Network Security

G. Sivakumar

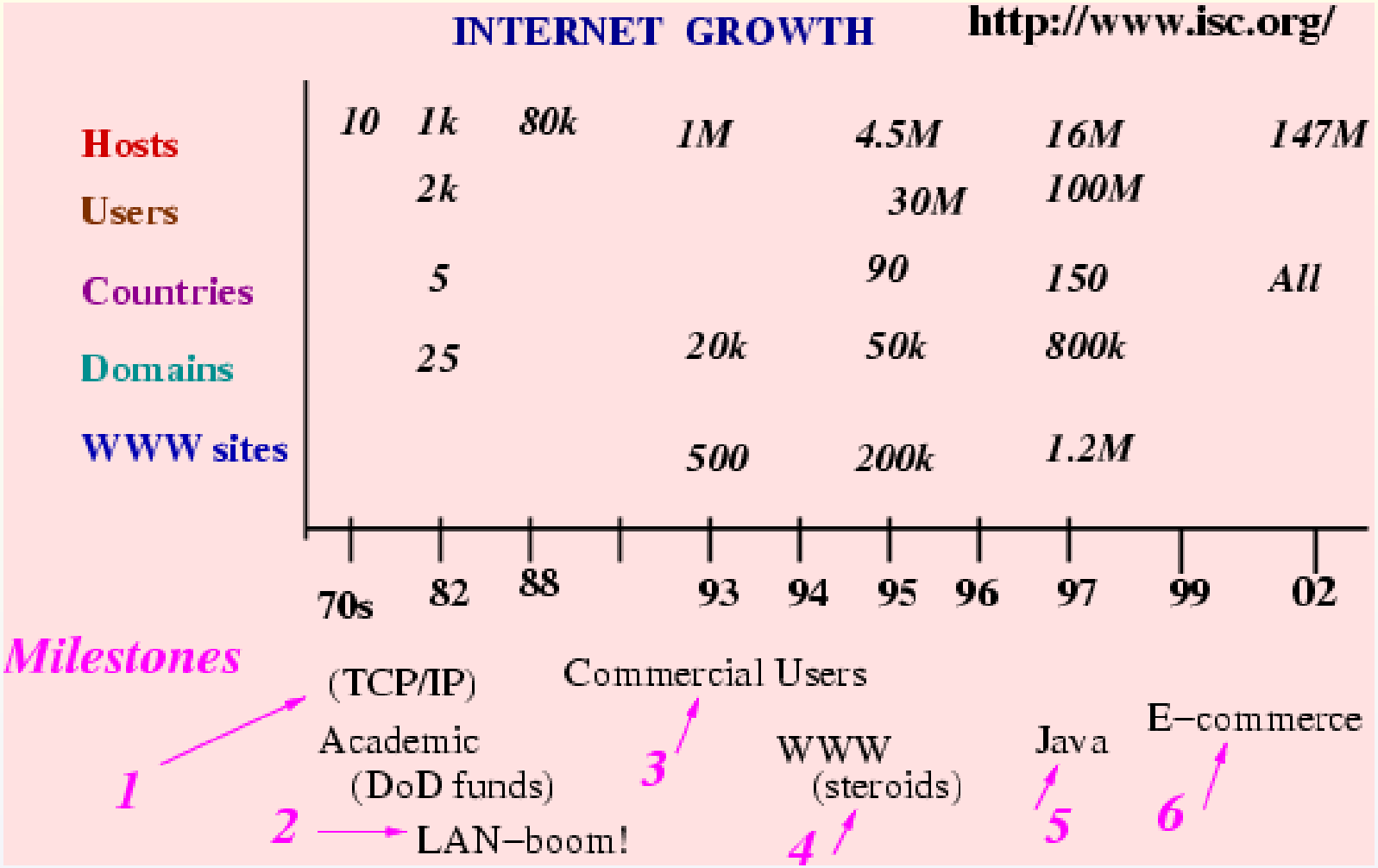
Computer Science and Engineering
IIT Bombay
siva@iitb.ac.in

May 26, 2005

Outline of This Lecture

- Network Security Threats and Requirements
- TCP/IP Essentials: How Internet Works
- Defending the Network (more tomorrow)
  - Perimeter Level (Firewalls)
  - Application/Services Level

Internet Growth

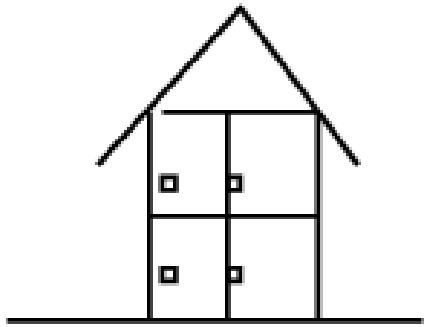


Information **AnyTime, AnyWhere, AnyForm, AnyDevice, ...**

WebTone like DialTone

The Dream

The Dream



- **Internet Outlets (like electric)**

Plug-in (*mobile/wireless ok!*)

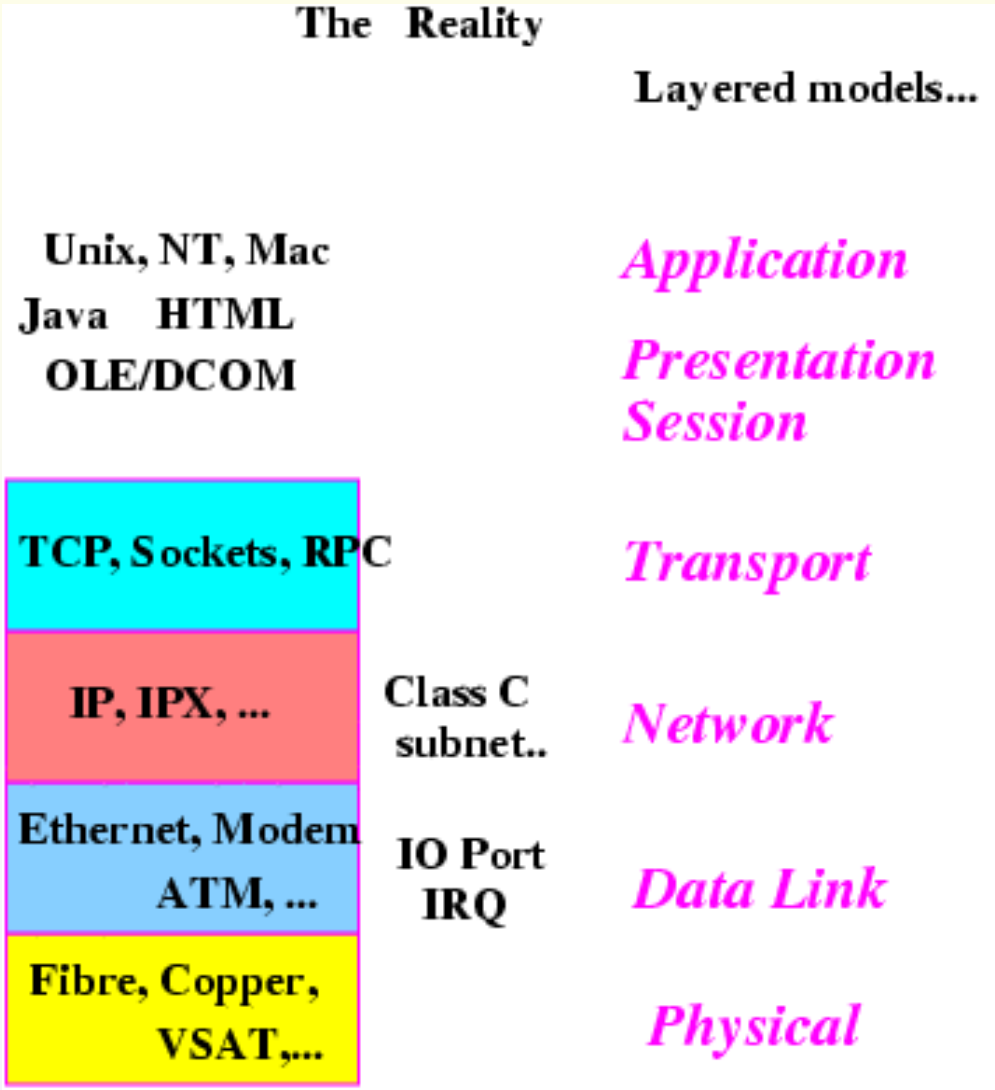
any "computer" *(phone,fax,washing machine, coffee machine, TV,...)*

Self-configuring, learning, fault-tolerant!

The promise held out by INTERNET!

- Why should a fridge be on Internet?
- Will **security** considerations make this a **nightmare**?

The Reality!


The Reality
Layered models...
Unix, NT, Mac
Java HTML
OLE/DCOM
Application
Presentation
Session
TCP, Sockets, RPC
Transport
IP, IPX, ...
Class C
subnet..
Network
Ethernet, Modem
ATM, ...
IO Port
IRQ
Data Link
Fibre, Copper,
VSAT,...
Physical

Security Concerns

Match the following!

Problems	Attackers
Highly contagious viruses	Unintended blunders
Defacing web pages	Disgruntled employees or customers
Credit card number theft	Organized crime
On-line scams	Foreign espionage agents
Intellectual property theft	Hackers driven by technical challenge
Wiping out data	Petty criminals
Denial of service	Organized terror groups
Spam E-mails	Information warfare
Reading private files	...
Surveillance	...

- Crackers vs. Hackers
- Note how much resources available to attackers.

Some Recent Attacks

See *www.securityfocus.com* and *www.sans.org* for more details

1. Nimda Worm (IIS/MIME bugs)
2. Code Red Worm (Buffer Overflow)
3. Code Red II Worm
4. Spam Mail (Open Relays/Formmail)
5. CGI Attacks
6. SubSeven Trojan
7. Microsoft FrontPage Attacks
8. DNS Attacks
9. FTP Attacks
10. SSH CRC-32 Compensation Detection Attack

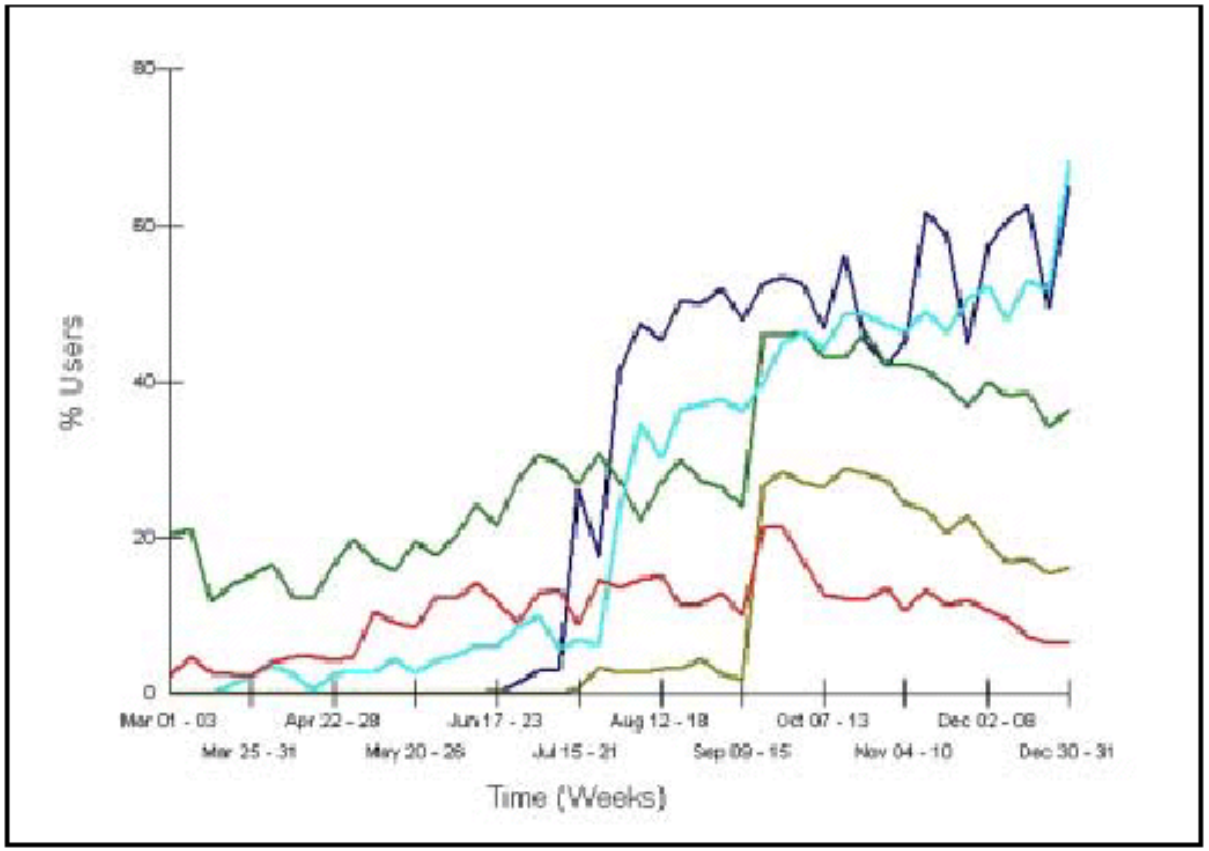
Nimda and friends

Nimda exploits

1. Microsoft IIS/PWS Escaped Characters Decoding Command Execution Vulnerability
2. Microsoft IE MIME Header Attachment Execution Vulnerability
3. Microsoft IIS and PWS Extended Unicode Directory Traversal Vulnerability
4. Microsoft Office 2000 DLL Execution Vulnerability

and spreads itself via E-mail, Web-server attack, Web-browser code, Open Network Shares.
Is this really a network problem? (analogy- airplanes and SARS virus)

Effect of Nimda, Code Red

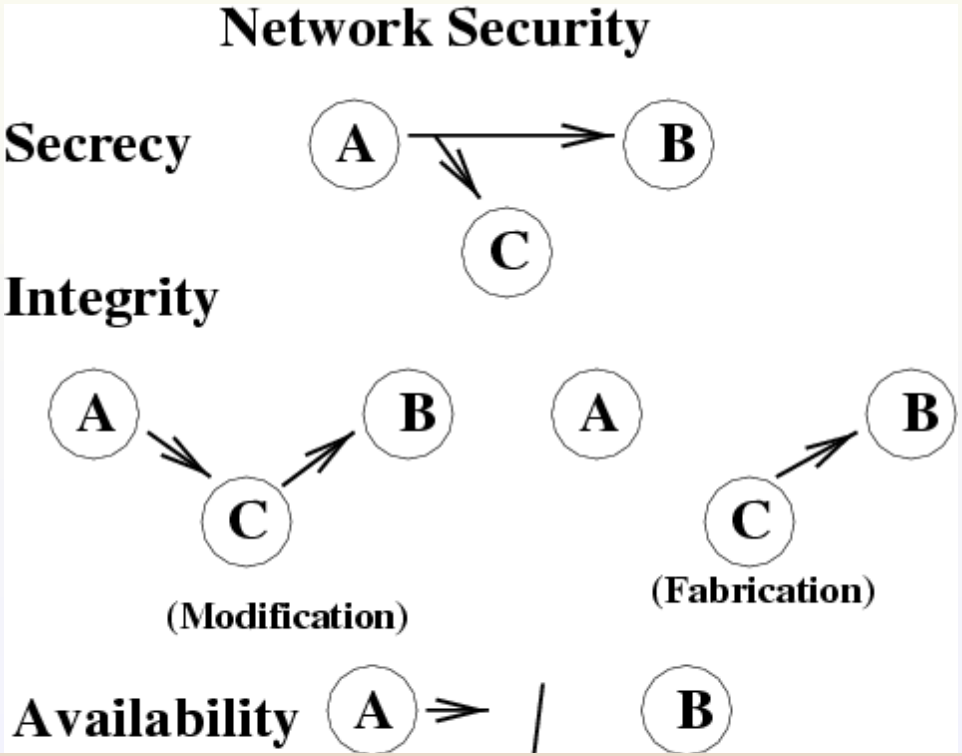


	% Users	# Attacks
Microsoft Indexing Server/Indexing Services ISAPI Buffer Overflow Attack	39.20	3486450
Generic HTTP Directory Traversal Attack	38.07	4095950
Generic HTTP 'cmd.exe' Request Attack	34.75	9473282
Microsoft IIS/PWS Escaped Characters Decoding Command Execution Attack	16.57	1944598
Microsoft IIS 4.0 / 5.0 Extended UNICODE Directory Traversal Attack	14.77	3861256

Figure 1. Code Red and Nimda Activity by User Percentage from March to November, 2001

Vulnerabilities

- **Application Security**
  - Buggy code
  - Buffer Overflows
- **Host Security**
  - Server side (multi-user/application)
  - Client side (virus)
- **Transmission Security**



Top Vulnerabilities to Windows Systems

See *http://www.sans.org* for more info (CVE numbers, how to check/protect etc.)

1. W1 Web Servers & Services
2. W2 Workstation Service
3. W3 Windows Remote Access Services
4. W4 Microsoft SQL Server (MSSQL)
5. W5 Windows Authentication
6. W6 Web Browsers
7. W7 File-Sharing Applications
8. W8 LSAS Exposures
9. W9 Mail Client
10. W10 Instant Messaging

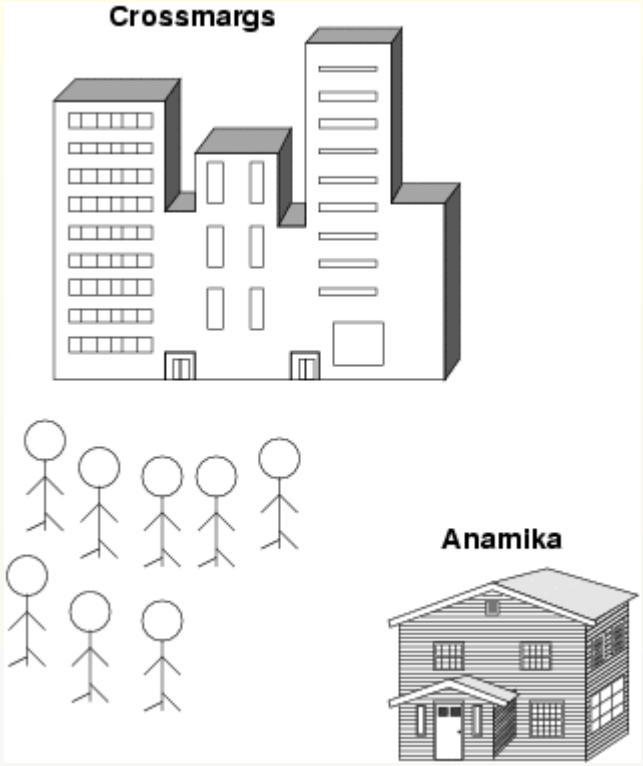
Top Vulnerabilities to UNIX Systems

See *http://www.sans.org* for more info

1. U1 BIND Domain Name System
2. U2 Web Server
3. U3 Authentication
4. U4 Version Control Systems
5. U5 Mail Transport Service
6. U6 Simple Network Management Protocol (SNMP)
7. U7 Open Secure Sockets Layer (SSL)
8. U8 Misconfiguration of Enterprise Services NIS/NFS
9. U9 Databases
10. U10 Kernel

Denial of Service

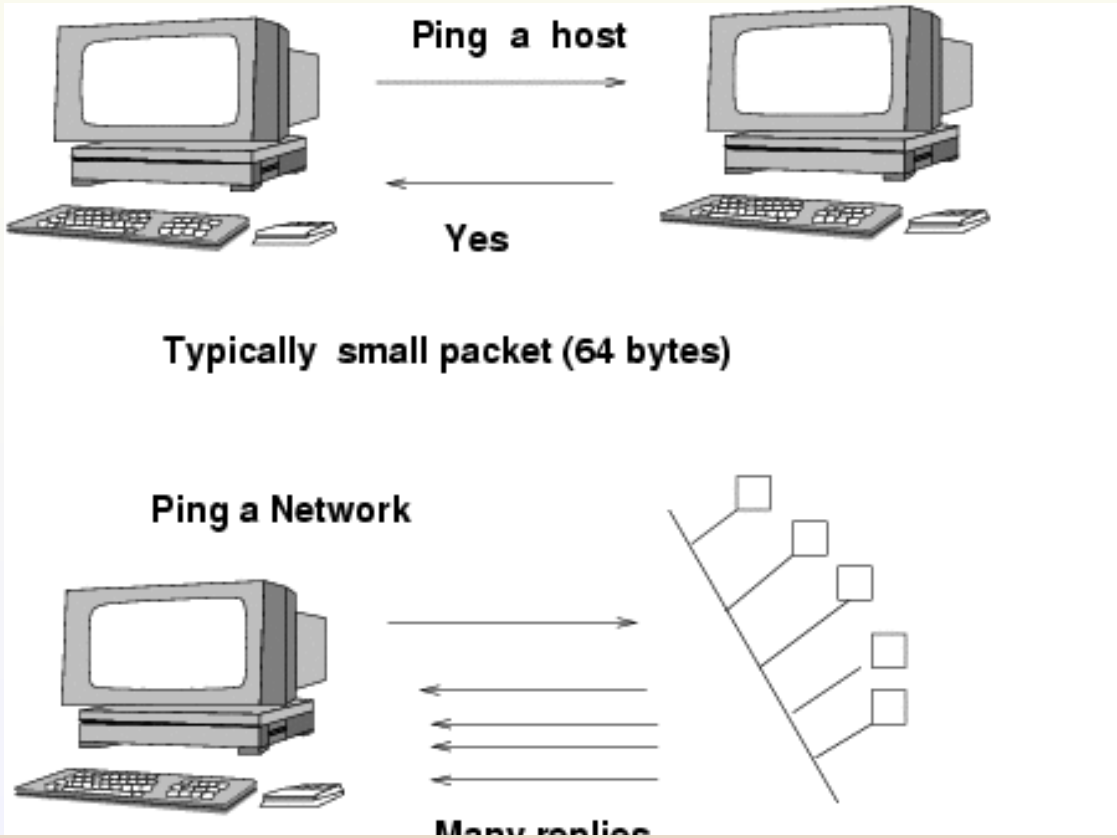
Small shop-owner versus Supermarket



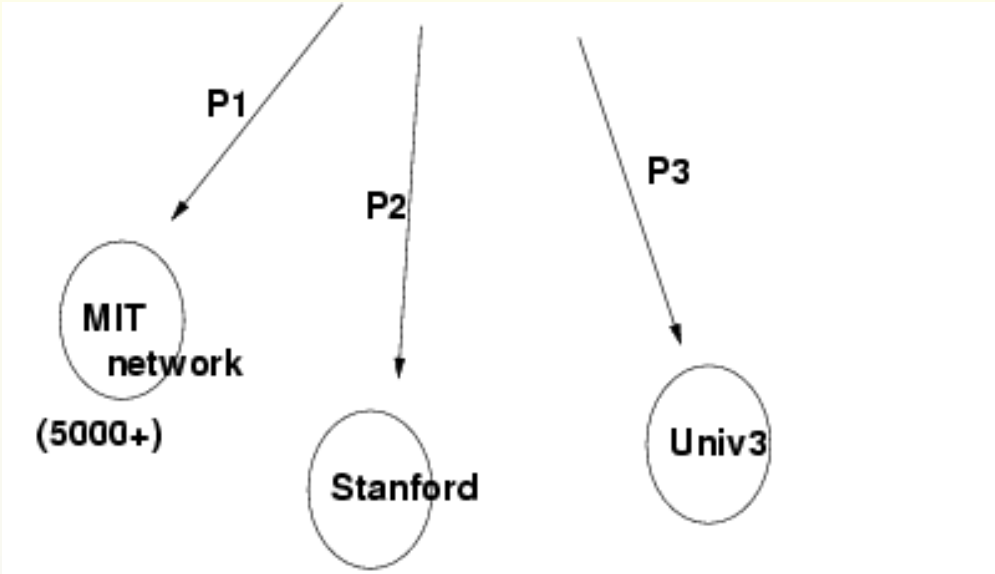
- What can the attacker do?
- What has he gained or compromised?
- What defence mechanisms are possible?
  - Screening visitors using guards (who looks respectable?)
  - VVIP security, but do you want to be isolated?

Yahoo DDoS attack

- Caused traffic to Yahoo to zoom to 100s of Mbps
- Broke the capacity of machines at Yahoo and its ISPs
- Internet Control Message Protocol (ICMP) normally used for good purposes.
- Ping used to check "are you alive?"



Yahoo DDoS attack



P1,P2,P3,... Fake broadcast ping from Victim

How many replies does unsupecting victim get?

From whom? (respectable?)

DDOS (distributed denial of service attack)

Freely available for "script kiddies'' to wreak havoc!

Security Requirements

Informal statements (formal is much harder)

- Confidentiality Protection from disclosure to unauthorized persons
- Integrity Assurance that information has not been modified unauthorizedly.
- Authentication Assurance of identity of originator of information.
- Non-Repudiation Originator cannot deny sending the message.
- Availability Not able to use system or communicate when desired.
- Anonymity/Pseudonomity For applications like voting, instructor evaluation.
- Traffic Analysis Should not even know who is communicating with whom. Why?
- Emerging Applications Online Voting, Auctions (more later)

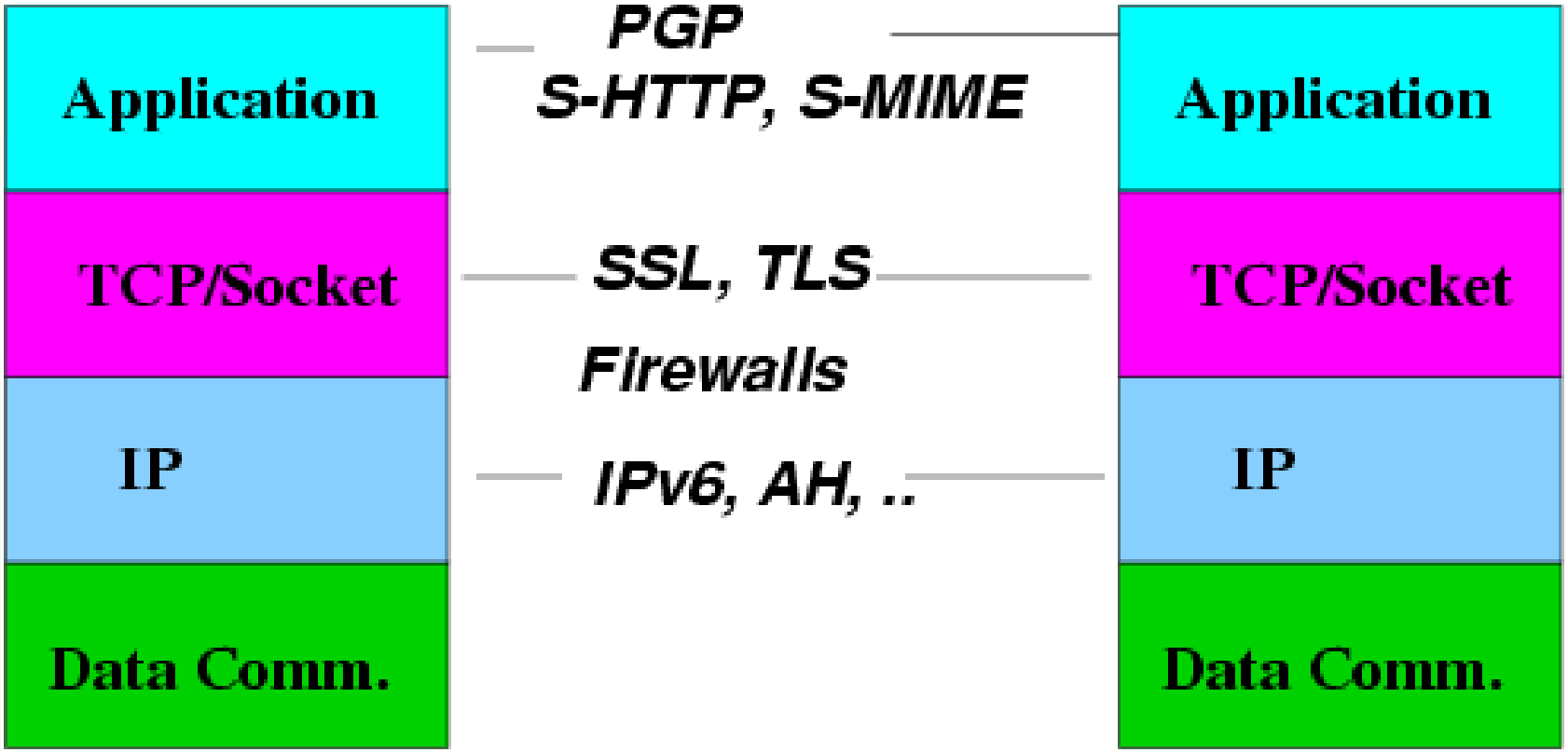
And all this with postcards (IP datagrams)!

Security Mechanisms

- **System Security:** "Nothing bad happens to my computers and equipment"
  virus, trojan-horse, logic/time-bombs, ...
- **Network Security:**
  - **Authentication Mechanisms** "you are who you say you are"
  - **Access Control** Firewalls, Proxies "who can do what"
- **Data Security:** "for your eyes only"
  - Encryption, Digests, Signatures, ...

We'll focus on Network security.

Network Security Mechanism Layers

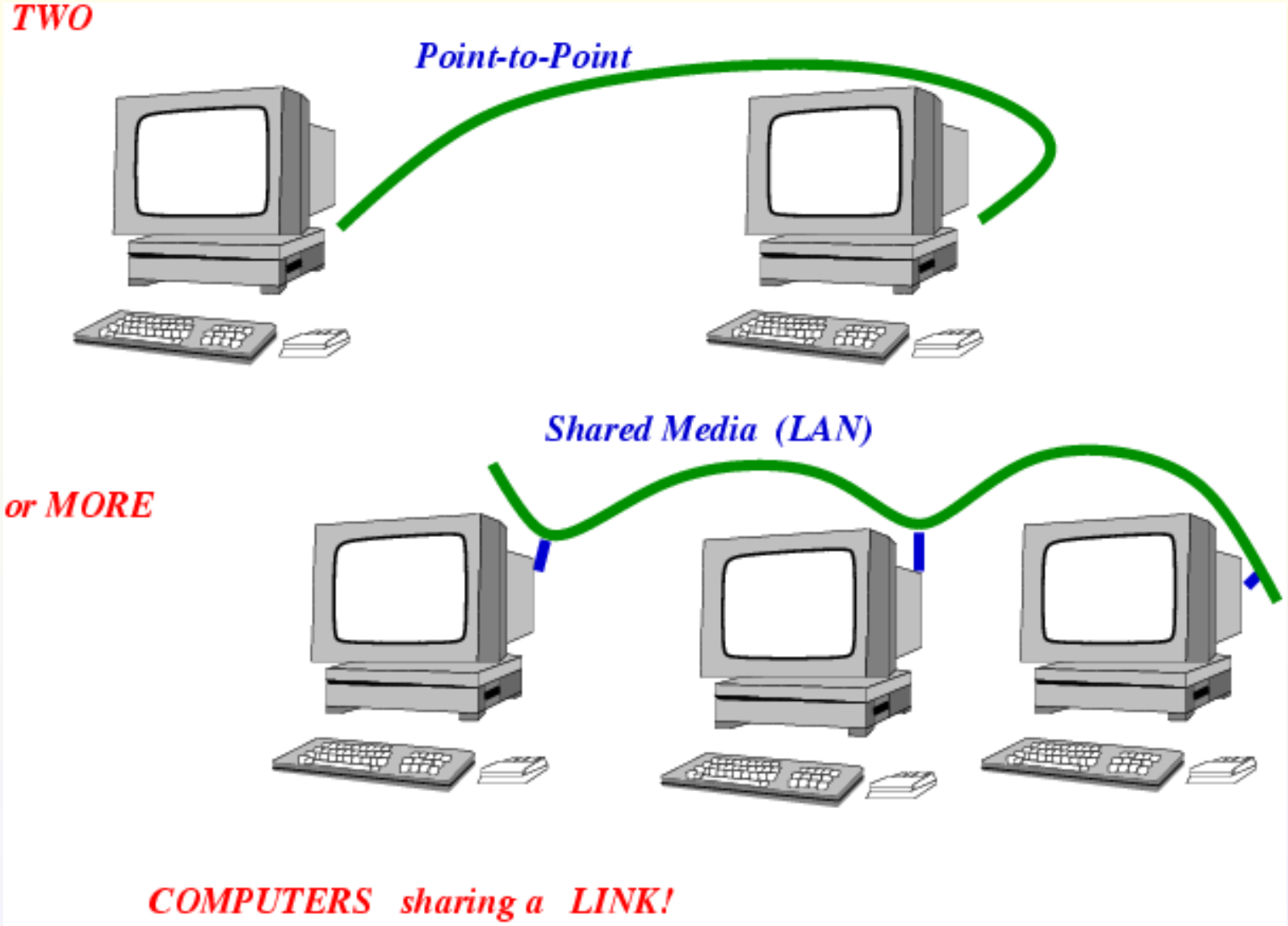


Encryption can be done at any level!

Higher-up: more overhead (for each application)

but better control

What is a Computer Network?



Point-to-Point Network

- No need to identify each other!
- Sharing of link easy
- Need for error detection/correction?
- Point-to-Point Protocol (RFC 1661, 2153)
  - A method for **encapsulating** multi-protocol datagrams.
  - A **Link Control Protocol (LCP)** for establishing, configuring, and testing the data-link connection.
  - A family of **Network Control Protocols (NCPs)** for establishing and configuring different network-layer protocols.
- Multiple links can be multiplexed (PPMLP)

Carrier Sense

- Politeness *make a link*

  If you hear some one talking, wait until she finishes.

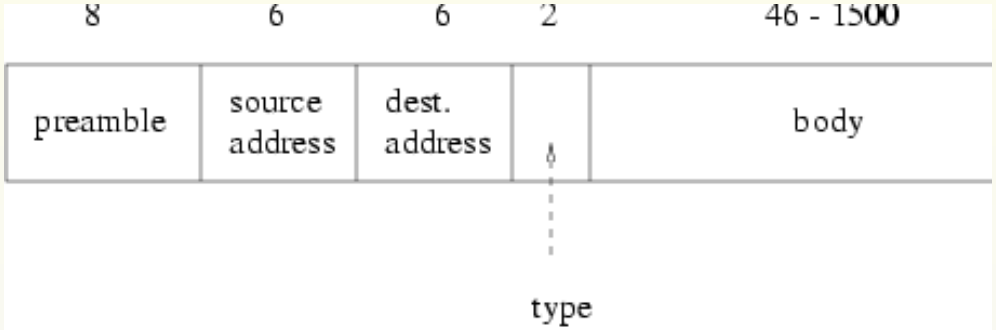
- Persistent (Greedy!)

  Start immediately after line becomes free. This leads to COLLISION.

- Non-Persistent

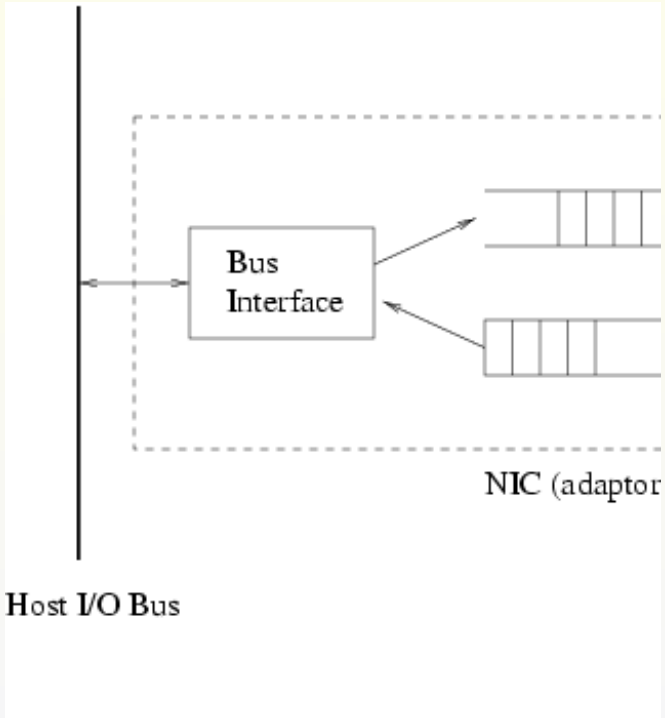
  Wait for some (random) time, before trying!

Ethernet Frame Format



- Preamble 10 MHz. square wave 10101010 for synchronization
- Body = Data + Padding
- Frame Length Min = 64 bytes, Max = 1518 bytes (why?)
- Ethernet Address (48 bits) Exmample: 08:00:0D:01:74:71

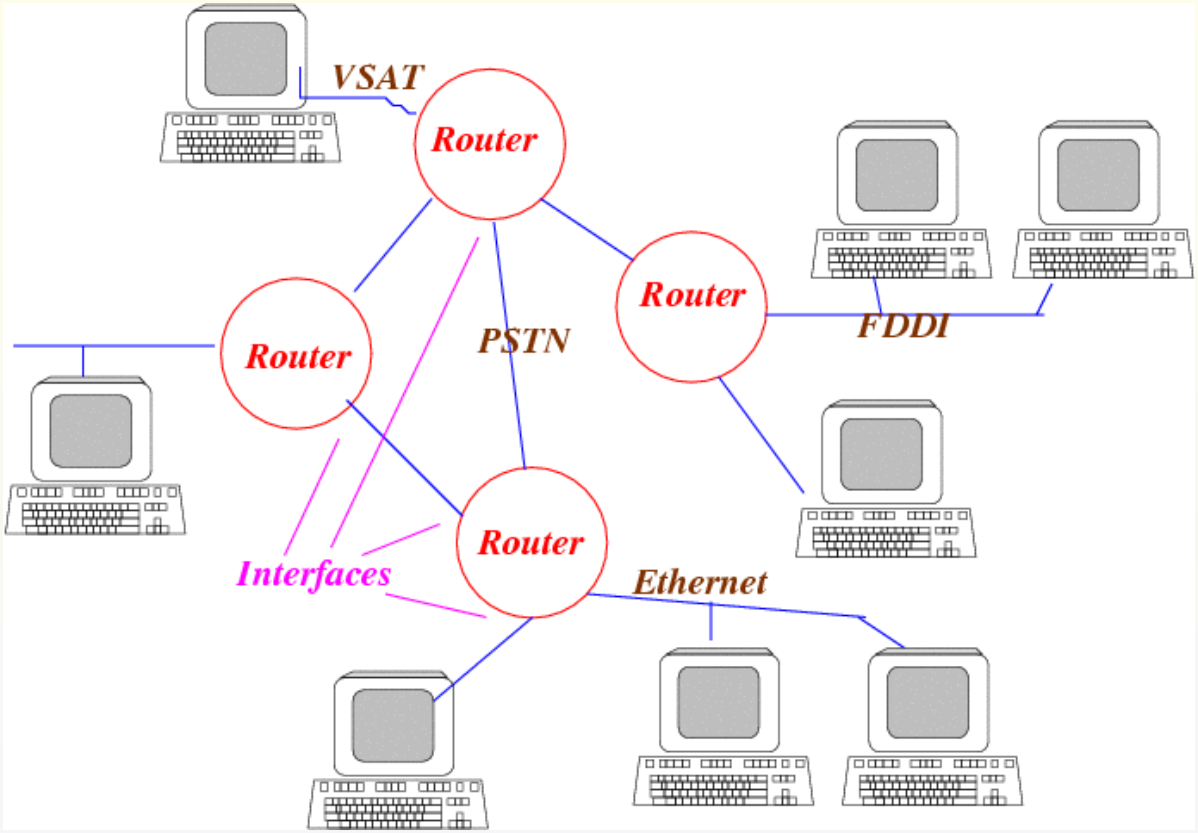
Ethernet Cards



- Polling vs. Interrupt (less work)
- Direct Memory Access (DMA) vs. Programmed IO

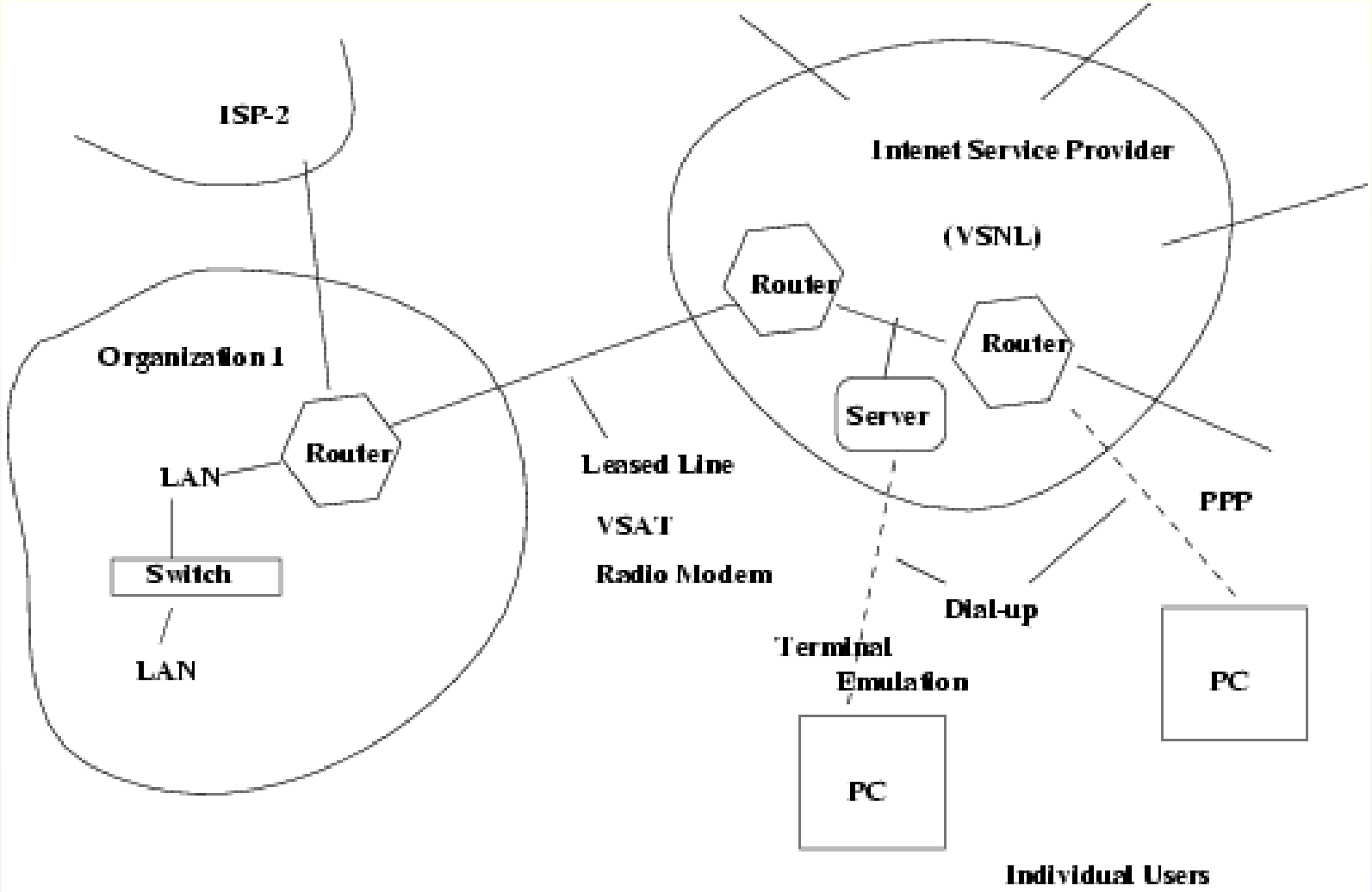
So, what's Internet?

- A bottom-up collection (**interconnection**) of networks



- TCP/IP is the **only** common factor
- Bureaucracy-free, reliable, cheap
- Decentralized, democratic, chaotic

Physical View of Internet

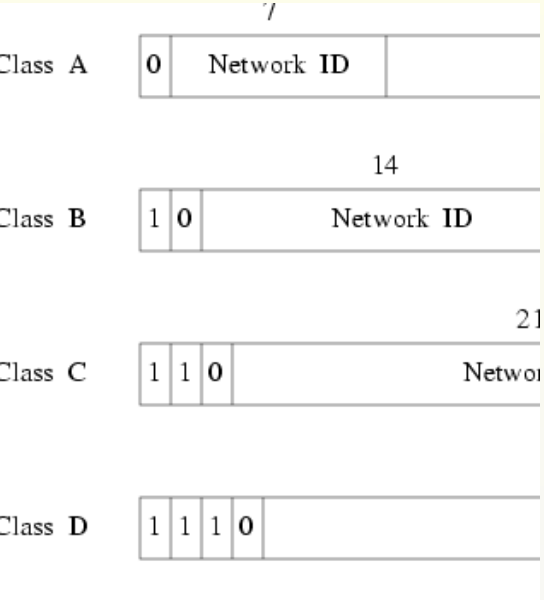


What is an IP address?

- Logical Address at Network Layer
- Not a physical address (Datalink/MAC address)
- Network cards/technology can be changed
- Machine itself can be changed
- Analogy with Organizations
  - Manager Sales, WIPRO, Bangalore
  - Mr. S. Ramesh, WIPRO, Bangalore
- One address per interface (not machine)
- One machine can have many addresses (Cabinet posts!)

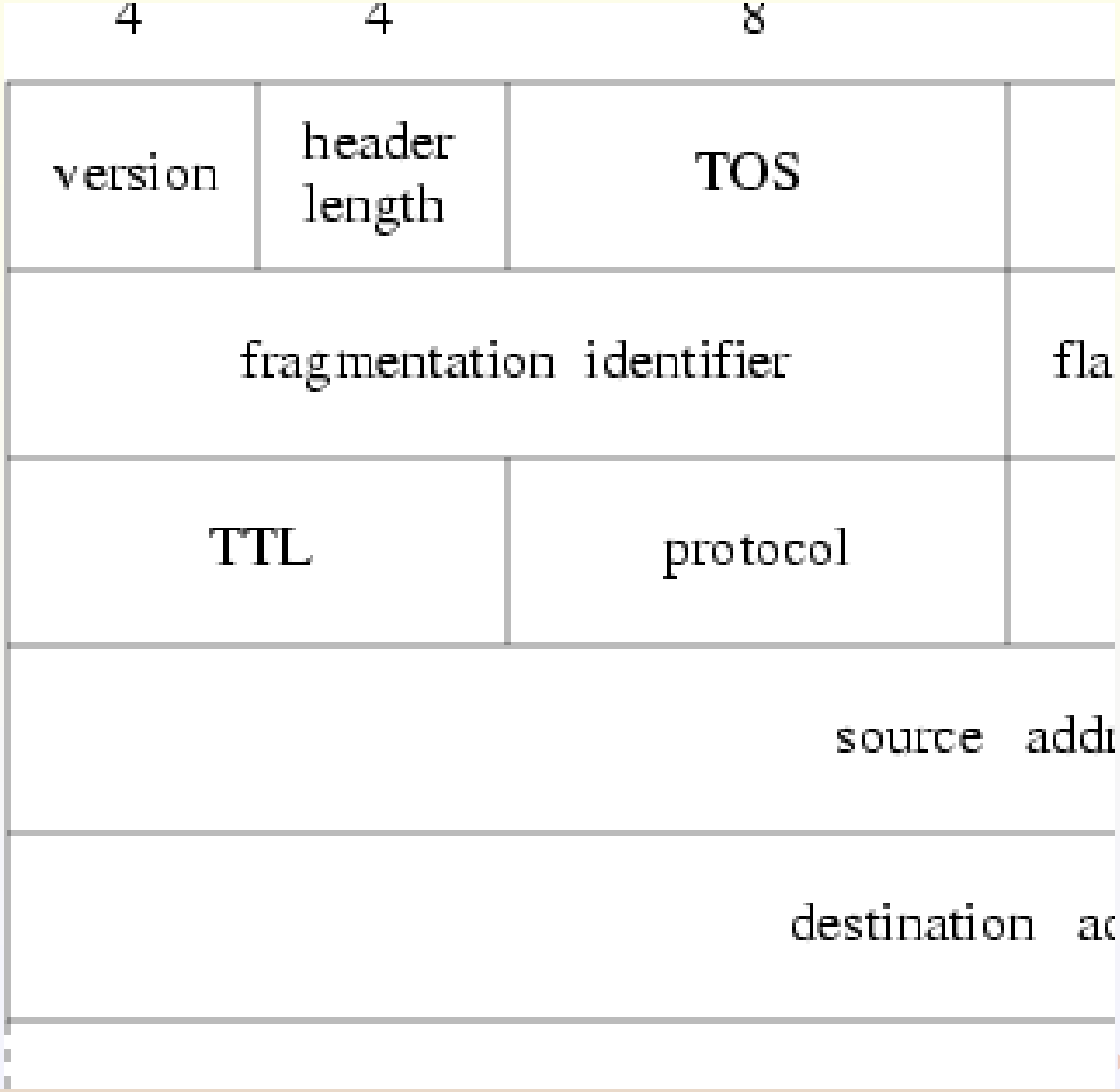
IP addresses

Two Parts: Network-number, Host-number

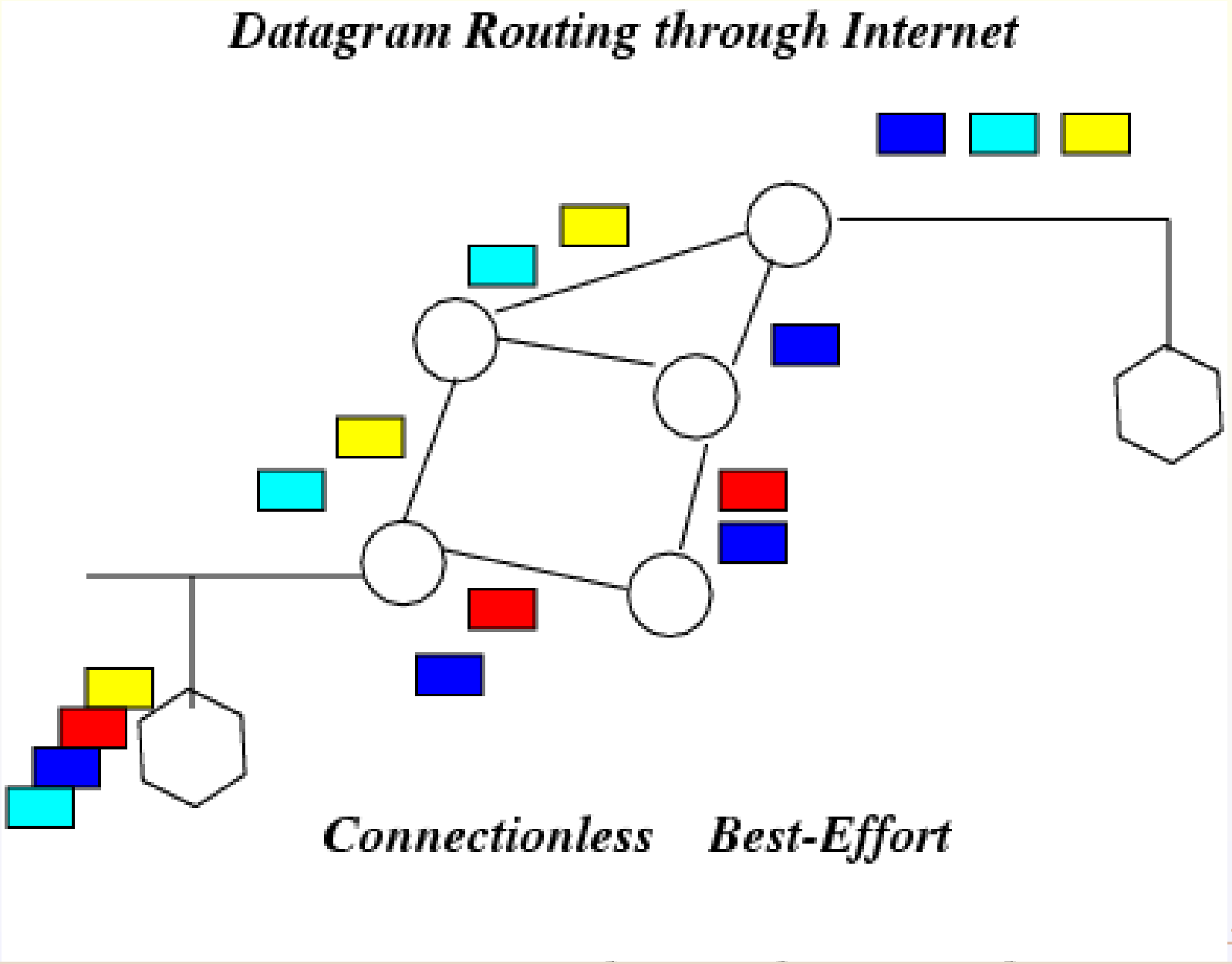


- Dotted decimal notation
- 144.16.111.2 (Class B)
- 202.54.44.120 (Class C)
- Machines on the same "network" have same "network" number. Like PIN code.
- Useful for "routing"

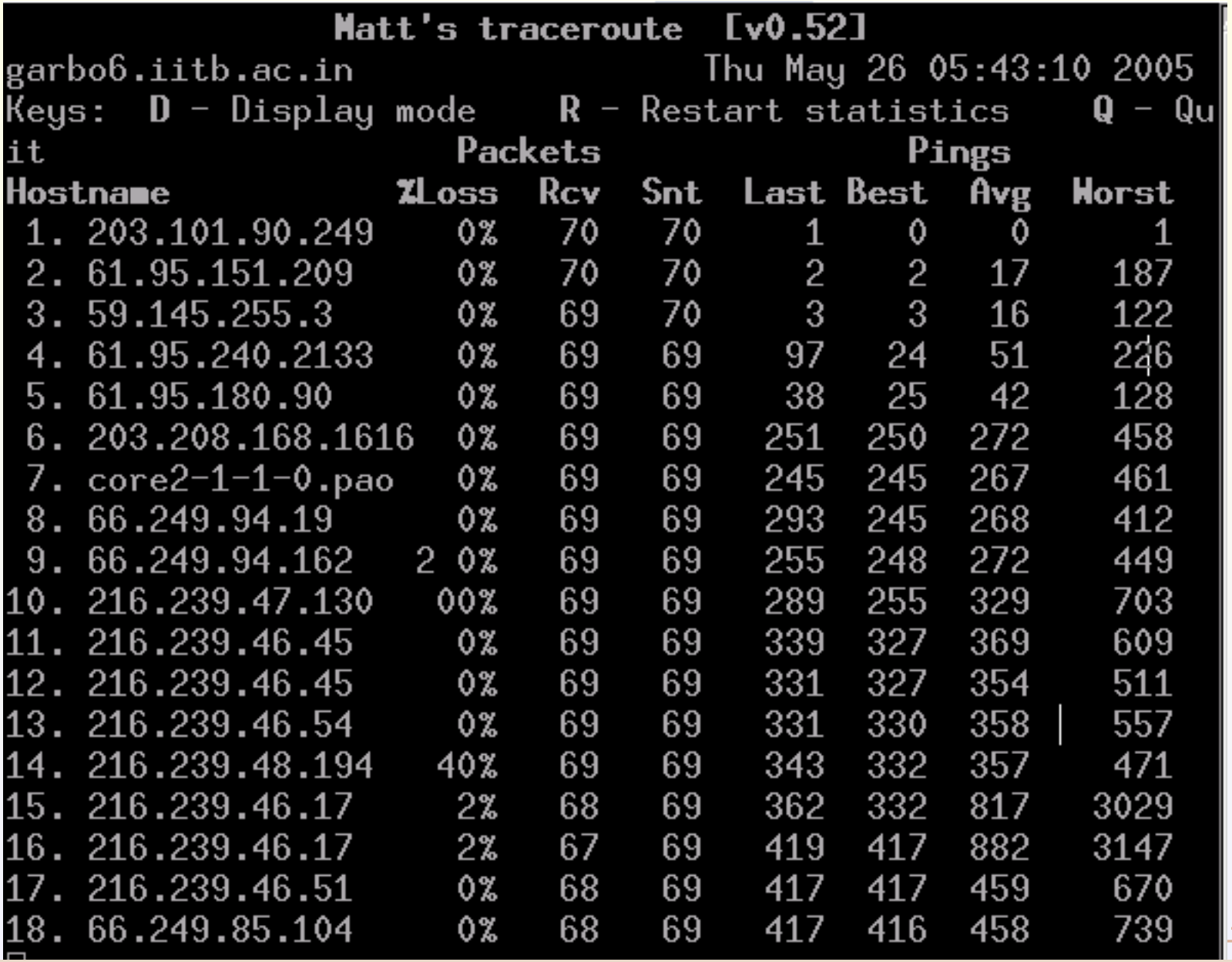
IP Datagram


4
4
8
version
header length
TOS
fragmentation identifier
fla
TTL
protocol
source addı
destination ac

Packet Switching in Internet



TRACEROUTE



```
                Matt's traceroute  [v0.52]
garbo6.iitb.ac.in                        Thu May 26 05:43:10 2005
Keys:  D - Display mode    R - Restart statistics    Q - Qu
it                          Packets                 Pings
Hostname                 %Loss  Rcv  Snt  Last Best  Avg  Worst
 1. 203.101.90.249         0%   70   70     1    0    0      1
 2. 61.95.151.209          0%   70   70     2    2   17    187
 3. 59.145.255.3           0%   69   70     3    3   16    122
 4. 61.95.240.2133         0%   69   69    97   24   51    246
 5. 61.95.180.90           0%   69   69    38   25   42    128
 6. 203.208.168.1616       0%   69   69   251  250  272    458
 7. core2-1-1-0.pao        0%   69   69   245  245  267    461
 8. 66.249.94.19           0%   69   69   293  245  268    412
 9. 66.249.94.162        2 0%   69   69   255  248  272    449
10. 216.239.47.130        00%   69   69   289  255  329    703
11. 216.239.46.45         0%   69   69   339  327  369    609
12. 216.239.46.45         0%   69   69   331  327  354    511
13. 216.239.46.54         0%   69   69   331  330  358    557
14. 216.239.48.194       40%   69   69   343  332  357    471
15. 216.239.46.17         2%   68   69   362  332  817   3029
16. 216.239.46.17         2%   67   69   419  417  882   3147
17. 216.239.46.51         0%   68   69   417  417  459    670
18. 66.249.85.104         0%   68   69   417  416  458    739
```

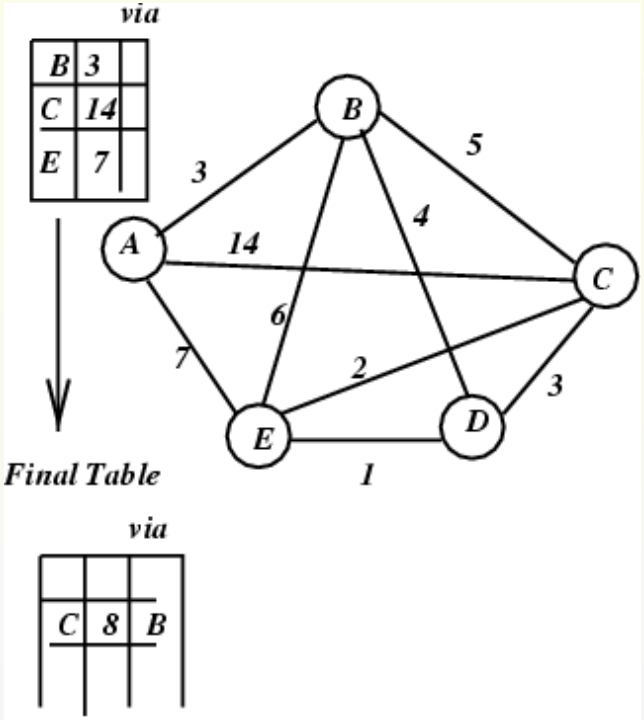
IP Routing

- Behaviour of Host
  - Destination on my net?
  - If yes, use ARP and deliver directly
  - If no, give to default gateway
- Behaviour of Gateway
  - Am I the destination IP?
  - If not, which interface to forward on?
  - Consult Routing Tables to decide

What are the security issues?

How Gateways Learn Routes

Routing Information Protocol (RIP) [RFC 1058]

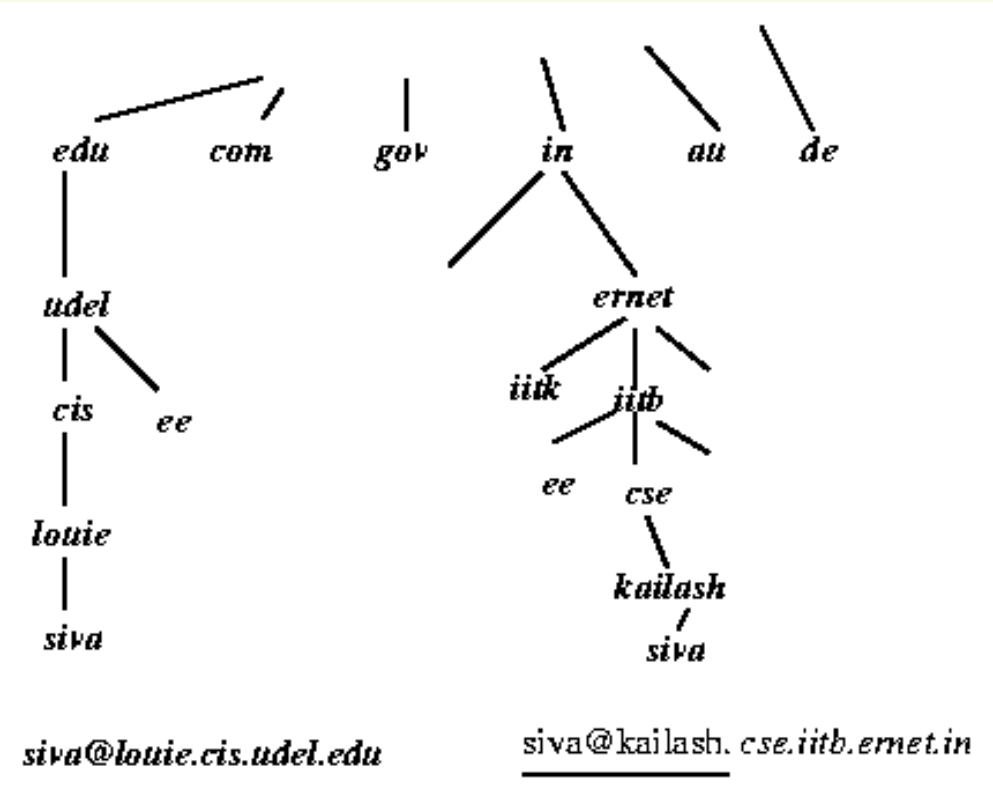


Open Shortest Path First (OSPF) [RFC 1131]

Security compromises possible!

Domain Name Service (DNS)

- Flat vs. Hierarchical Name Space
- How to find the name of K. R. Narayan's cook?
- Logical View of Internet



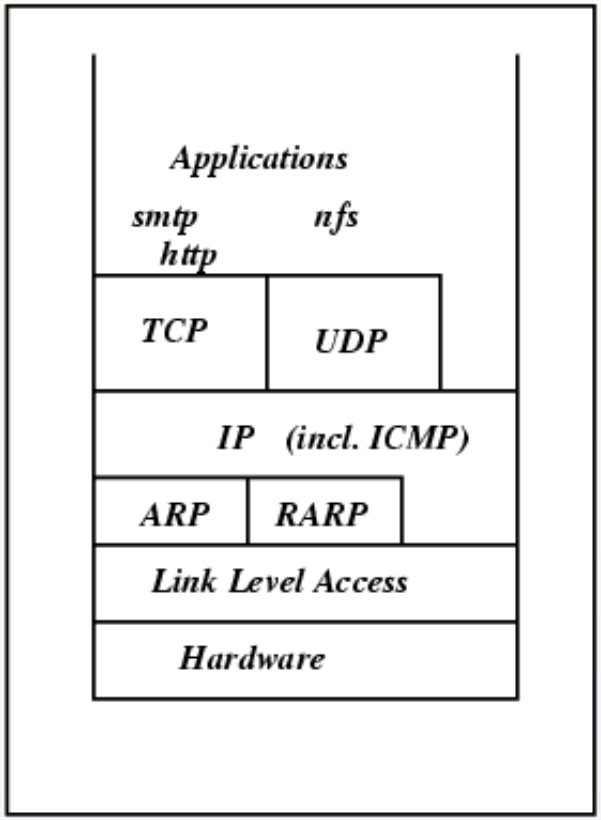
How DNS works

- Globally distributed data base
- Caching to improve performance
- Name Server Daemons
  - BIND, named
- Resolver clients
  - nslookup
- Reverse Address Mapping Also

Security issues galore!

TCP/IP Stack

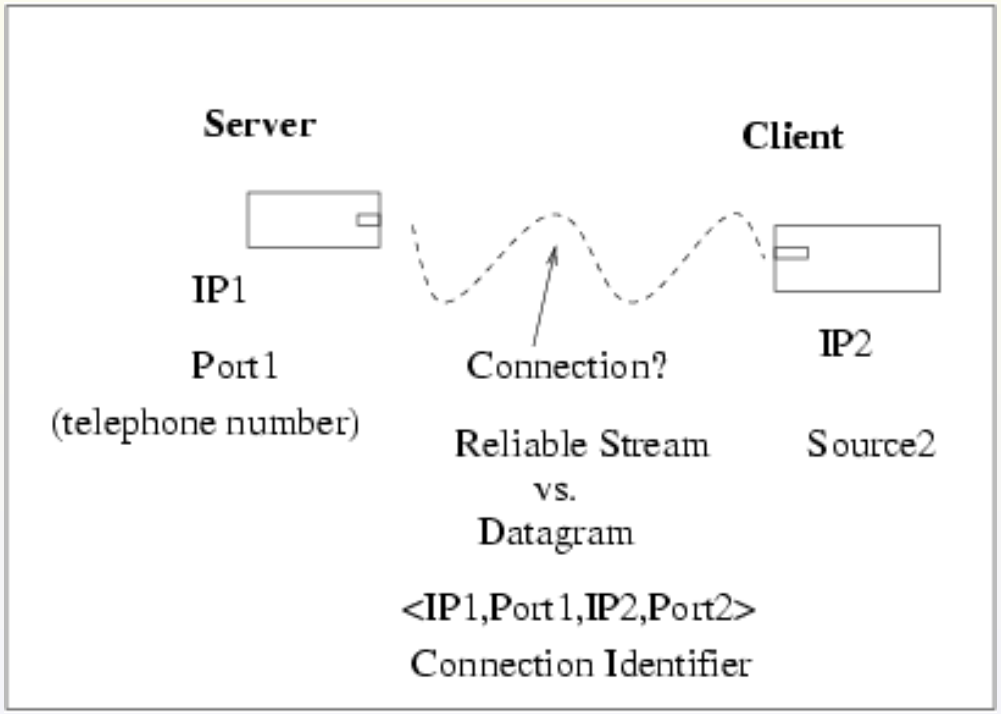
- Open Standard (RFCs)
- Defacto Industry Standard
- Suitable for LAN and WAN
- IP is *connectionless* datagram service
- Adaptive Features (congestion and faults)



What is a Socket?

Analogy with Telephone

Instrument, Number, Line



Example Applications

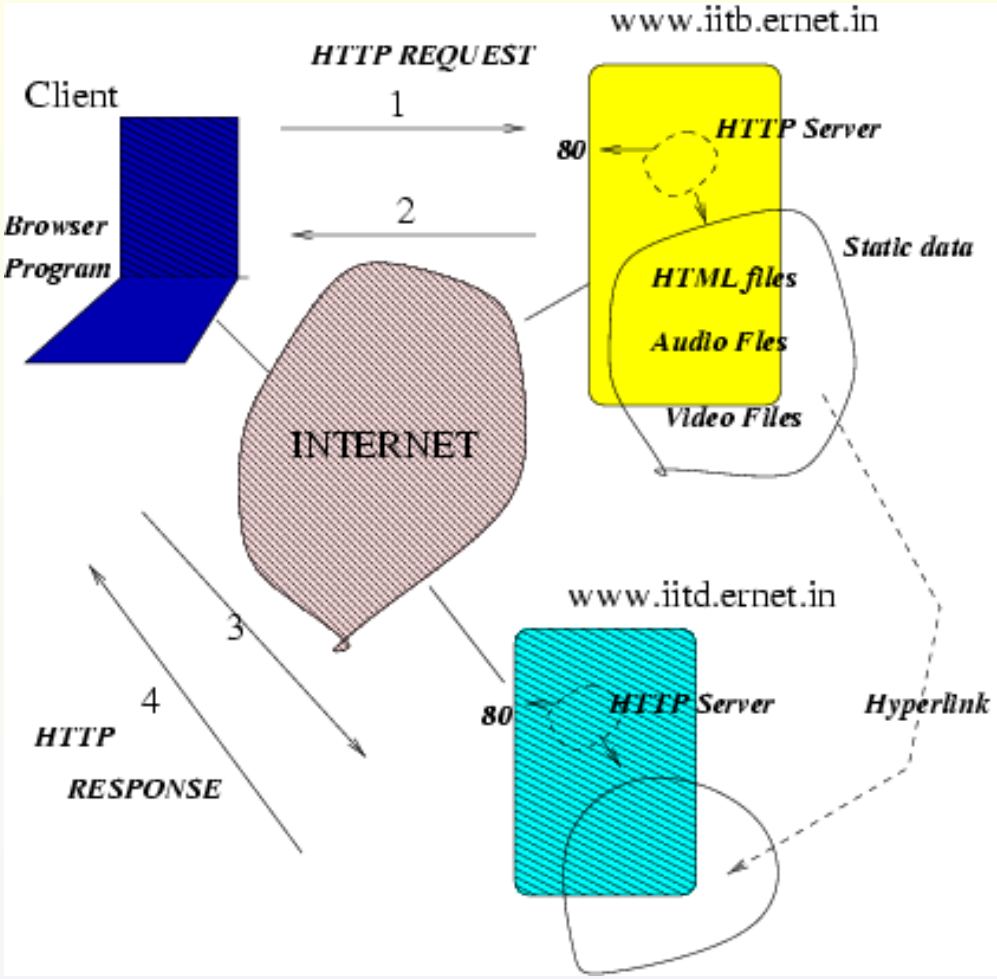
From */etc/services* on Unix

- **Connection Oriented (TCP)**

Client	Server	Port
Mail	smtpd	25
Telnet	telnetd	23
FTP	ftpd	20,21
WWW Browser	httpd	80

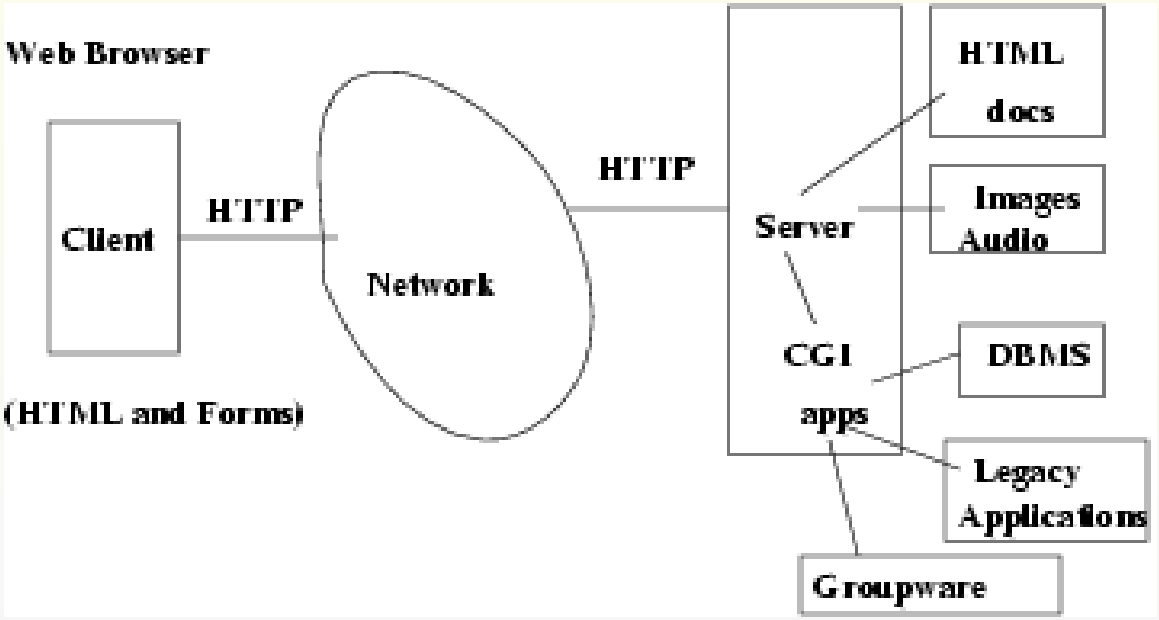
- **Connectionless (UDP)**
  - NFS
  - DNS
  - ...

Web Model



- Hyper-Text Transfer Protocol (HTTP)
- Browser decides how to display

CGI and Databases



Emerging Scenario

- Explosive Growth in Internet, Corporate Intranets
- Surge in E-commerce
- Critical Dependence on "Information Infrastructure"
- "Information Warfare"
- Hence need for:
  - Performance
  - Reliability (Fault Tolerance)
  - Scaleability (With growth in size)
  - Security

Broad Outline of Security Plan (RFC 2196)

- Identify what you are trying to protect.
- Determine what you are trying to protect it from.
- Determine how likely the threats are.
- Implement measures which will protect your assets in a cost-effective manner.
- Review the process continuously and make improvements each time a weakness is found.

  Cost of protecting yourself against a threat should be less than the cost of recovering if the threat were to strike you.

More on firewalls and secure services later!

References

1. "Computer Networks" Andrew Tannenbaum, 3rd Edition, Prentice Hall, (approx. Rs. 125)
2. "Data Communications" Bertsekas and Gallagher, 1992, Prentice Hall, (approx. Rs. 125)
3. "Internetworking With TCP/IP, Volume I: Principles, Protocols, and Architecture Volume II: Design, Implementation, and Internals and Volume III: Client-Server Programming," Douglas E. Comer. 1991, Second Edition, Prentice Hall.
4. "Unix Network Programming" Richard Stevens, Prentice Hall.
5. *Cryptography and Network Security: Principles and Practice* by William Stallings (2nd Edition), Prentice Hall Press; 1998.
6. *Practical Unix and Internet Security,* Simson Garfinkel and Gene Spafford, O'Reilly and Associates, ISBN 1-56592-148-8.
7. Web sites
   - *www.cerias.purdue.edu* (Centre for Education and Research in Information Assurance and Security)