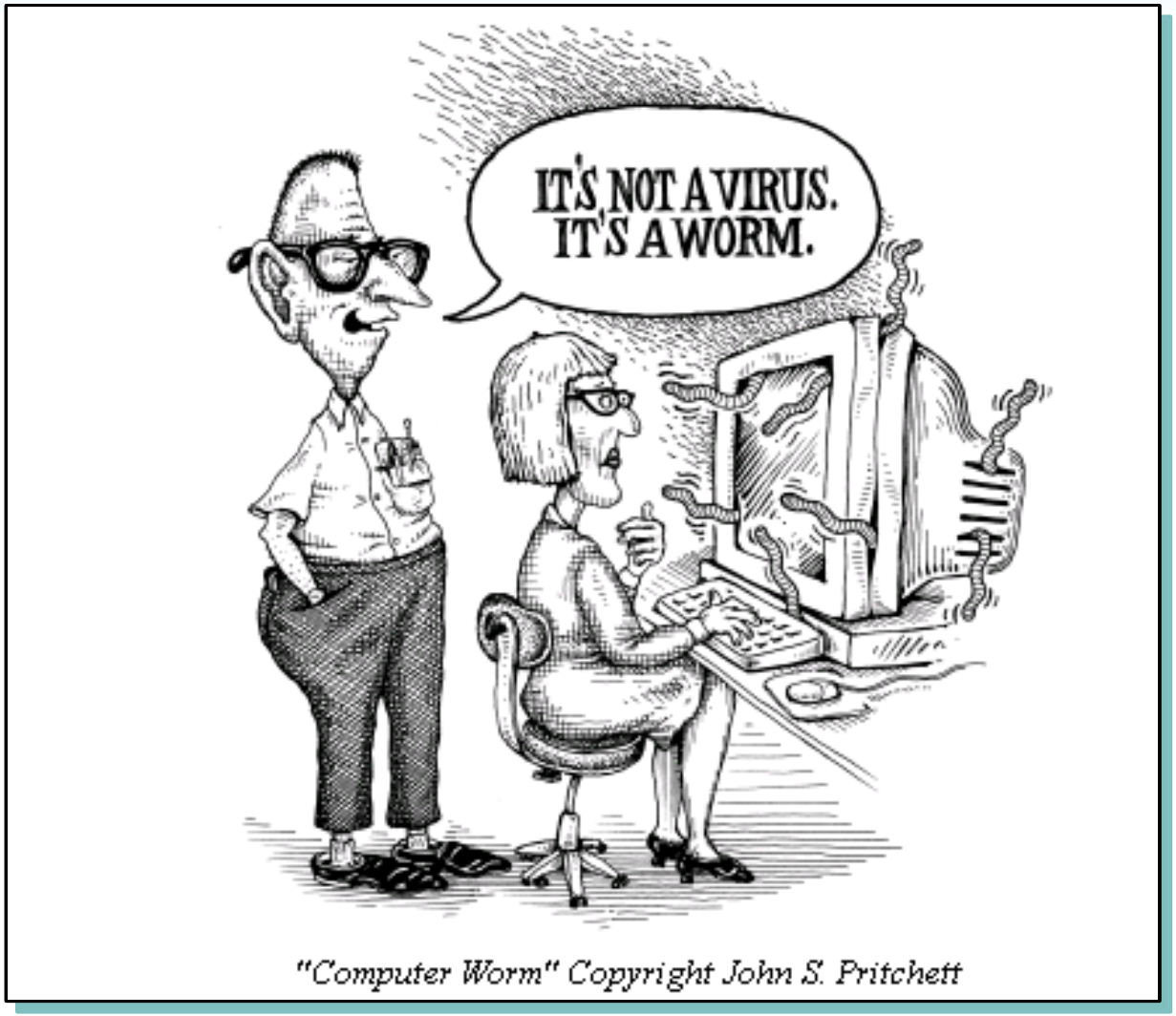
- A virus is a submicroscopic parasitic particle that infects cells in biological organisms.
- Viruses are non-living particles that can only replicate when an organism reproduces the viral RNA or DNA.
- Viruses are considered non-living by the majority of virologists
- www.virology.net



Viruses

- Viruses: code embedded within a program that causes a copy of itself to be inserted in other programs and performs some unwanted function
- *Infects* other programs
- *Code* is the *DNA* of the virus

Worms


IT'S NOT A VIRUS.
IT'S A WORM.
"Computer Worm" Copyright John S. Pritchett

Worms

- Worms: program that can replicate itself and send copies to computers across the network and performs some unwanted function
- Uses *network connections* to spread from system to system

Useful Websites

- http://www.rfc-editor.org/rfcsearch.html
  Search RFCs
- http://www.cert.org
  Center for Internet security
- http://www.counterpane.com/alerts.html
  Some recent alerts

Assignment #3

- **Research** these two RFCs: **RFC1129** and **RFC968**. Given a **brief** - paragraph, not a single sentence – **description** based on the abstract, introduction, or basic content
- Pick **google.com** and one other site. Using **whois** and **ARIN**, get as much information as possible about the IP addressing, the DNS and the site (location, owner, etc.)
- **Due next Wednesday, December 6** – or you can email it earlier

Homework

- **Read Chapter Fifthteen – and review slides**
- ...Next Class We'll Cover **Artificial Intelligence...**

…Have A Nice Weekend

“The City” At 1200 Feet In December