Computer Networks Fundamentals

WHAT IS A NETWORK?

- A *network* is simply two or more computers that are linked together.
- The most common types of networks are:
  - *Local Area Networks (LANS)* and
  - *Wide Area Networks (WANS).*
- The primary difference between the two is that a *LAN* is generally confined to a limited geographical area, whereas a *WAN* covers a large geographical area. Most *WANs* are made up of several connected *LANs.*

TYPES OF NETWORKS

- ***Local Area Network (LAN)*** – a network that spans a small area such as a building or an office.
  - Software applications and other resources are stored on a ***file server***.
  - ***Print servers*** **enable** multiple users to share the same printer.
- ***Wide Area Network (WAN)*** – a network that spans a wide geographical area;

BENEFITS OF A NETWORK

- *Information sharing:* Authorized users can use other computers on the network to access and share information and data. This could include special group projects, databases, etc.
- *Hardware sharing:* One device connected to a network, such as a printer or scanner, can be shared by many users.
- *Software sharing:* Instead of purchasing and installing a software program on each computer, it can be installed on the server. All of the users can then access the program from a single location.
- *Collaborative environment:* Users can work together on group projects by combining the power and capabilities of diverse equipment.

Ambrose, Bergerud, Busche, Morrison, and Wells-Pusins: IC3 BASICS, Thomson Course Technology, 2003

RISKS OF NETWORK COMPUTING

- The security of a computer network is challenged everyday by:
  - Equipment malfunctions
  - System failures
    - Note: equipment malfunctions and system failures may be caused by natural disasters such as floods, storms, or fires, and electrical disturbances
  - Computer hackers
  - Virus attacks

Ambrose, Bergerud, Busche, Morrison, and Wells-Pusins: IC3 BASICS, Thomson Course Technology, 2003

COMMUNICATIONS MEDIA

- ***Communications Channel***
  - To transfer data from one computer to another requires some type of link through which the data can be transmitted. This link is known as the *communications channel.*
  - To send data through the channel requires some type of *transmission media,* which may be either physical or wireless.

NETWORK/COMMUNICATION PROTOCOLS

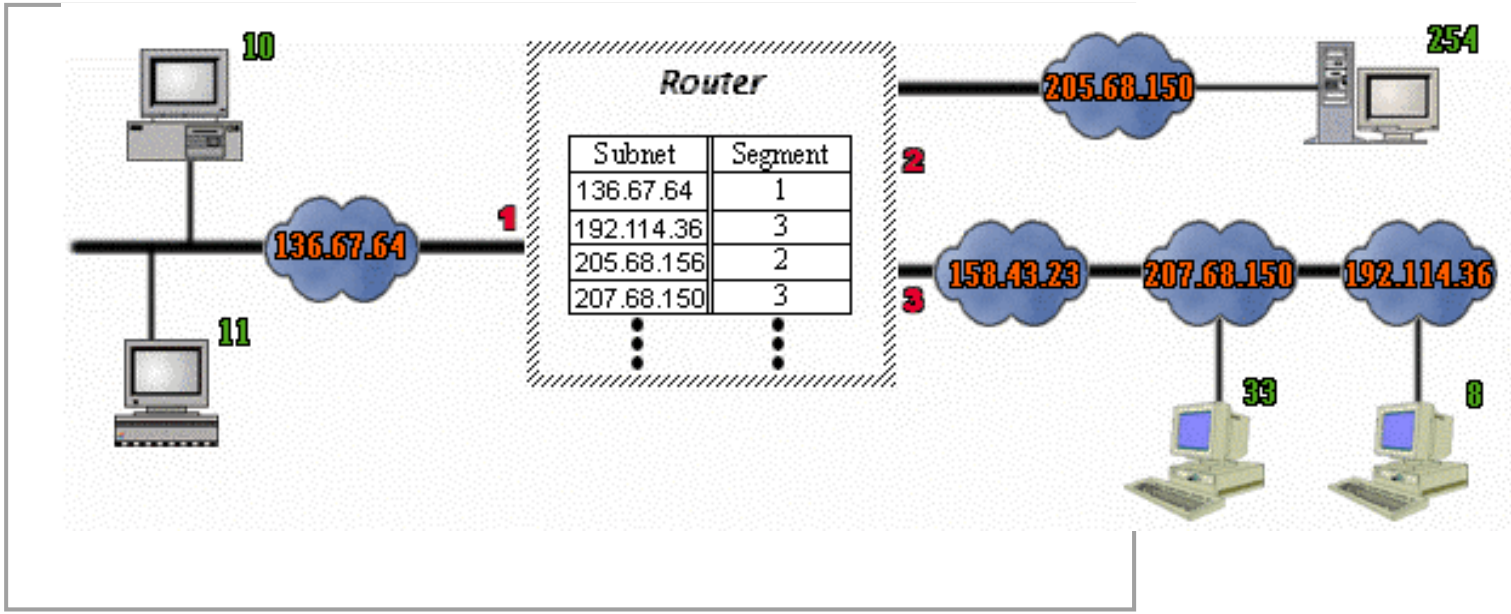
- ***A protocol*** is simply an agreed-on set of rules and procedures for transmitting data between two or more devices.
- ***Features determined by the protocol are***:
  - How the sending device indicates it has finished sending the message.
  - How the receiving device indicates it has received the message.
  - The type of error checking to be used.

Ambrose, Bergerud, Busche, Morrison, and Wells-Pusins: IC3 BASICS, Thomson Course Technology, 2003

NETWORK/COMMUNICATIONS PROTOCOLS

- On the Internet, the major protocol is ***TCP/IP*** (an acronym for Transmission Control Protocol/Internet Protocol).

ROUTERS



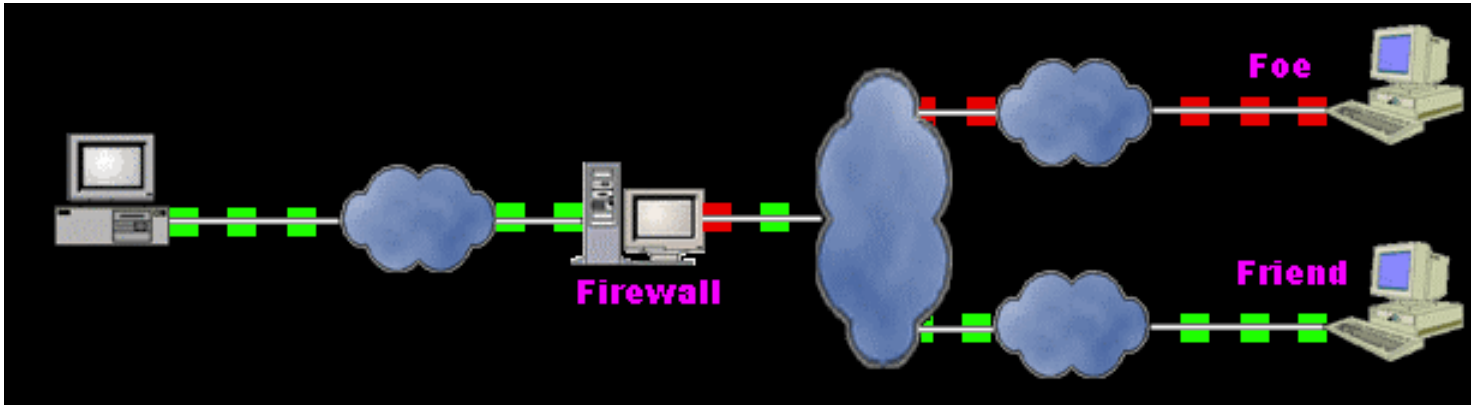
- Routers connect two or more networks and forward data packets between them. When data arrives from one of the segments, the router decides, according to it's routing table, to which segment to forward that data.

GATEWAY

- "Gateway" is a term that was once used to refer to a routing device. Today, in the TCP/IP world, the term "router" is used to describe such a device.

  The term gateway now refers to special-purpose devices, that perform protocol conversions. Gateways implement application layer conversions of information received from various protocols.

EXAMPLE OF FIREWALL



- Firewalls are systems that establish access control policies among networks. They can block information from entering a network or from getting out of that network, they can permit different users to perform different kinds of operations, according to the user's authorizations.

NETWORK ARCHITECTURE

- *Network architecture* – refers to the way a network is designed and built. The two major types are:
  - *Peer-to-peer architecture* – Computers connect with each other in a workgroup to share files, printers, and Internet access. This is used to connect a small number of computers.
  - *Client/server architecture* – sends information from a client computer to a server, which then relays the information back to the client computer, or to other computers on the network

Bandwidth

- Data rate measured in bits (not bytes) per seconds
- Kbps (Kilobits per seconds)
- Mbps (Megabits per seconds)
- Gbps (Gigabits per seconds)

LAN (Local Area Network)

- A network of computers that are in the same physical location, such as home or building
- Usually connected using Ethernet
  - A standard on how computers communicate over a shared media (cable)

Old: BNC connector for coaxial cable

http://en.wikipedia.org/wiki/Image:BNC_connector.jpg

New: RJ45 for twisted pair cable

http://en.wikipedia.org/wiki/Image:Ethernet_RJ45_connector_p1160054.jpg

Switch/Router

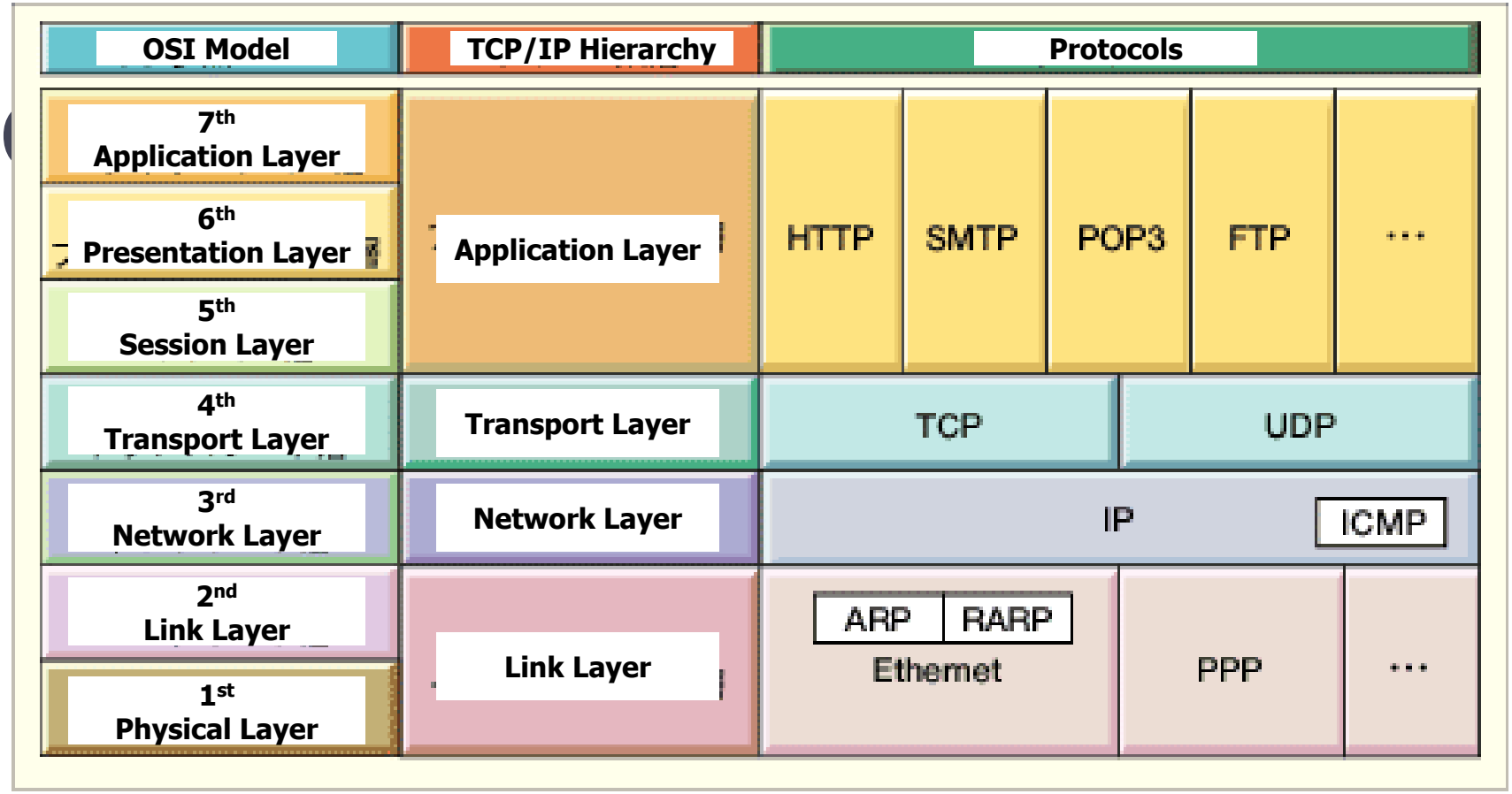
- To connect multiple segments of networks into a larger one
- Switch
  - Like hub but with intelligent
  - Better performance
- Router
  - Forward packets from one LAN to another

TCP/IP

- A family of protocols that makes the Internet works
- The Robustness Principle
  - “Be liberal in what you accept, and conservative in what you send” - Jon Postel

TCP/IP Network Model

- Different view – 4 layers
  - Layer 1 : Link (we did not look at details)
  - Layer 2 : Network
  - Layer 3 : Transport
  - Layer 4 : Application



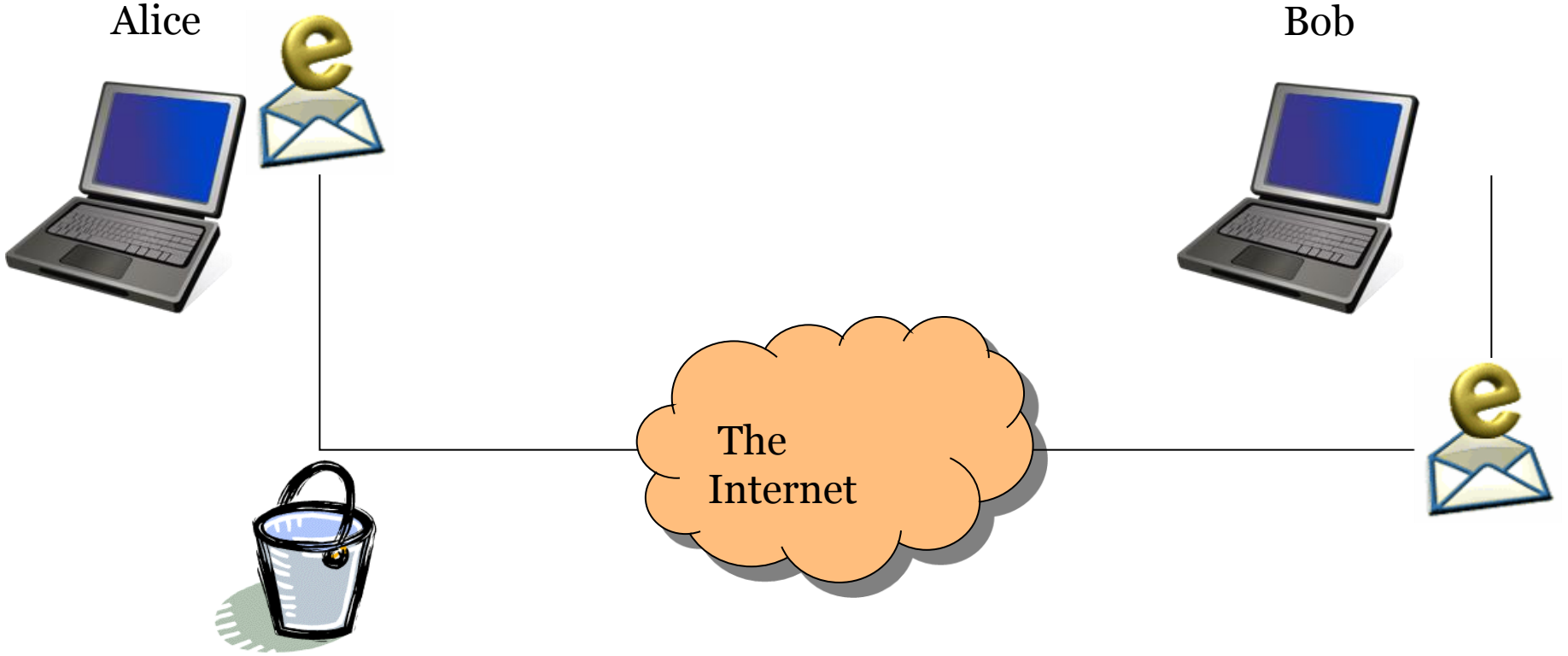
Link Layer : includes device driver and network interface card
Network Layer : handles the movement of packets, i.e. Routing
Transport Layer : provides a reliable flow of data between two hosts
Application Layer : handles the details of the particular application

TCP/IP (cont)

Application Layer Eg. WWW, FTP, IRC, Email, telnet, …	Data
Transport Layer Eg. TCP, UDP	Segments
Network Layer Eg. IP	**Packets**
Link Layer Eg. Ethernet, WiFi	Frames
Physical Layer Eg. Ethernet Cable, fiber-optics	Bits

Packets

- A small chunk of data transmitted over the Internet



VPN (Virtual Private Network)

- A secure tunnel to a private network through a public network
- Once established, local node appears to be a node in the private network in a secure manner

Host & IP Address

"A host is a computer connected directly to the Internet"

✗"Your home computer is not a host"

- Each host needs a globally unique IP address
- IPv4 address
  - A 32-bit number, arranged in 4 numbers separated by "."
  - Eg. 74.125.19.147

TCP/IP protocol family

- IP : Internet Protocol
  - UDP : User Datagram Protocol
    - RTP, traceroute
  - TCP : Transmission Control Protocol
    - HTTP, FTP, ssh

What is an internet?

- A set of *inter*connected *net*works
- The **I**nternet is the most famous example

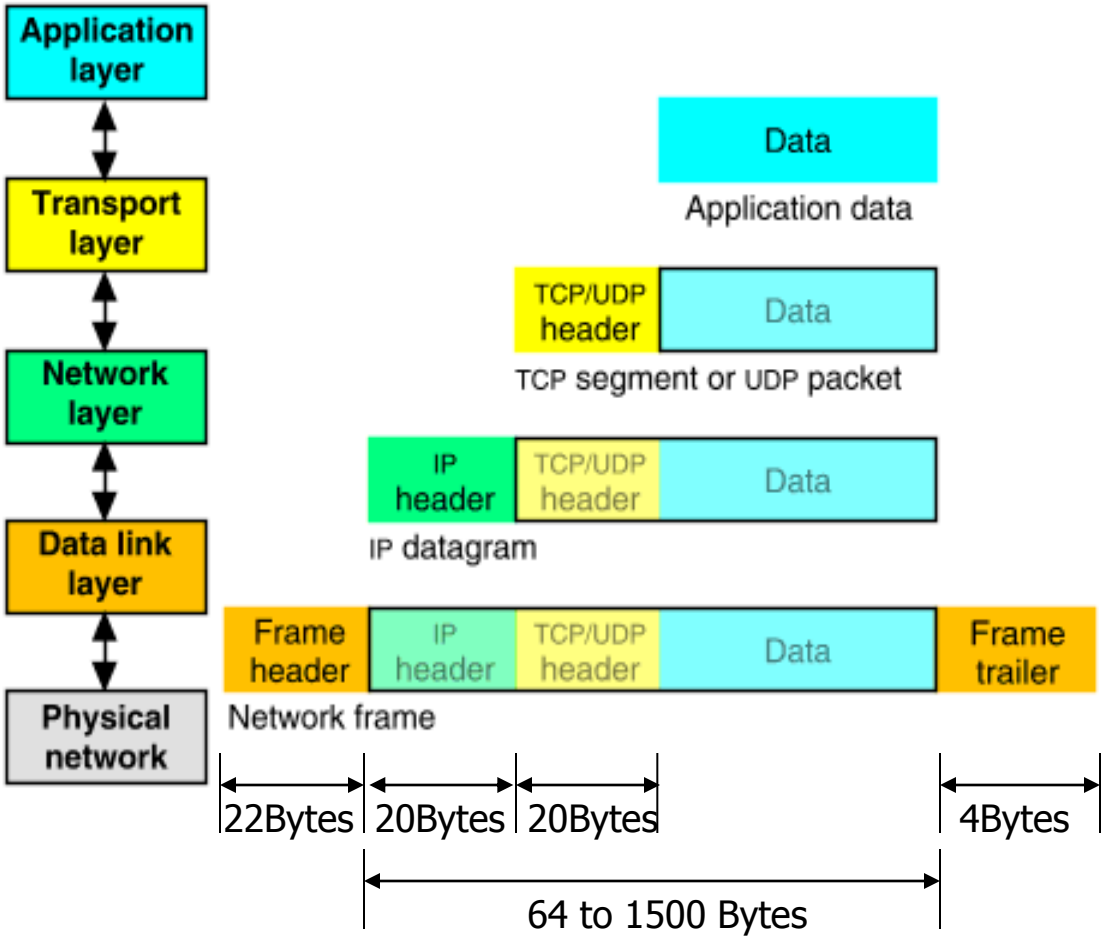
- Networks can be completely different
  - Ethernet, ATM, modem, …
  - (TCP/)IP is what links them

What is an internet? (cont)

- *Routers* (nodes) are devices on multiple networks that pass traffic between them
- Individual networks pass traffic from one router or endpoint to another
- TCP/IP hides the details as much as possible

Packet Encapsulation

- The data is sent down the protocol stack
- Each layer adds to the data by prepending headers



IP

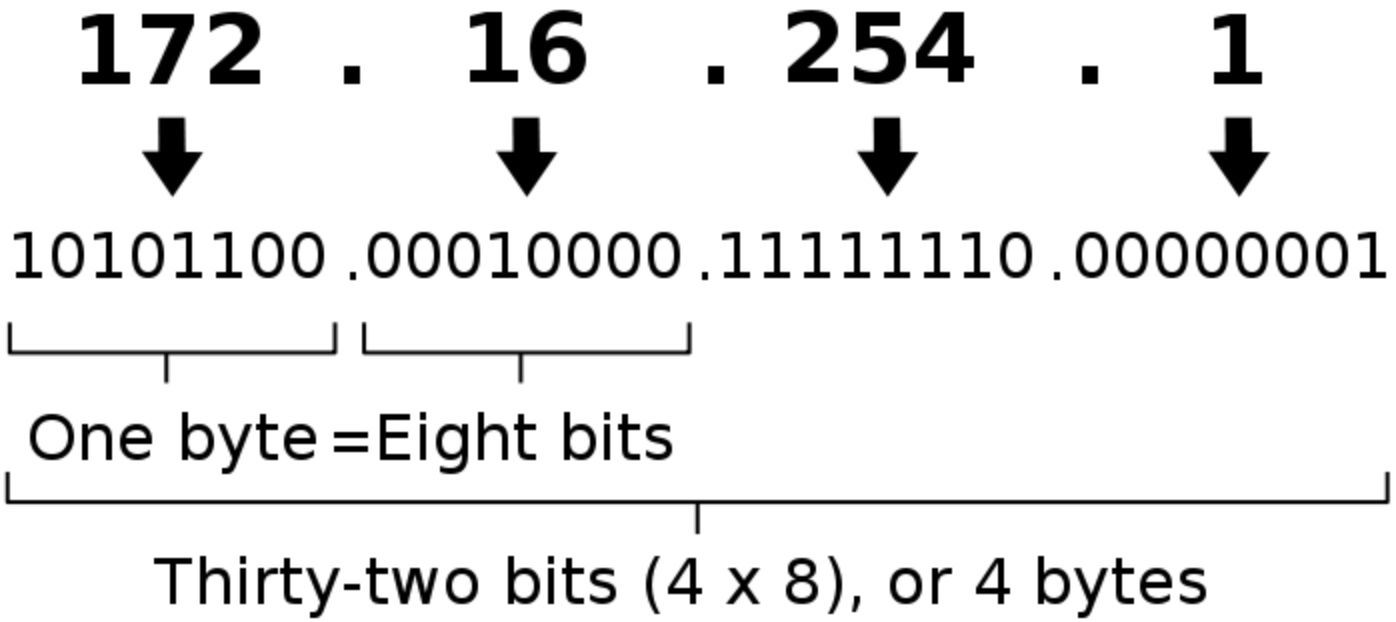
- Responsible for end to end transmission
- Sends data in individual packets
- Maximum size of packet is determined by the networks
  - Fragmented if too large
- Unreliable
  - Packets might be lost, corrupted, duplicated, delivered out of order

IP addresses

- 4 bytes
  - e.g. 163.1.125.98
  - Each device normally gets one (or more)
  - In theory there are about 4 billion available

- But…

An IPv4 address (dotted-decimal notation)



Routing

- How does a device know where to send a packet?
  - All devices need to know what IP addresses are on directly attached networks
  - If the destination is on a local network, send it directly there

Routing (cont)

- If the destination address isn't local
  - Most non-router devices just send everything to a single local router
  - Routers need to know which network corresponds to each possible IP address

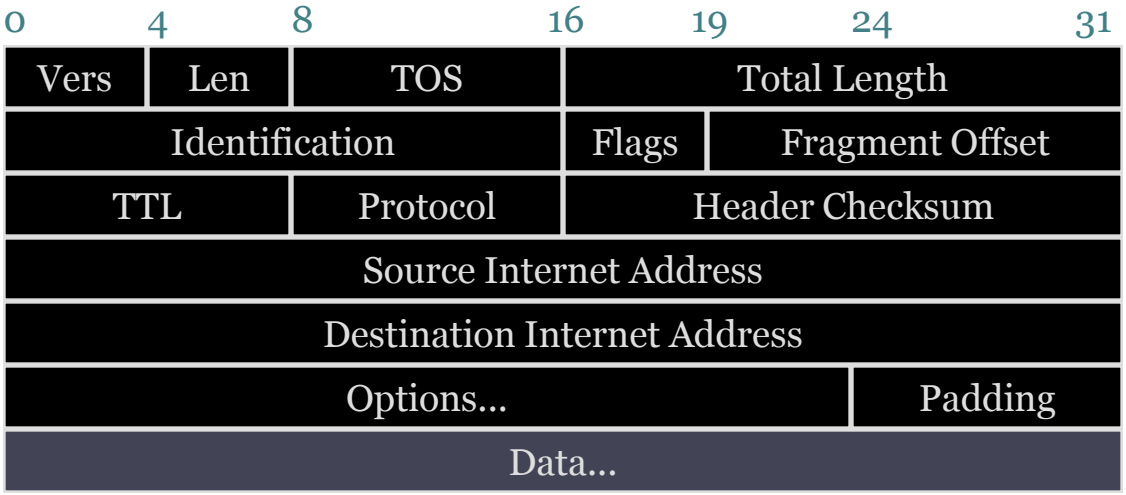
Allocation of addresses

- Controlled centrally by ICANN
  - Fairly strict rules on further delegation to avoid wastage
    - Have to demonstrate actual need for them
- Organizations that got in early have bigger allocations than they really need

IP packets

- Source and destination addresses
- Protocol number
  - 1 = ICMP, 6 = TCP, 17 = UDP
- Various options
  - e.g. to control fragmentation
- Time to live (TTL)
  - Prevent routing loops

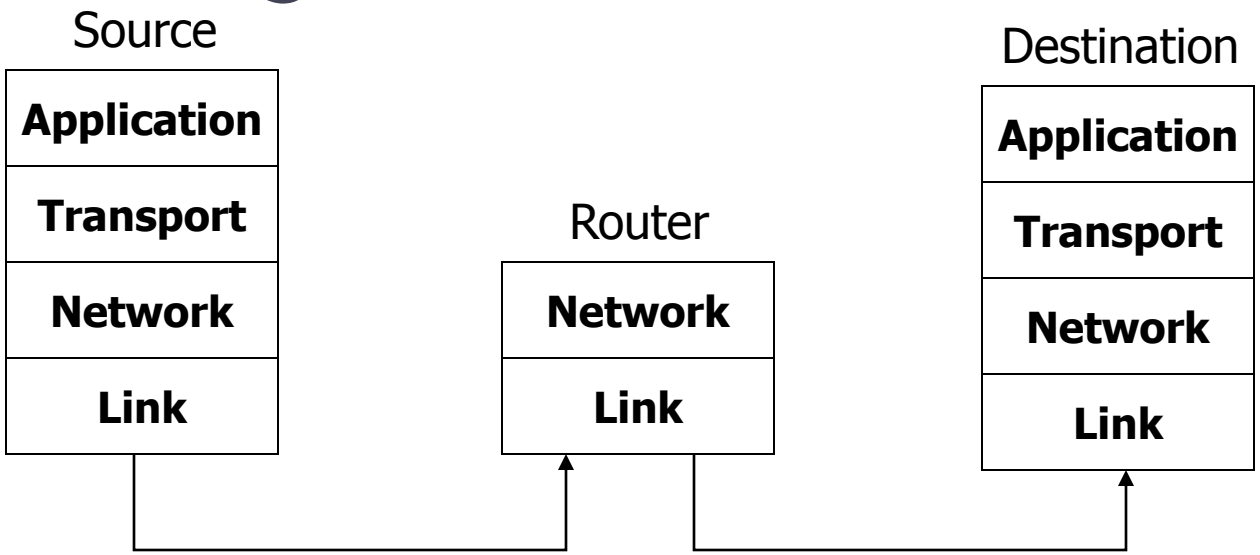
IP Datagram



Field	Purpose
Vers	IP version number
Len	Length of IP header (4 octet units)
TOS	Type of Service
T. Length	Length of entire datagram (octets)
Ident.	IP datagram ID (for frag/reassembly)
Flags	Don't/More fragments
Frag Off	Fragment Offset

Field	Purpose
TTL	Time To Live - Max # of hops
Protocol	Higher level protocol (1=ICMP, 6=TCP, 17=UDP)
Checksum	Checksum for the IP header
Source IA	Originator's Internet Address
Dest. IA	Final Destination Internet Address
Options	Source route, time stamp, etc.
Data…	Higher level protocol data

IP Routing

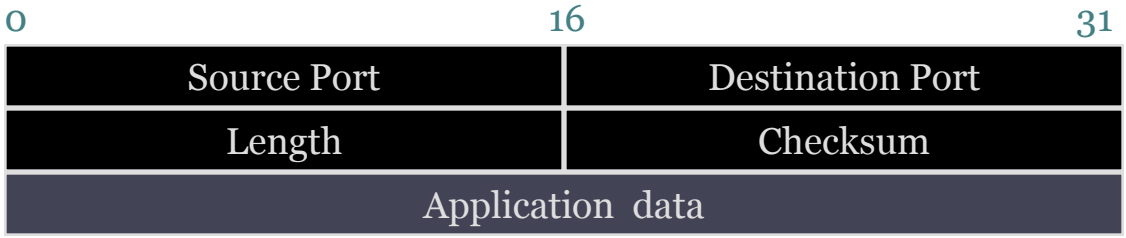


- Routing Table
  - Destination IP address
  - IP address of a next-hop router
  - Flags
  - Network interface specification

UDP

- Thin layer on top of IP
- Adds packet length + checksum
  - Guard against corrupted packets
- Also source and destination *ports*
  - Ports are used to associate a packet with a specific application at each end
- Still unreliable:
  - Duplication, loss, out-of-orderness possible

UDP datagram



Field	Purpose
Source Port	16-bit port number identifying originating application
Destination Port	16-bit port number identifying destination application
Length	Length of UDP datagram (UDP header + data)
Checksum	Checksum of IP pseudo header, UDP header, and data

Typical applications of UDP

- Where packet loss etc is better handled by the application than the network stack
- Where the overhead of setting up a connection isn't wanted

- VOIP
- Most games

TCP

- Reliable, *full-duplex*, *connection-oriented*, *stream* delivery
  - Interface presented to the application doesn't require data in individual packets
  - Data is guaranteed to arrive, and in the correct order without duplications
    - Or the connection will be dropped
  - Imposes significant overheads

Applications of TCP

- Most things!
  - HTTP, FTP, …
- Saves the application a lot of work, so used unless there's a good reason not to

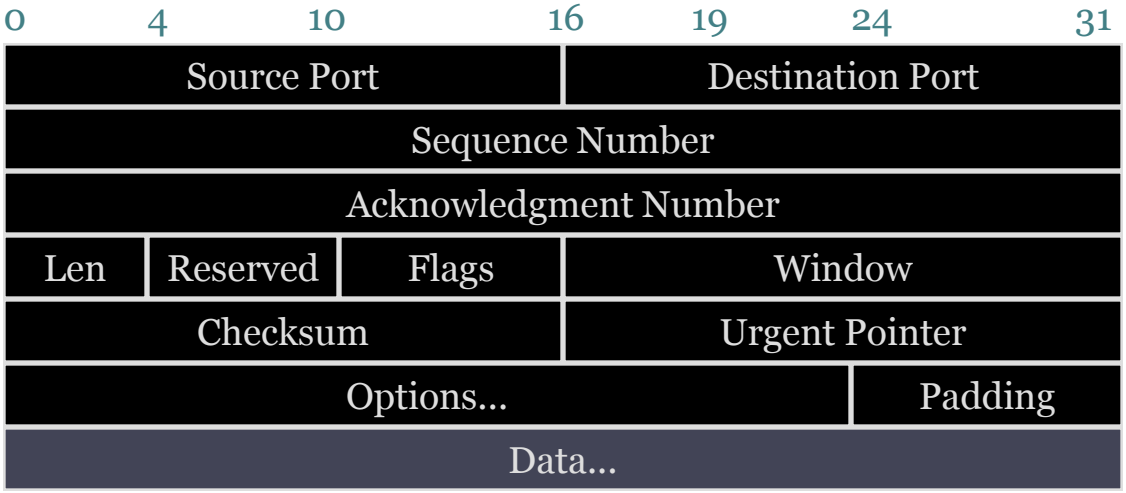
TCP implementation

- Connections are established using a *three-way handshake*
- Data is divided up into packets by the operating system
- Packets are numbered, and received packets are acknowledged
- Connections are explicitly closed
  - (or may abnormally terminate)

TCP Packets

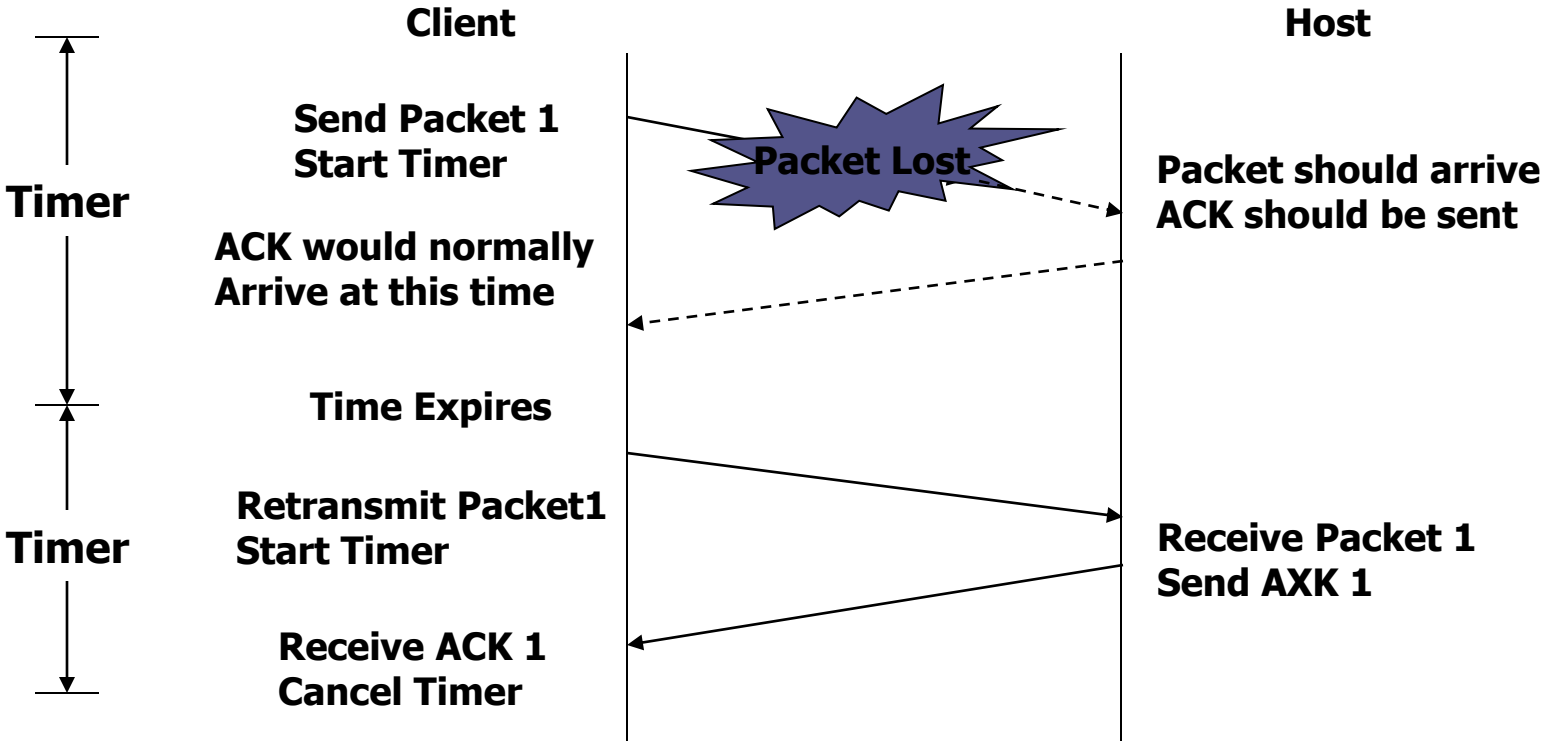
- Source + destination ports
- Sequence number (used to order packets)
- Acknowledgement number (used to verify packets are received)

TCP Segment



Field	**Purpose**
Source Port	Identifies originating application
Destination Port	Identifies destination application
Sequence Number	Sequence number of first octet in the segment
Acknowledgment #	Sequence number of the next expected octet (if ACK flag set)
Len	Length of TCP header in 4 octet units
Flags	TCP flags: SYN, FIN, RST, PSH, ACK, URG
Window	Number of octets from ACK that sender will accept
Checksum	Checksum of IP pseudo-header + TCP header + data
Urgent Pointer	Pointer to end of “urgent data”
Options	Special TCP options such as MSS and Window Scale

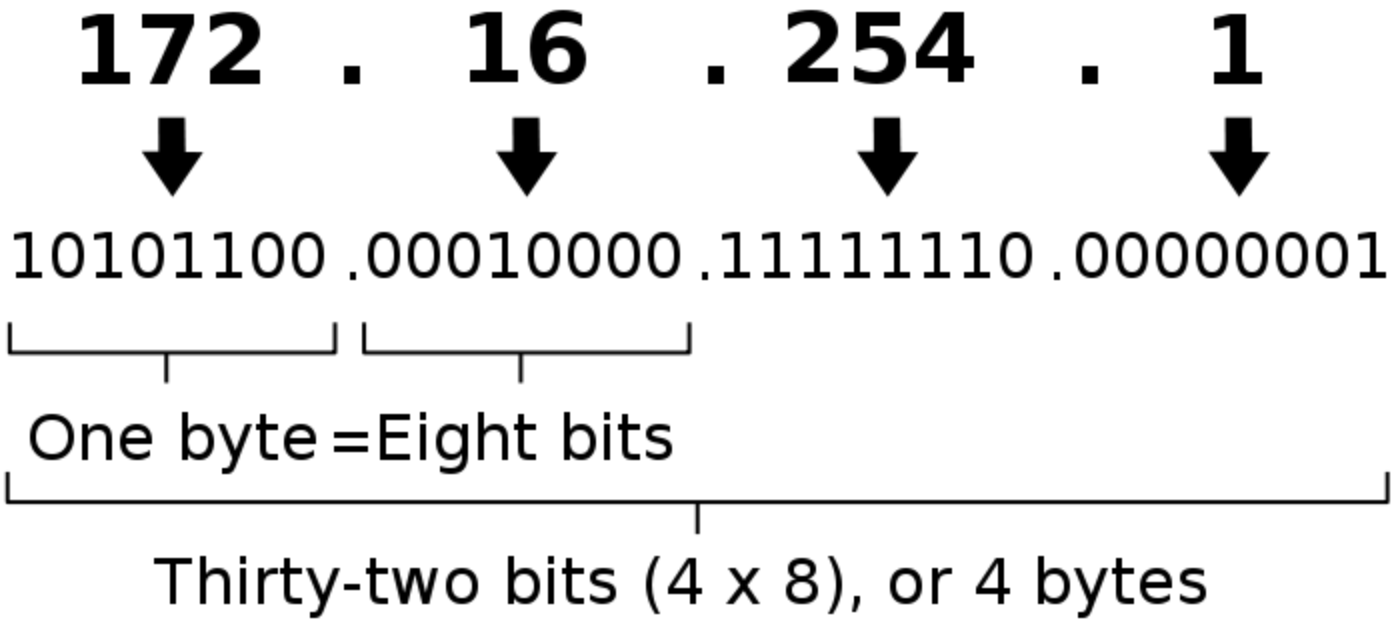
TCP : Data transfer

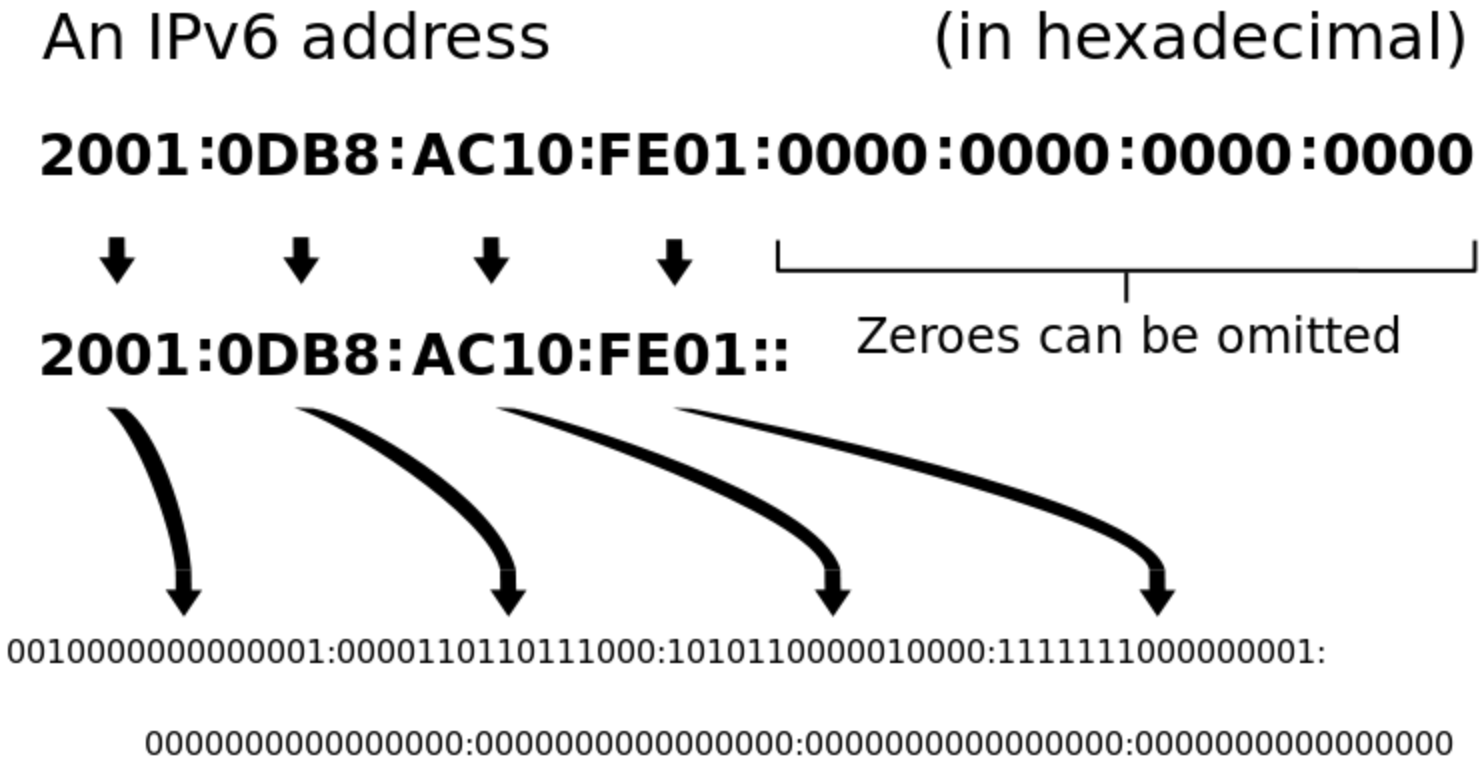


IPv6

- 128 bit addresses
  - Make it feasible to be very wasteful with address allocations
- Lots of other new features
  - Built-in autoconfiguration, security options, …

An IPv4 address (dotted-decimal notation)




An IPv6 address
(in hexadecimal)
2001:0DB8:AC10:FE01:0000:0000:0000:0000
2001:0DB8:AC10:FE01::
Zeroes can be omitted
0010000000000001:0000110110111000:1010110000010000:1111111000000001:
0000000000000000:0000000000000000:0000000000000000:0000000000000000