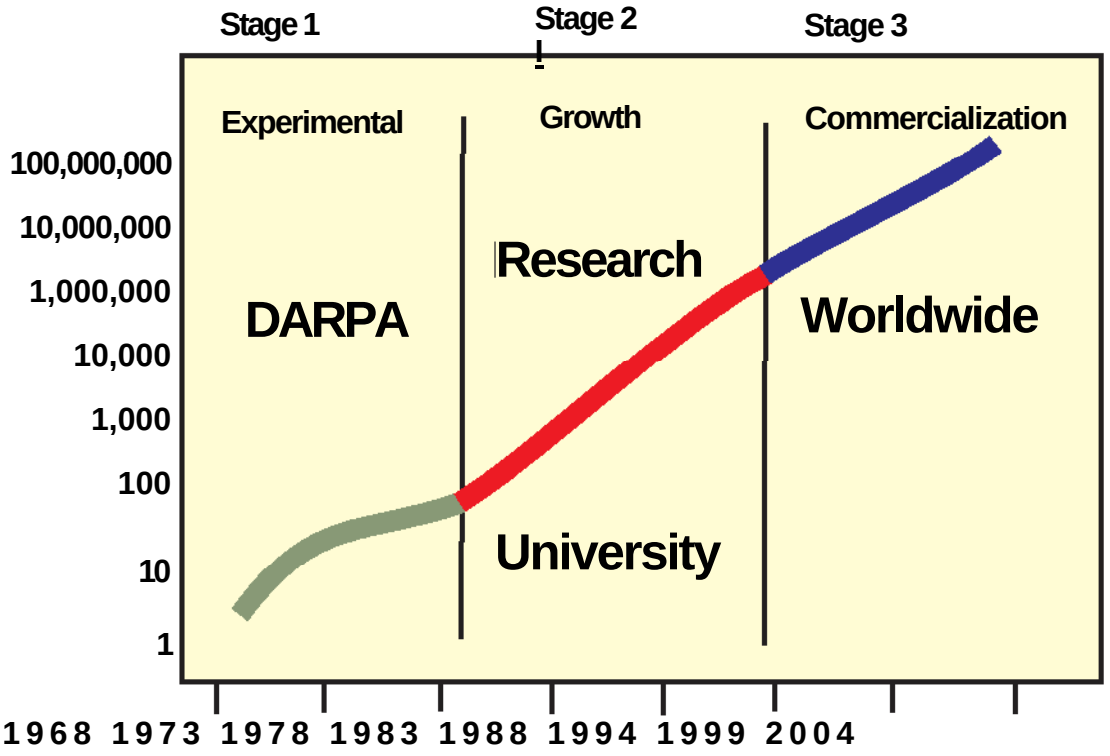
Introduction to TCP/IP

SHARE Summer 2010 Boston

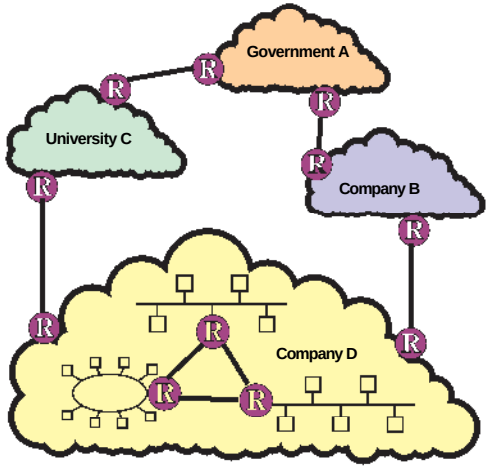
Laura Knapp
AES WW Business Consultant
laurak@aesclever.com
laura@lauraknapp.com

TCP/IP History

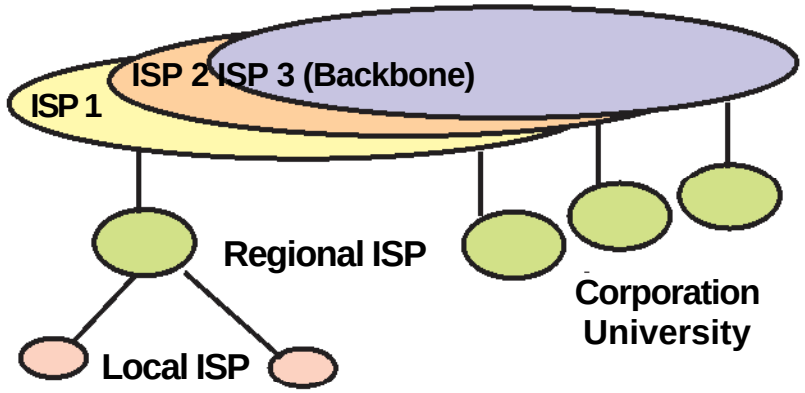


Jan 2009 over 600,000,000

In the 1980's



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)

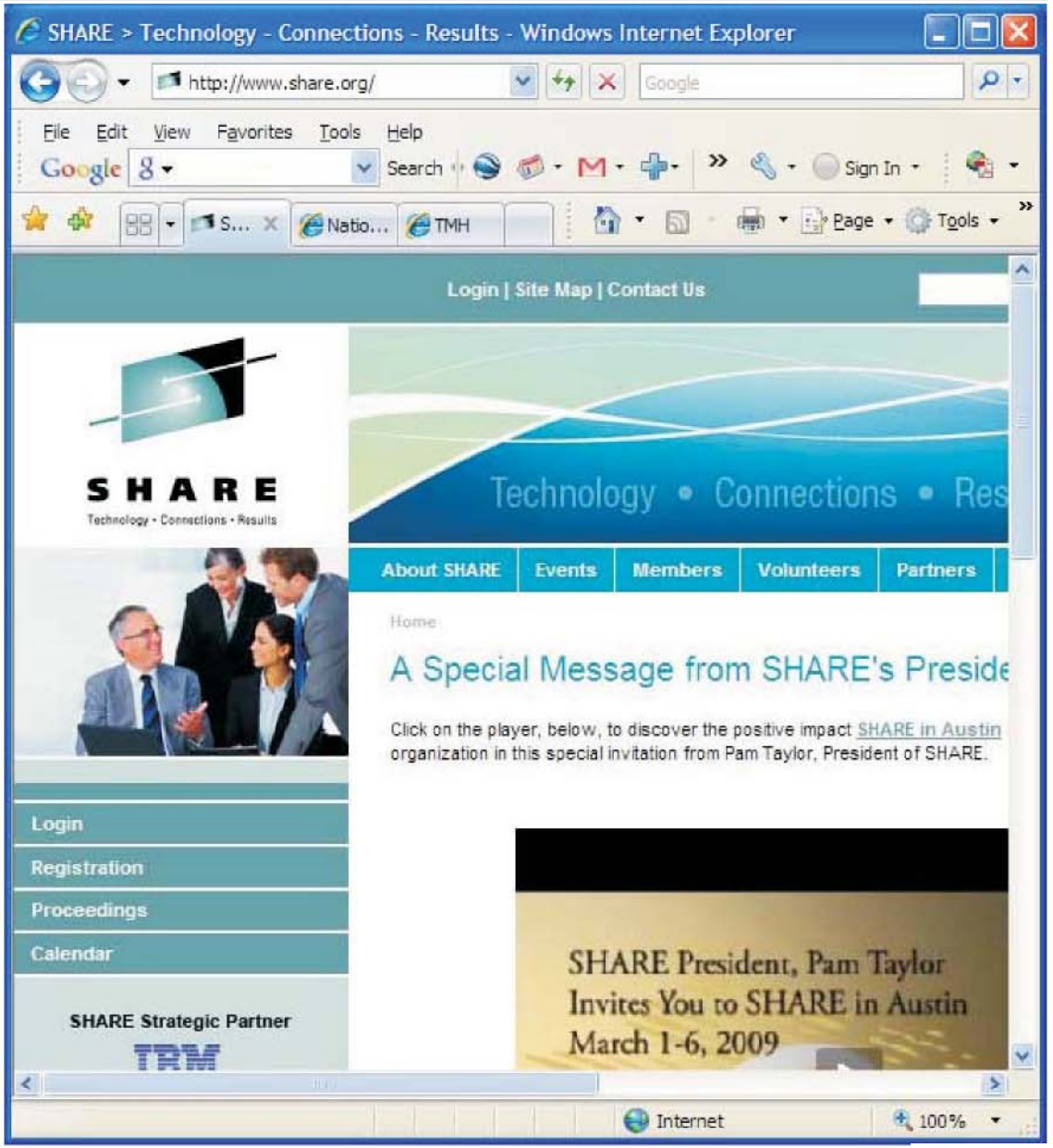
HTML – Hypertext Markup Language

PHTML – aka PHP – another scripting language

BPEL – Business Process Execution Language

JSML – JScript Markup Language

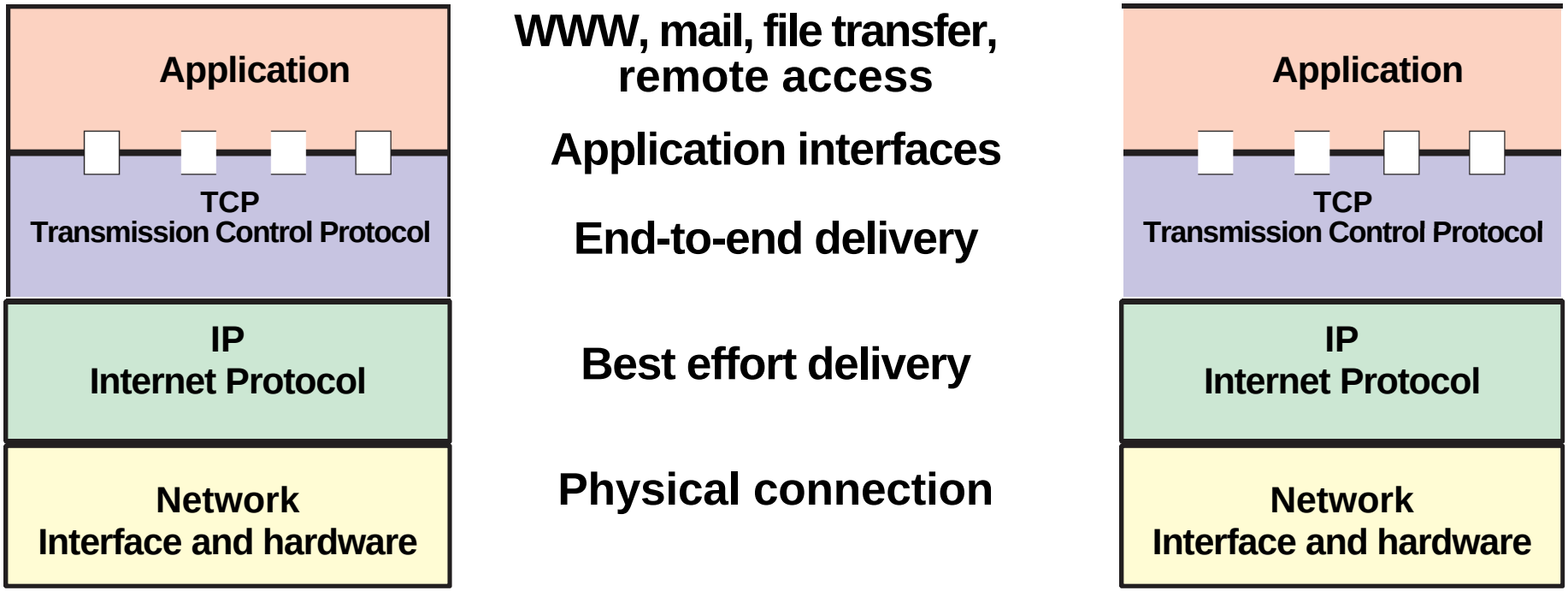
……..



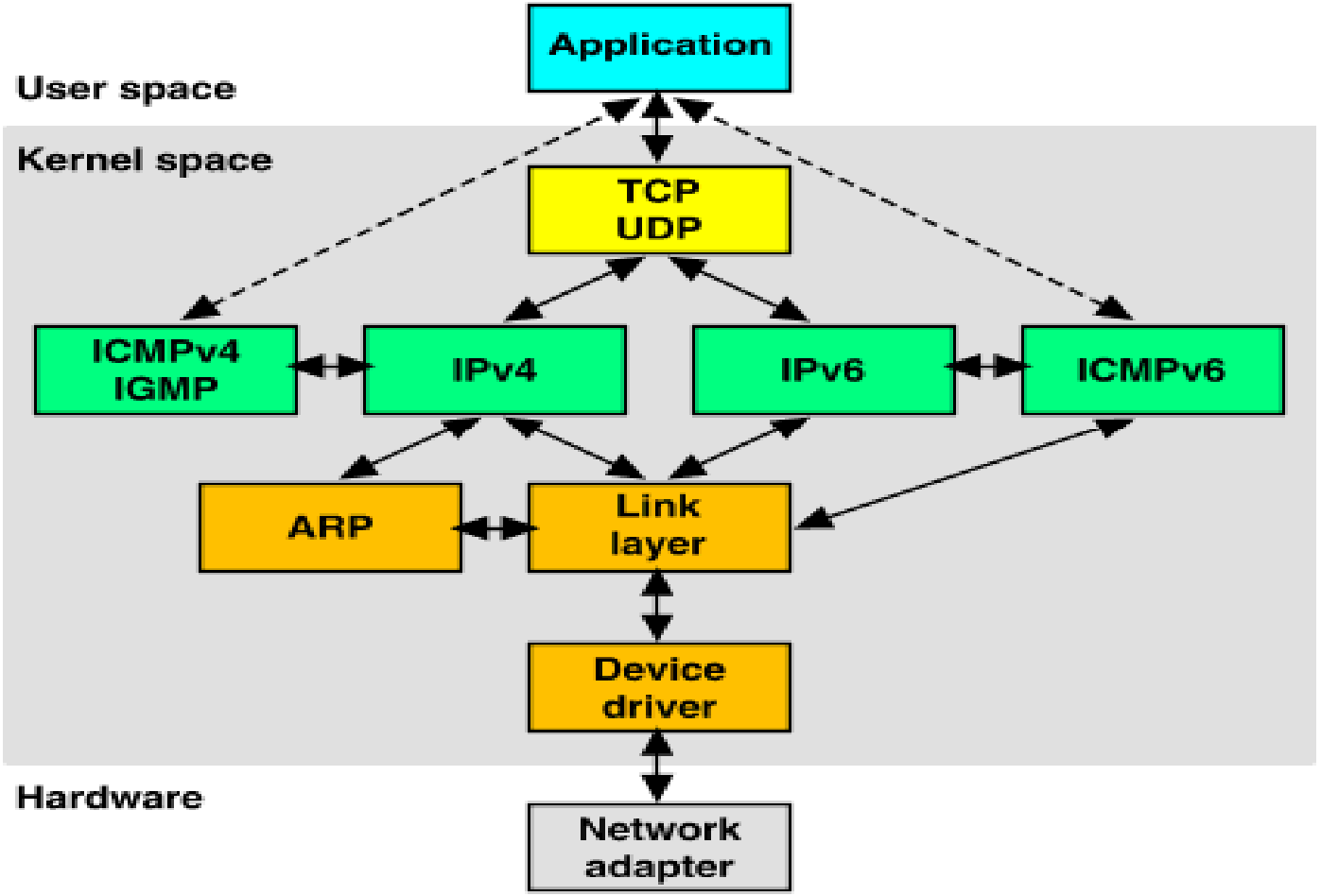
TCP/IP Layered Architecture

Browser

Server



TCP/IP Stacks



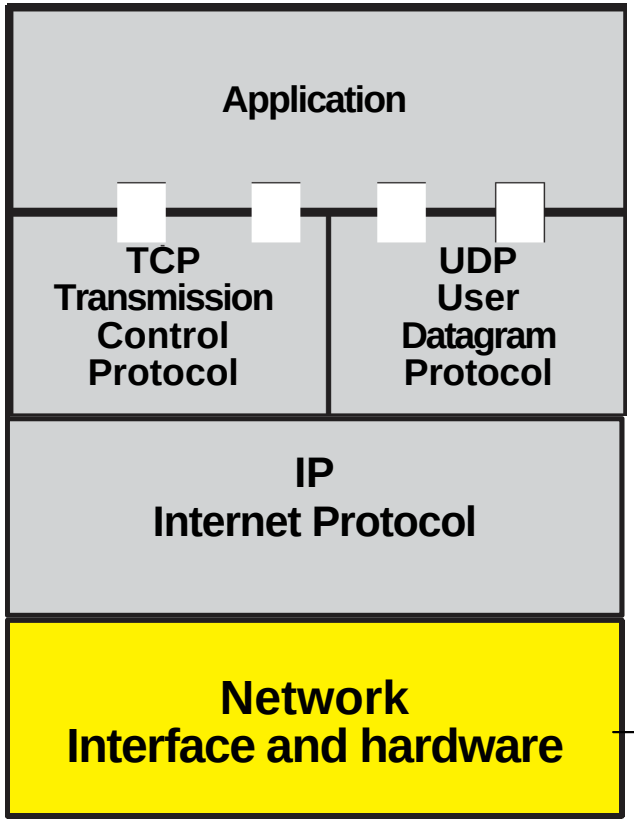
Source: http://uw713doc.sco.com/en/NET_tcpip/tcpN.tcpip_stack.html

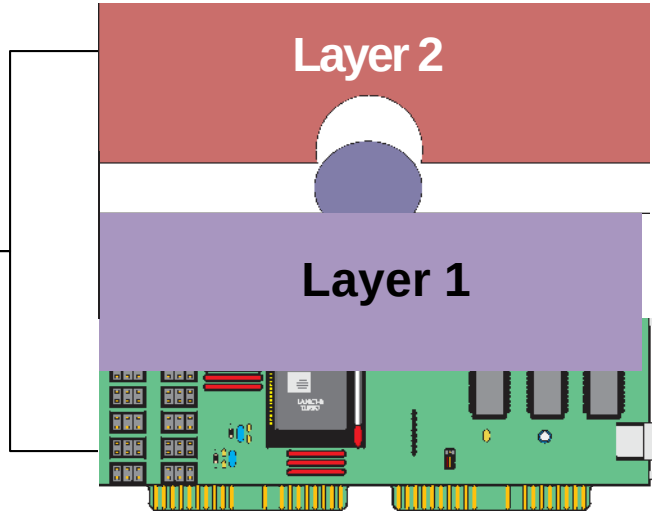
Network Interface Layer

7(8) Layer OSI Model

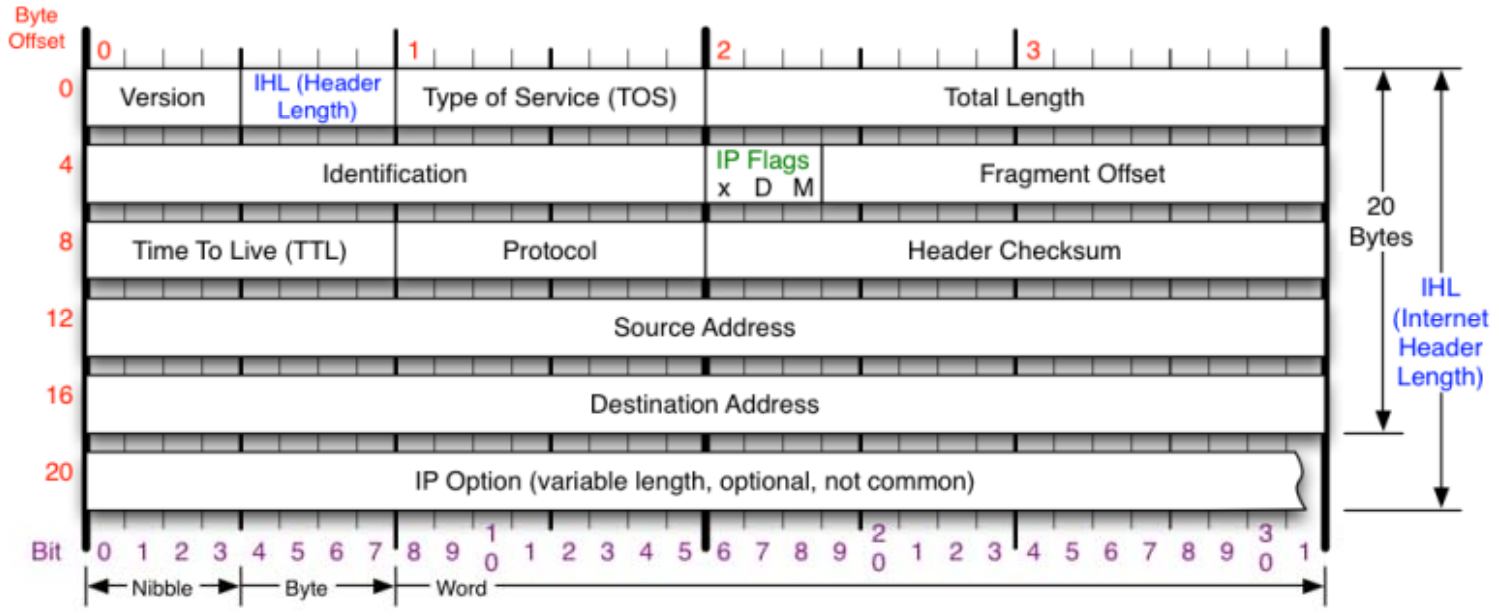
Layer Function	
8	End User (Politics)
7	Application
6	Presentation
5	Session
4	Transport
3	Network
2	Data Link
1	Physical

4 layer TCP/IP Model





IP Header



Version

Version of IP Protocol. 4 and 6 are valid. This diagram represents version 4 structure only.

Header Length

Number of 32-bit words in TCP header, minimum value of 5. Multiply by 4 to get byte count.

Protocol

IP Protocol ID. Including (but not limited to):

1 ICMP	17 UDP	57 SKIP
2 IGMP	47 GRE	88 EIGRP
6 TCP	50 ESP	89 OSPF
9 IGRP	51 AH	115 L2TP

Total Length

Total length of IP datagram, or IP fragment if fragmented. Measured in Bytes.

Fragment Offset

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.

Header Checksum

Checksum of entire IP header

IP Flags

x D M

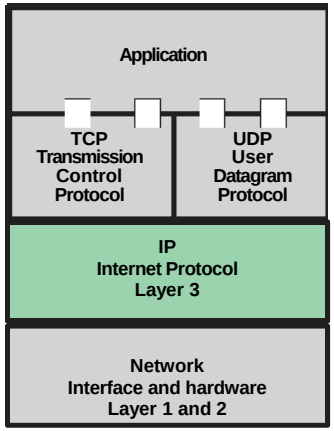
x 0x80 reserved (evil bit)
D 0x40 Do Not Fragment
M 0x20 More Fragments follow

RFC 791

Please refer to RFC 791 for the complete Internet Protocol (IP) Specification.

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

IP - Internet Protocol



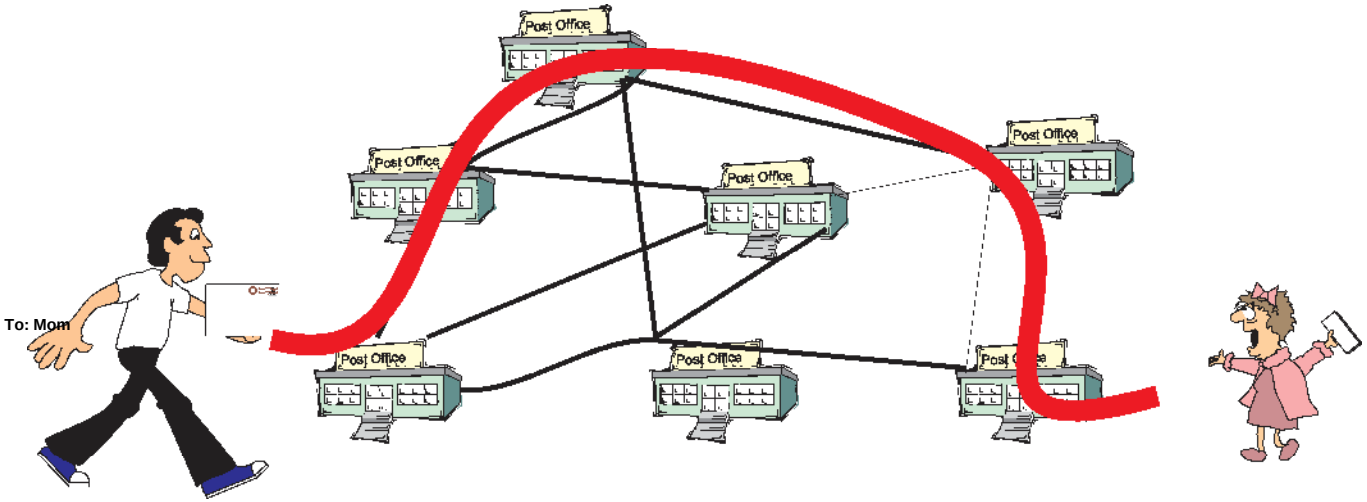
Data transferred in self contained units called datagrams

20 byte IP header

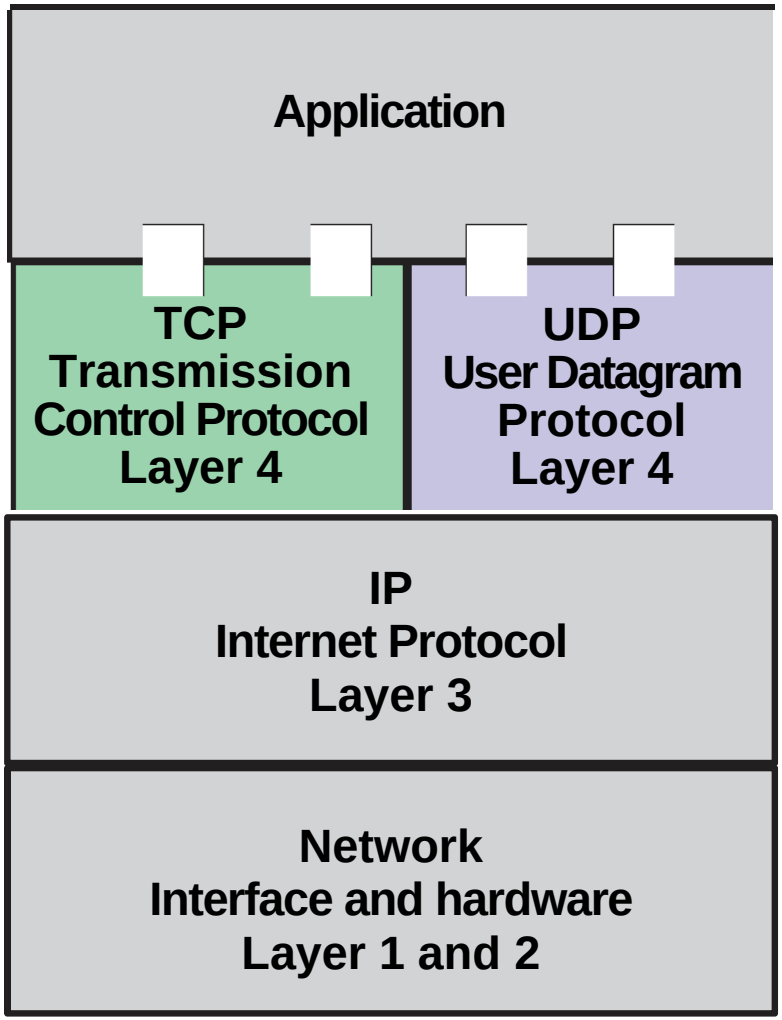
Best effort delivery -- no guarantee

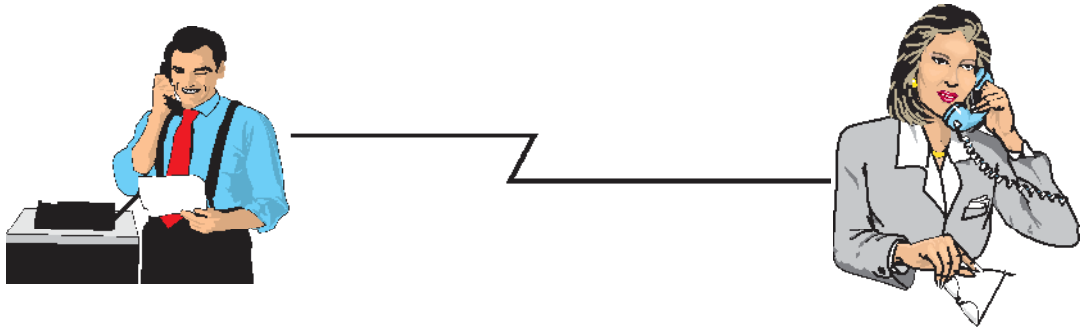
Dynamic path selection for every datagram

Handles datagram fragmentation & reassembly



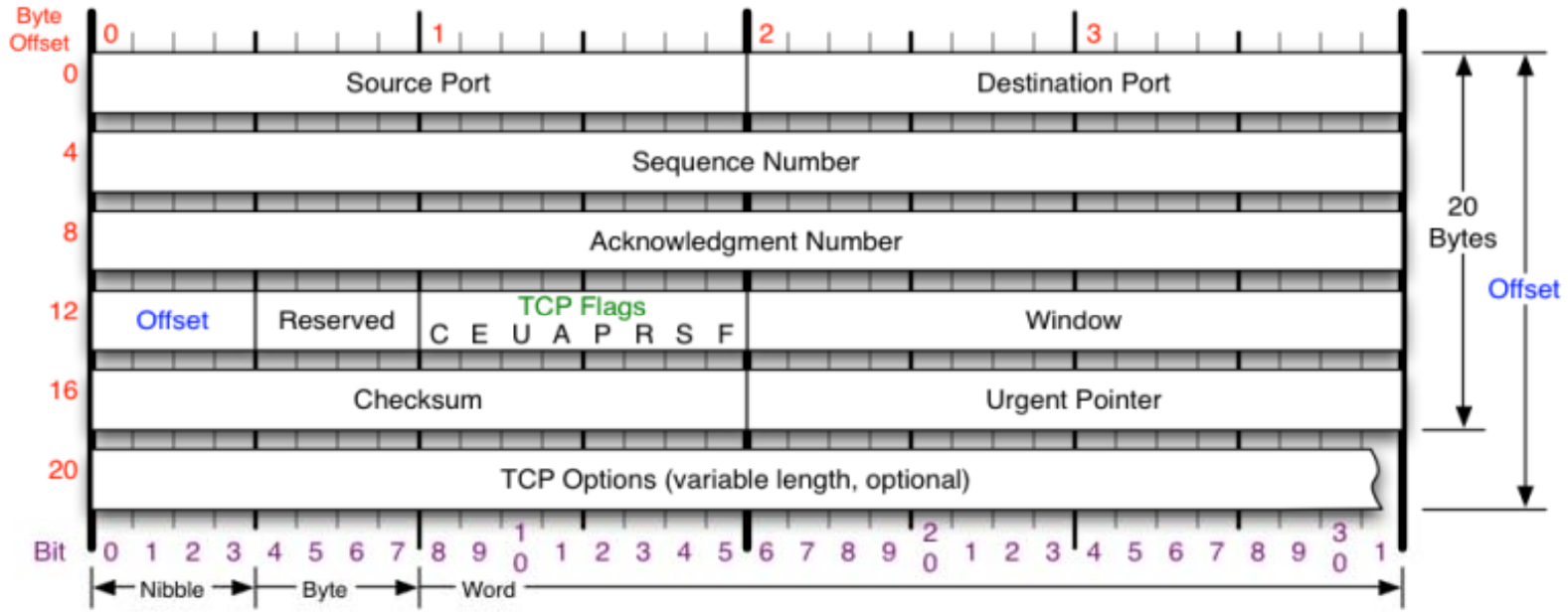
TCP - Transmission Control Protocol





- Connection established
- End-to-end acknowledgments
- Orderly delivery of datagrams to application
- Error and flow control
- Connection takedown

TCP - Header



TCP Flags

C E U A P R S F

Congestion Window
C 0x80 Reduced (CWR)
E 0x40 ECN Echo (ECE)
U 0x20 Urgent
A 0x10 Ack
P 0x08 Push
R 0x04 Reset
S 0x02 Syn
F 0x01 Fin

Congestion Notification

ECN (Explicit Congestion Notification). See RFC 3168 for full details, valid states below.

Packet State	DSB	ECN bits
Syn	0 0	1 1
Syn-Ack	0 0	0 1
Ack	0 1	0 0
No Congestion	0 1	0 0
No Congestion	1 0	0 0
Congestion	1 1	0 0
Receiver Response	1 1	0 1
Sender Response	1 1	1 1

TCP Options

0 End of Options List
1 No Operation (NOP, Pad)
2 Maximum segment size
3 Window Scale
4 Selective ACK ok
8 Timestamp

Checksum

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

Offset

Number of 32-bit words in TCP header, minimum value of 5. Multiply by 4 to get byte count.

RFC 793

Please refer to RFC 793 for the complete Transmission Control Protocol (TCP) Specification.

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

TCP - Connection Flow

Client

Server

Socket

Connect
Let's Talk
SYN-SENT

SYN
Seq Num = 3557
ACK Num = 0

Socket
Bind
Listen
LISTEN

ACK/SYN
ACK Num = 3558
Seq Num = 91248

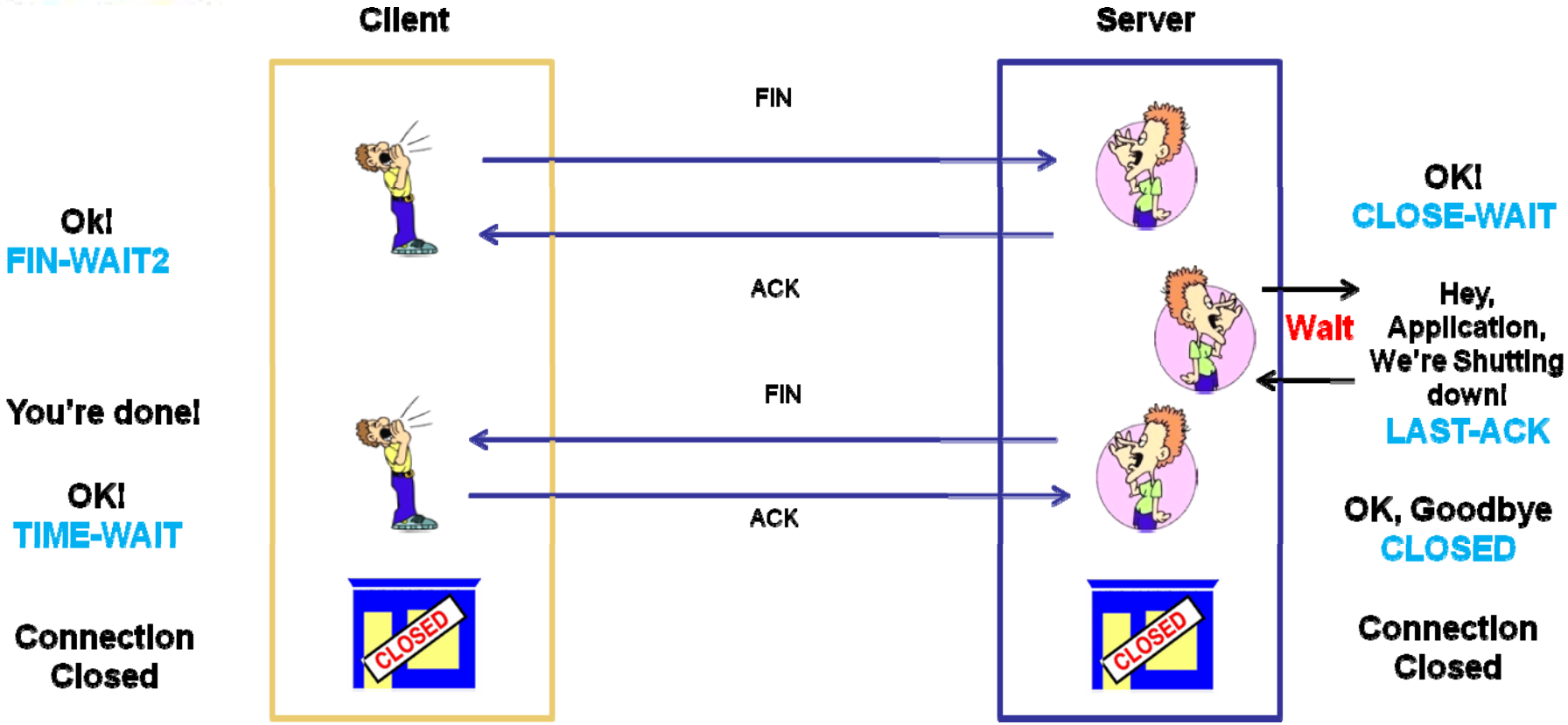
OK, Let's Talk
SYN-RCVD

Thanks!
ESTABLISHED

ACK
ACK Num = 91249

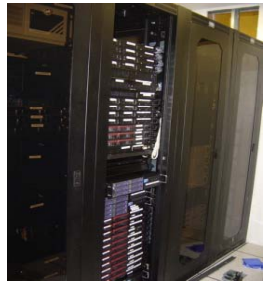
Accept
Conversation
Established
ESTABLISHED

TCP – Connection Termination



TCP - Acknowledgments

Sends datagram
Starts timer



Host A

Acknowledgment was not received

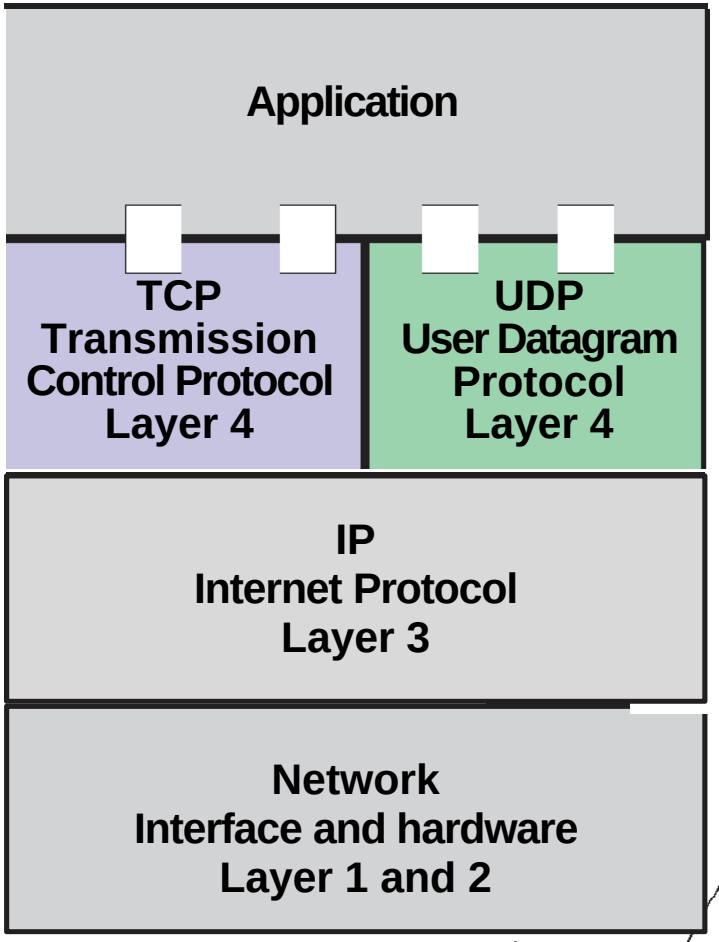
Timer expires and datagram retransmitted

Host B

Host B receives datagram and acknowledges receipt

Host A receives acknowledgment, resets timer, and clears buffer

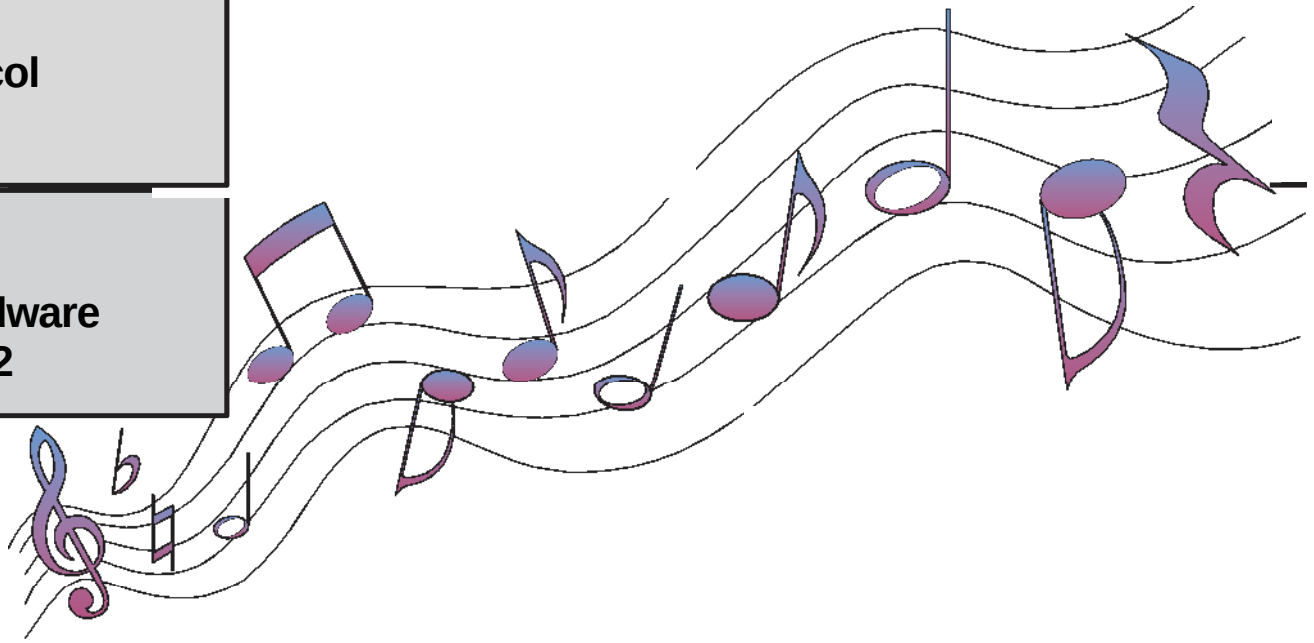
UDP - User Datagram Protocol



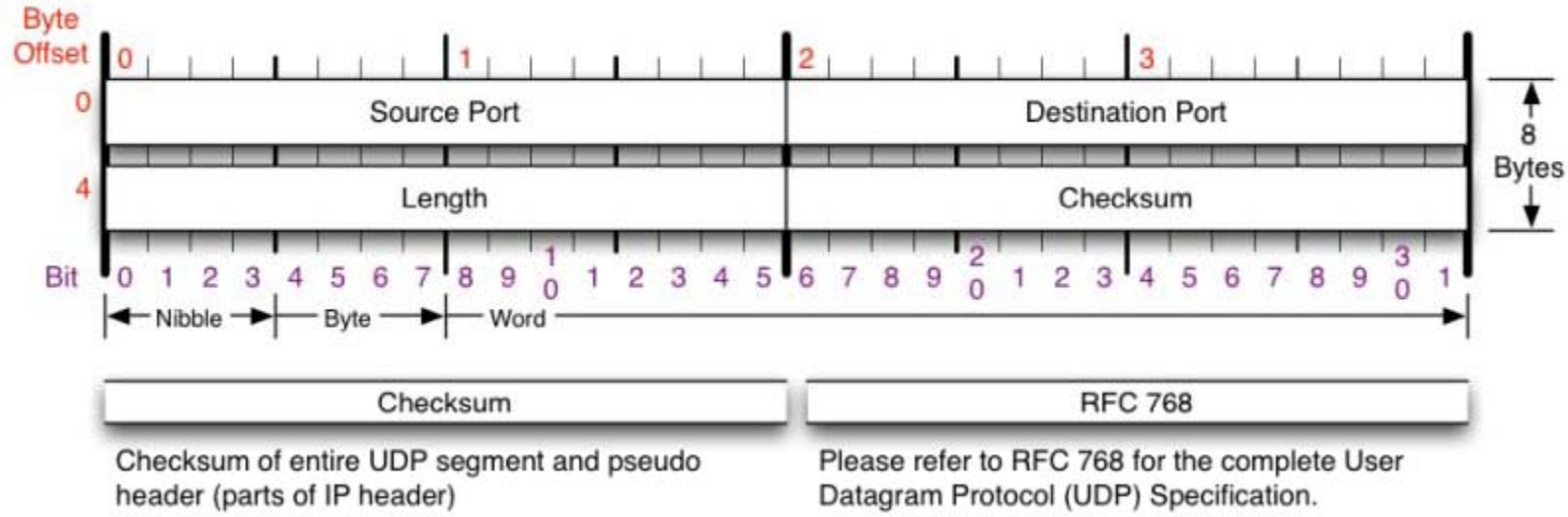
Program to program datagram transfer

Fast mechanism

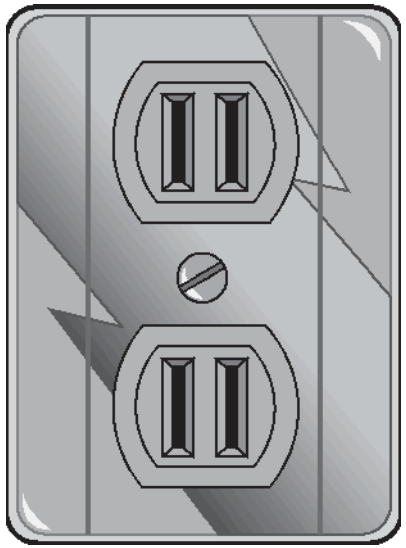
Used for management frames, streaming audio



UDP - Header


Byte Offset
0
4
Source Port
Destination Port
Length
Checksum
8 Bytes
Bit
0 1 2 3 4 5 6 7 8 9 10 1 2 3 4 5 6 7 8 9 20 1 2 3 4 5 6 7 8 9 30 1
Nibble
Byte
Word
Checksum
RFC 768
Checksum of entire UDP segment and pseudo header (parts of IP header)
Please refer to RFC 768 for the complete User Datagram Protocol (UDP) Specification.

TCP/IP Ports/Sockets



Sockets

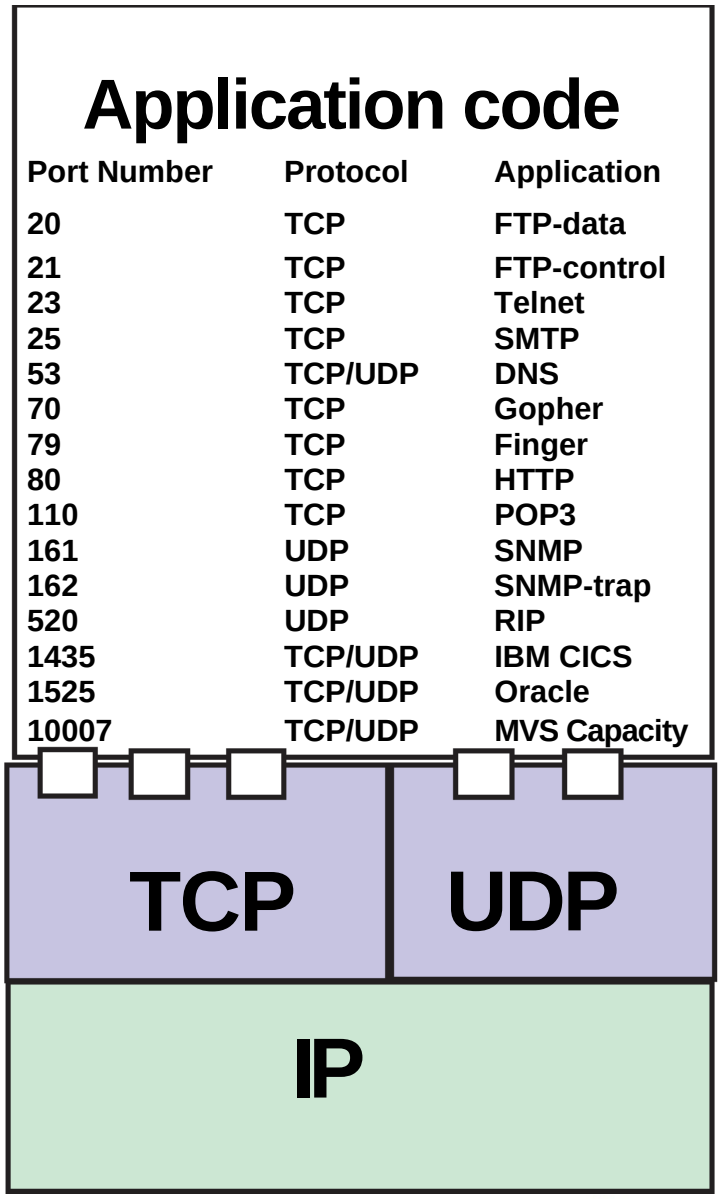
- Network I/O for UNIX
- Library of C routines
  - Berkeley UNIX (BSD) API

Also called Ports

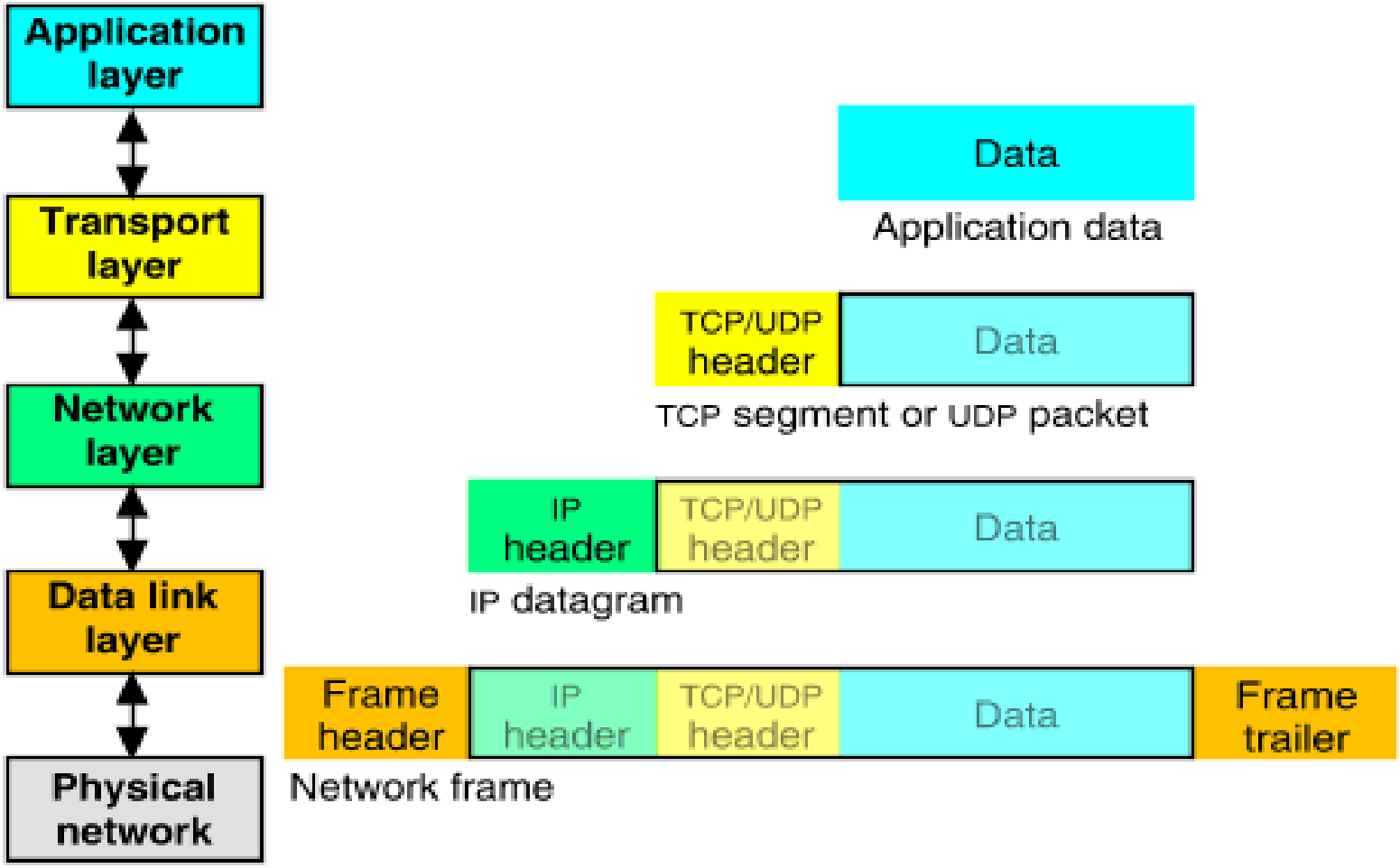
- Well known 0 – 1023
- Registered 1024 – 49151
- Dynamic 49152 - 65535
  - (also called Private)

Application address

- IP Address
  - Protocol (TCP or UDP)
- Port Number



Encapsulation of Application Data



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

IP Addressing

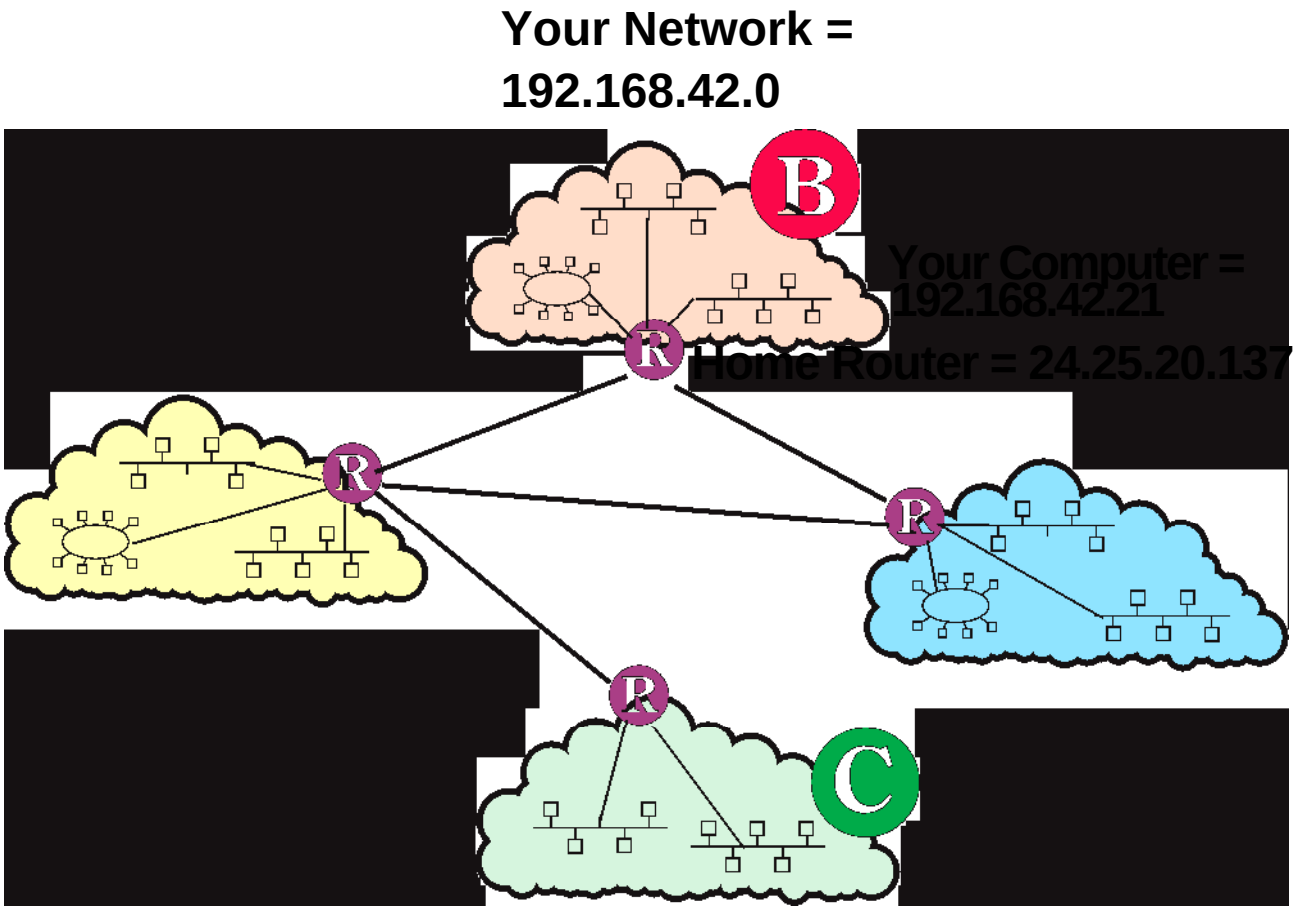
IP address is 32 bits long

Expressed as 4 decimal numbers

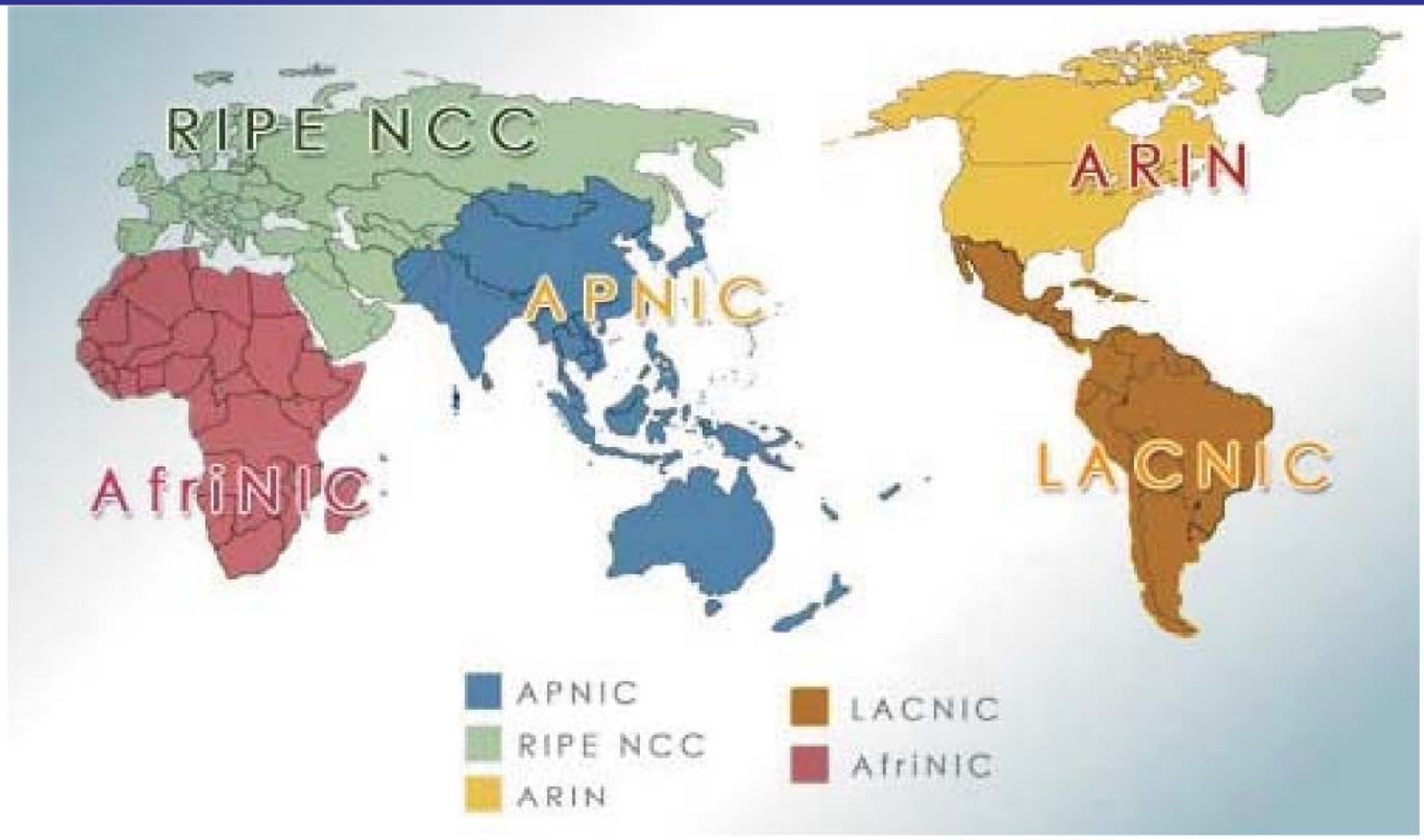
Format: 24.25.20.137
- Divided into 2 parts
  - Network address
  - Host address

Network address assigned:
- ISP
- Registrar

Host address assigned:
- Locally



IP Address Assignment



Public network addresses originally assigned to using organizations

Today regional authority assigns to Internet Service Providers (ISPs)

Network Address Translation

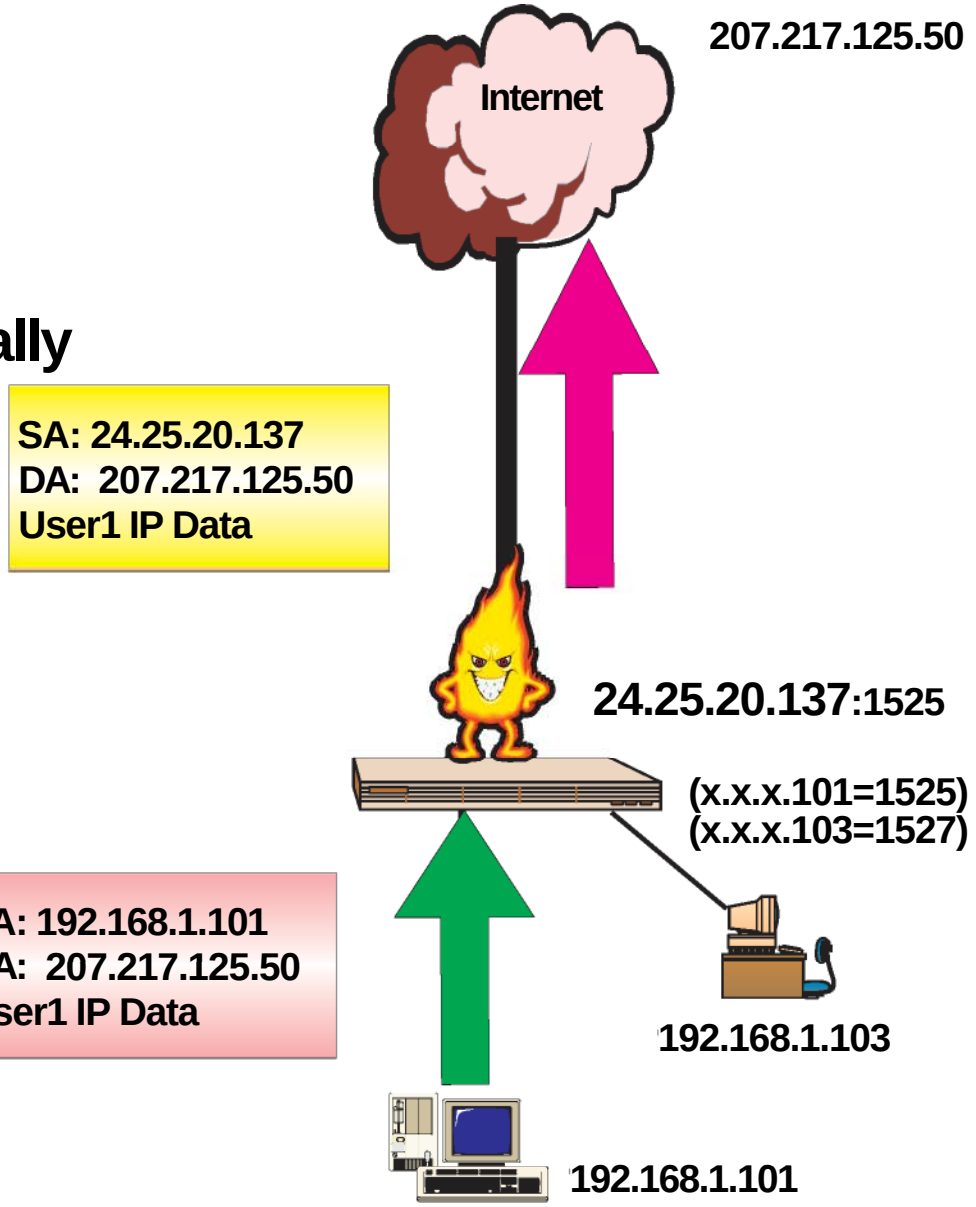
Hides internal addresses and systems from outsiders

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

How does my URL get transformed into an IP address?

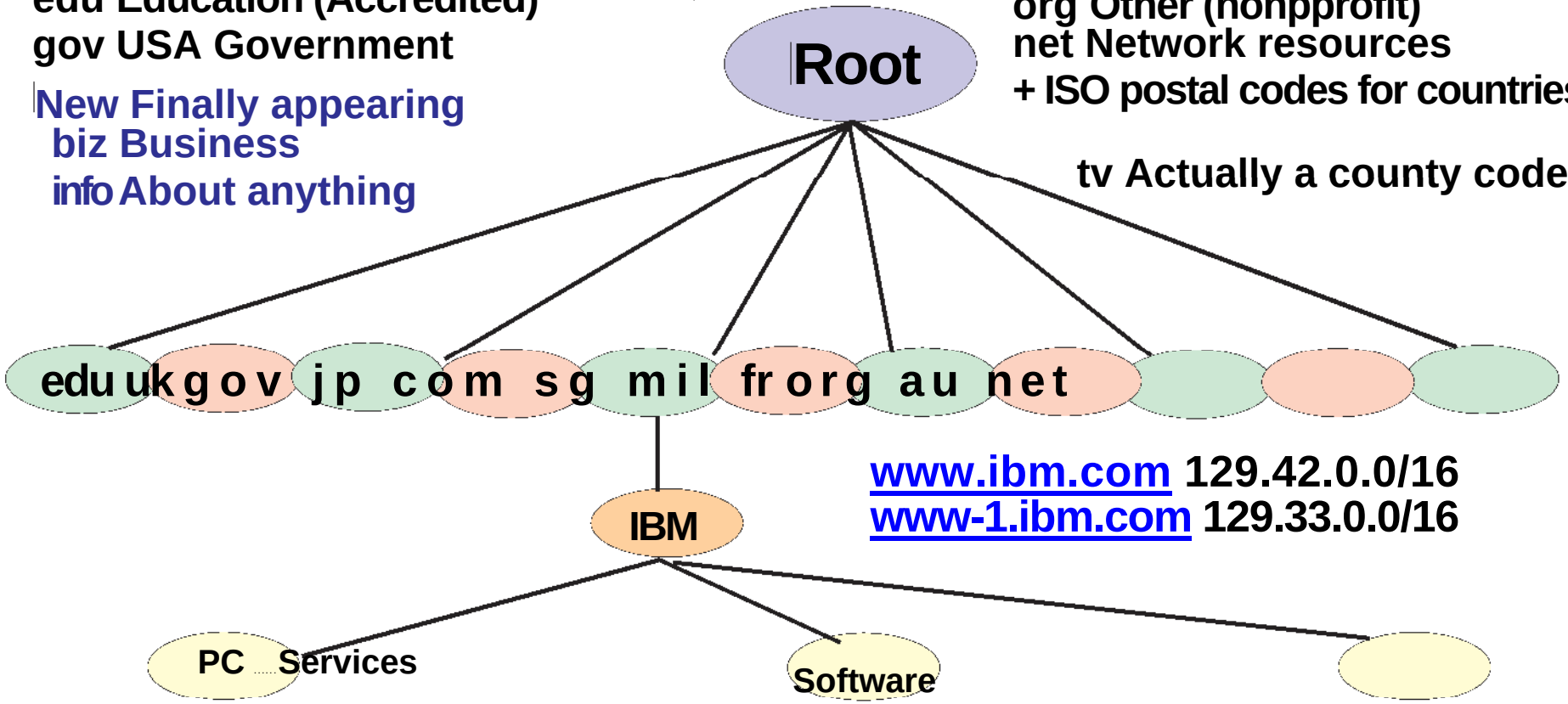
DNS and TCP/IP Addresses

com Commercial
edu Education (Accredited)
gov USA Government

New Finally appearing
biz Business
info About anything

mil USA Military
org Other (nonpprofit)
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

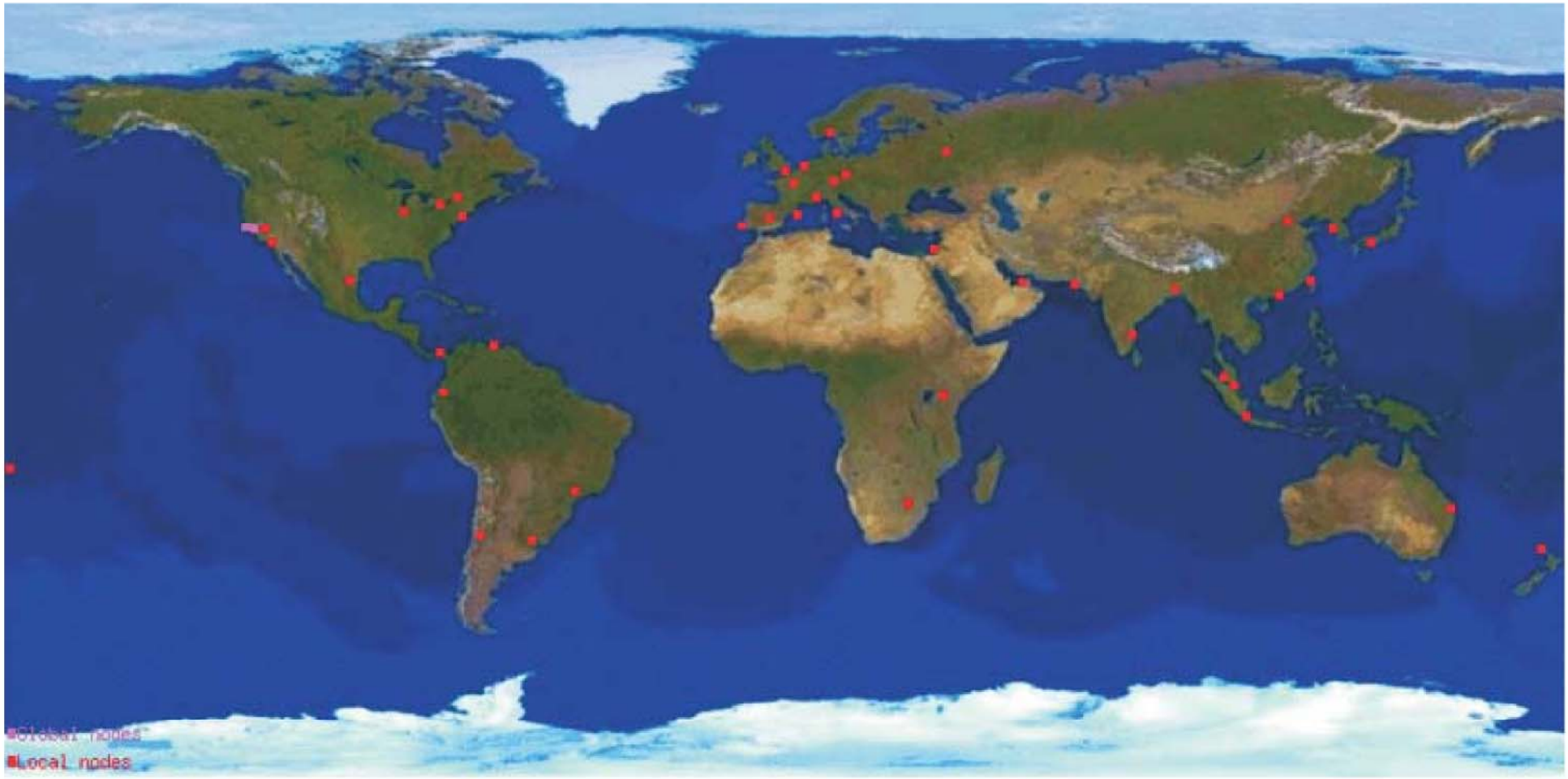
64.26.254.20 204.146.30.51 129.42.18.103

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

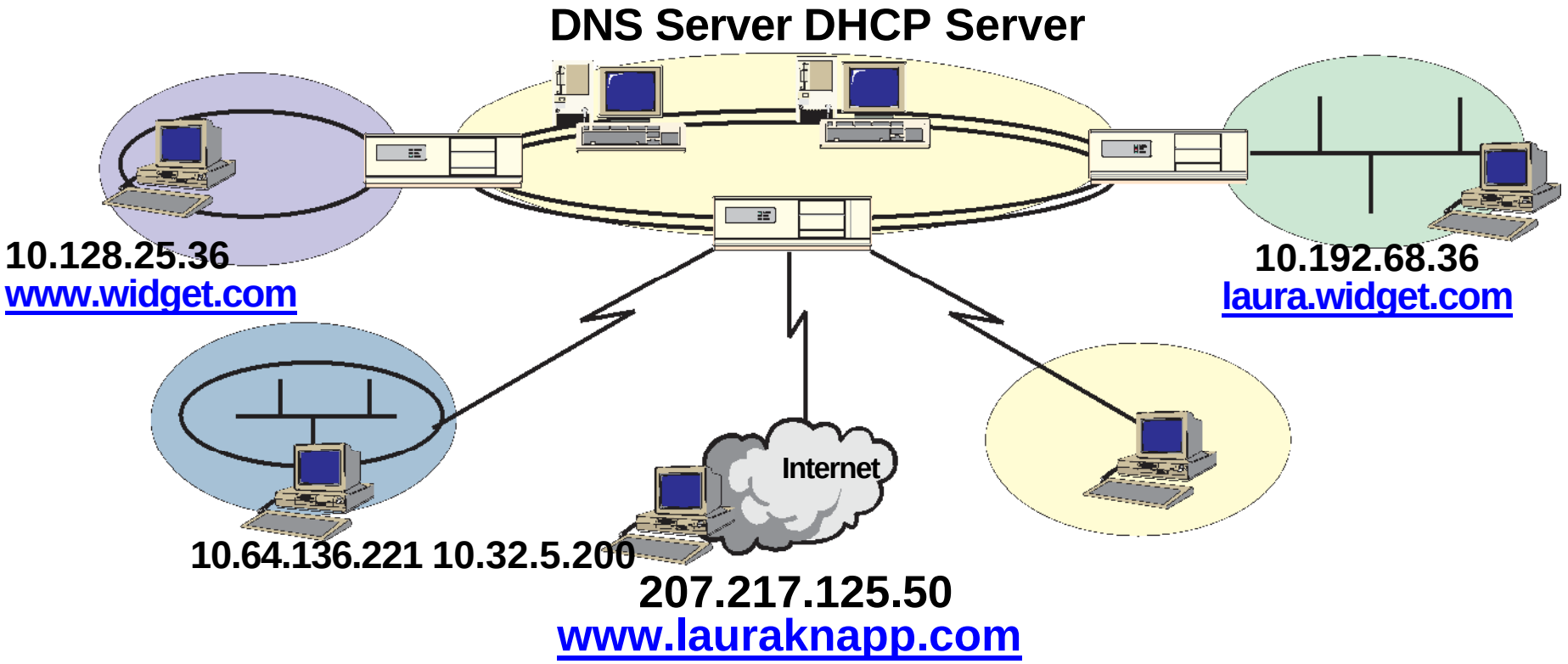
www.lauraknapp.com

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

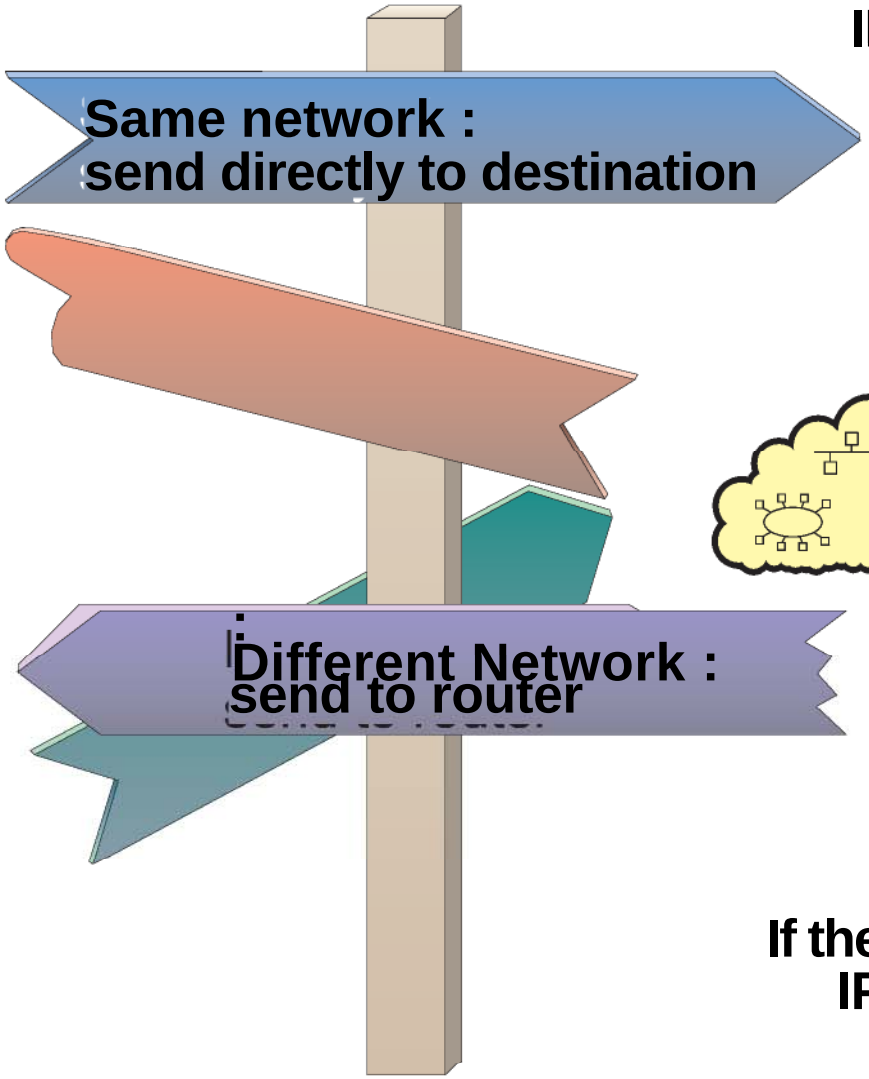
Dynamic IP



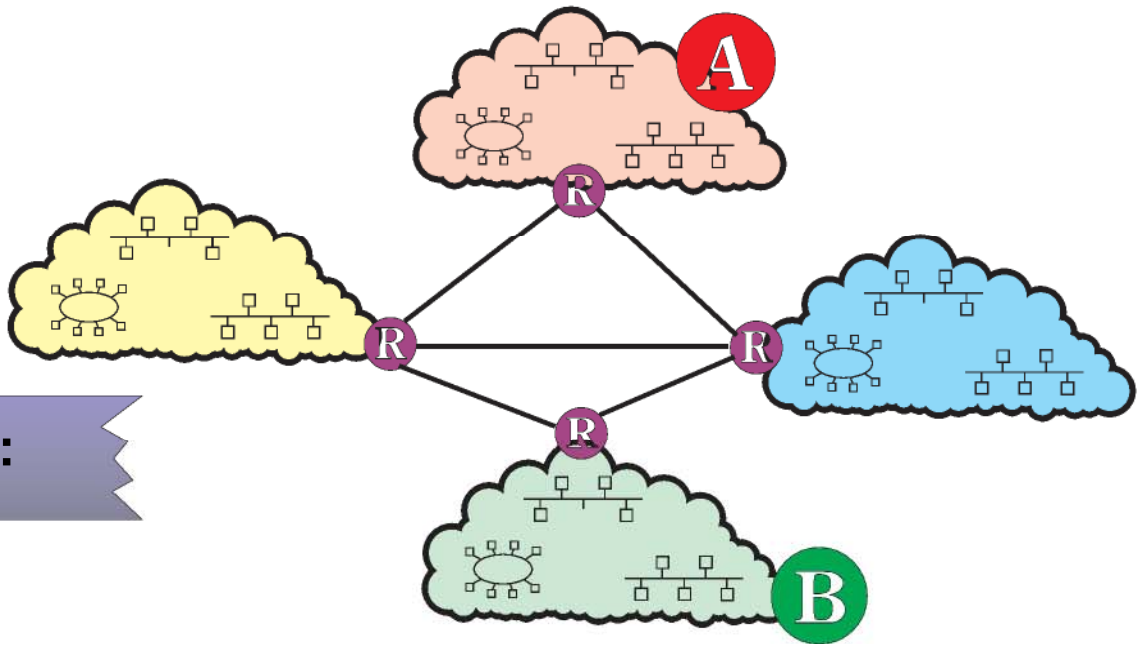
How did my browser resolve the Web server name to an IP address?
DNS server - Domain Name System Server

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

Routing

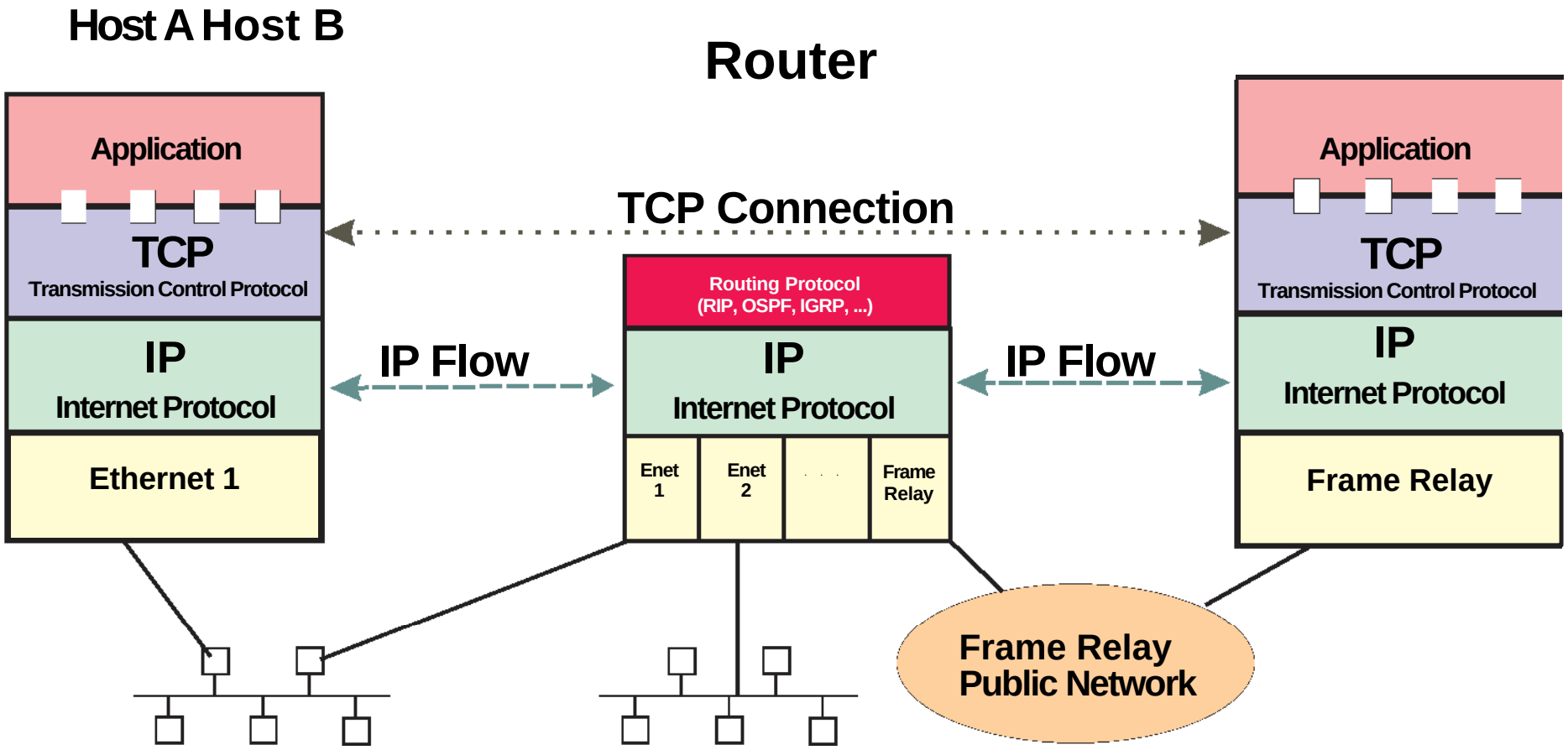


IP delivers datagrams directly from origin to destination if they are on the same network



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

IP Routing

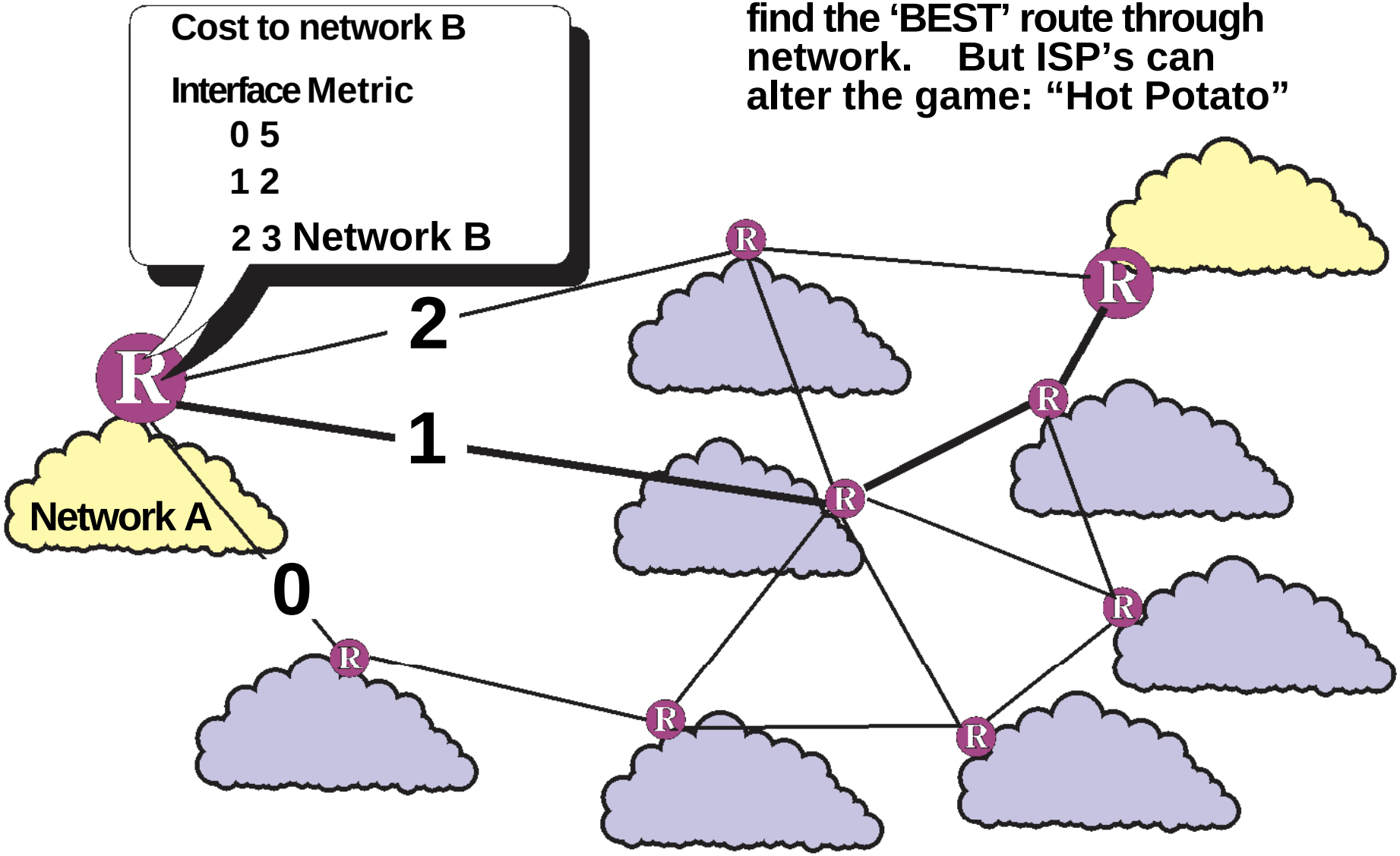


The routing function is performed by the IP protocol and routers

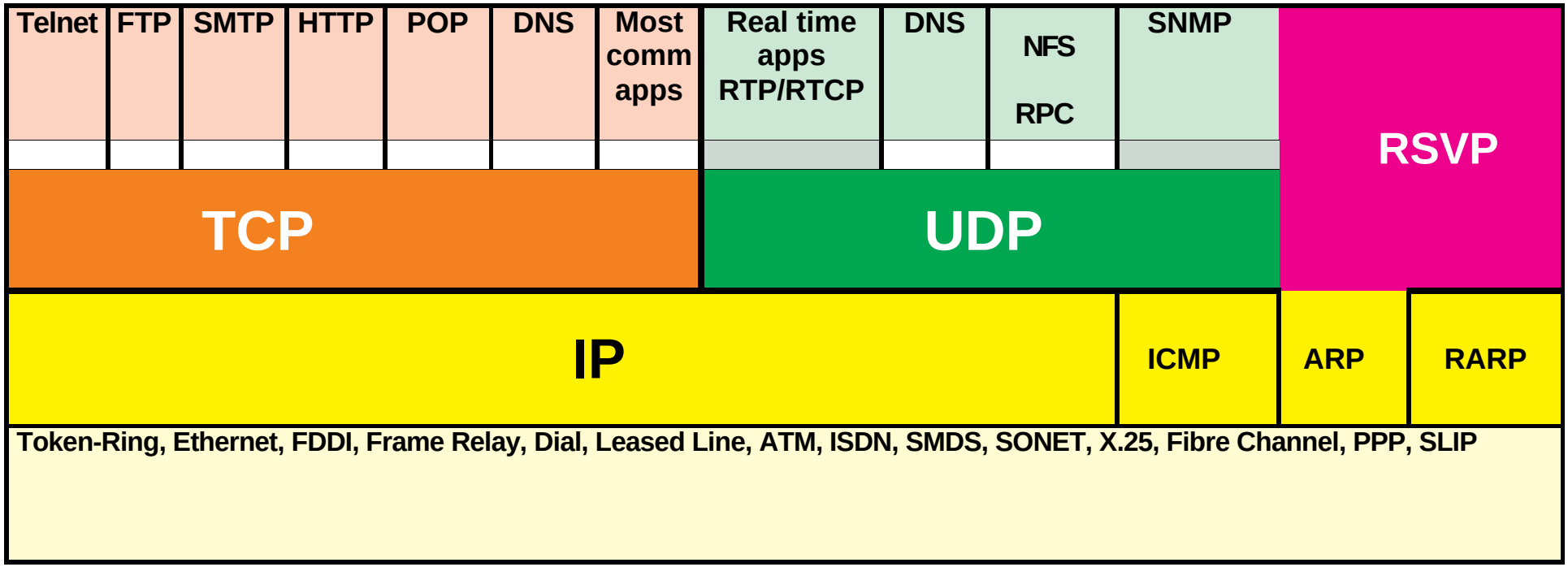
RIP - Routing Information Protocol
OSPF - Open Shortest Path First
IGRP - Interior Gateway Routing Protocol

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

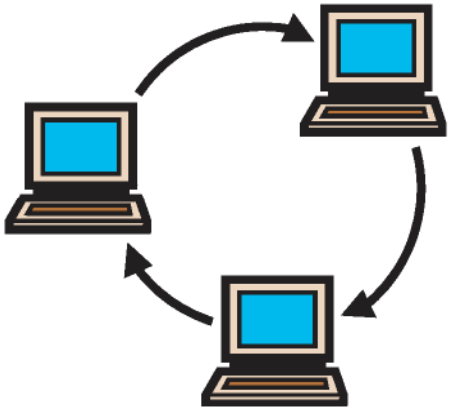
Telnet - Teletype Network
FTP - File Transfer Protocol
SMTP - Simple Mail Transfer Protocol
HTTP - Hypertext Transport Protocol
NFS - Network File System
RPC - Remote Procedure Call
SNMP - Simple Network Management Protocol

Internet Capabilities (Basics)

Internet Mail
Simple Mail Transfer Protocol
(SMTP)

Terminal Emulation
(TELNET)

Simple Network
Management Protocol
(SNMP)



File Transfer Protocol
(FTP)

Application Advances

USENET

Commerce

Internet Talk Radio

Nutella
MP3 Libraries

Real-time audio/video

IRC
(Internet Relay Chat)

BLOGs

You Tube

Animation

VoIP
Voice over IP

Listserve

Wiki

LDAP/DEN/Active Directory

JAVA/ActiveX

VRML
(Virtual Reality Markup Language)

BitTorrent

MUD
(Multiple User Dimension
/Dialogue/Dungeon)

NetMeeting

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

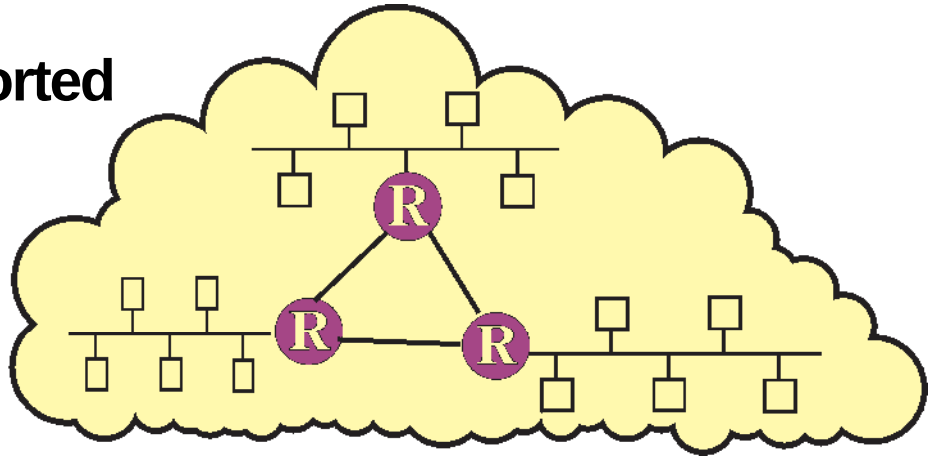
TCP/IP has a heritage of equality ...

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

Questions?

laurak@aesclever.com
www.aesclever.com
650-617-2400

Our other presentations:

Monday, 3:00 am - 4:00 am: Introduction to TCP/IP

Tuesday, 11:00 am – 12:00 pm: What every network manager needs to know about security

Tuesday 1:30 pm – 2:30 pm: Diagnosing Mainframe Network Problems with Packet Trace

Wednesday 11:00 am – 12:00 pm: Cloud Computing Environment

Wednesday 1:30 pm – 2:30 pm: Hot Topics in Networking and Security

Wednesday 4:30 pm – 5:30 pm: Wireless Security Challenges

Thursday 11:00 am – 12:00 pm: Virtualization – The Evolution of the Data Center