

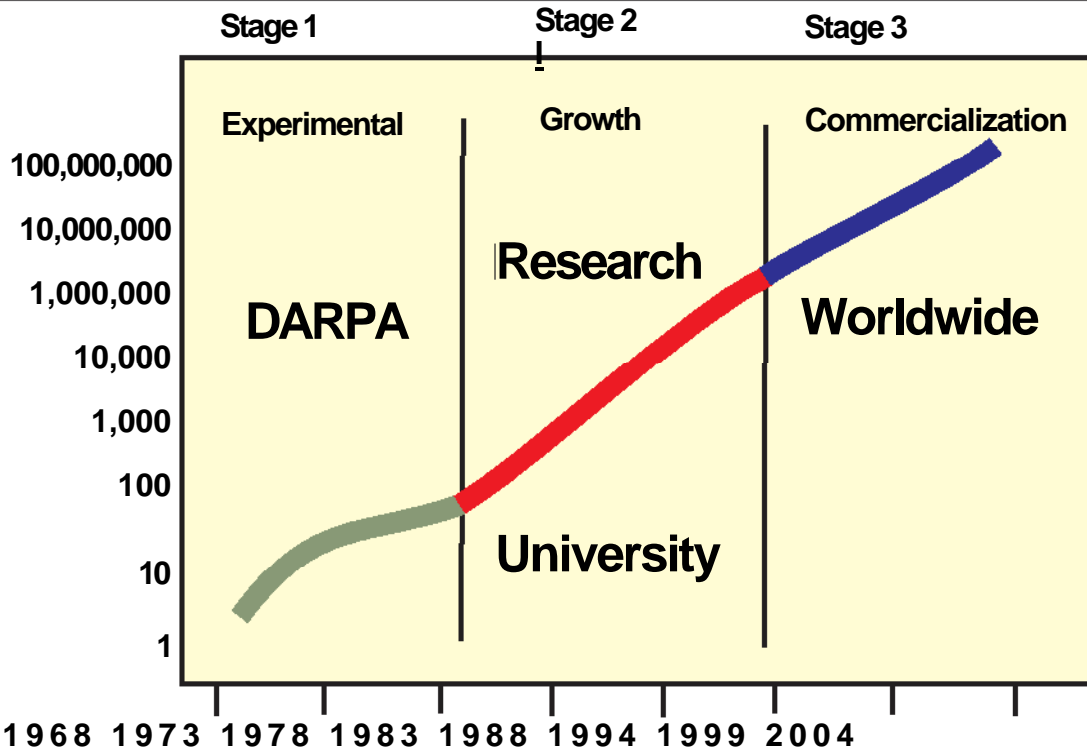
Introduction to TCP/IP

SHARE Summer 2010 Boston



Laura Knapp
AES WW Business Consultant
laurak@aesclever.com
laura@lauraknapp.com

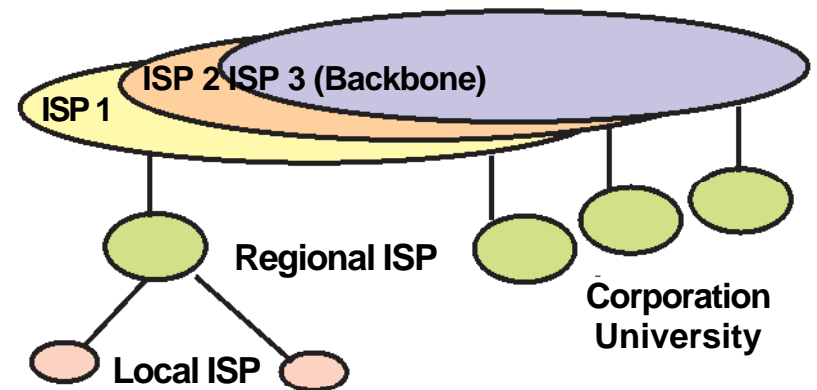
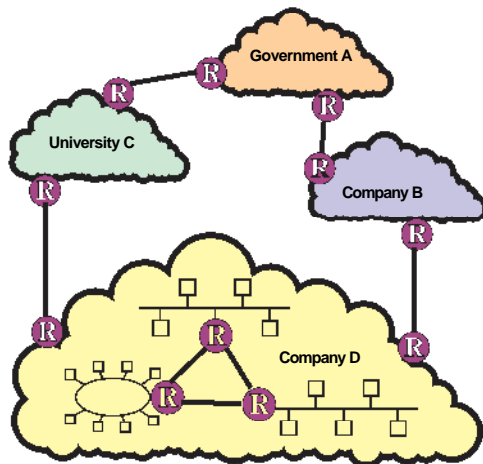
TCP/IP History



Jan 2009
over
600,000,000

In the 1980's 1968 1973 1978 1983 1988 1994 1999 2004

Today



Internet - World Wide Web - WWW

Infrastructure (Just to name a few)

Hardware: Routers, Switches

Protocols – TCP/IP, ICMP, RSVP, IMAP,

Facilitators – DNS, DHCP, Firewalls, Intrusion Detection, Virus scanners

.....

Content (Just to name a few)

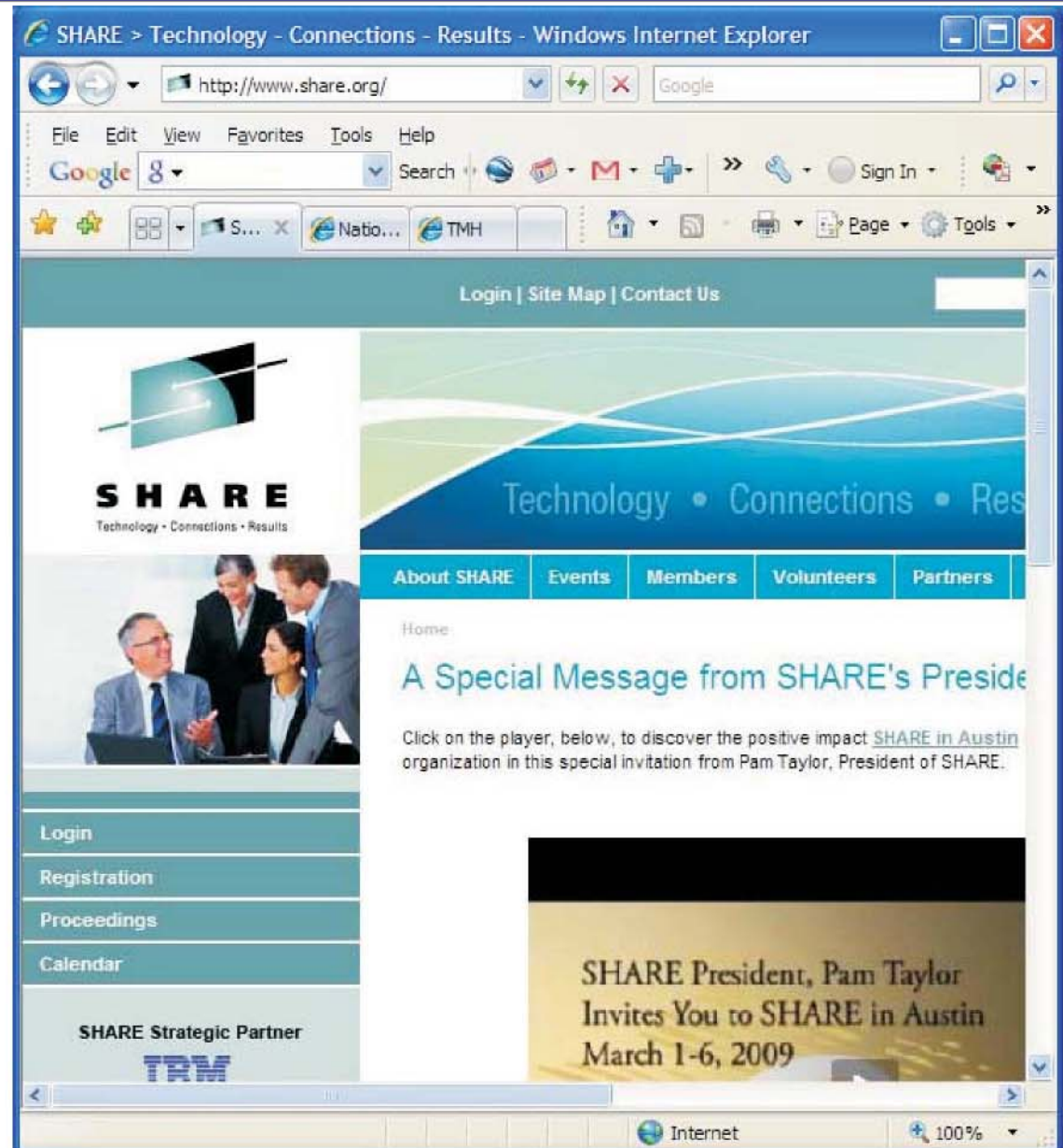
HTML – Hypertext Markup Language

PHTML – aka PHP – another scripting language

BPEL – Business Process Execution Language

JSML – JScript Markup Language

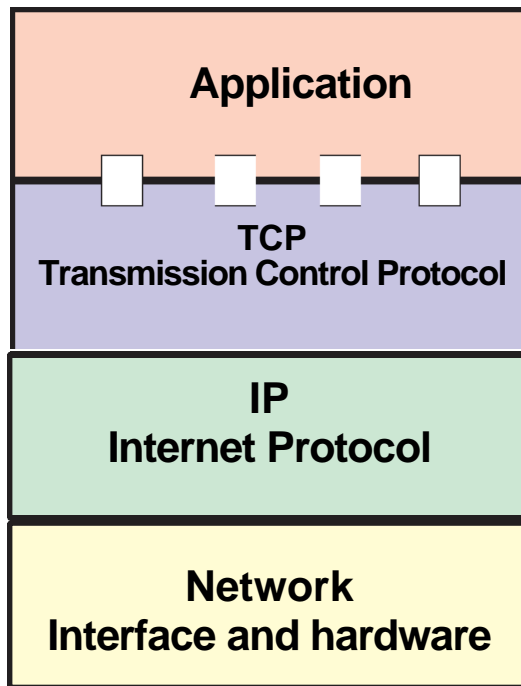
.....



TCP/IP Layered Architecture



Browser



**WWW, mail, file transfer,
remote access**

Application interfaces

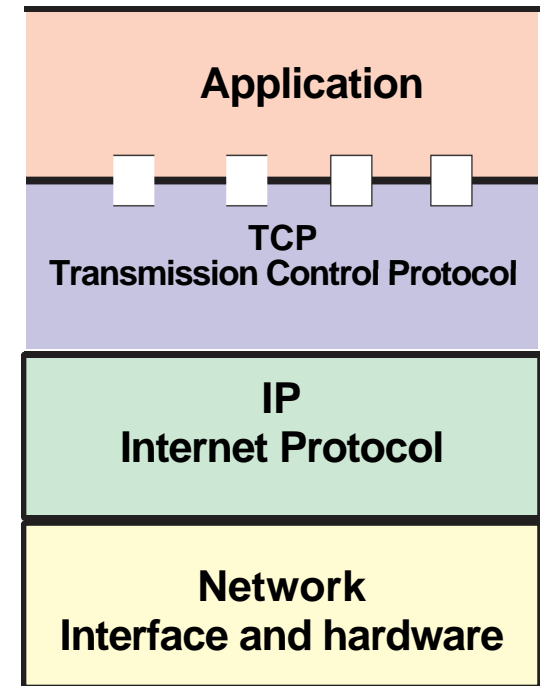
End-to-end delivery

Best effort delivery

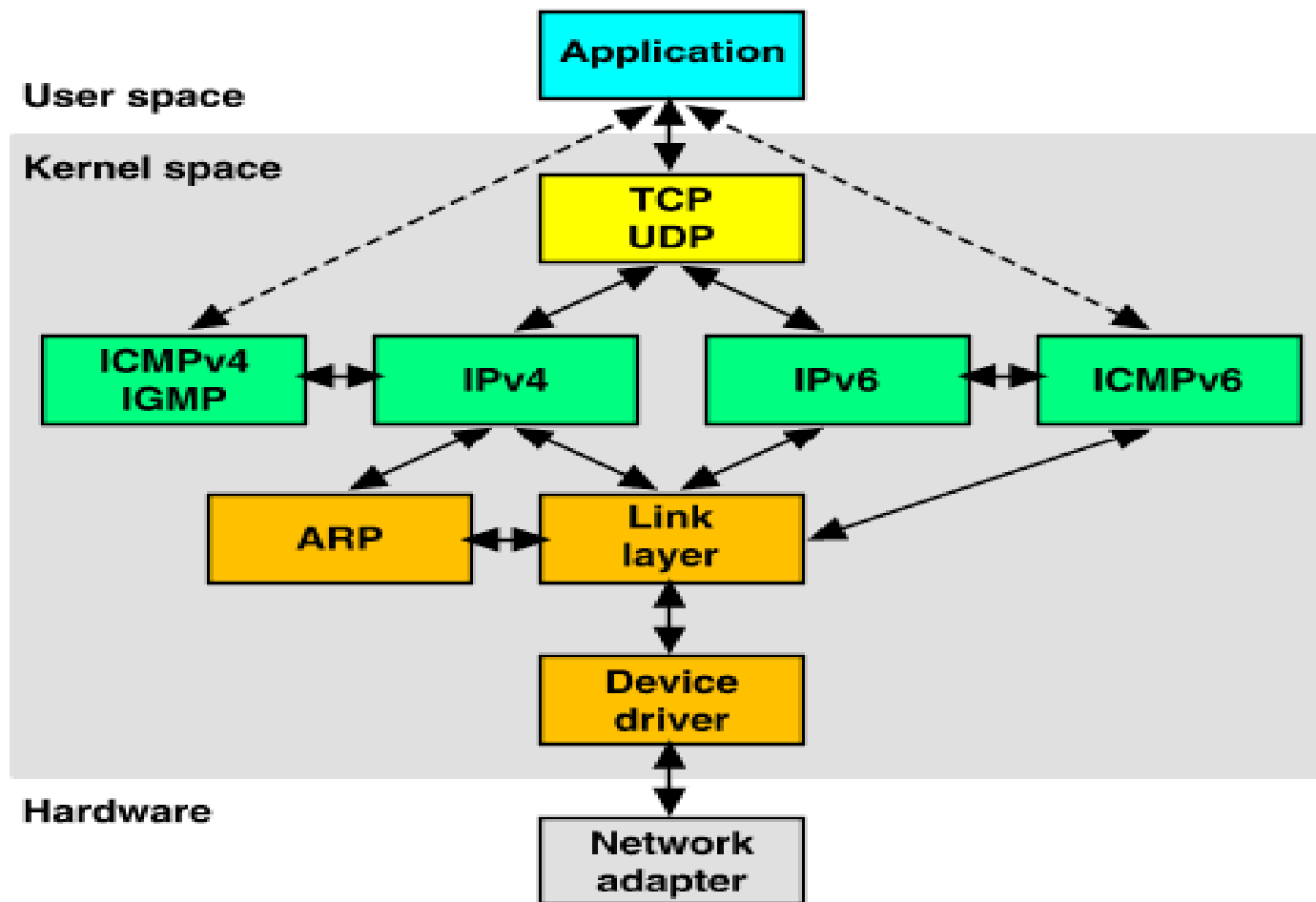
Physical connection



Server



TCP/IP Stacks



Source: http://uw713doc.sco.com/en/NET_tcpip/tcpN.tcpip_stack.html

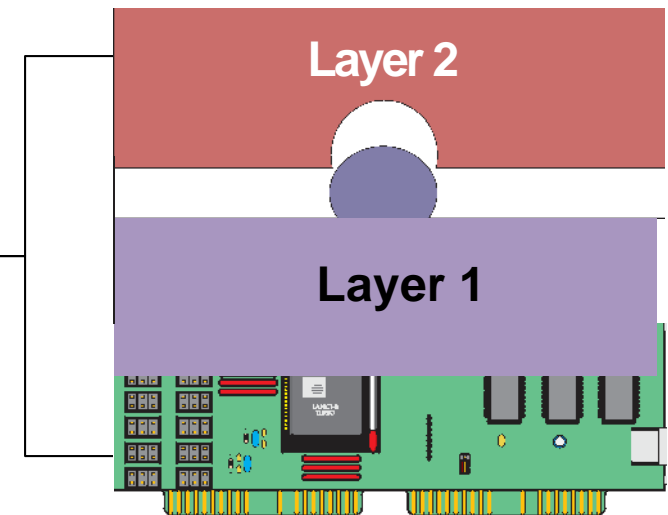
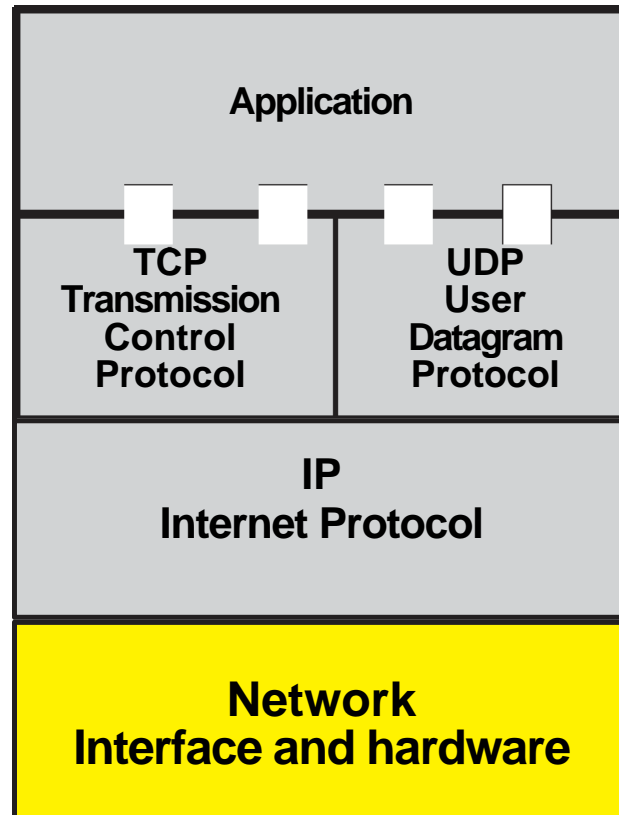
Network Interface Layer

7(8) Layer OSI Model

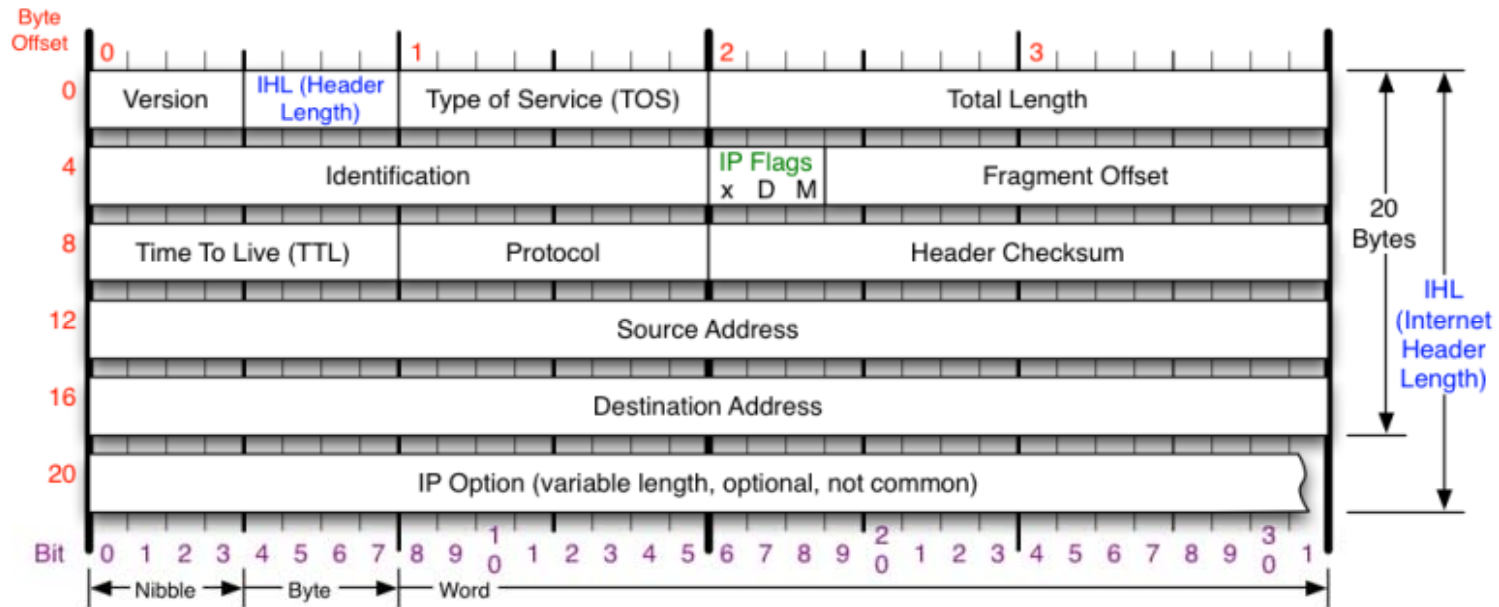
Layer Function

8	End User (Politics)
7	Application
6	Presentation
5	Session
4	Transport
3	Network
2	Data Link
1	Physical

4 layer TCP/IP Model



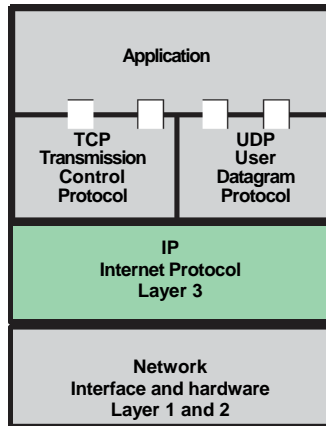
IP Header



<p>Version</p> <p>Version of IP Protocol. 4 and 6 are valid. This diagram represents version 4 structure only.</p>	<p>Protocol</p> <p>IP Protocol ID. Including (but not limited to):</p> <table border="0"> <tr> <td>1 ICMP</td> <td>17 UDP</td> <td>57 SKIP</td> </tr> <tr> <td>2 IGMP</td> <td>47 GRE</td> <td>88 EIGRP</td> </tr> <tr> <td>6 TCP</td> <td>50 ESP</td> <td>89 OSPF</td> </tr> <tr> <td>9 IGRP</td> <td>51 AH</td> <td>115 L2TP</td> </tr> </table>	1 ICMP	17 UDP	57 SKIP	2 IGMP	47 GRE	88 EIGRP	6 TCP	50 ESP	89 OSPF	9 IGRP	51 AH	115 L2TP	<p>Fragment Offset</p> <p>Fragment offset from start of IP datagram. Measured in 8 byte (2 words, 64 bits) increments. If IP datagram is fragmented, fragment size (Total Length) must be a multiple of 8 bytes.</p>	<p>IP Flags</p> <table border="0"> <tr> <td>x</td> <td>D</td> <td>M</td> </tr> </table> <p>x 0x80 reserved (evil bit) D 0x40 Do Not Fragment M 0x20 More Fragments follow</p>	x	D	M
1 ICMP	17 UDP	57 SKIP																
2 IGMP	47 GRE	88 EIGRP																
6 TCP	50 ESP	89 OSPF																
9 IGRP	51 AH	115 L2TP																
x	D	M																
<p>Header Length</p> <p>Number of 32-bit words in TCP header, minimum value of 5. Multiply by 4 to get byte count.</p>	<p>Total Length</p> <p>Total length of IP datagram, or IP fragment if fragmented. Measured in Bytes.</p>	<p>Header Checksum</p> <p>Checksum of entire IP header</p>	<p>RFC 791</p> <p>Please refer to RFC 791 for the complete Internet Protocol (IP) Specification.</p>															

Source: <http://nmap.org/book/images/hdr/MJB-IP-Header-800x576.png>

IP - Internet Protocol



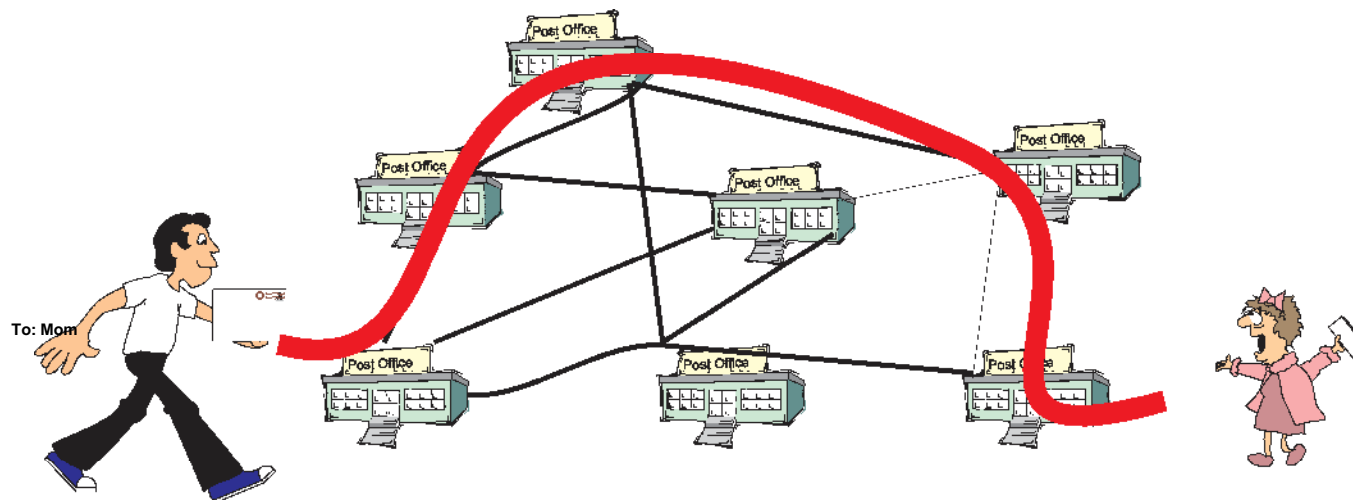
Data transferred in self contained units called datagrams

20 byte IP header

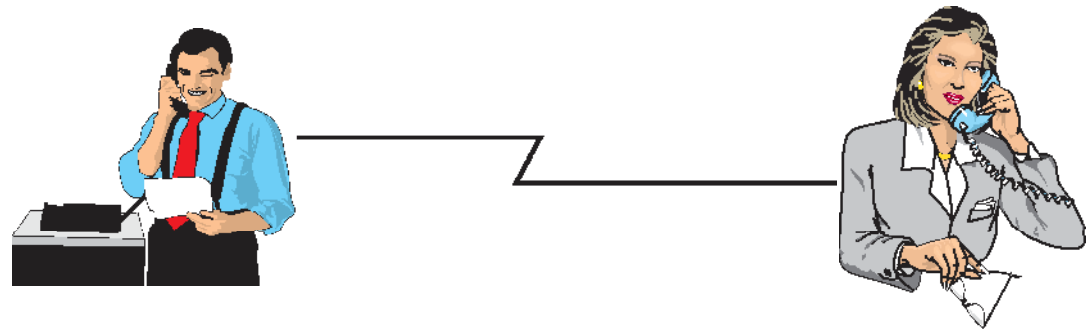
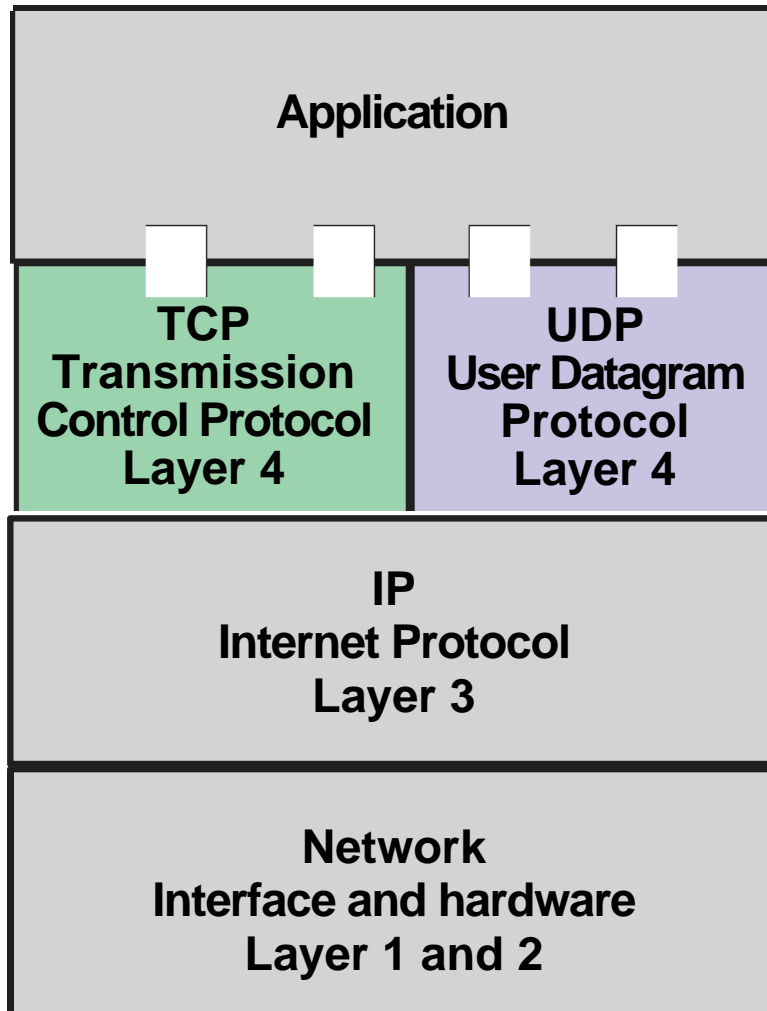
Best effort delivery -- no guarantee

Dynamic path selection for every datagram

Handles datagram fragmentation & reassembly



TCP - Transmission Control Protocol



Connection established

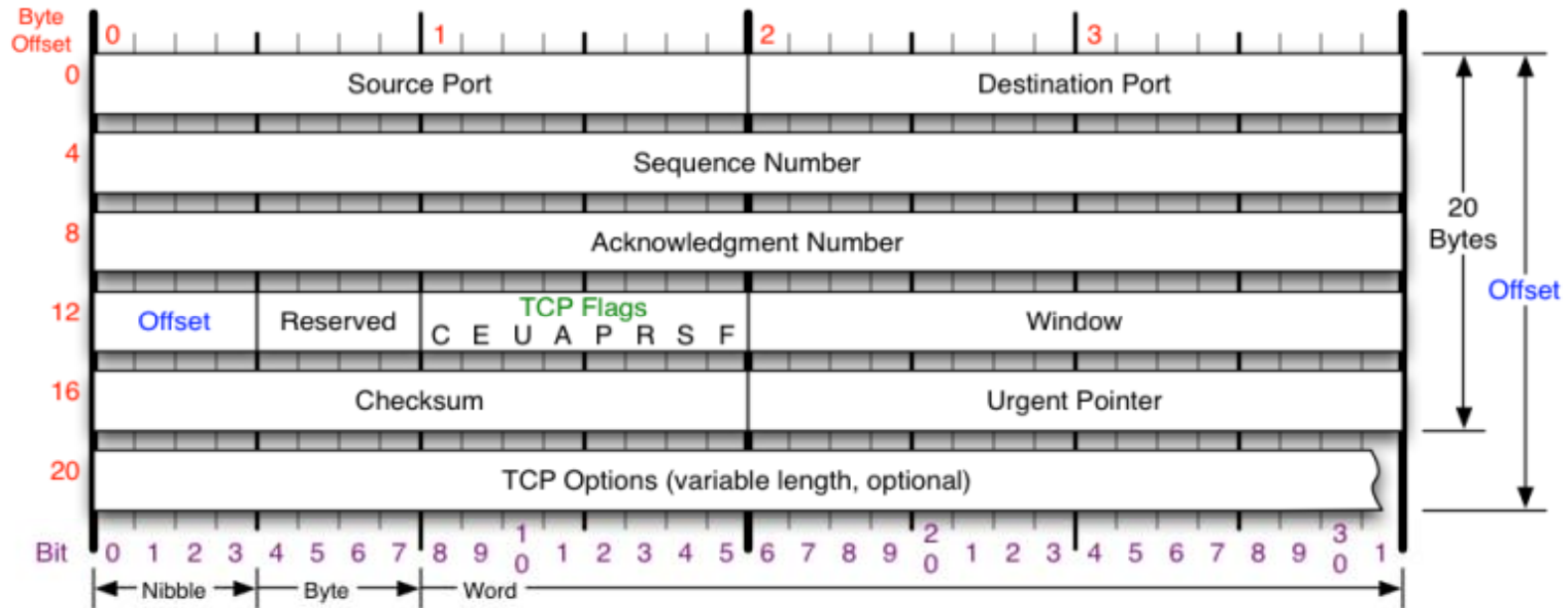
End-to-end acknowledgments

Orderly delivery of datagrams to application

Error and flow control

Connection takedown

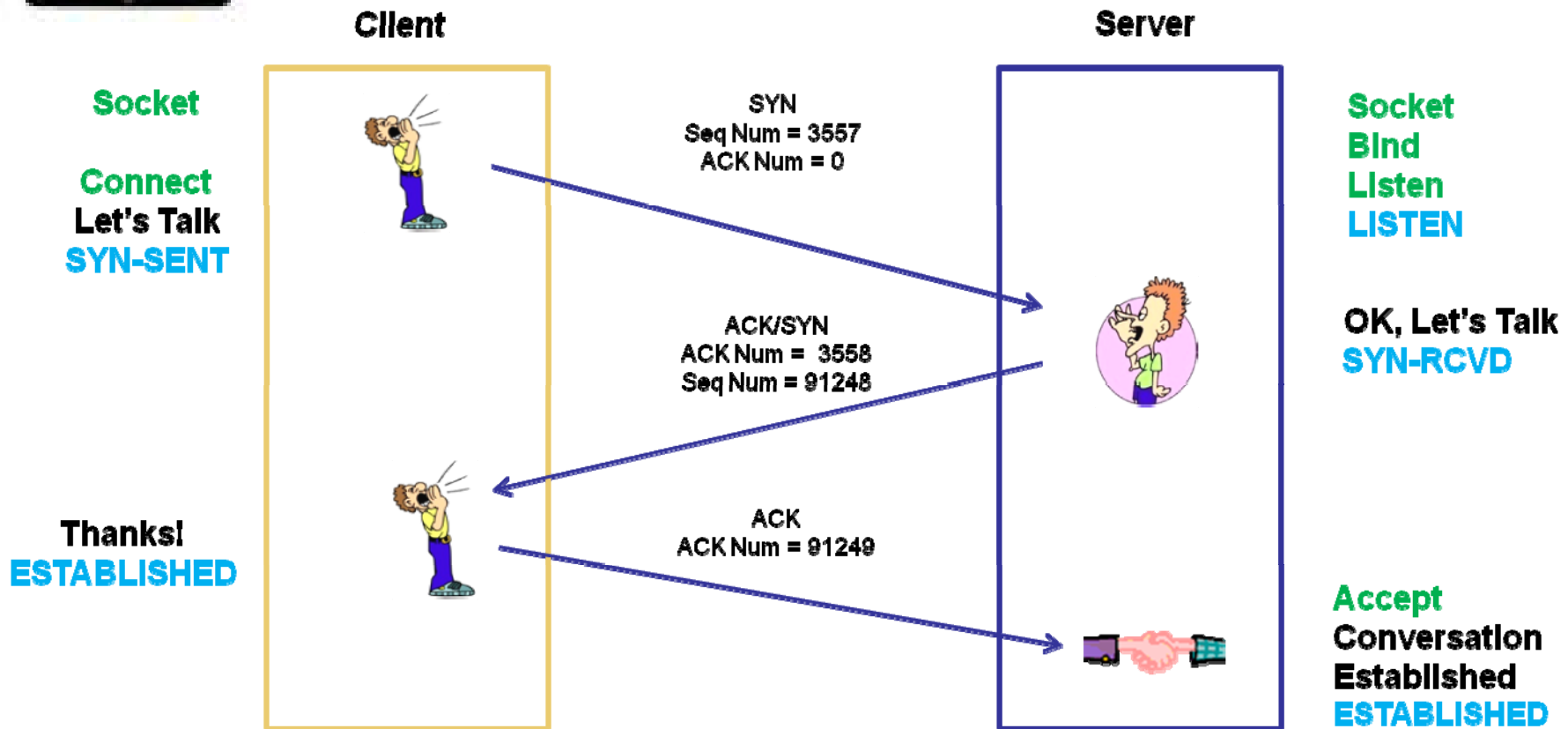
TCP - Header



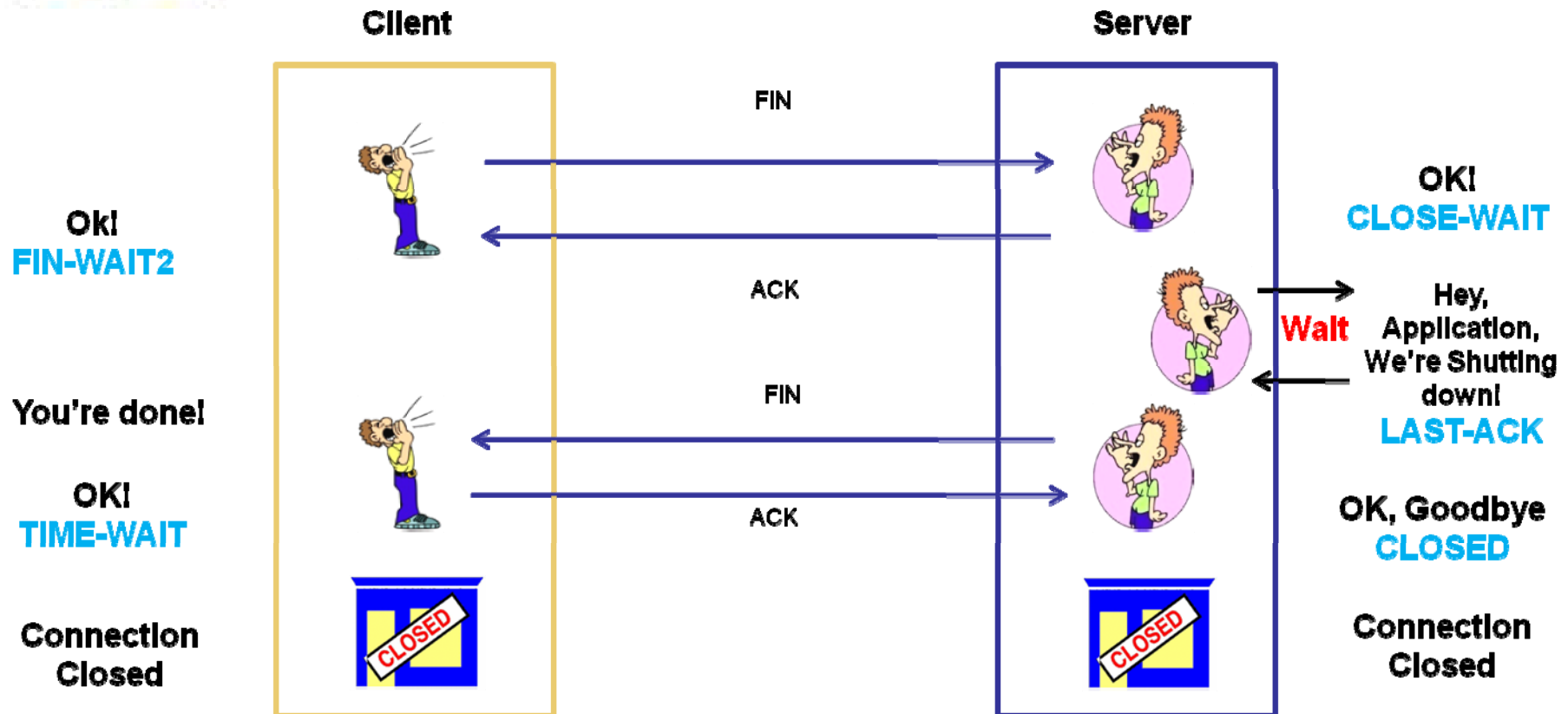
TCP Flags	Congestion Notification	TCP Options	Offset																											
C E U A P R S F	ECN (Explicit Congestion Notification). See RFC 3168 for full details, valid states below.	0 End of Options List 1 No Operation (NOP, Pad) 2 Maximum segment size 3 Window Scale 4 Selective ACK ok 8 Timestamp	Number of 32-bit words in TCP header, minimum value of 5. Multiply by 4 to get byte count.																											
<p>Congestion Window</p> <p>C 0x80 Reduced (CWR)</p> <p>E 0x40 ECN Echo (ECE)</p> <p>U 0x20 Urgent</p> <p>A 0x10 Ack</p> <p>P 0x08 Push</p> <p>R 0x04 Reset</p> <p>S 0x02 Syn</p> <p>F 0x01 Fin</p>	<table border="1"> <thead> <tr> <th>Packet State</th> <th>DSB</th> <th>ECN bits</th> </tr> </thead> <tbody> <tr> <td>Syn</td> <td>00</td> <td>11</td> </tr> <tr> <td>Syn-Ack</td> <td>00</td> <td>01</td> </tr> <tr> <td>Ack</td> <td>01</td> <td>00</td> </tr> <tr> <td>No Congestion</td> <td>01</td> <td>00</td> </tr> <tr> <td>No Congestion</td> <td>10</td> <td>00</td> </tr> <tr> <td>Congestion</td> <td>11</td> <td>00</td> </tr> <tr> <td>Receiver Response</td> <td>11</td> <td>01</td> </tr> <tr> <td>Sender Response</td> <td>11</td> <td>11</td> </tr> </tbody> </table>	Packet State	DSB	ECN bits	Syn	00	11	Syn-Ack	00	01	Ack	01	00	No Congestion	01	00	No Congestion	10	00	Congestion	11	00	Receiver Response	11	01	Sender Response	11	11	<p>Checksum</p> <p>Checksum of entire TCP segment and pseudo header (parts of IP header)</p>	<p>RFC 793</p> <p>Please refer to RFC 793 for the complete Transmission Control Protocol (TCP) Specification.</p>
Packet State	DSB	ECN bits																												
Syn	00	11																												
Syn-Ack	00	01																												
Ack	01	00																												
No Congestion	01	00																												
No Congestion	10	00																												
Congestion	11	00																												
Receiver Response	11	01																												
Sender Response	11	11																												

Source <http://nmap.org/book/images/hdr/MJB-TCP-Header-800x564.png>

TCP - Connection Flow



TCP – Connection Termination



TCP - Acknowledgments



**Sends datagram
Starts timer**

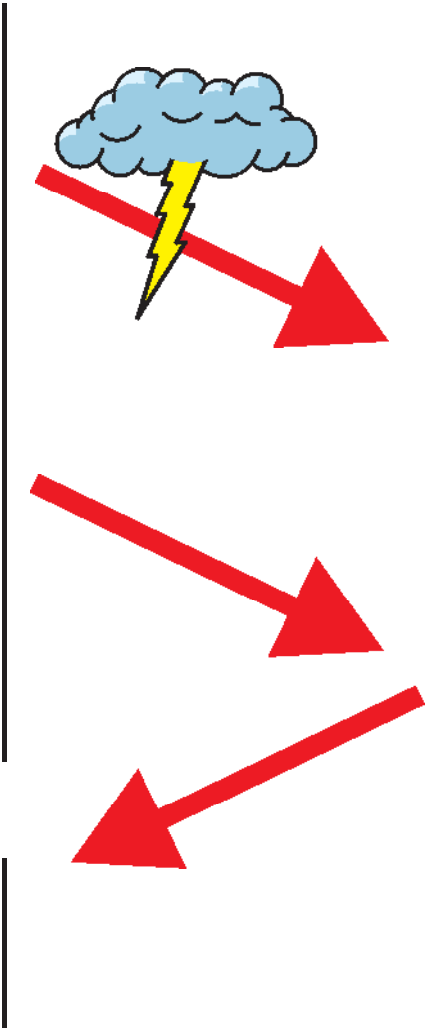
Host A

**Acknowledgment
was not received**



**Timer expires
and datagram retransmitted**

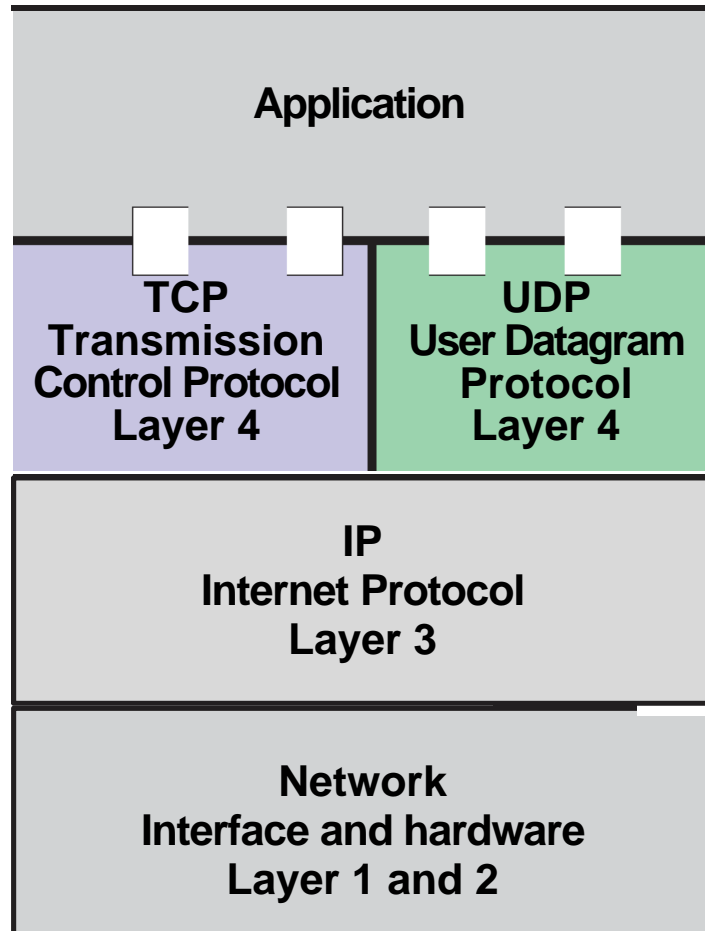
**Host A receives acknowledgment,
resets timer, and clears buffer**



Host B

**Host B receives datagram
and acknowledges receipt**

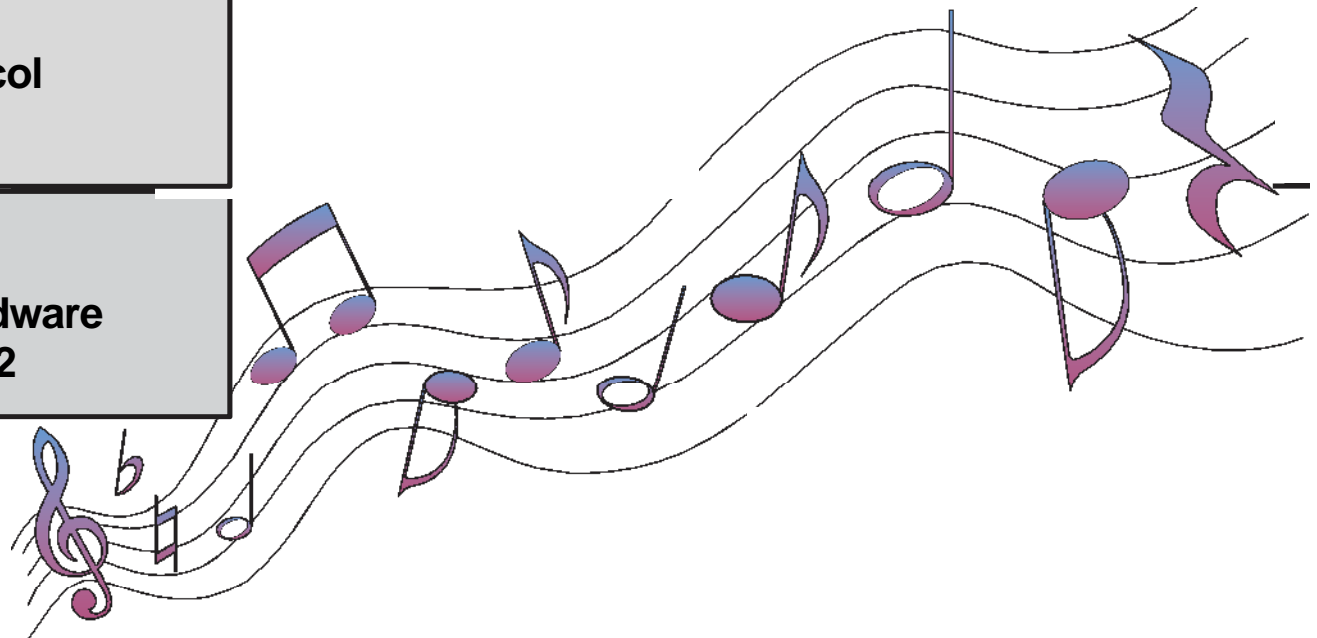
UDP - User Datagram Protocol



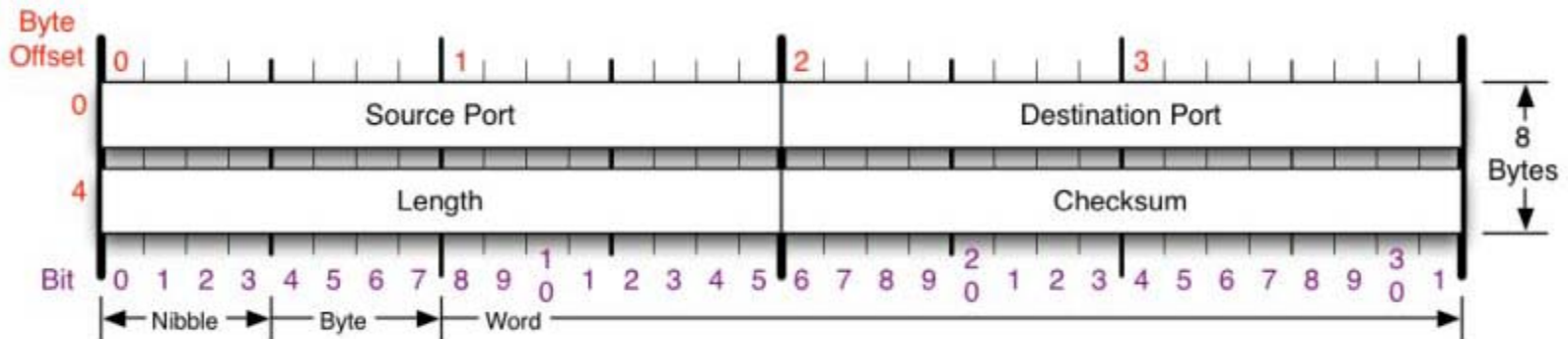
Program to program datagram transfer

Fast mechanism

Used for management frames, streaming audio



UDP - Header



Checksum

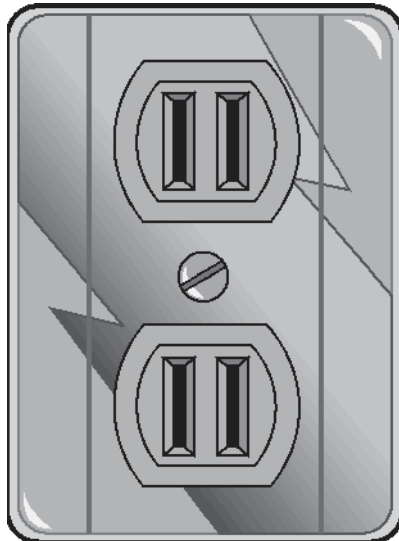
Checksum of entire UDP segment and pseudo header (parts of IP header)

RFC 768

Please refer to RFC 768 for the complete User Datagram Protocol (UDP) Specification.

TCP/IP Ports/Sockets

Sockets



Network I/O for UNIX
Library of C routines
Berkeley UNIX (BSD) API

Also called Ports

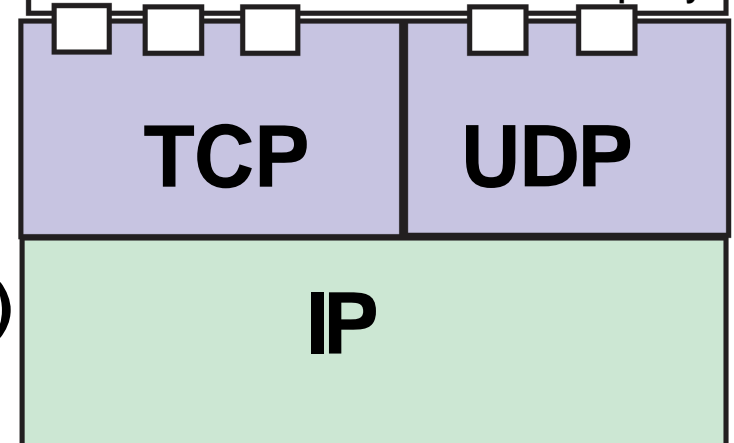
Well known 0 – 1023
Registered 1024 – 49151
Dynamic 49152 - 65535
(also called Private)

Application address

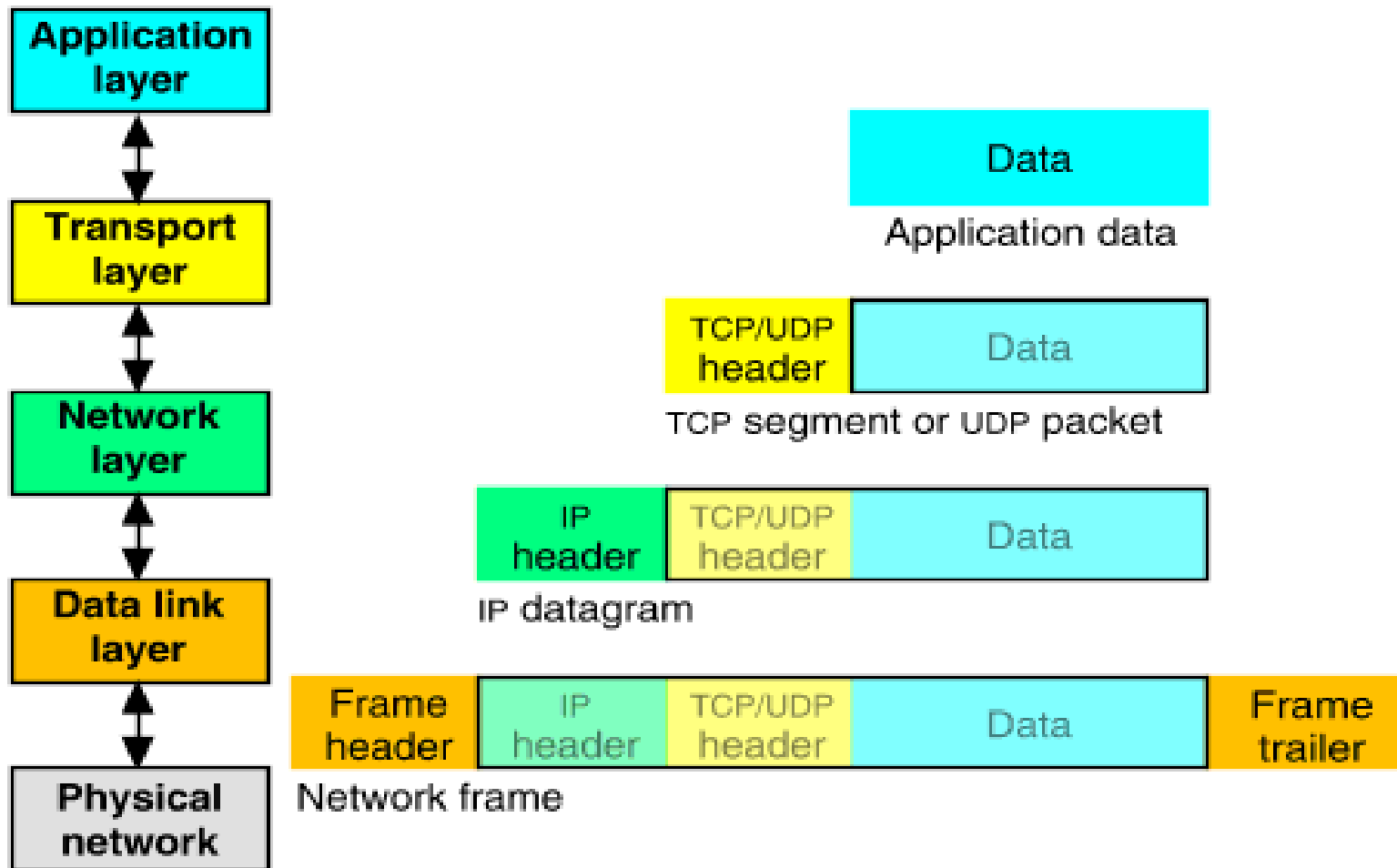
IP Address
Protocol (TCP or UDP)
Port Number

Application code

Port Number	Protocol	Application
20	TCP	FTP-data
21	TCP	FTP-control
23	TCP	Telnet
25	TCP	SMTP
53	TCP/UDP	DNS
70	TCP	Gopher
79	TCP	Finger
80	TCP	HTTP
110	TCP	POP3
161	UDP	SNMP
162	UDP	SNMP-trap
520	UDP	RIP
1435	TCP/UDP	IBM CICS
1525	TCP/UDP	Oracle
10007	TCP/UDP	MVS Capacity



Encapsulation of Application Data



Source: http://uw713doc.sco.com/en/NET_tcpip/tcpN.tcpip_stack.html

IP Addressing

IP address is 32 bits long

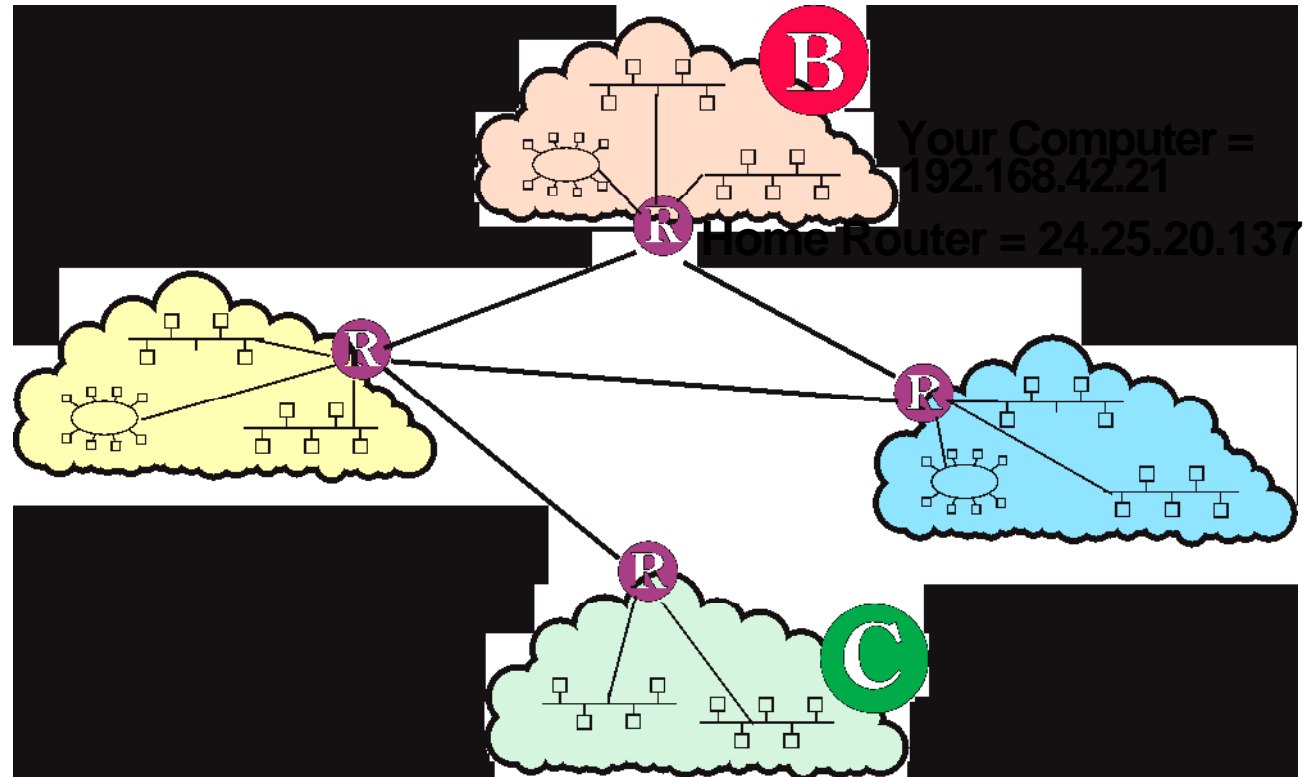
Expressed as 4 decimal numbers

Format: 24.25.20.137
Divided into 2 parts
Network address
Host address

Network address assigned:
ISP
Registrar

Host address assigned:
Locally

Your Network =
192.168.42.0

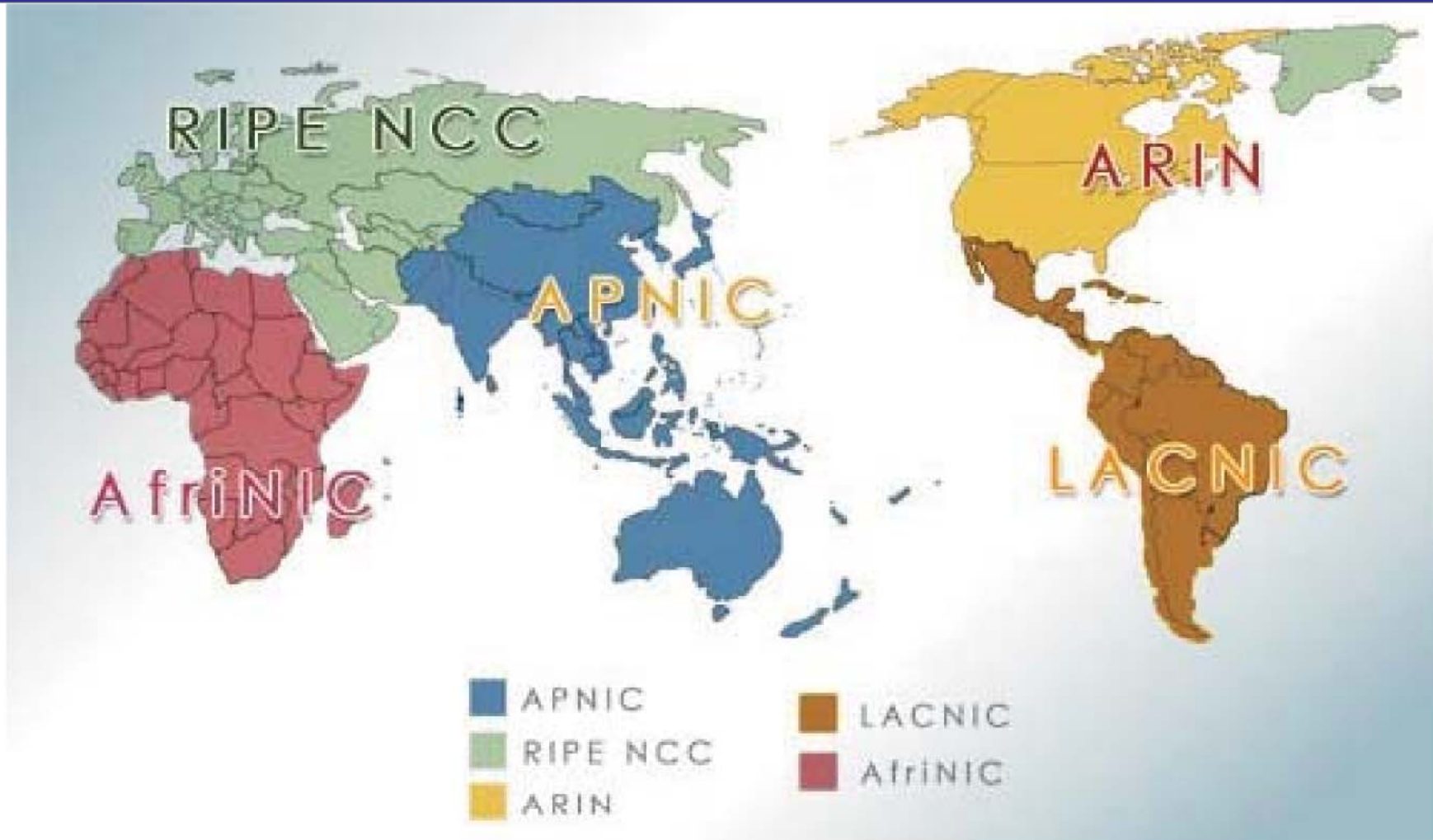


Your Computer =
192.168.42.21
Home Router = 24.25.20.137

Network = 207.217.0.0
(207.217/16)

lauraknapp.com =
207.217.125.50

IP Address Assignment



Public network addresses originally assigned to using organizations

Today regional authority assigns to Internet Service Providers (ISPs)

Network Address Translation

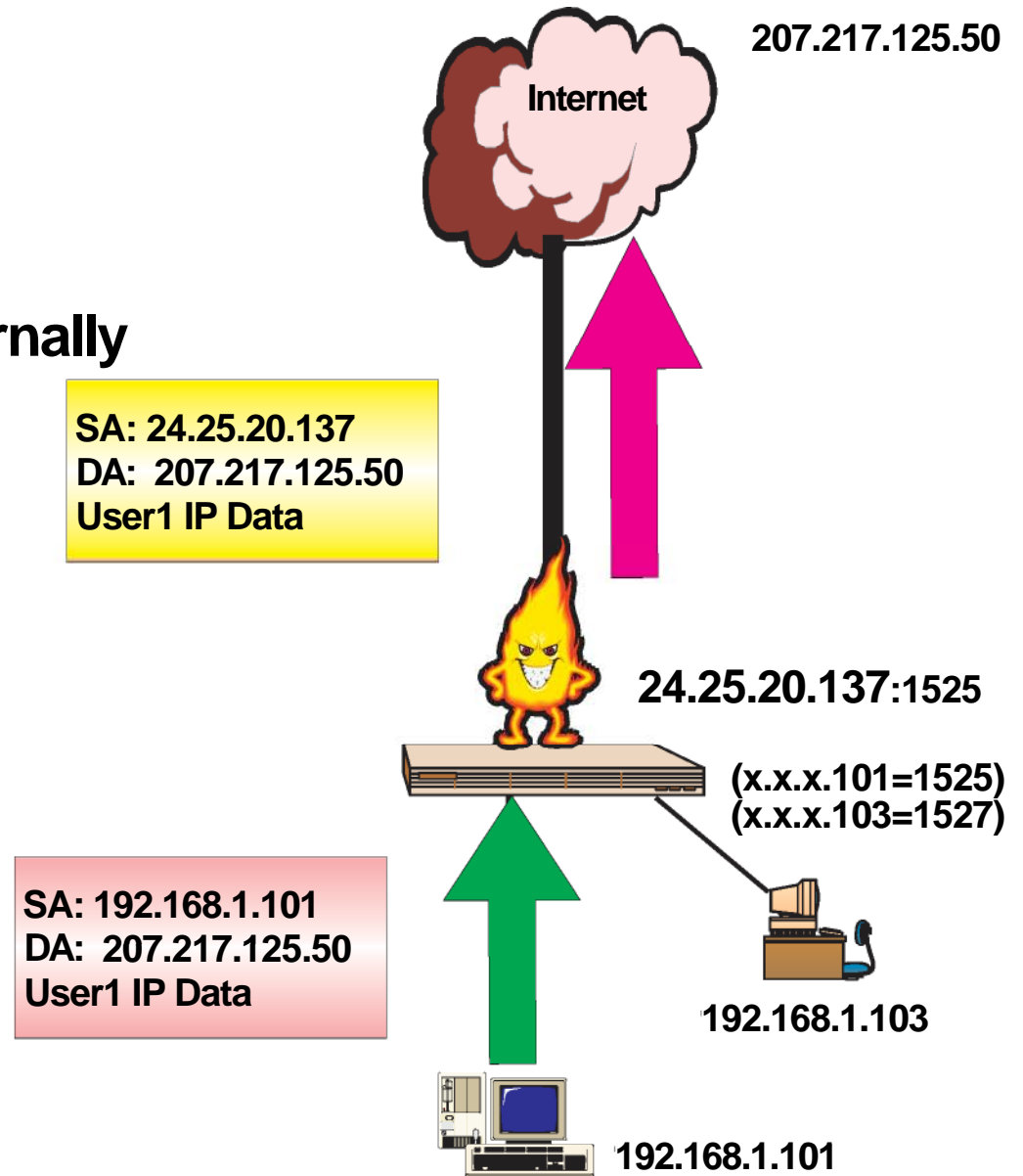
Hides internal addresses and systems from outsiders

Use Private IP Addresses internally
Everything appears to be coming from the firewall

High performance

Transparent to clients

Configuration options on mapping internal to external addresses implemented by either firewall or router



Names and Addresses

The screenshot shows a Windows Internet Explorer browser window with the address bar displaying <http://www.lauraknapp.com/tech.htm>. The website content includes a header with the title "Technology Sites" and a date "06/07/10". A vertical navigation menu on the left contains links for Home, About Me, New House Progress, Technology Sites, Presentations, and ljk. The main content area is divided into four sections: "General Technology", "Internet II", "Security and Hacker Sites", and "Mainframe". Each section contains a list of links, many of which are preceded by a small globe icon.

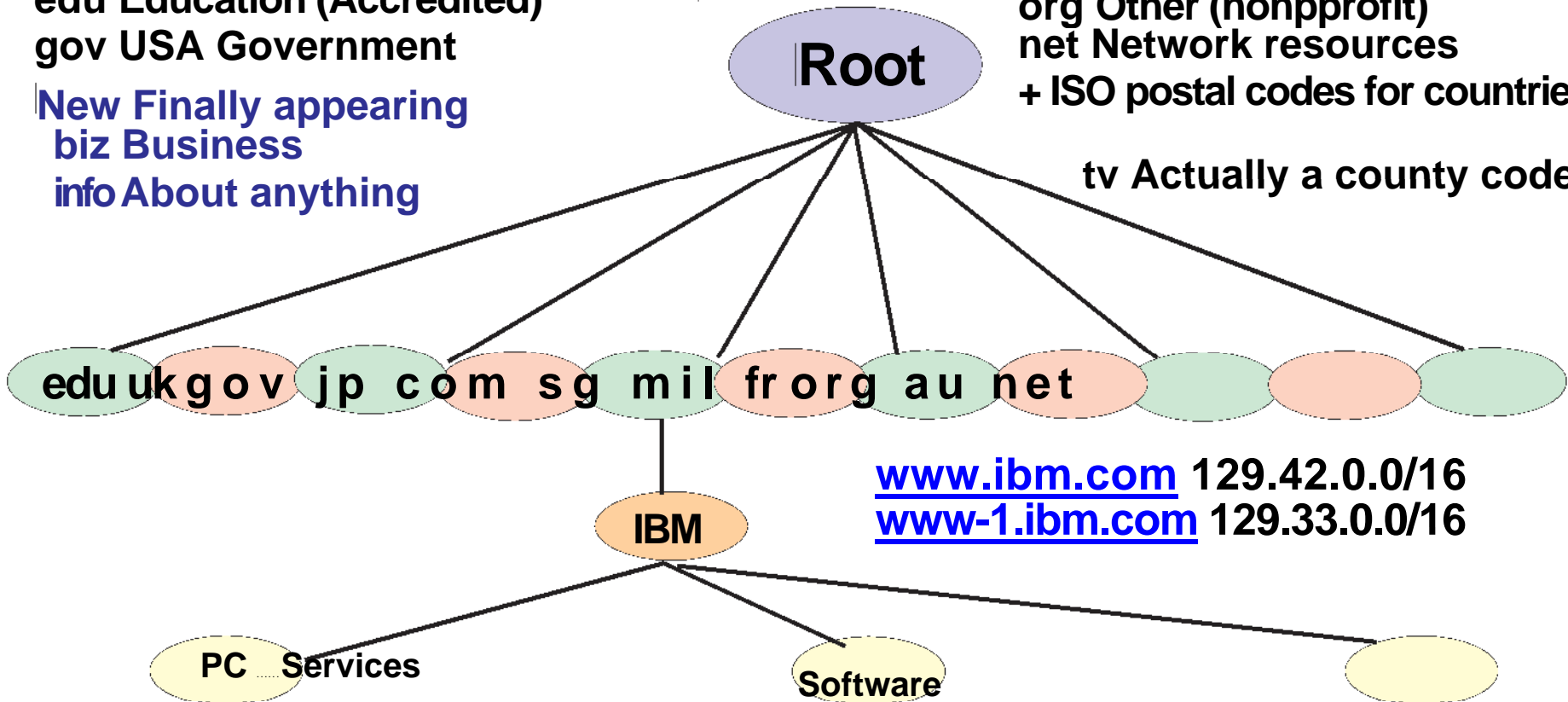
General Technology	Internet II
<ul style="list-style-type: none">Internet DetailsTUCOWS Shareware softwareIP WikipediaWebopedia HomeIP WebopediaLight Reading: Networking the Telecom IndustryZDNet on IP TechnologiesIP ProtocolsCisco IP Protocol HandbookIT ToolboxThe RegisterIP Address Tracker	<ul style="list-style-type: none">Internet2Internet2 DetailsInternet2 WikipediaInternet2 DashboardUS Government and Internet II
Security and Hacker Sites	Mainframe
<ul style="list-style-type: none">CERTInternet Security WikipediaCNET News on Internet Security	<ul style="list-style-type: none">MainframeZonezJournalMarist ListserversIBM System z RedbooksMainframe World BlogMainframeupdate blogLinuxVM WIKI

How does my URL get transformed into an IP address?

DNS and TCP/IP Addresses

com Commercial
 edu Education (Accredited)
 gov USA Government
 New Finally appearing
 biz Business
 info About anything

mil USA Military
 org Other (nonprofit)
 net Network resources
 + ISO postal codes for countries
 tv Actually a county code



www.ibm.com 129.42.0.0/16
www-1.ibm.com 129.33.0.0/16

64.26.254.20 204.146.30.51 129.42.18.103
www.pc.ibm.com
 (points to Lenovo.com)

www.software.ibm.com
www-306.ibm.com/software

www.services.ibm.com

DNS “F” Root Servers Worldwide



13 root servers lettered a through m
These are the 46 instances of the f root server

DNS Lookup of TCP/IP Addresses



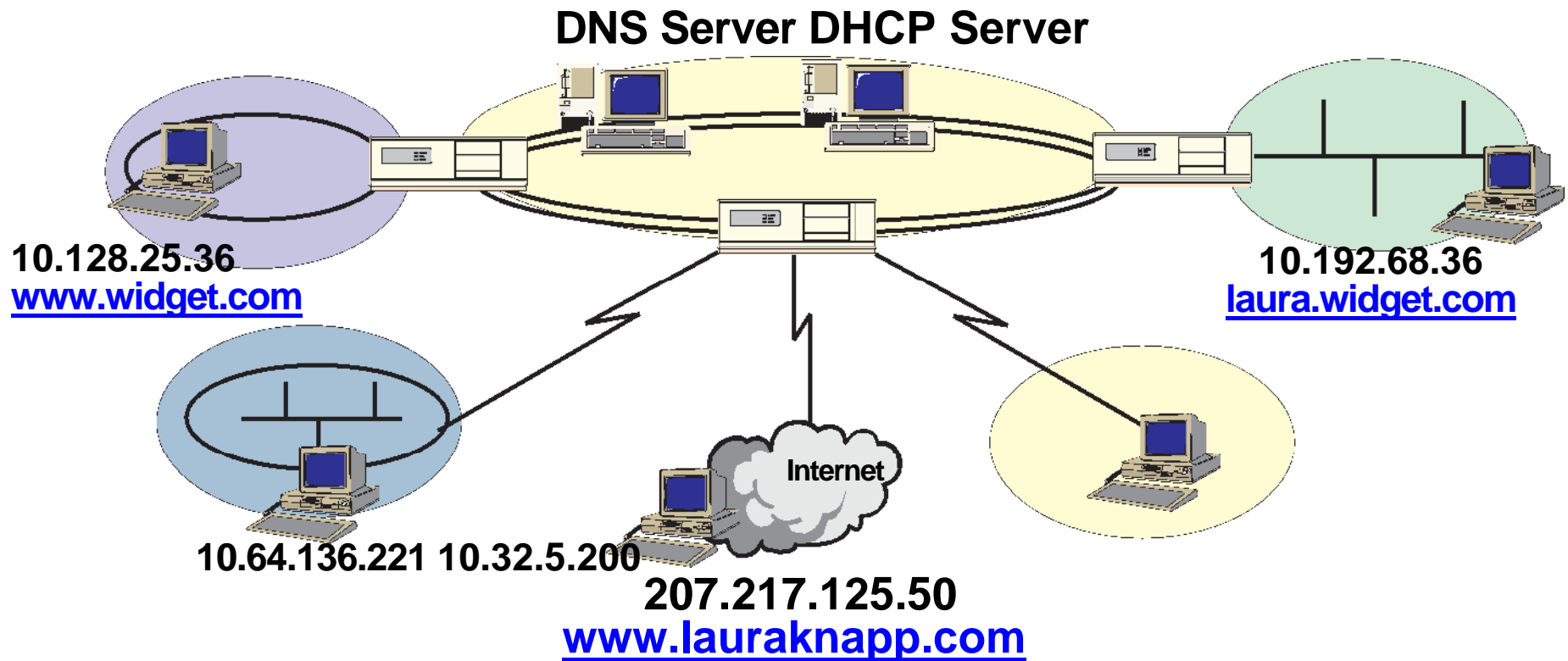
www.lauraknapp.com

DNS resolves to
207.217.125.50

If you send E-mail to
tom@lauraknapp.com
I access it at
pop.lauraknapp.com
which resolves to
207.217.125.33

More than one IP
address is typical

Dynamic IP



**How did my browser resolve the Web server name to an IP address?
DNS server - Domain Name System Server**

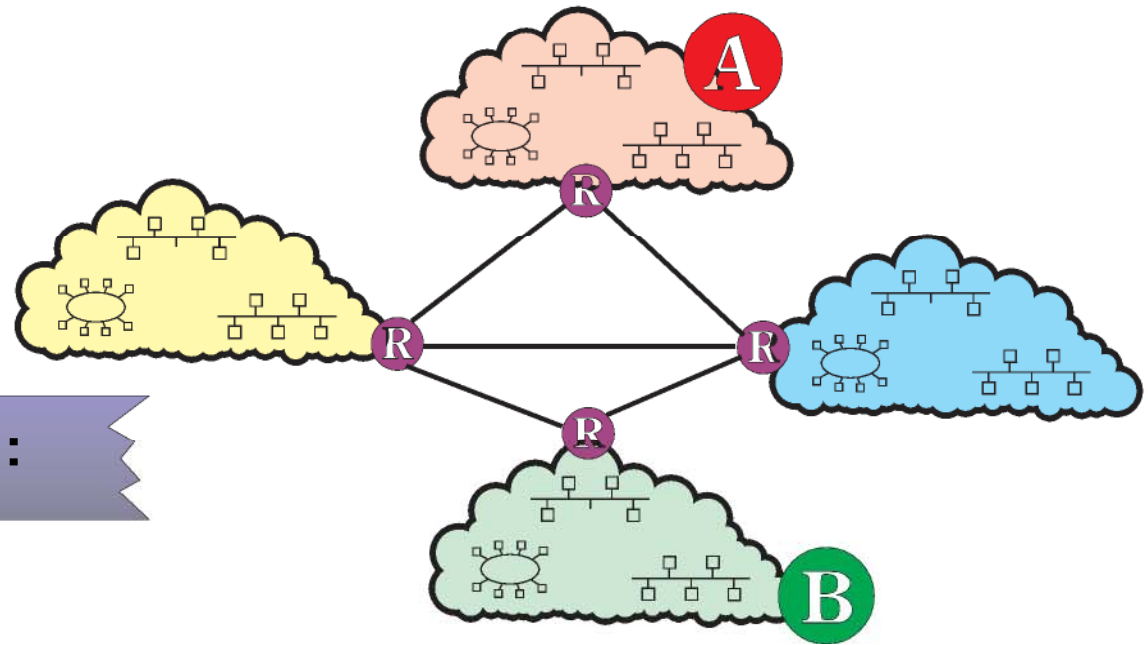
**How can I function on an IP network if I didn't configure an IP address?
DHCP - Dynamic Host Configuration Protocol**

Routing

Same network :
send directly to destination

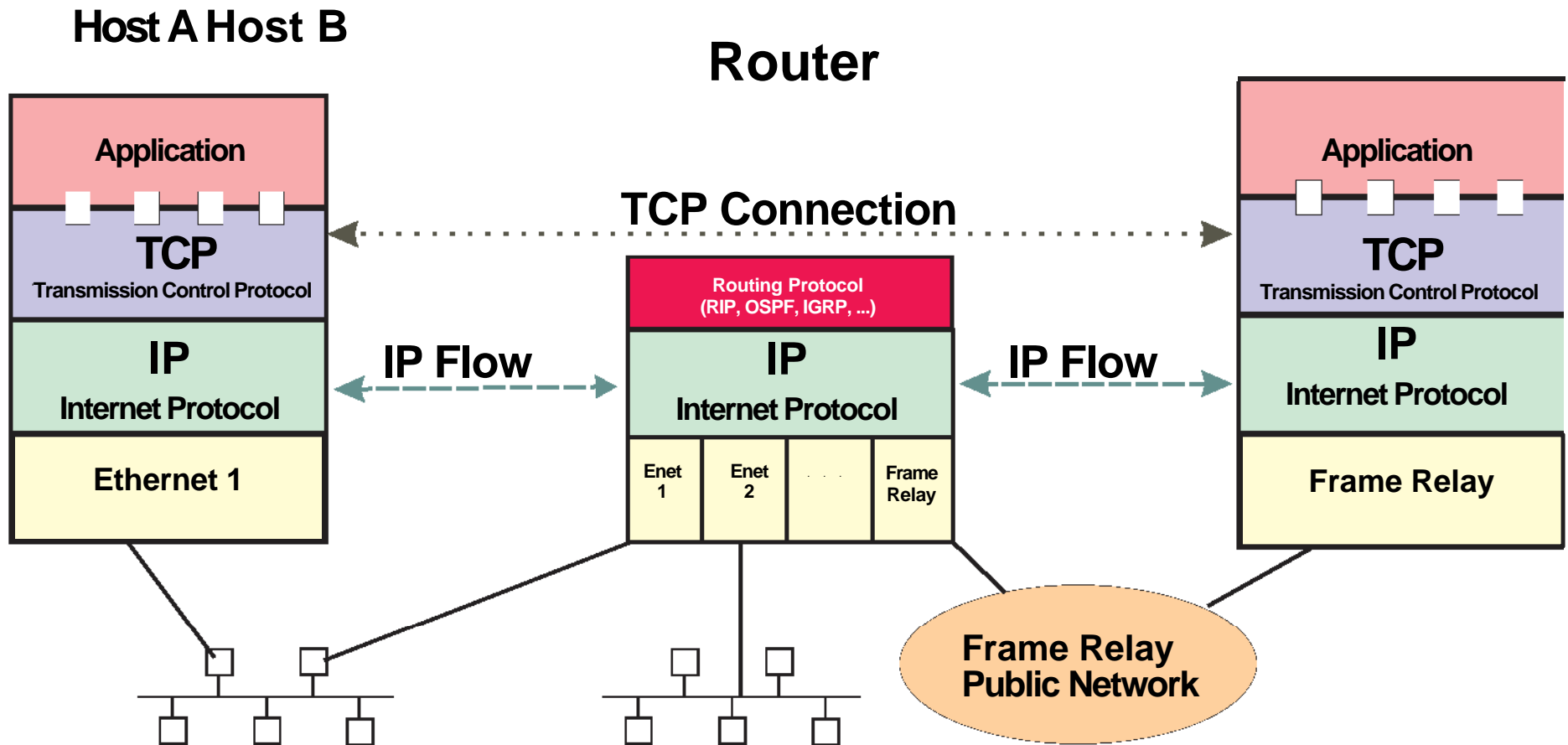
IP delivers datagrams directly from origin to destination if they are on the same network

Different Network :
send to router



If the destination is on a different network,
IP sends the frame to a router that will
forward through the network

IP Routing

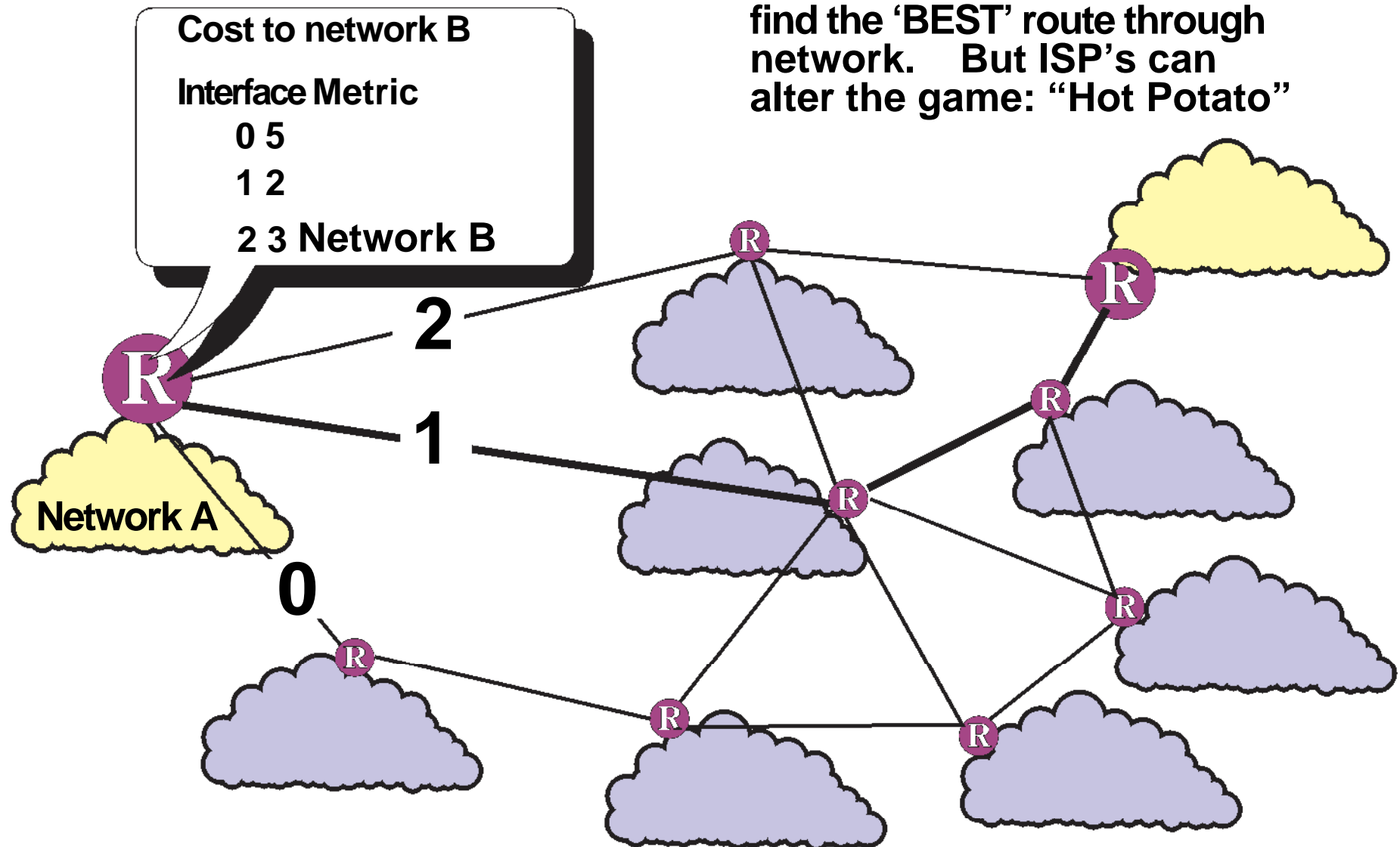


The routing function is performed by the IP protocol and routers

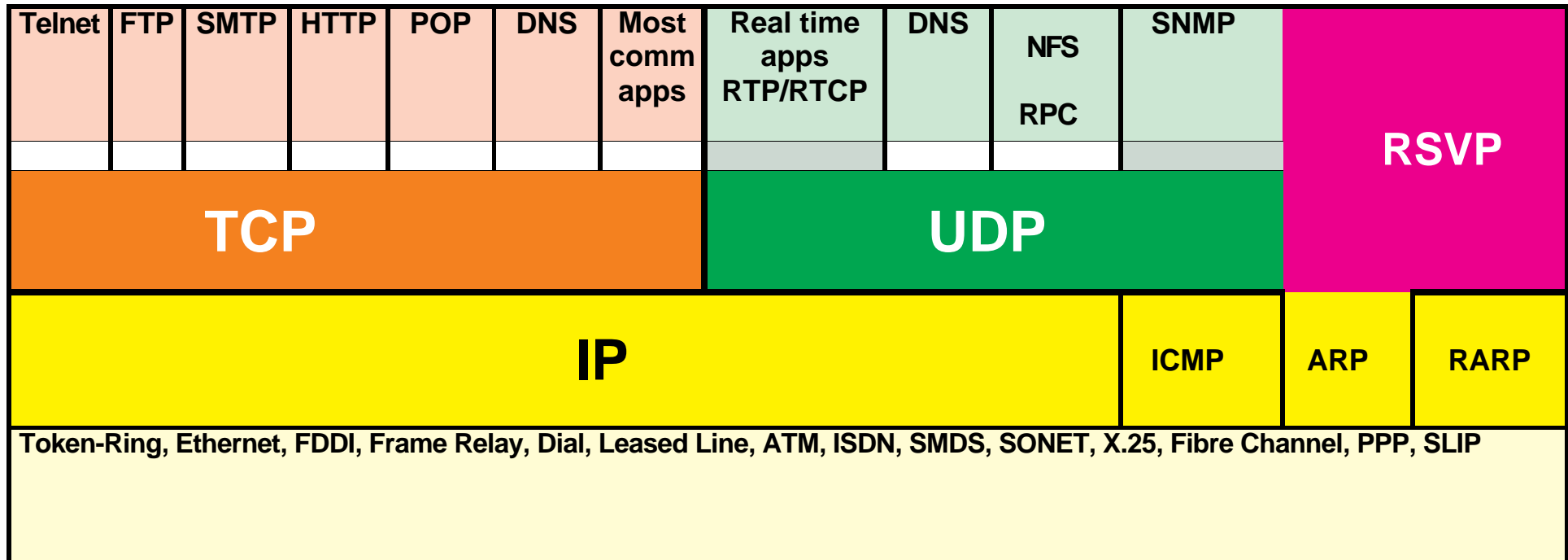
RIP - Routing Information Protocol
OSPF - Open Shortest Path First
IGRP - Interior Gateway Routing Protocol

Support for Alternate Routes

Different algorithms used to find the 'BEST' route through network. But ISP's can alter the game: "Hot Potato"



TCP/IP Protocol Suite



IP - Internet Protocol

ICMP - Internet Control Message Protocol

ARP - Address Resolution Protocol

RARP - Reverse Address Resolution Protocol

TCP - Transmission Control Protocol

UDP - User Datagram Protocol

POP - Post Office Protocol

DNS - Domain Name System

Telnet - Teletype Network

FTP - File Transfer Protocol

SMTP - Simple Mail Transfer Protocol

HTTP - Hypertext Transport Protocol

NFS - Network File System

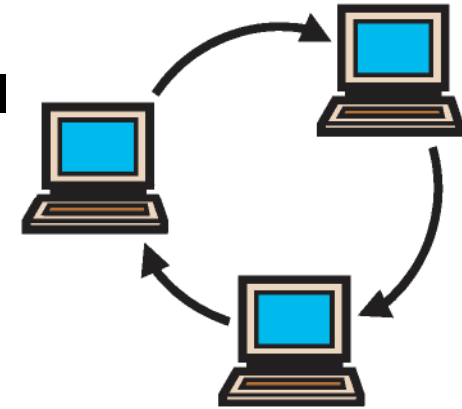
RPC - Remote Procedure Call

SNMP - Simple Network Management Protocol

Internet Capabilities (Basics)



**Internet Mail
Simple Mail Transfer Protocol
(SMTP)**



**File Transfer Protocol
(FTP)**

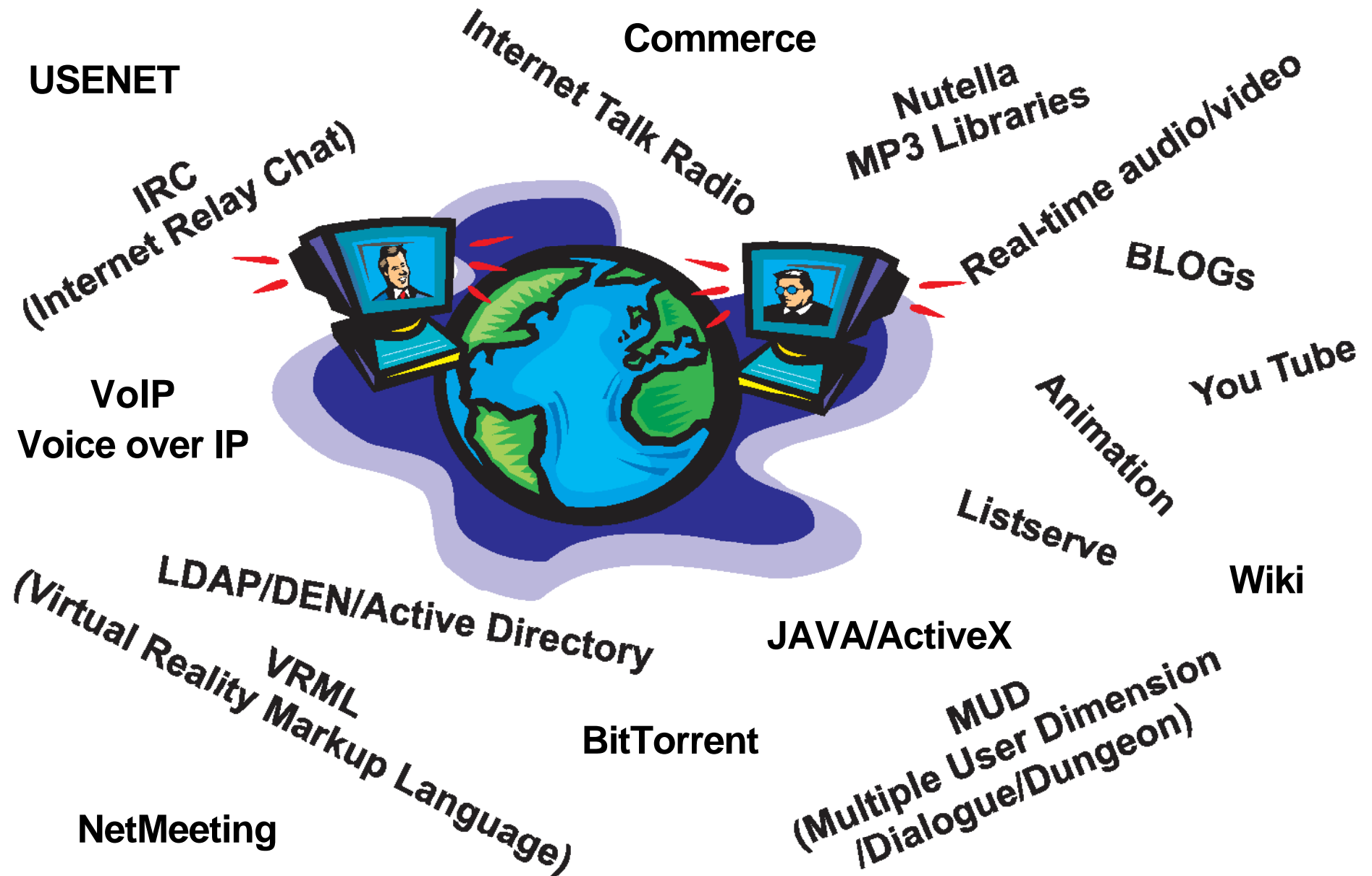


**Terminal Emulation
(TELNET)**



**Simple Network
Management Protocol
(SNMP)**

Application Advances



TCP/IP Standards

IAB - Internet Architecture Board

Sets direction

Determines standards

Guides evolution of Internet

Coordinates developments in TCP/IP

IETF - Internet Engineering Task Force

Solutions for engineering problems

Produce RFCs (Request for Comments)

IRTF - Internet Research Task Force

Coordinates research activities

Longer term solutions

ICANN - Internet Corporation for Assigned Names and Numbers

Regional registries (ARIN--Americas)**

**Administer top-level domain names (TLDs)
and public IP address blocks**

**** Many domain registrars today – One master list**



TCP/IP Summary

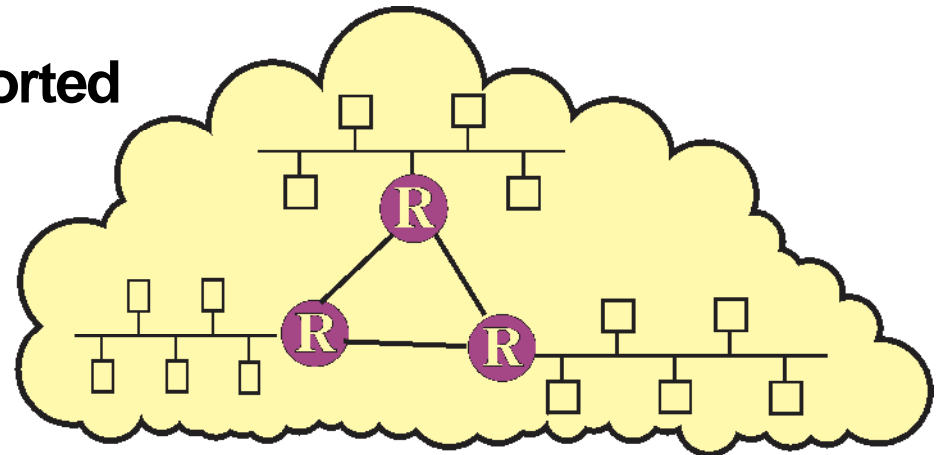
TCP/IP has a heritage of equality ...

IP network designed to span Wide and Local Area Networks

**Hosts (systems) are equal
PC or mainframe or midrange**

Connection and connectionless support

Application environments supported
Client/server networking
Peer-peer networking
Distributed computing
Network computing
Terminal emulation



Designed for independence and interoperability