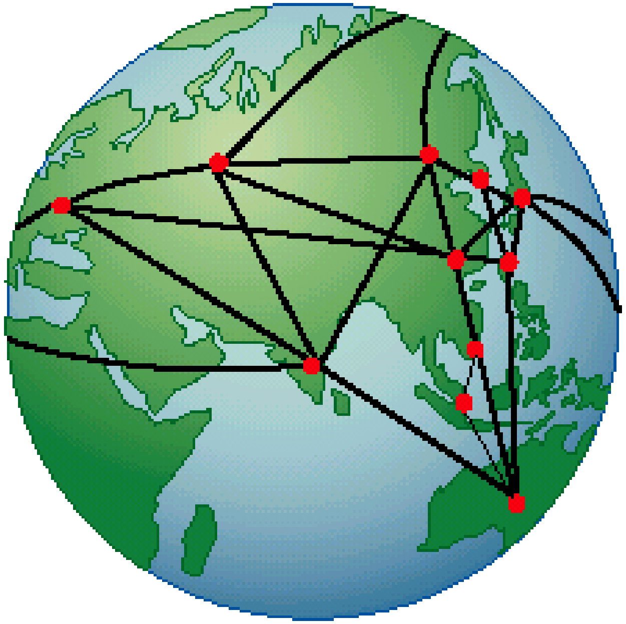
Computer Networks



Computer Networks

Lin Weiguo **Prof.**

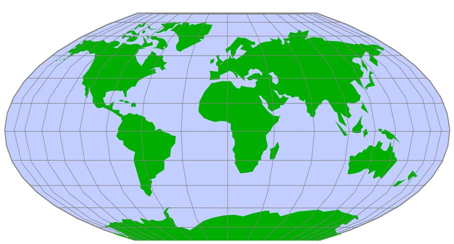
School of Computer Science & Cybersecurity

linwei@cuc.edu.cn

http://tlc.cuc.edu.cn

Roadmap

Introduction → Physical Layer → Data Link Layer → Medium Access Sublayer → Network Layer → Transport Layer → Application Layer



Chapter 1

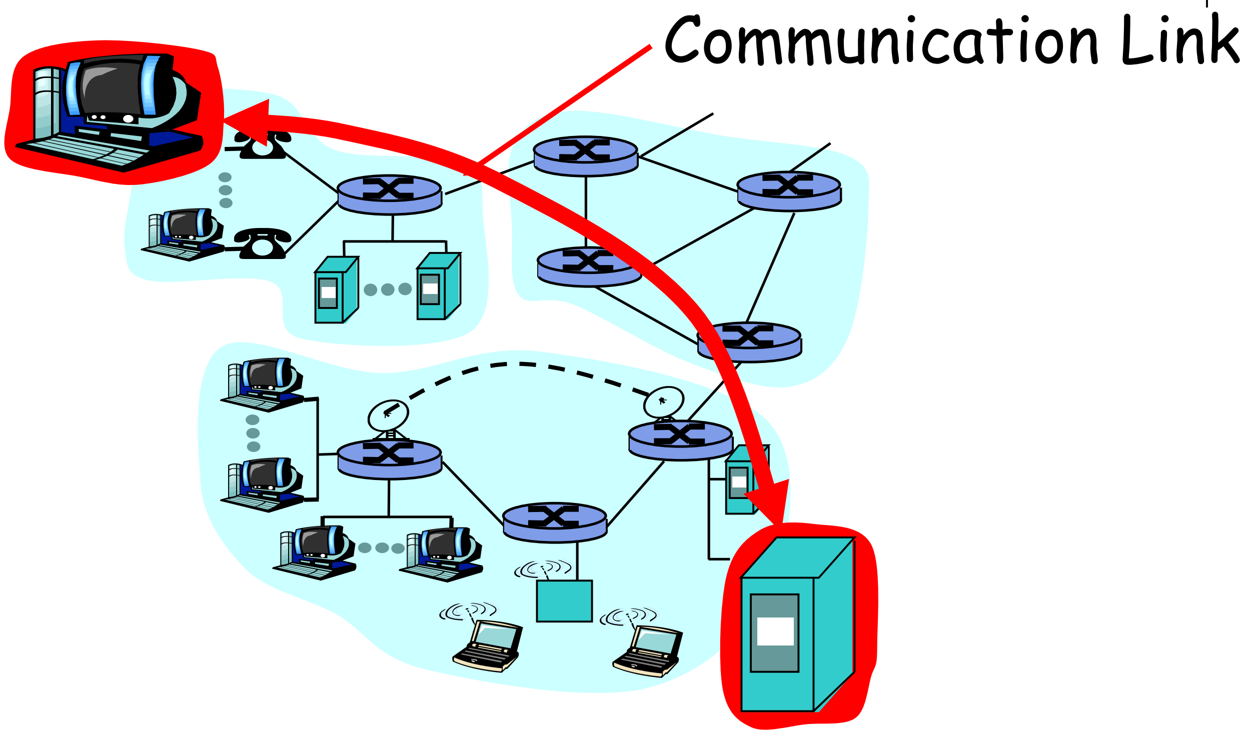
Introduction

Topics

- 1.1 Uses of computer networks
- 1.2 Network Hardware
- 1.3 Network Software
- 1.4 Reference Models
- 1.5 Example Networks
- 1.6 Network Standardization

Some of the overall issues we'll be dealing with in this course.

A Computer Network



A collection of **computers** interconnected by **communication** links

1.1 Uses of Computer Networks

- Business Applications
- Home Applications
- Mobile Users
- Social Issues

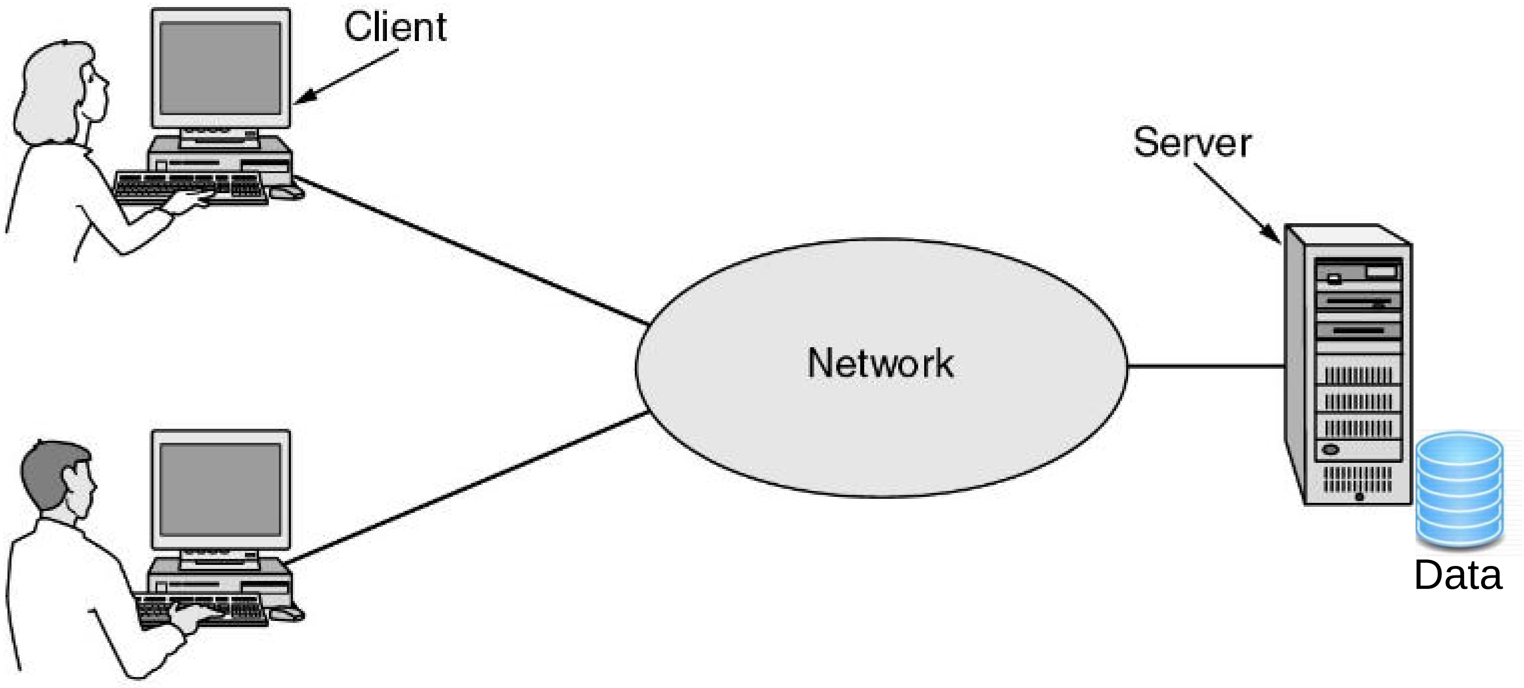
Business Applications

- Companies have a great number of computers
  - Monitor productions, keep track of inventories, do the payroll…
- Those computers may have worked in isolation from the others, but at some point, management may have decided to connect them to be able to distribute information throughout the company.

1st goal: Resource Sharing

- The goal is to make all programs, equipment, and especially data available to anyone on the network without regard to the physical location of the resource and the user.
- Equipment:
  - Printers, Scanner, CD-Burners…
- Information:
  - Customer records, Product information ,inventories, financial statements, tax information …

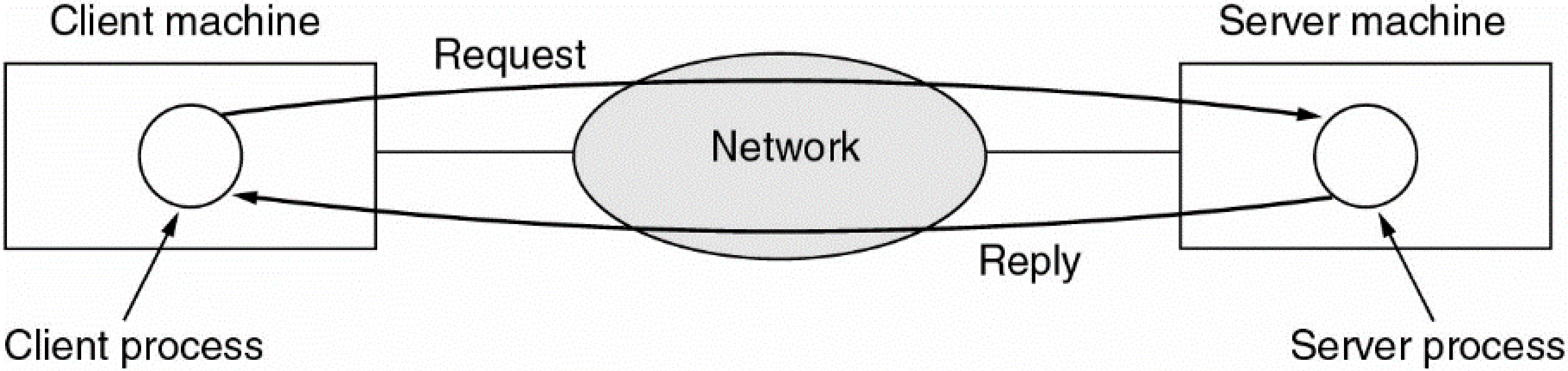
Client machine and Server machine



A network with two clients and one server.

Client/Server model

- The **C/S model** is widely used and forms the basis of much network usage. The most popular realization is that of a **Web application**.



The client/server model involves requests and replies.

2nd goal: A Computer network to do with people

- A second goal of setting up a computer network has to do with people rather than information or even computers. A computer network can provide a powerful communication medium among employees.
  - Email
  - VoIP
  - Videoconferencing
  - Cooperate with other to work: desktop sharing

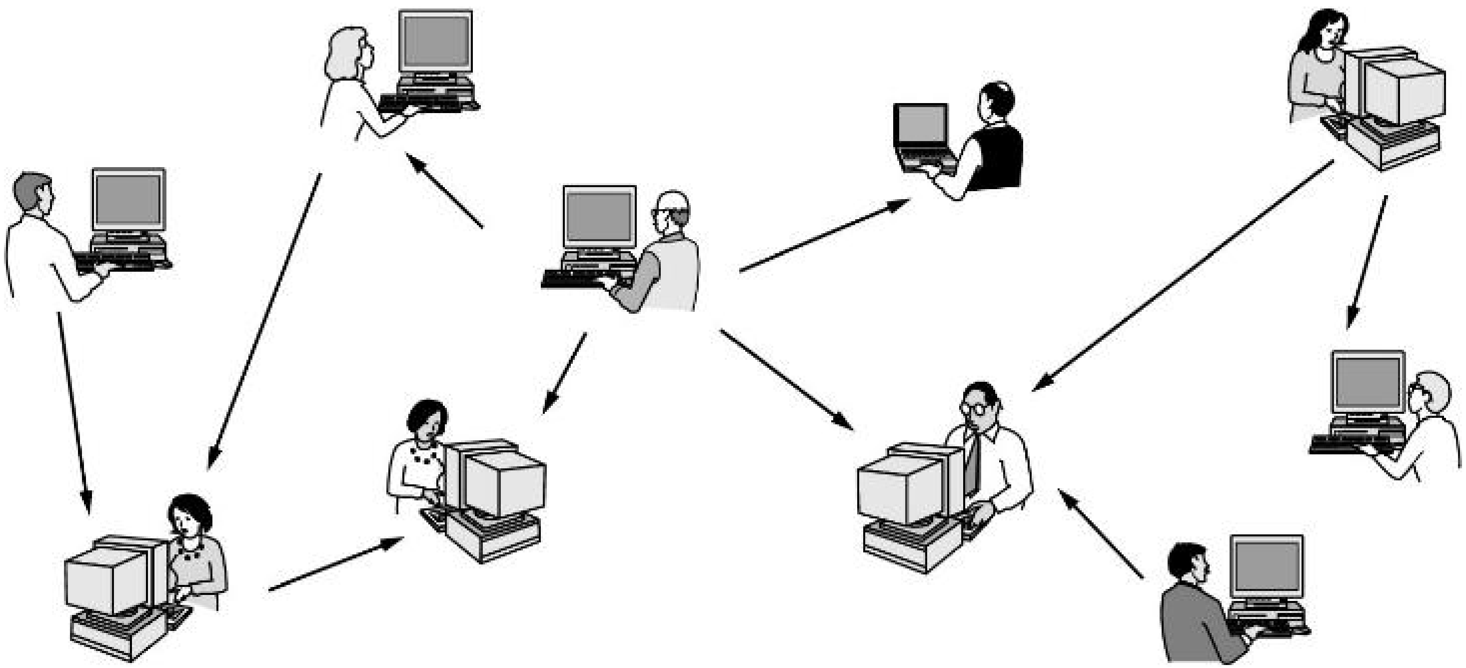
3rd goal: e-Commerce

- A third goal for many companies is doing business electronically with other companies, especially suppliers and customers.
- e-Commerce
  - B2B: Business to business.
  - B2C: Business to consumer.
  - C2C: Consumer to consumer.

Home Applications

- Access to remote information
  - Web
- Person-to-person communication
  - Email,IM, VoIP
- e-commerce
- Interactive entertainment
  - Online Video, Gaming

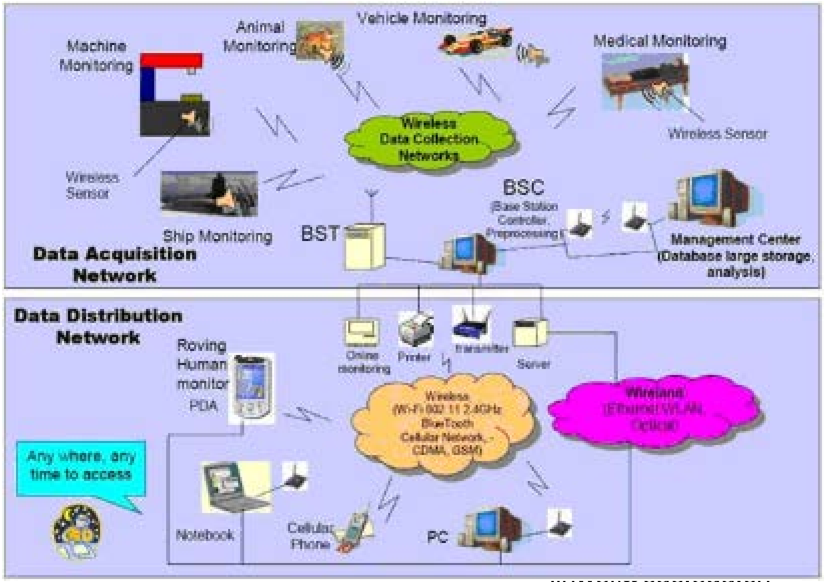
P2P - Peer to Peer



In peer-to-peer system there is no fixed division into clients and servers.

Other applications

- Ubiquitous computing
  - IOT (Internet of Things)
    - Sensor Networks
    - RFID (Radio Frequency IDentification)



Mobile Users

Combinations of wireless networks and mobile computing.

Wearable Computers

Social Issues

- Social networking issues
- Employee rights vs employer rights
- Government vs citizen
- Hacker and criminal
- Copyright protection
- ……

Again, The Internet addiction ?

1.2 Network Hardware

- Taxonomy of Networks
- Personal Networks
- Local Area Networks
- Wide Area Networks
- Wireless Networks

Classifying networks

- By transmission technology
- By scale

Transmission technology

- Types of transmission technology
  - Broadcast links
  - Point-to-point links

Point-to-point links

- Point-to-point links connect individual pairs of machines.
- Packets : short messages
  - To go from the source to the destination, a packet on a network made up of point-to-point links may have to first visit one or more intermediate machines.
  - Often multiple routes, of different lengths, are possible
- Unicasting:
  - exactly one sender and one receiver

Broadcast Networks

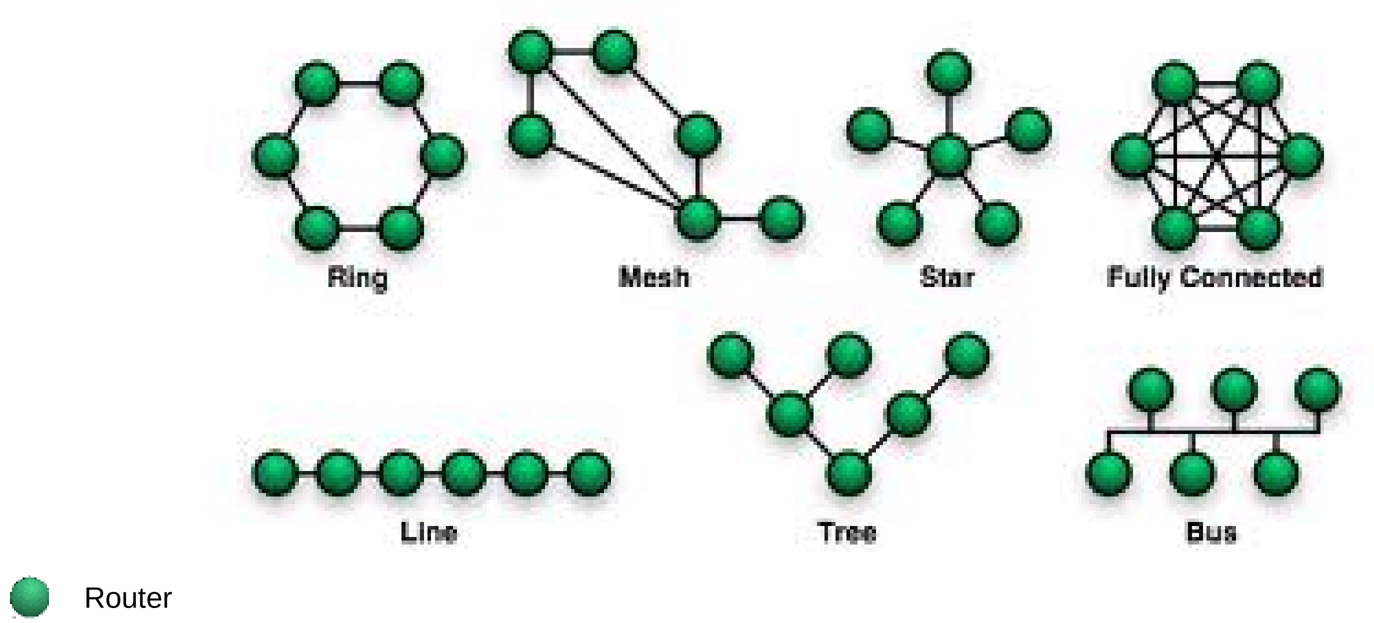
- Broadcast networks have a single communication channel that is shared by all the machines on the network.
- Packets sent by any machine are received by all the others.
  - An address field within the packet specifies the intended recipient. Upon receiving a packet, a machine checks the address field. If the packet is intended for the receiving machine, that machine processes the packet; if the packet is intended for some other machine, it is just ignored.

Broad/Multi-casting

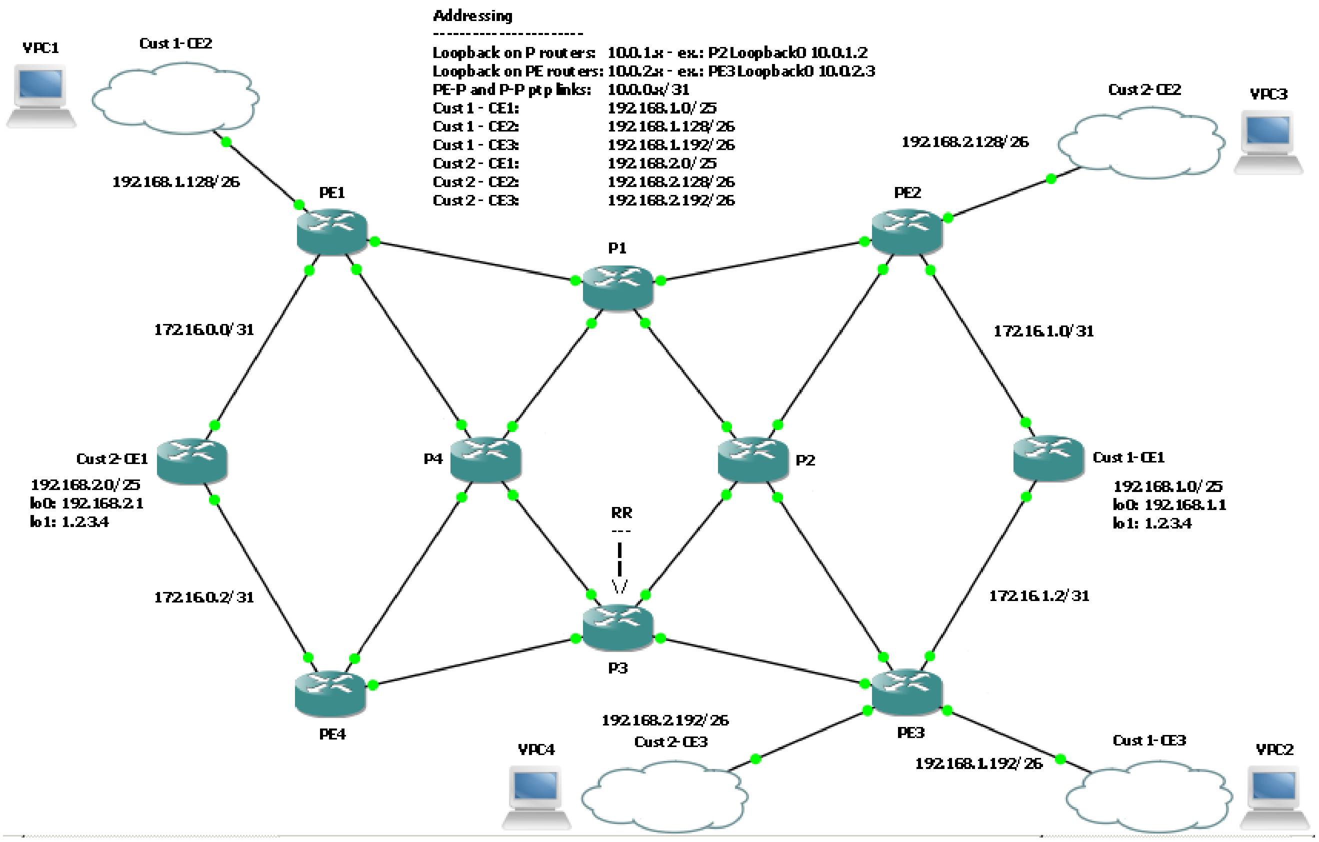
- Broadcasting
  - address a packet to all destinations by using a special code in the address field .
- Multicasting
  - Some broadcast systems also support transmission to a subset of the machines

Network Topologies

- Think of a topology as a network's virtual shape or structure.



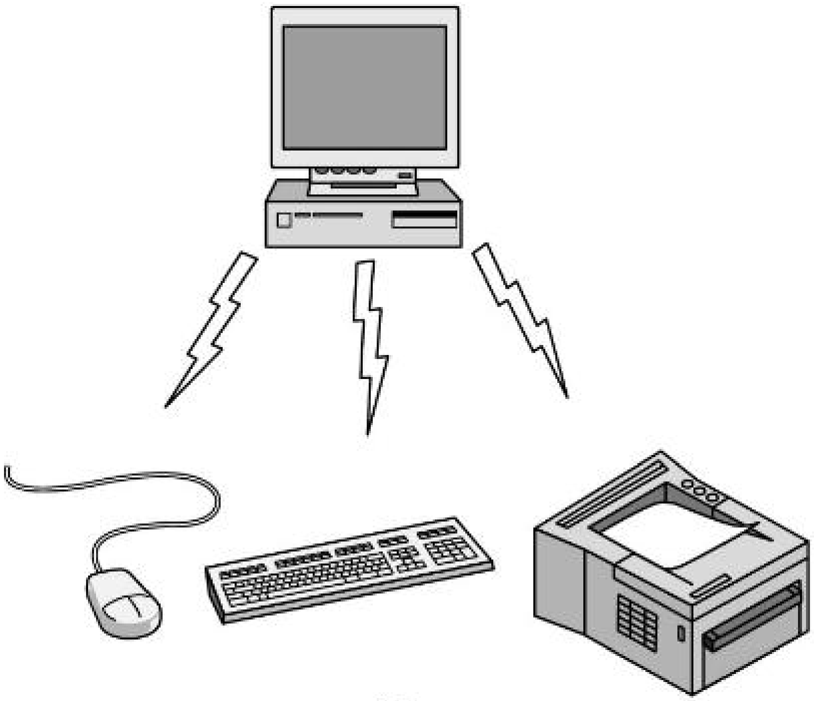
Example of a Real network



Classification by scale.

Interprocessor distance	Processors located in same	Example
1 m	Square meter	Personal area network
10 m	Room	Local area network
100 m	Building	Local area network
1 km	Campus	Local area network
10 km	City	Metropolitan area network
100 km	Country	Wide area network
1000 km	Continent	Wide area network
10,000 km	Planet	The Internet

PAN (Personal area networks)



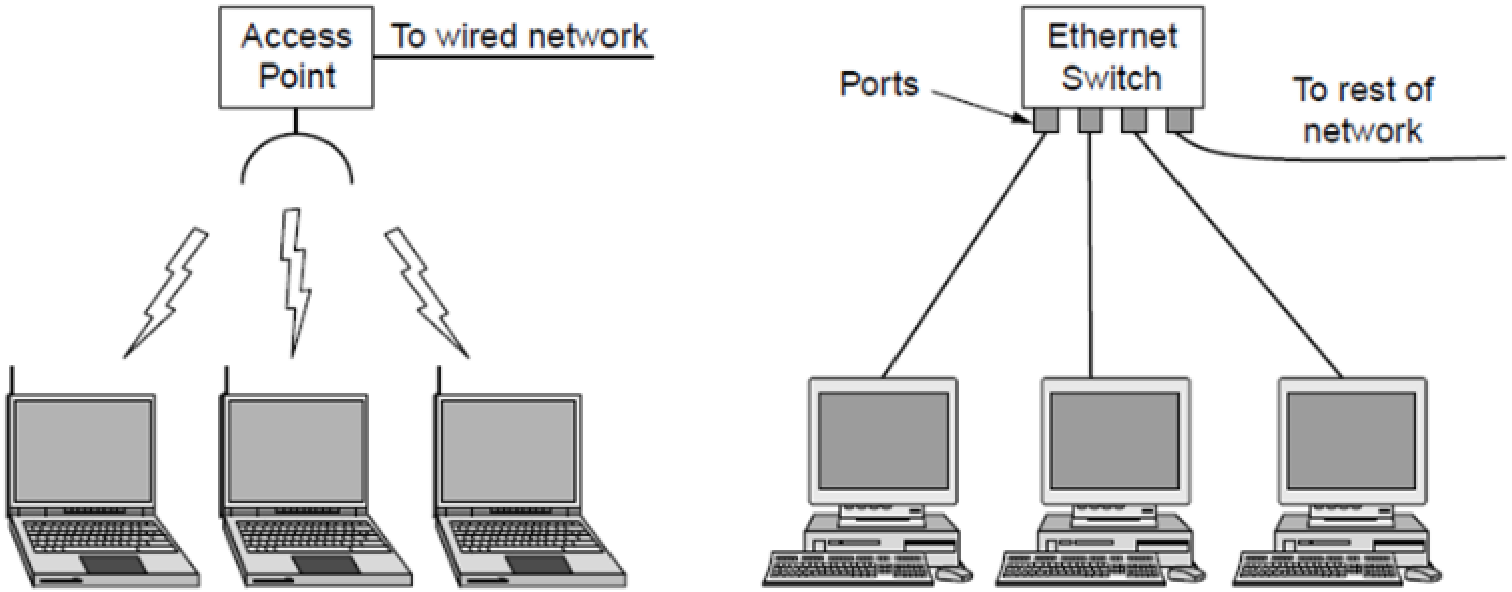
(a)

Bluetooth (IEEE 802.15)

Local Area Networks

- A LAN is a privately owned network that operates with in and nearby a single building like a home, office or factory.
- LANs are widely used to connect personal computers and consumer electronics to let them share resources and exchange information.

Wireless and wired LANs



Wireless and wired LANs.
(a) 802.11. (b) Switched Ethernet.

WLAN (Wireless LAN)

Wireless LAN (Wi-Fi IEEE 802.11)

Wired LAN

- Wired LANs charactoristics
  - Use copper wires, optical fibers
  - Are restricted in size
  - Run at speeds of 10Mbps to 1Gbps
  - Low delay
  - Make very few errors

Ethernet: IEEE802.3

- Ethernet is the most common type of wired LAN
- **Switched Ethernet**
  - Each computer speaks the Ethernet protocol and connects to a box called a switch with a point-to-point link.
  - A switch has multiple ports, each of which can connect to one computer. The job of the switch is to relay packets between computers that are attached to it, using the address in each packet to determine which computer to send it to.

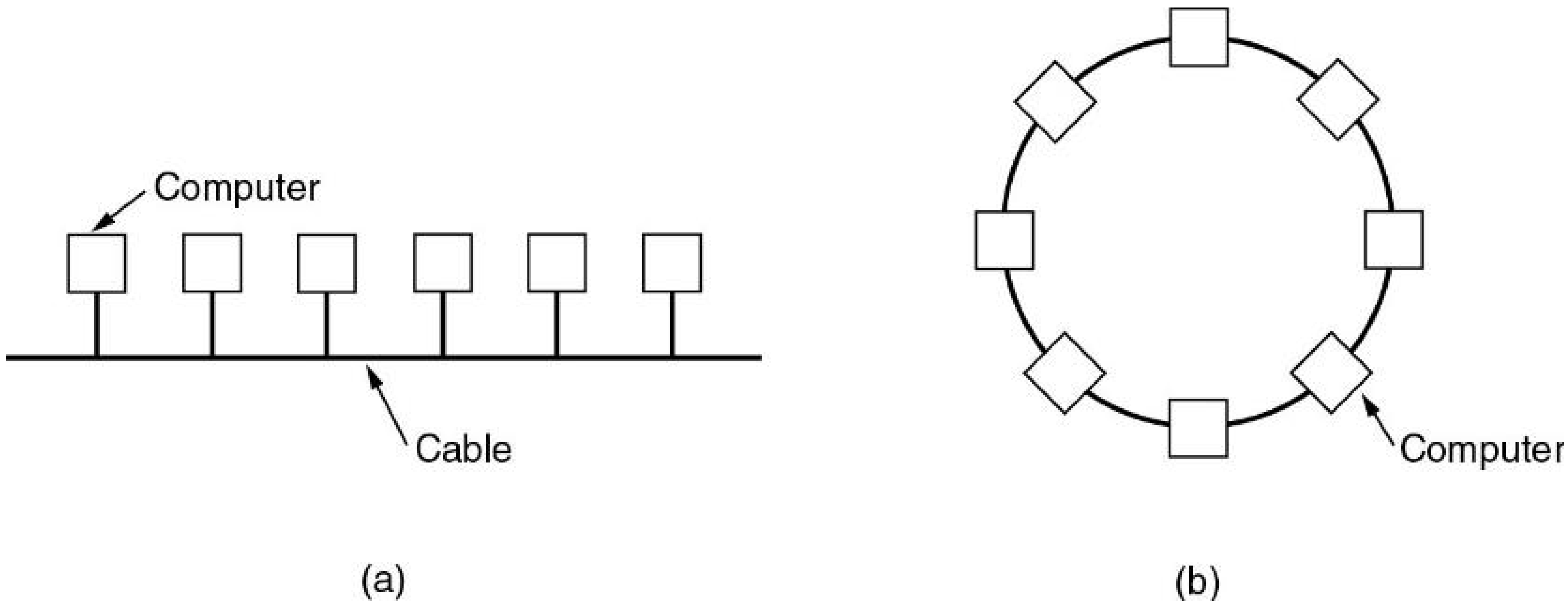
Expand and divide a LAN

- Expand a LAN to make it larger
  - Switches can be plugged into each other using their ports
- Divide one larger physical LAN into smaller logical LANs.
  - VLAN(virtual LAN)
    - Each switch port is tagged with a “color”, the switch then forwards packets so that computers attached to the same color ports are separated from the others.

Classic Ethernet

- The original Ethernet design broadcasts all the packets over a single linear cable.
- At most one machine could successfully transmit at a time, and distributed arbitration mechanism was used to resolve conflicts.
  - Computers could transmit whenever the cable was idle
  - If two or more packets collided, each computer just waited a random time and tried later.

Classic LAN Topologies



Two broadcast networks

(a) Bus (IEEE 802.3, Ethernet)

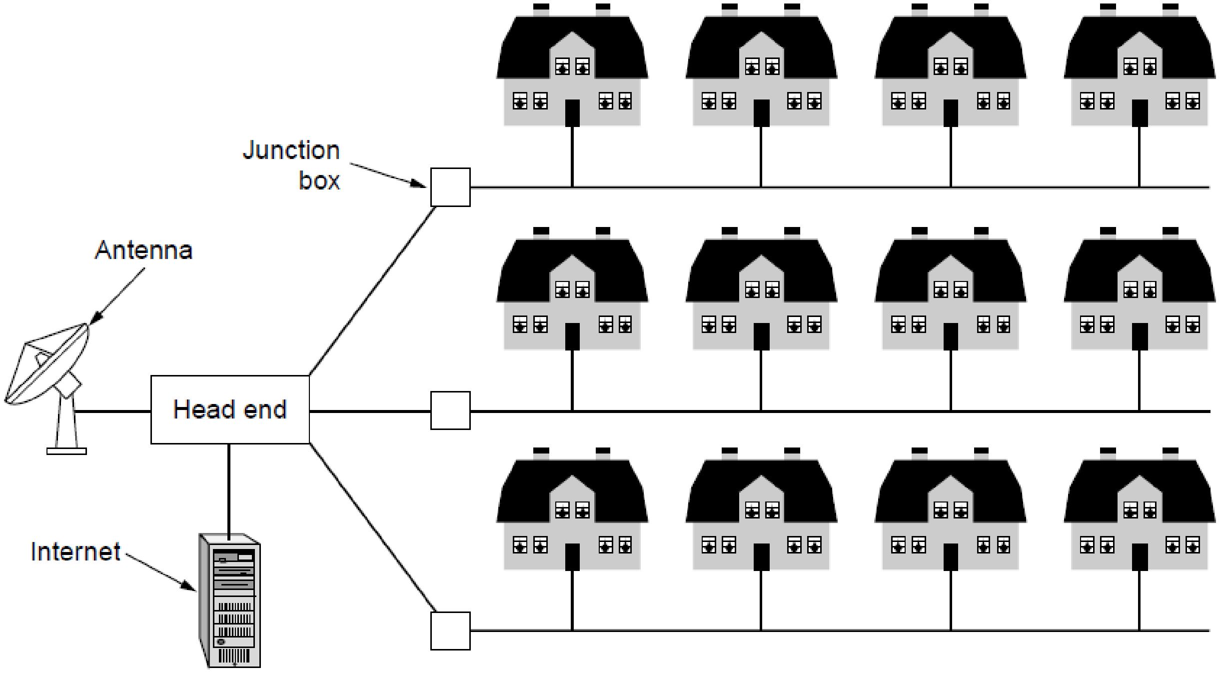
(b) Ring (IEEE 802.5, Token Ring)

Channel Allocation methods for Broadcast networks

- Static allocation
  - Divide time into discrete intervals and use a round-robin algorithm, allowing each machine to broadcast only when its time slot comes up.
  - It wastes channel capacity when a machine has nothing to say during its allocated slot, so most systems attempt to allocate the channel dynamically.
- Dynamic allocation
  - Centralized: there is a single entity which determines who goes next.
  - Decentralized : there is no central entity , each machine must decide for itself whether to transmit.

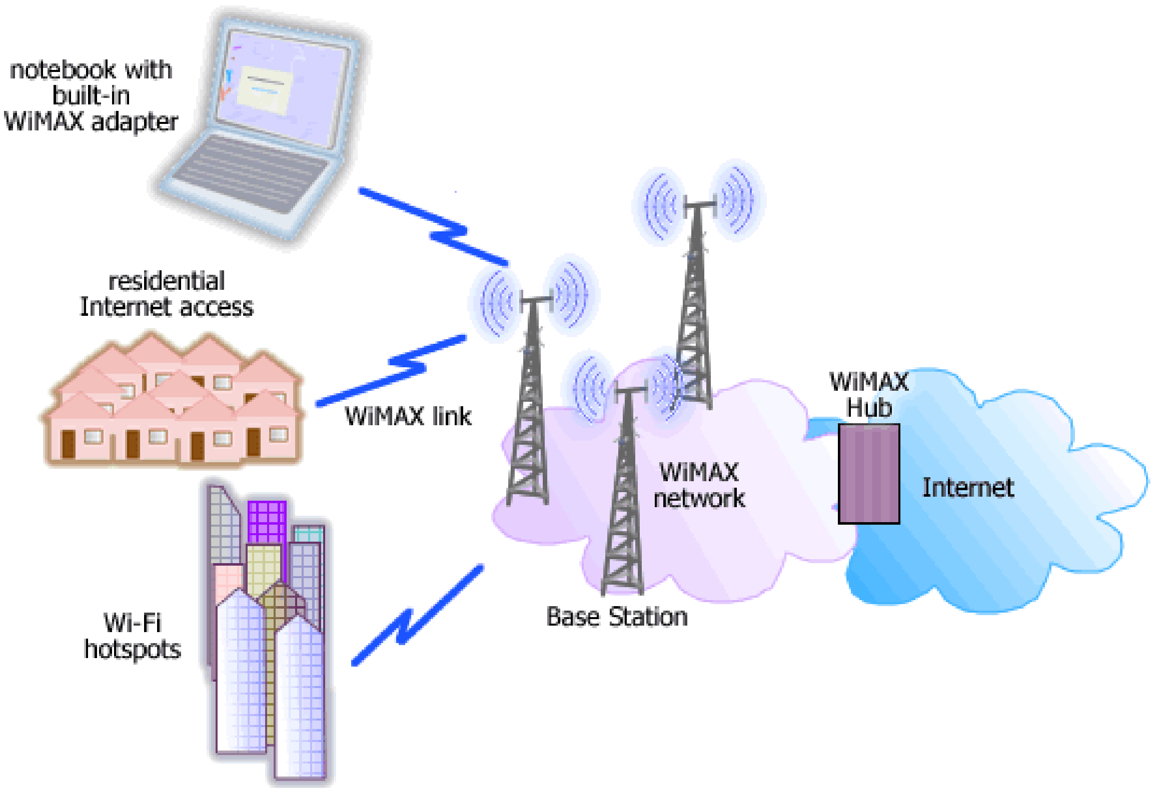
Metropolitan Area Networks

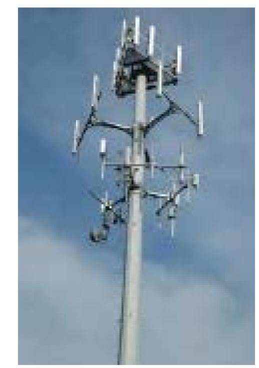
- MAN covers a city



A metropolitan area network based on cable TV.

Wireless MAN

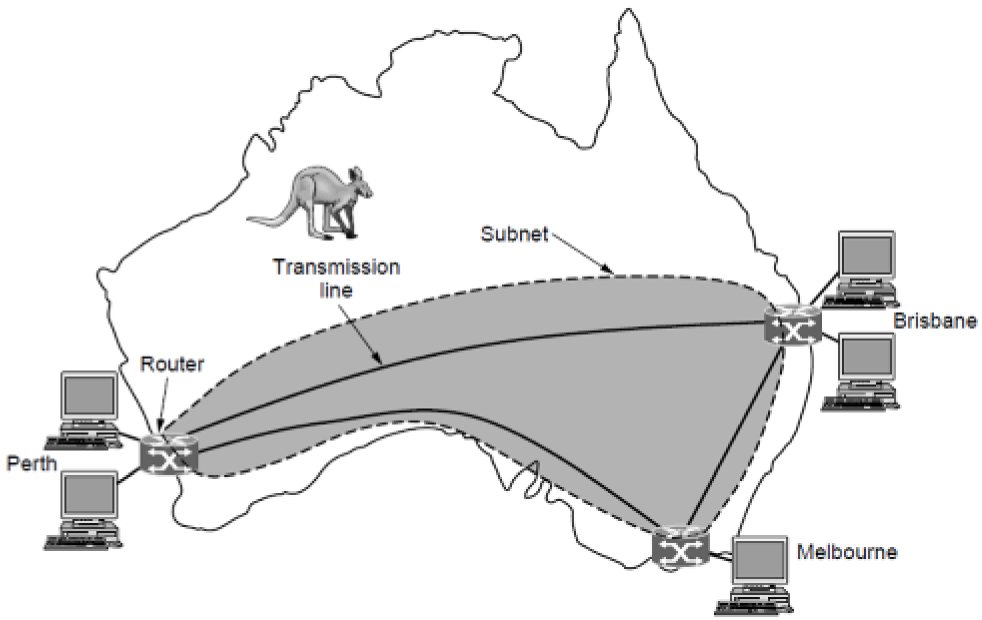




WiMax IEEE 802.16

Wide Area Networks

- A WAN spans a large geographical area, often a country or continent.



WAN that connects three branch offices in Australia

Communication subnet

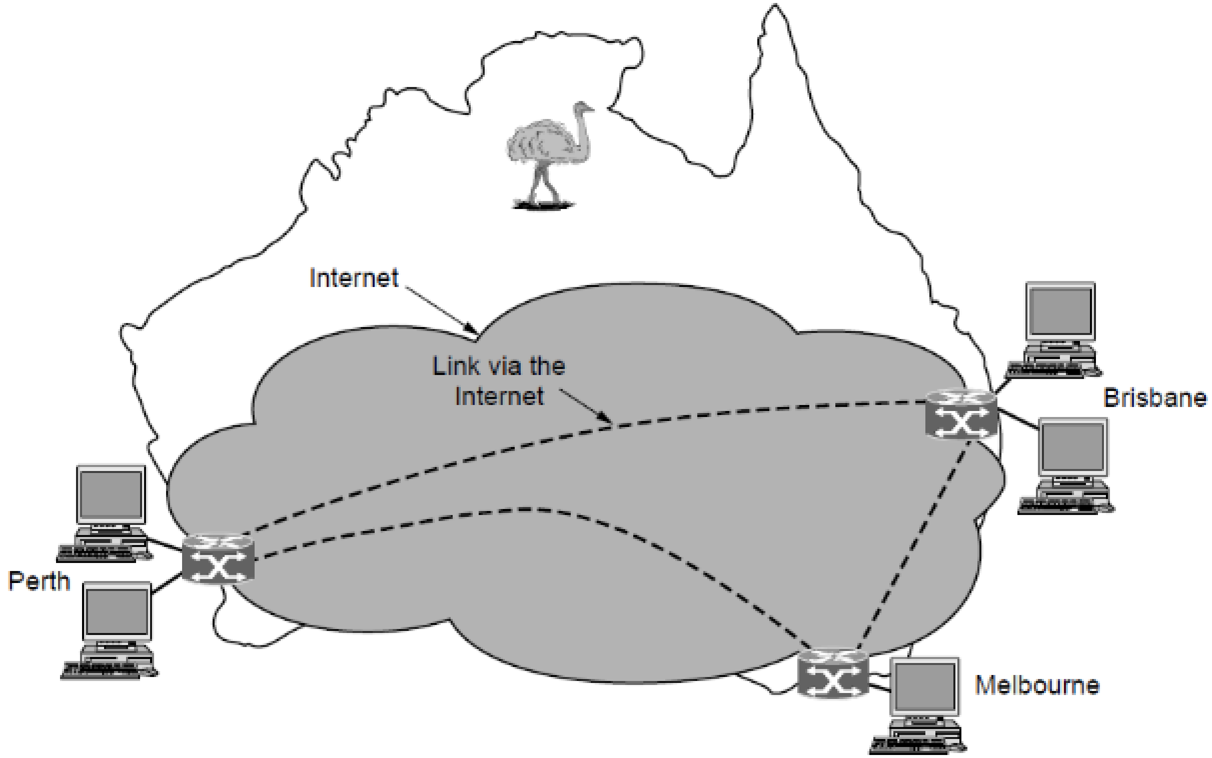
- Transmission lines
  - copper wire, optical fiber, or even radio links.
  - Most companies do not have transmission lines lying about, so instead they lease the lines.
- Switching elements
  - Switches are the specialized computers called routers that connect two or more transmission lines
- Subnet:
  - A collection of routers and communication lines that moved packets from the source host to the destination.

Differences between WAN &LAN

- In WAN, the hosts and subnet are owned and operated by different people
- The routers will usually connect different kinds of networking technology.
- What is connected to the subnet:
  - Individual computers
  - Could be entire LANs
    - This is how larger networks are built from smaller ones

WAN via the Internet

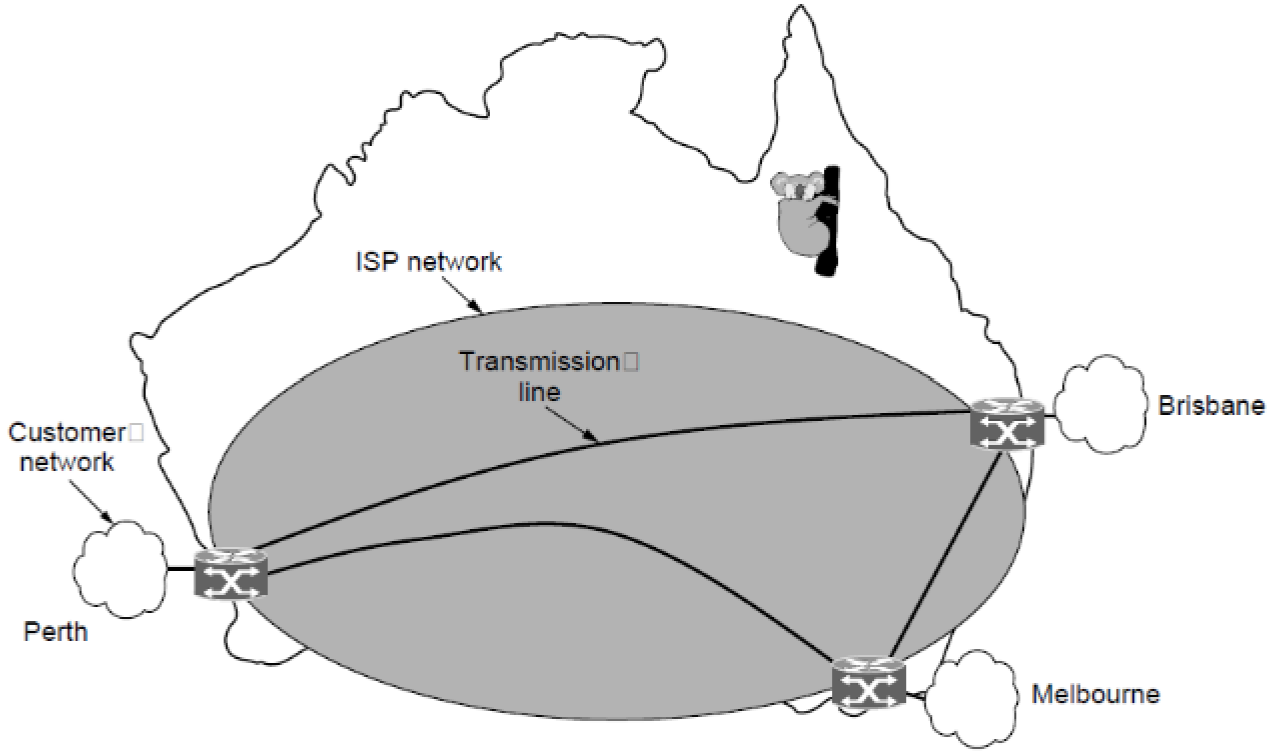
- VPN: flexible but lack control



WAN using a virtual private network.

WAN via ISP network

- The subnet is run by Internet Service Provider



WAN using an ISP network.

WAN Terms

- Packet / Cell
  - the message is cut into packets before sending
- Packet-switched / store-and-forward
  - the packet is received at each intermediate router in its entirety, stored there until the required output line is free, and then forwarded.
- Routing algorithm
  - There may be many paths in the network that connect two computers. How the network makes the decision as to which path to use is called the routing algorithm.

Internet

- Internetworks:
  - Collection of interconnected networks.
  - internet (lower case i) is generic term.
  - Internet (upper case I) is worldwide connection to all kinds of machines.

1.3 Network Software

- Protocol Hierarchies
- Design Issues for the Layers
- Connection-Oriented and Connectionless Services
- Service Primitives
- The Relationship of Services to Protocols

Philosophy of Protocol Hierarchies

- Layering:
  - To reduce their design complexity, most networks are organized as a stack of layers or levels, each one built upon the one below it.
- Services:
  - The purpose of each layer is to offer certain service to the higher layer, shielding those layers from the details of how the offered services are actually implemented.

Layer n Protocol

- Layer n on one machine carries on a conversation with layer n on another machine. The rules and conventions used in this conversation are collectively known as the **layer n protocol**.
- A protocol is an agreement between communicating parties on how communication is to proceed.

What Is A Protocol

- **Human protocols:**
- "what's the time?"
- "How are you doing?"
- "I have a question"

- Specific messages sent
- Specific actions taken when messages received, or other events

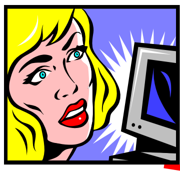
Network protocols:

- Machines rather than humans
- All communication activity in Internet governed by protocols

•Protocols define format, order of messages sent and received among network entities, and actions taken on message transmission and receipt.

Protocol Example

- Human



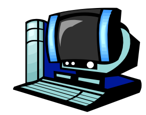
“Hello”

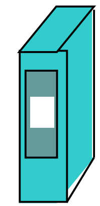
“Hello”

“Got the time?”

“It’s 10:30”

Network





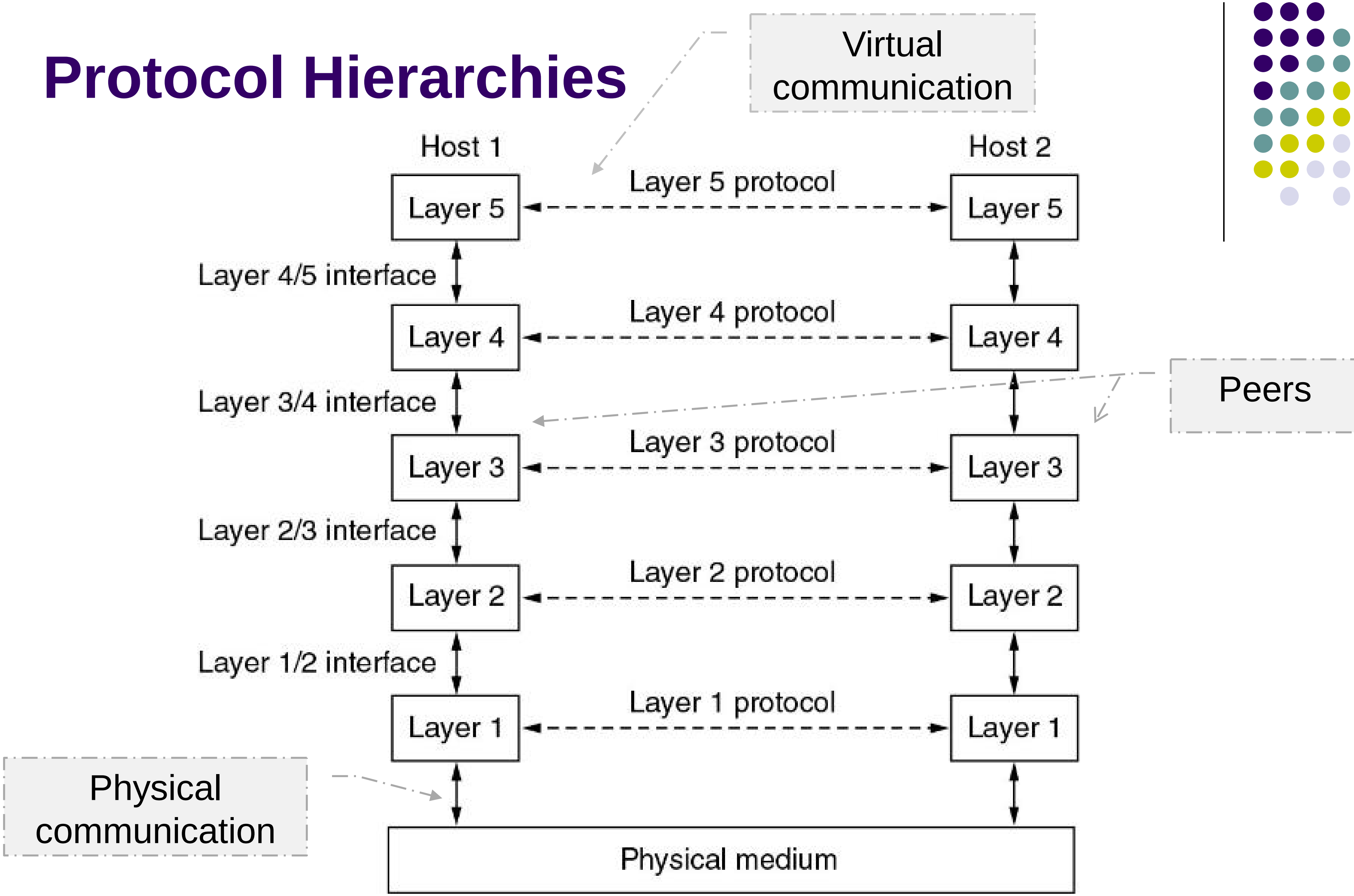
TCP connection request

TCP connection reply

HTTP request

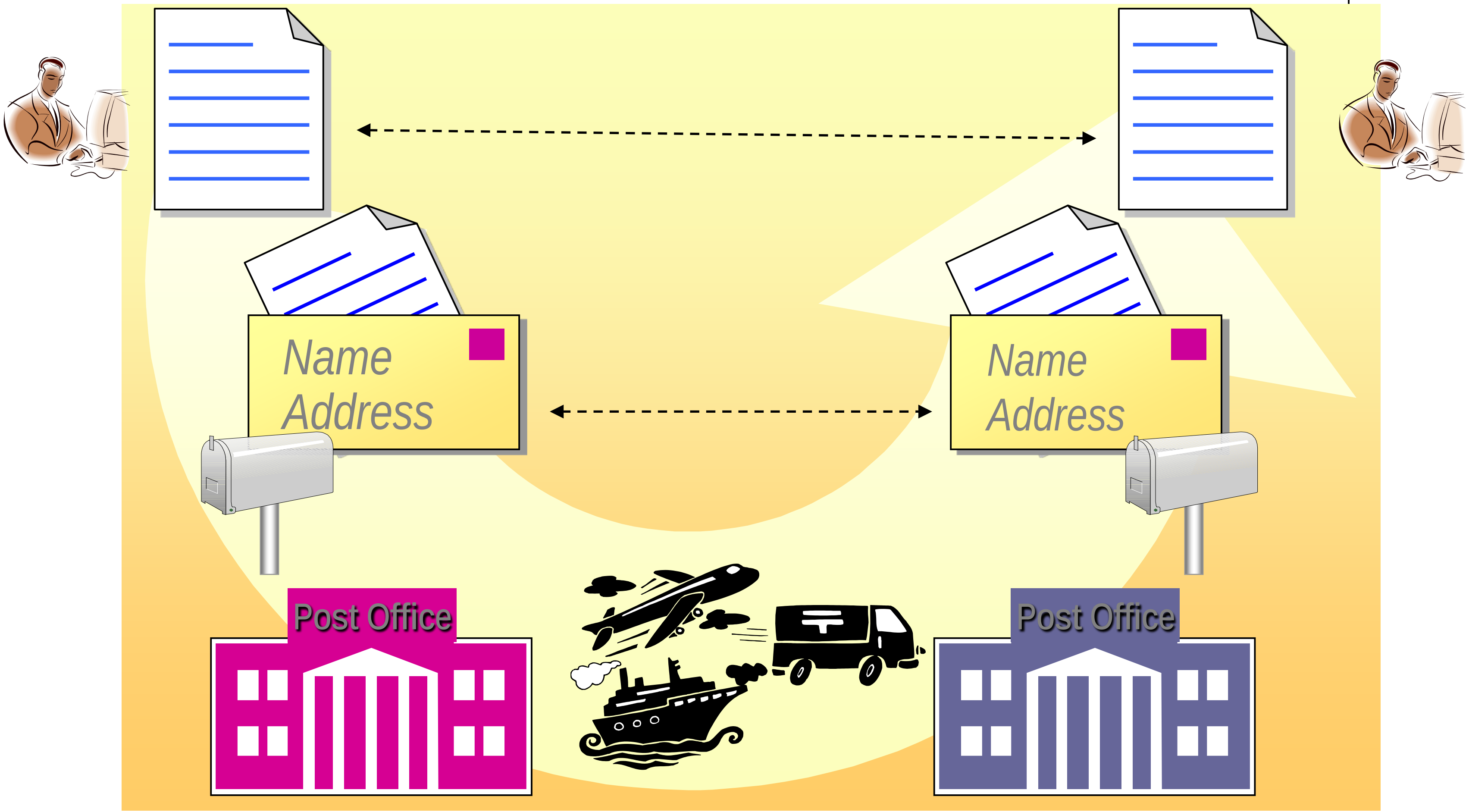
HTTP response

Protocol Hierarchies



Layers, protocols, and interfaces.

Hierarchy Example



Terminology

- **Peers**

  The entities comprising the corresponding layers on different machines are called peers. The peers may be processes, hardware devices, or even human beings. In other words, it is the peers that communicate by using the protocol.

- **Interface**:

  Between each pair of adjacent layers is an interface. The interface defines which primitive operations and services the lower layer makes available to the upper one.

KISS principle

- **"Keep It Simple, Stupid",**
  - Important to keep it **simple** and **clean** to reduce complexity.
    - How many layers?
    - Clean interfaces
  - Important that each layer perform a specific collection of well-understood functions.

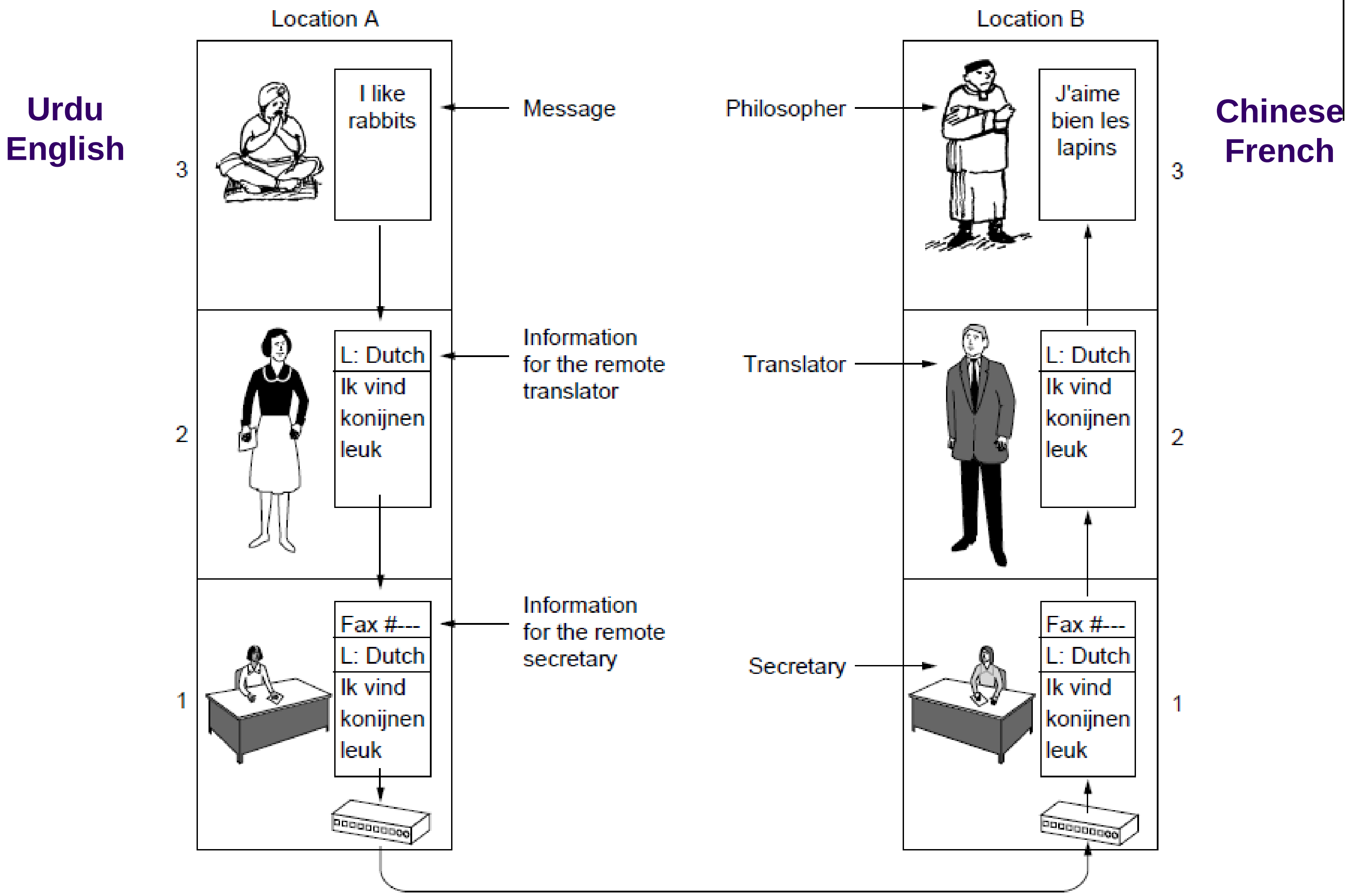
Network architecture

- Network architecture: A set of layers and protocols.
  - The spec must contain enough information to allow an implementer to write the program or build the hardware for each layer so that it will correctly obey the appropriate protocol.
  - Functional interfaces and implementation details are not part of the spec, since that's not visible outside the machine.
  - It is not even necessary that the interfaces on all machines in a network be the same, provided that each machine can correctly use all the protocols.

Protocol stack

- **Protocol stack:**
  - A list of protocols used by a system, one protocol per layer, is called a protocol stack.
- Network architectures, protocol stacks, and the protocols themselves are the principal subjects of this course

Analogy of Protocol Hierarchies



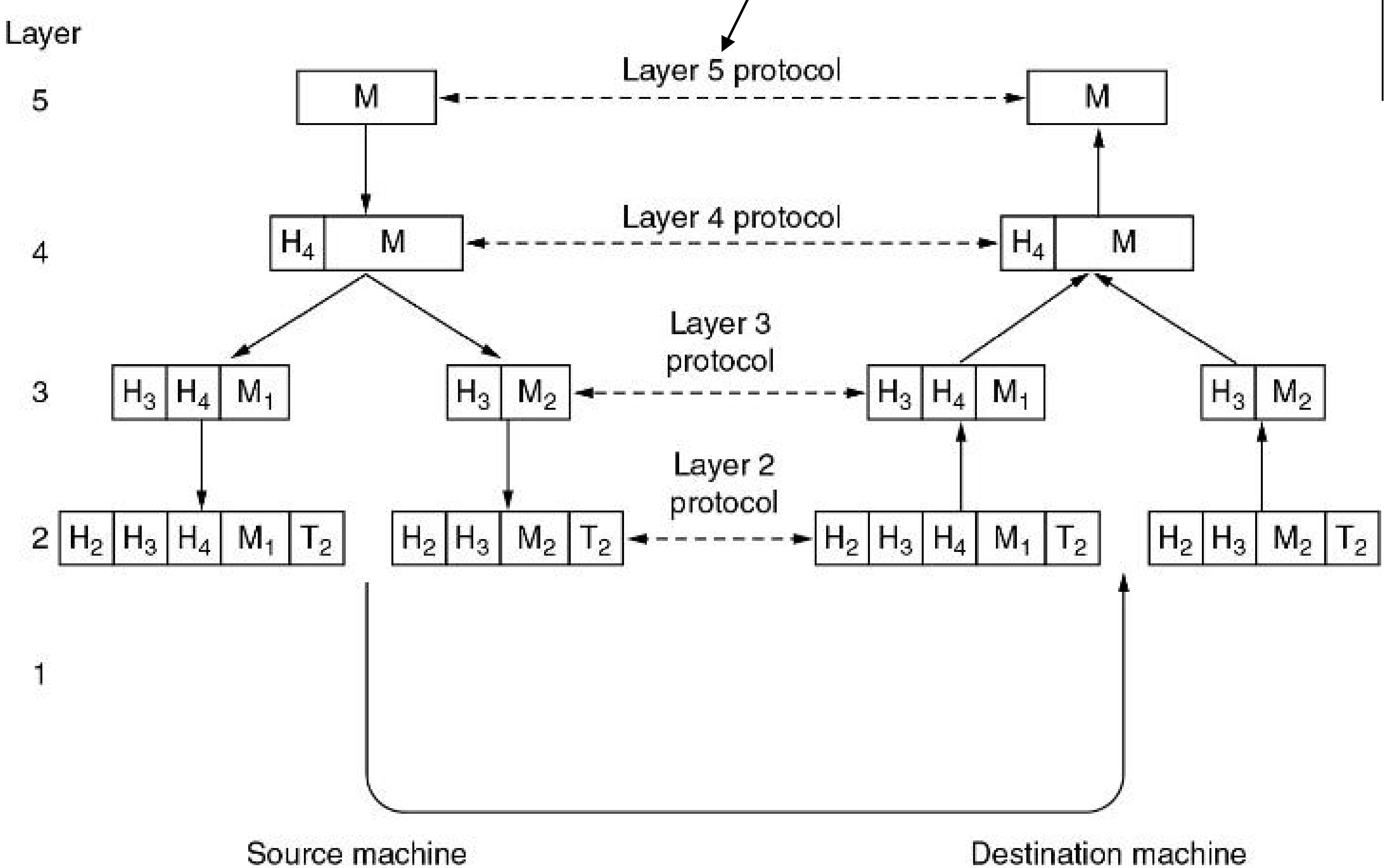
The philosopher-translator-secretary architecture.

Virtual Communication: Sino-US Talk

Xi Jinping meets with Barack Obama.

Information flow

“Horizontal”



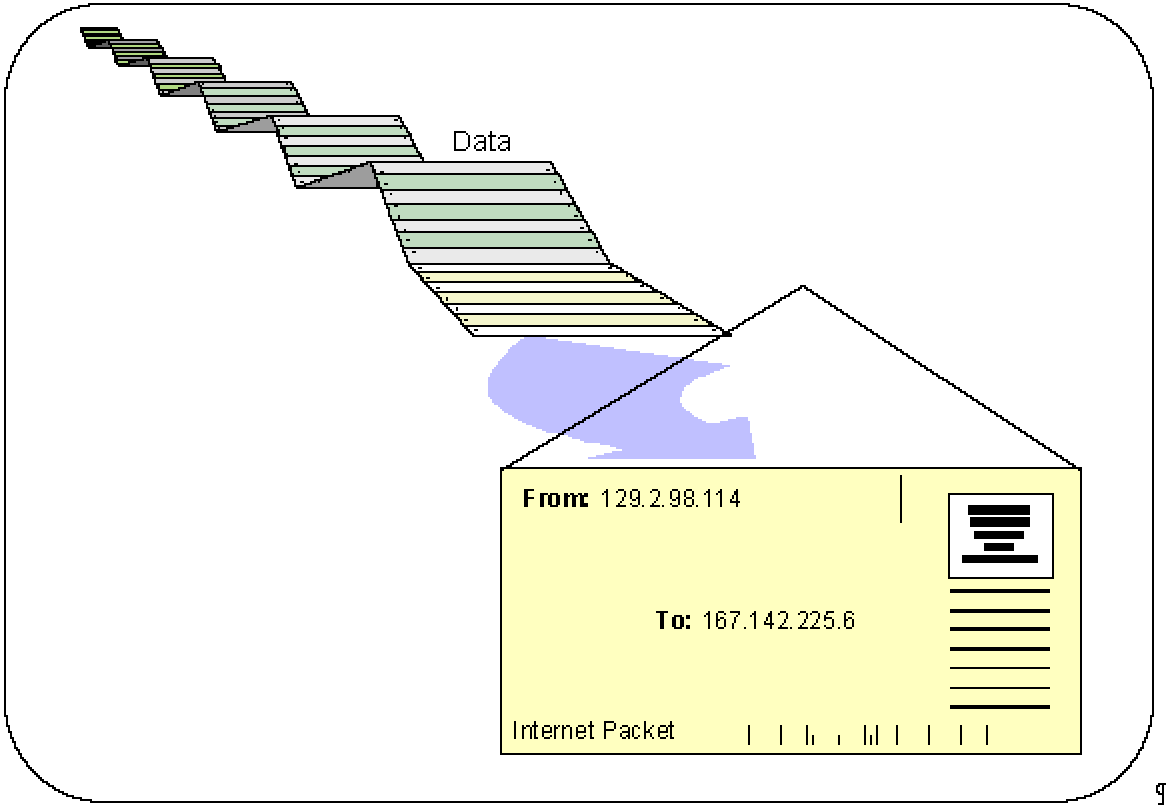
Example information flow supporting virtual communication in layer 5.

Layer4 thinks "SendtoPeer" rather than “CallNextLayerDown".

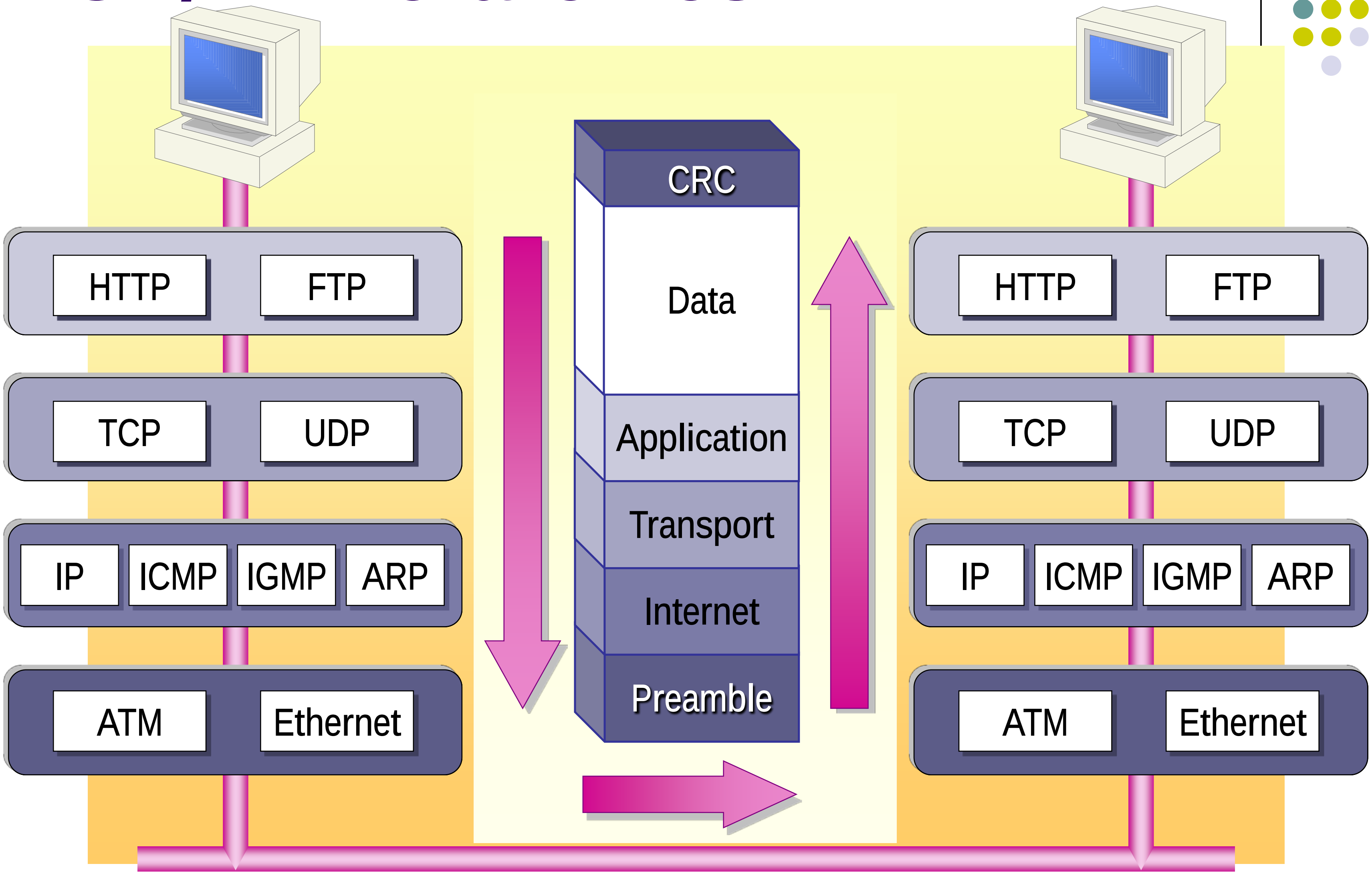
Terminology

- **Header:**
  - Upper layer puts a header in front of the message to identify the message and passes the result to lower layer
  - The header includes control information such as sequence numbers to keep the right order.
- **Size of messages**
  - There is always a limit to the size of messages imposed by certain layer protocol. So incoming messages must be broken into smaller units (packets) in this layer.

An Internet Envelope



TCP/IP Hierarchies



Software or hardware?

- Although this section is called '‘network software”, it is worth pointing out that the lower layers of a protocol hierarchy are frequently implemented in hardware or firmware. Nevertheless, complex protocol algorithms are involved, even if they are embedded (in whole or in part) in hardware.

Design Issues for the Layers

- Reliability
- Network Evolution
- Resource Location
- Against Threats

Reliability

- Reliability: Making a network that operates correctly even though it is made up of a collection of components that are themselves unreliable.
- Mechanisms:
  - Error detection
    - Find errors in received information.
  - Error correction
    - Fix errors in received information.
  - Routing
    - Find a working path through a network.

Network Evolution issue

- Protocol Layering
  - Support change
- Addressing or Naming
  - Every layer needs a mechanism for identifying senders and receivers.
- Internetworking
  - Different network technologies often have different limitations.
- Scalable
  - Design work well when the network gets large

Resource Location

- Networks provide a service to hosts from their underlying resource, such as the capacity of transmission lines.
  - Statistical multiplexing
    - Share network bandwidth dynamically
  - Flow control
    - Keep a fast sender from swamping a slow receiver with data.
  - Congestion
    - Network overloading
  - Quality of Service
    - Differential service for real-time delivery and other.

Against Threats

- Confidentiality
  - Against eavesdropping
- Authentication
  - Prevent impersonation
- Integrity
  - Prevent surreptitious changes to messages

Connection-Oriented vs. Connectionless Services

- Layers can offer two different types of service to the layers above them:
  - Connection-oriented
  - Connectionless

Connection-oriented service

- Like the telephone system. The system establishes a connection, uses it, and closes it.
- Acts like a tube(**Circuit**). Data comes out the other end in the same order as it goes in.
  - Connection Setup (negotiation)
  - Data Transfer
  - Connection Termination

Connectionless service

- Like the postal system. Each message carries the full destination address and each one is routed through the intermediate nodes inside the system independent of all the subsequent messages.
- It is possible that the first one sent can be delayed so that the subsequent messages arrive first.
  - Message has a name: a packet in network layer
  - Store-and-forward switching vs. cut-through switching.

Quality of service

- Each service can be characterized by a QoS:
  - Reliability: Will the message arrive?
    - A reliable service is implemented by **ack**nowledgement (a receipt from the receiver).
  - Delay (Latency)
    - Delays and overhead are introduced in the **ack** process

Reliable connection-oriented service

- A reliable connection-oriented service guarantees success. They never lose data.
  - Message sequence - message boundaries and order are maintained.
  - Byte streams - messages are broken up or combined; flow is bytes. Can pair mechanism with upper-layer requirements.
- A typical situation in which a reliable connection-oriented service is appropriate is file transfer.

Unreliable Connectionless Service

- **Connectionless Service /Datagram Service:**
  - For some applications, the transit delay introduced by acks are unacceptable. Like Voice Over IP.
  - Not all applications require connections. Like junk mail. It's not worth the cost to determine if it actually arrived. Needs a high probability of arrival, but 100% not required. Connectionless, no acknowledgment.
- **Acknowledged datagram service:**
  - As above, but improved reliability via acknowledgment.
- **Request-reply service:**
  - Acknowledgment is in the form of a reply.

Connection-Oriented and Connectionless Services

	Service	Example
Connection-oriented	Reliable message stream	Sequence of pages
	Reliable byte stream	Movie download
	Unreliable connection	Voice over IP
Connection-less	Unreliable datagram	Electronic junk mail□
	Acknowledged datagram	Text messaging
	Request-reply	Database query

Six different types of service.

Service Primitives

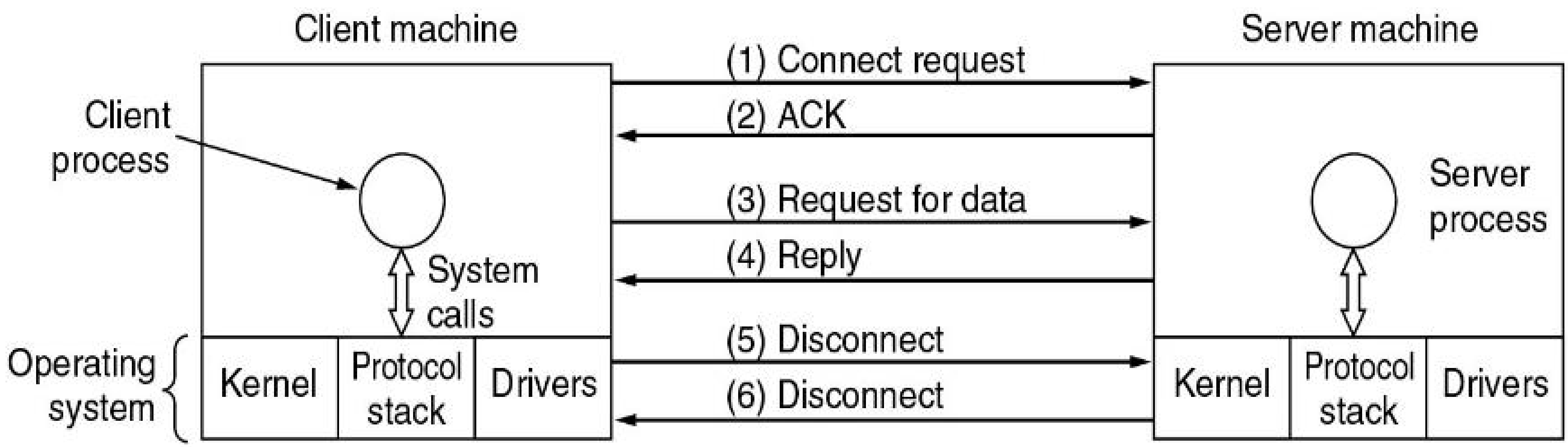
- A **service** is formally specified by a set of primitives (operations) available to a user process to access the service.
  - These primitives tell the service to perform some action or report on an action taken by a peer entity.
  - If the protocol stack is located in the operating system, as it often is, the primitives are normally system calls

Service Primitives

Primitive	Meaning
LISTEN	Block waiting for an incoming connection
CONNECT	Establish a connection with a waiting peer
RECEIVE	Block waiting for an incoming message
SEND	Send a message to the peer
DISCONNECT	Terminate a connection

Five service primitives for implementing a simple connection-oriented service.

Service Primitives

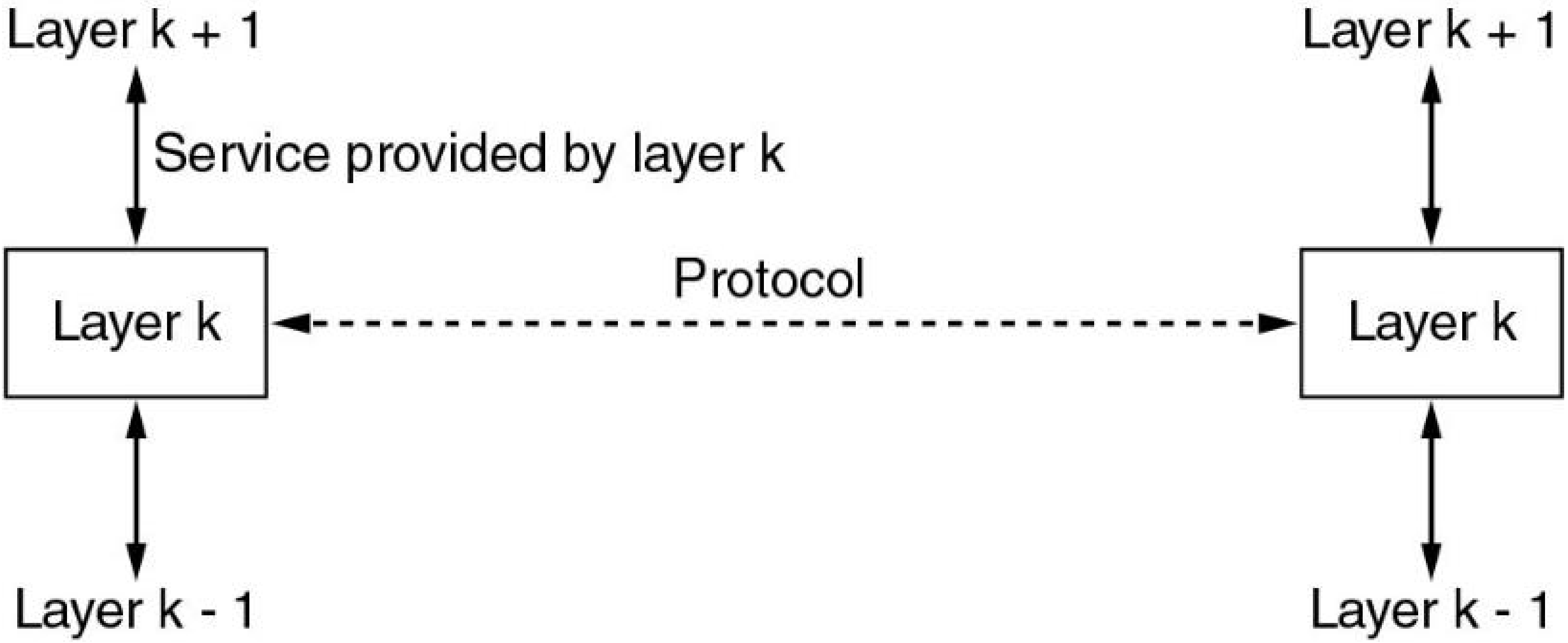


Packets sent in a simple client-server interaction on a connection-oriented network.(but life is not so simple)

Services to Protocols Relationship

- A service is a set of primitives (operations) that a layer provides to the layer above it. The service defines what operations the layer is prepared to perform on behalf of its users, but it says nothing at all about how these operations are implemented.
- A protocol, in contrast, is a set of rules governing the format and meaning of the packets, or messages that are exchanged by the peer entities within a layer. Entities use protocols to implement their service definitions.

Layer K: a service and a protocol.



In other words, services relate to the interfaces between layers. In contrast, protocols relate to the packets sent between peer entities on different machines.

1.4 Reference Models

- The OSI Reference Model
- The TCP/IP Reference Model
- The Model used in this course
- A Comparison of the OSI and TCP/IP
- A Critique of the OSI Model and Protocols
- A Critique of the TCP/IP Reference Model

OSI vs. TCP/IP reference model

- The protocols associated with the ***OSI(Open System Interconnect) model*** are rarely used any more, the model itself is actually quite general and still valid, and the features discussed at each layer are still very important.
- The ***TCP/IP model*** has the opposite properties: the model itself is not of much use but the protocols are widely used.

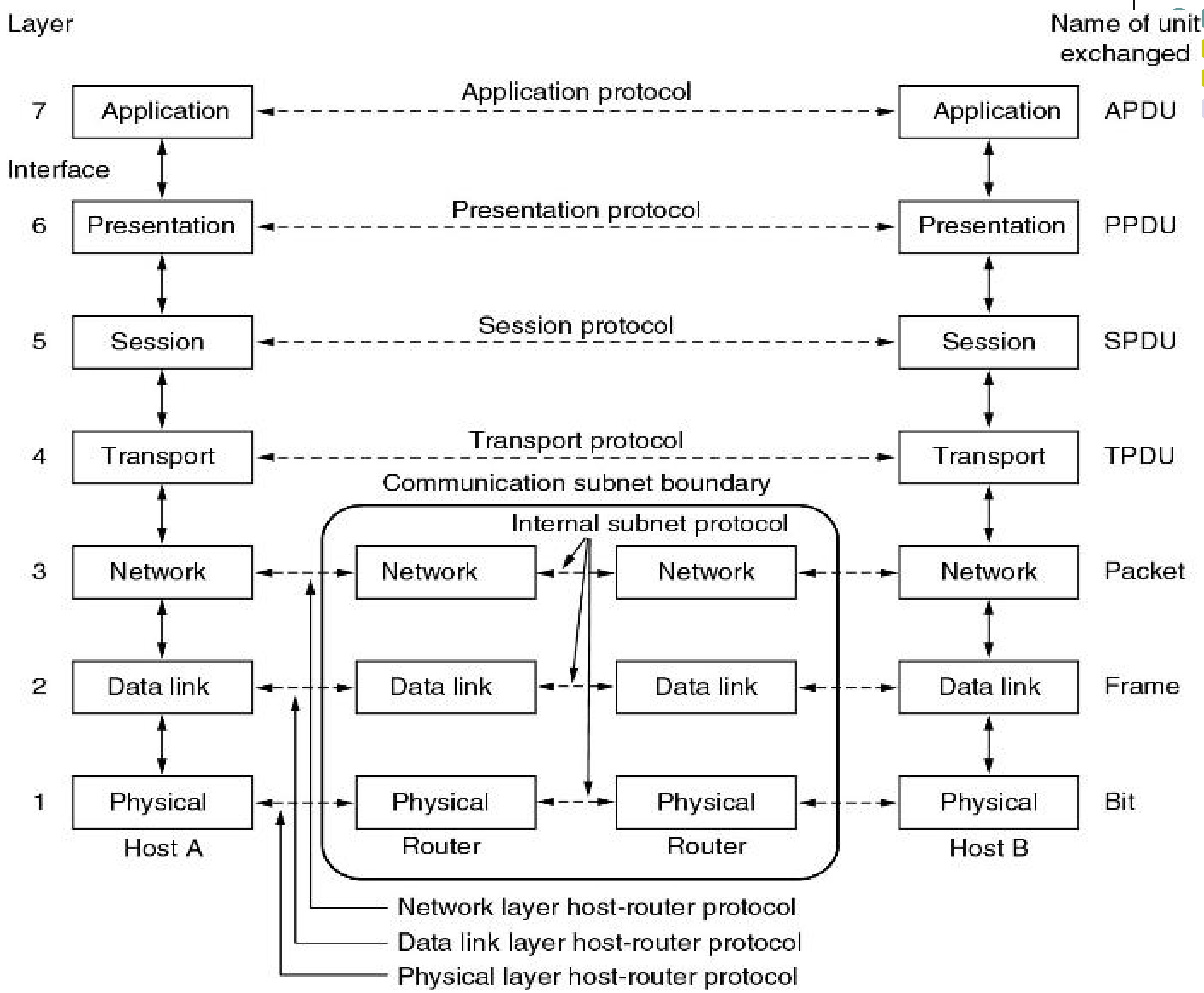
The OSI Reference Model

Developed by **ISO**: International Standards Organization
(1983,revised in 1995)

Principles used to develop OSI Layering:

1. Need a layer for each different level of abstraction.
2. Each layer performs a well defined function.
3. Each layer should be standardizable.
4. Layer boundaries should minimize data flow across those boundaries.
5. The right number of layers - don't put too many functions together, but not too many layers either.

The OSI Reference Model



The OSI reference model.

1983,1995

Physical Layer

- **Purpose**
  - Transmits raw bits across a medium.
- **Concerns are**
  - Voltage: how many volts for 1 / 0
  - Timing: how many ns a bit lasts
  - Duplexing: transmission in both directions?
  - Connectors: how many pins? What is each pin?
  - etc.

Data Link Layer

- **Purpose:**
  - Transform a raw transmission line into a line that appears free of undetected transmission errors to the networks layer
- **Concerns:**
  - **Framing** - Breaks apart input data into frames and transmit the frames sequentially.
  - **Error handling** – if the service is reliable, the receiver confirms correct receipt of each frame by sending back an **acknowledgement** frame.
  - **Flow control** - keeps a fast transmitter from drowning a slow receiver in data.
  - **Medium Access Control** – how to control access to the shared channel for broadcast networks.

Network Layer

- **Purpose**
  - Route packets from source to destination
- **Concerns**
  - **Routing** - What path is followed by packets from source to destination. Can be based on a static table, can be determined when the connection is created, or can be highly dynamic, being determined anew for each packet, to reflect the current network load.
  - **Congestion** - Controls the number packets in the subnet.
  - **Qos –** Quality of service provided(delay, transit time, jitter…)
  - **Heterogeneity** - Interfacing so one type of network can talk to another. Addressing, packet size, protocols...

Transport Layer

- Purpose
  - Accept data from above it, split it up into smaller units if need be, pass them to network layer, and ensure that the pieces all arrive correctly at the other end.
- Concerns
  - **Service Decisions** - What type of service to provide; error-free point to point, datagram, etc.
  - **End-to-end**: it carries data all the way from the source to the destination.
  - **Reliability** - Ensures that packets arrive at their destination. Reassembles out of order messages.
  - **Hides network** - Allows details of the network to be hidden from higher level layers.
  - **Mapping** - Determines which messages belong to which connections.
  - **Flow control** - keeps a fast transmitter from flooding a slow receiver.

Session Layer

- Purpose
  - Allow users on different machines to establish sessions between them
- Concerns
  - **Dialog control** - keep track of whose turn it is to transmit
  - **Token Management** – prevent two parties from attempting the same critical operation at the same time
  - **Synchronization** – checkpointing long transmissions to allow them to pick up from where they left off in the event of a crash and subsequent recovery.

Presentation Layer

- Purpose
  - Make it possible for computers with different data representations to communicate
- Concerns
  - Syntax and semantics of information transmitted.
  - Understands the nature of the data being transmitted. Converts ASCII/EBCDIC, big endian/little endian

Application Layer

- contains a variety of protocols that are commonly needed by users.
  - **HTTP**
  - **FTP**
  - **SMTP**
  - **…**

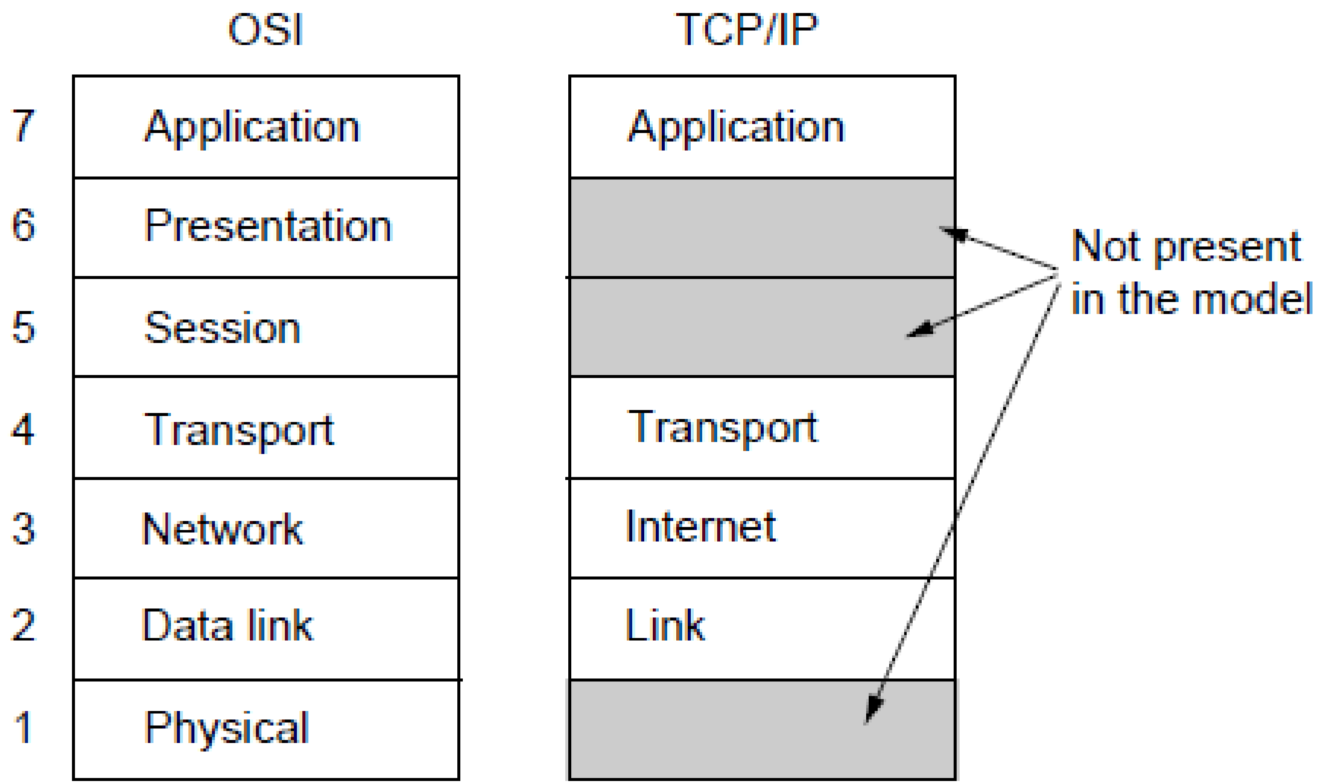
The TCP/IP Reference Models

- Link layer
- Internet layer
- Transport layer
- Application layer

U.S. DoD ARPANET

- Was a research network sponsored by the DoD
- Network be able to survive loss of subnet hardware, with existing conversations not being broken off .
- A flexible architecture was needed since applications with divergent requirements were envisioned, ranging from transferring files to real-time speech transmission

The TCP/IP Reference Models



The TCP/IP reference model

(Cerf & Kahn1974, Clark 1988)

The Key

a ***packet-switching*** network based on a ***connectionless layer*** that runs across different networks.

Link Layer

- Describes what link such as serial lines and classic Ethernet must do to meet the needs of the connectionless internet layer.
- It is not really a layer at all, in the normal sense of the term, but rather an ***interface*** between hosts and transmission links.

The Internet Layer

- Permit hosts to inject packets into any network and have them travel independently to the destination (potentially on a different network, like international mail)
- Routing and Congestion control
  - **IP (Internet Protocol)**
  - ICMP(Internet Control Message Protocol)

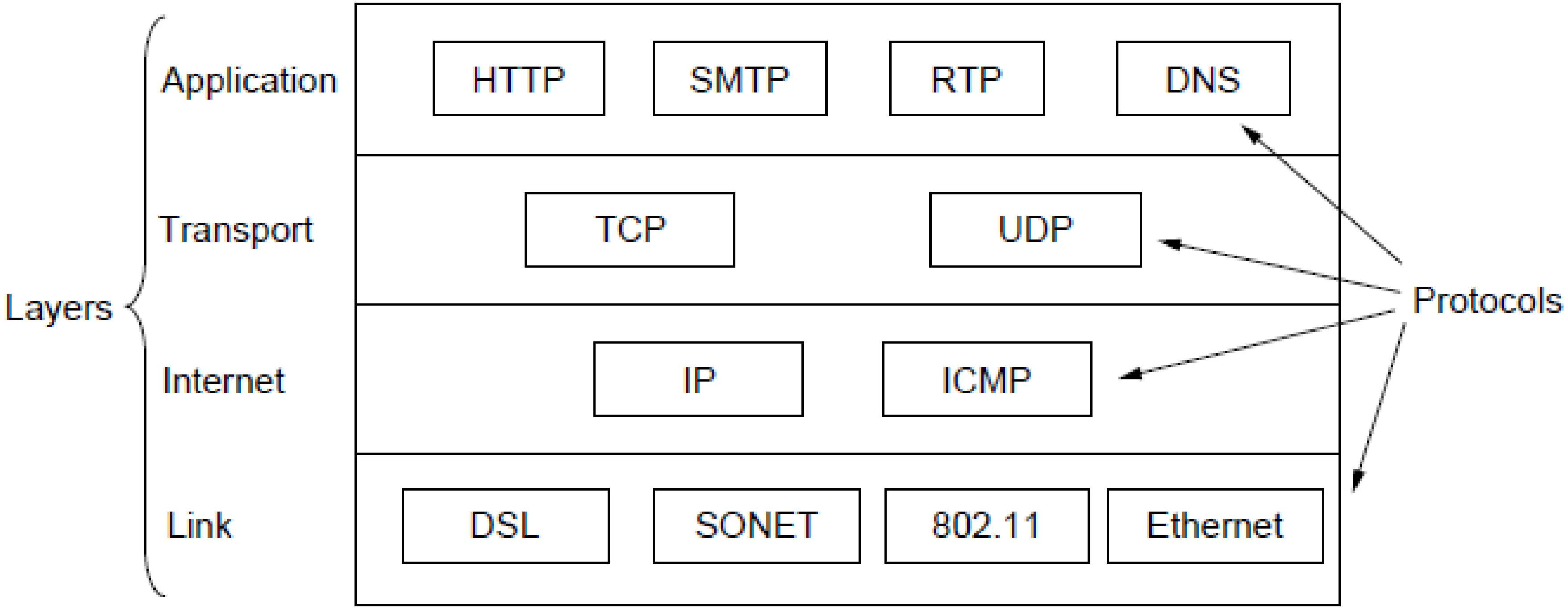
Transport Layer

- End2End: Allows peer entities to communicate.
  - **TCP** - Transmission Control Protocol provides a reliable connection oriented protocol that delivers a byte stream from one node to another. Guarantees delivery and provides flow control.
  - **UDP** - User Datagram Protocol provides an unreliable connection-less protocol for applications that provide their own.

Application Layer

- Terminal - Telnet
- File transfer – FTP
- The Web - HTTP
- …

The TCP/IP Reference Models



The TCP/IP reference model with some protocols we will study

The model used in this course

5	Application
4	Transport
3	Network
2	Link
1	Physical

The reference model used in this course.

Comparing OSI and TCP/IP Models

- Concepts central to the OSI model
  - Services
  - Interfaces
  - Protocols
- OSI has good definition of service, interface, and protocol as discussed before.   Fits well with object oriented programming concepts. Protocols are better hidden.

Comparing OSI and TCP/IP Models

- The TCP/IP model did not originally distinguish between service, interface, and protocol.
- With TCP/IP, the protocols came first; model was just a description of the protocols. But then the model isn't good for any other protocols.

Different philosophy

- Which is first?

Reference Model

vs

Corresponding protocols

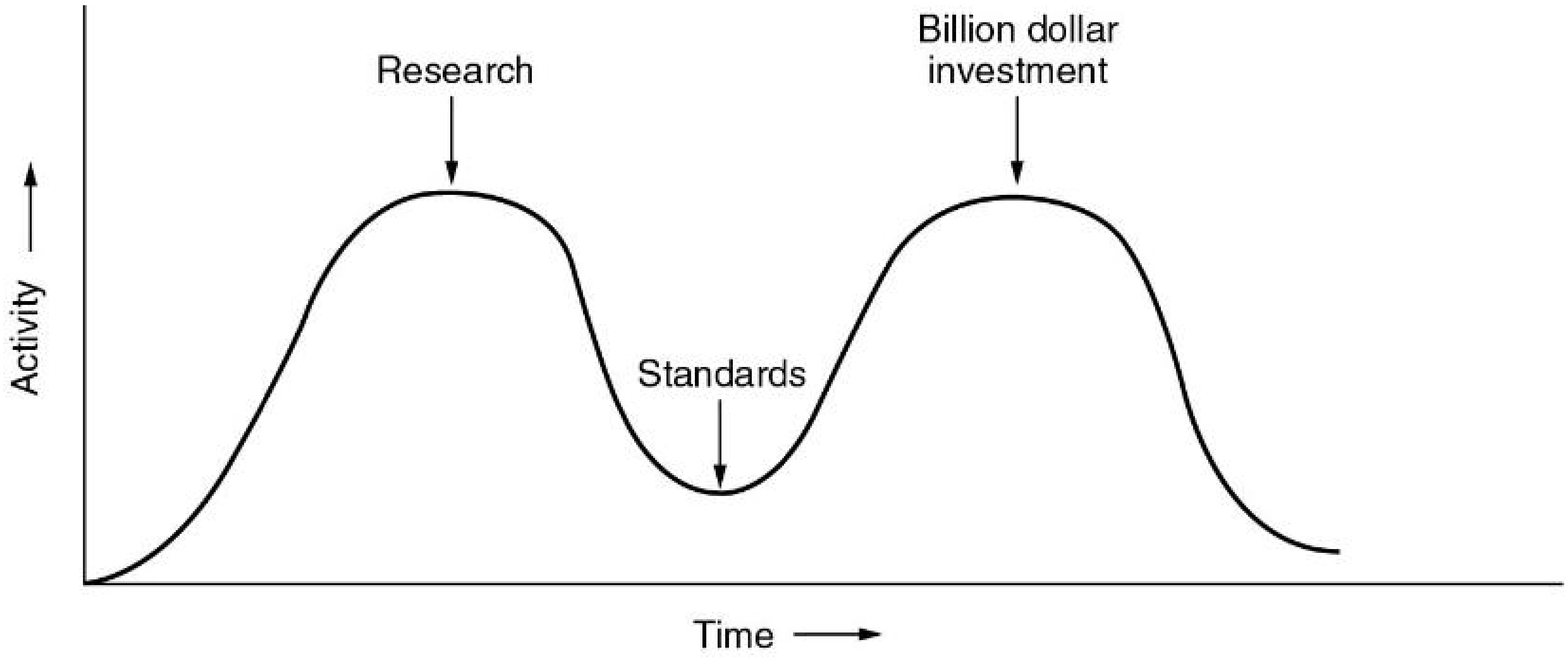
Specific differences

- Number of layers: 7 vs. 4
- Connectionless vs. connection-oriented
  - OSI supports both in the network layer, but only Connection-oriented communication in the transport layer
  - TCP/IP supports only connectionless mode in the network layer but supports both in the transport layer, giving the users a choice.

A Critique of the OSI Model and Protocols

- Why OSI did not take over the world
  - Bad timing
  - Bad technology
    - Flawed, too complex
    - More political than technical of 7 layers decision
  - Bad implementations
    - Huge, unwieldy, Poor quality
  - Bad politics
    - Academia vs Bureaucrats

Bad Timing



The apocalypse of the two elephants.

A Critique of the TCP/IP Reference Model

- Service, interface, and protocol not distinguished
- Not a general model
- Link “layer” not really a layer
- No mention of physical and data link layers
- Minor protocols deeply entrenched, hard to replace

1.5 Example Networks

- The Internet
- 3G Mobile Phone Networks
- Wireless LANs: 802.11
- RFID and Sensor networks

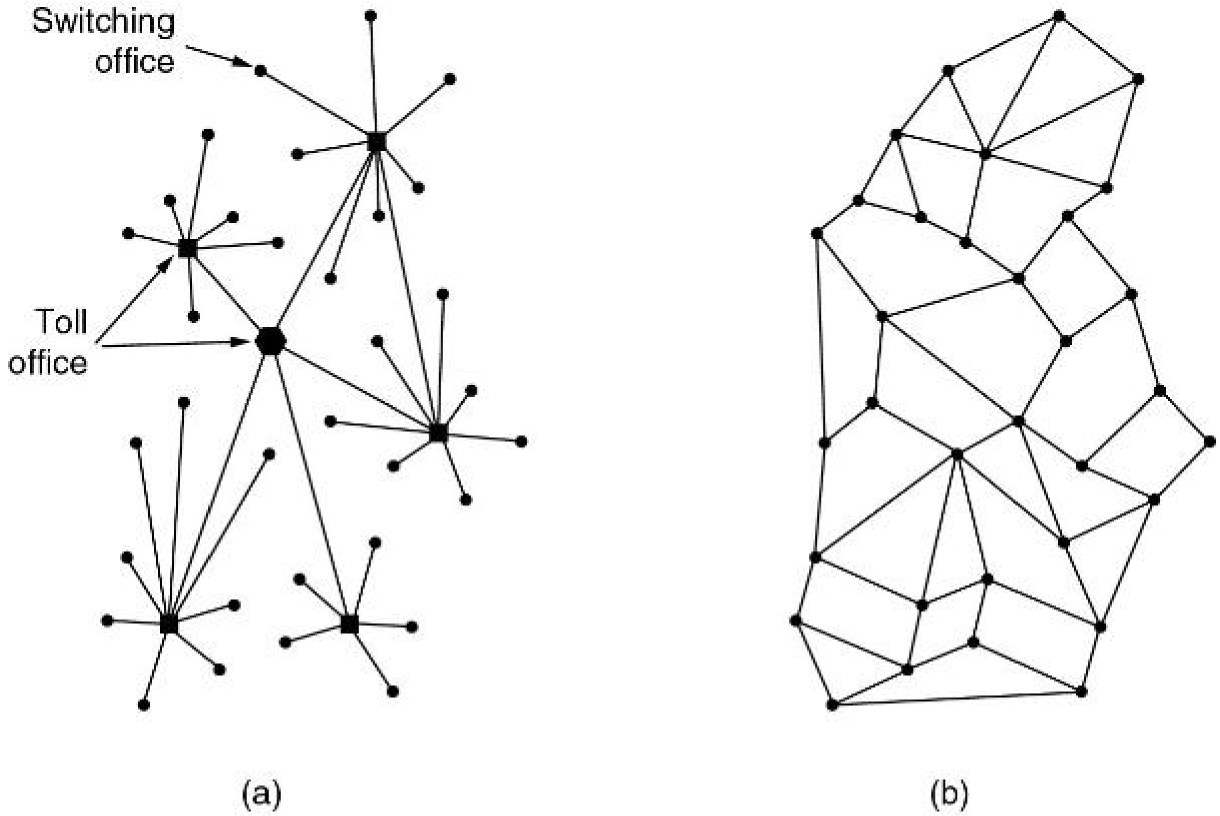
The history

- The story begins in the late 1950s. At the height of the Cold War, the DoD wanted a command-and-control network that could survive a nuclear war.
- **This leads to the ARPANET:**

  1968 Originally intended as reliable network, with multiple routing. Used TCP/IP precursor, which got built into early UNIX.

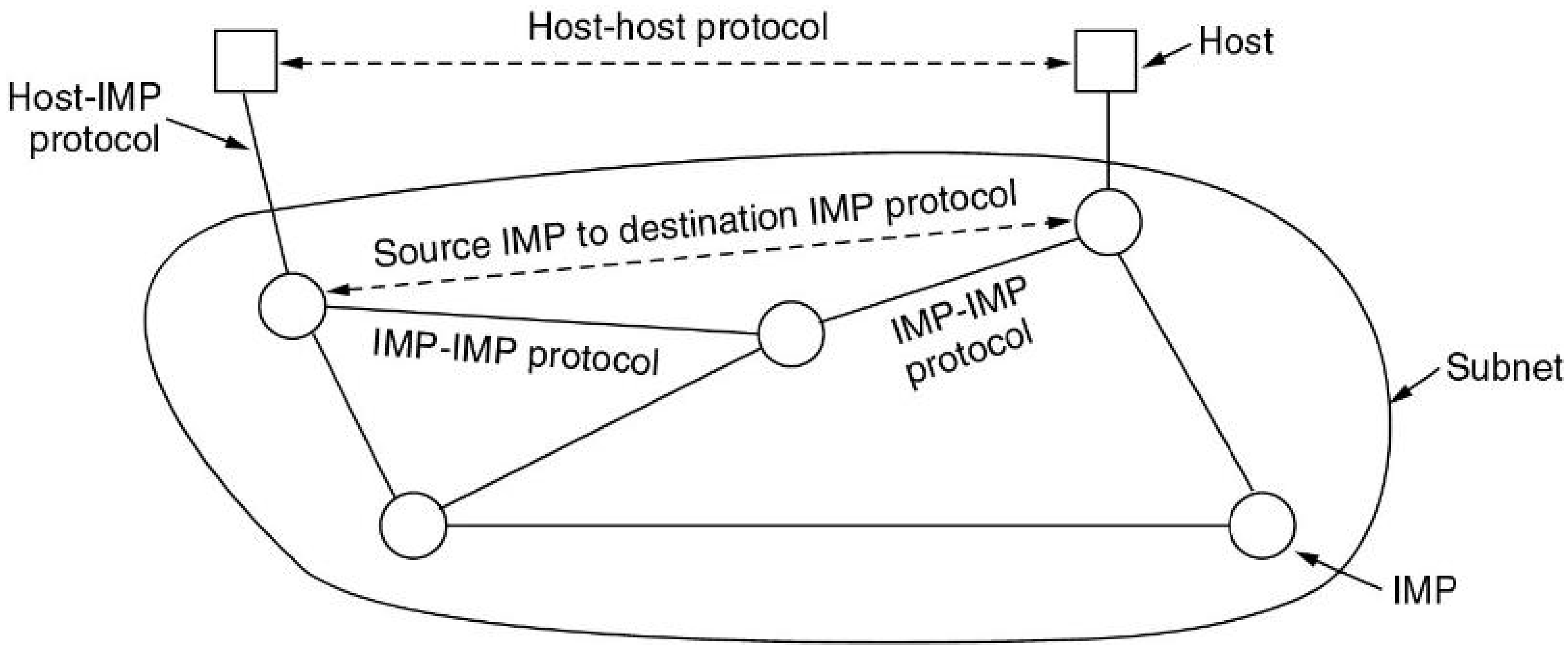
(ARPA, the Advanced Research Projects Agency)

The ARPANET



(a) Structure of the telephone system.
(b) Baran's proposed distributed switching system.

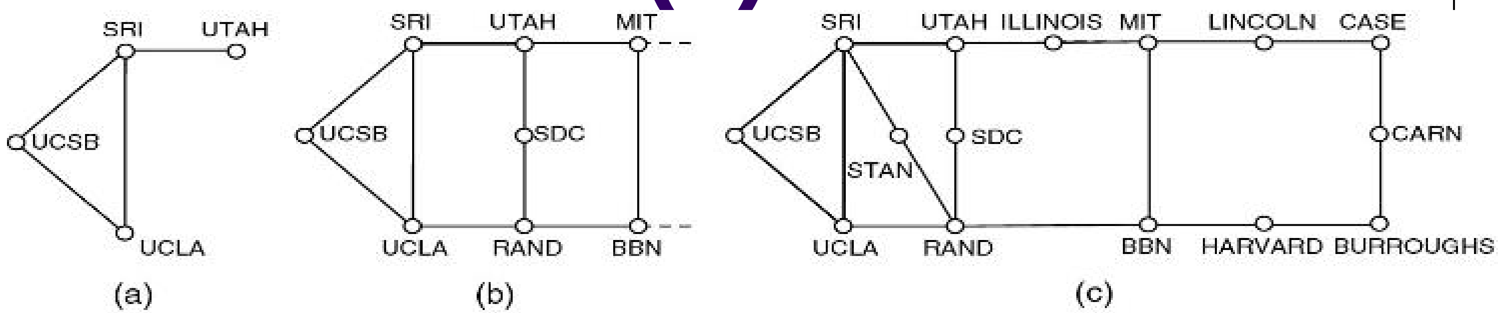
The ARPANET (2)



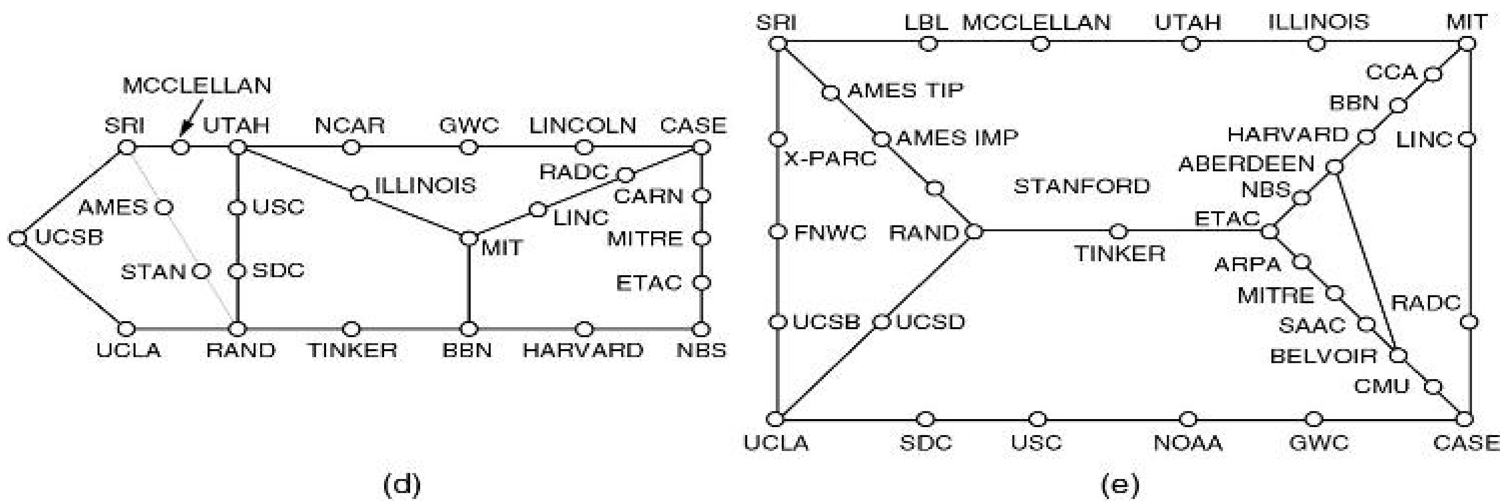
IMPs (Interface Message Processors)

The original ARPANET design.

The ARPANET (3)

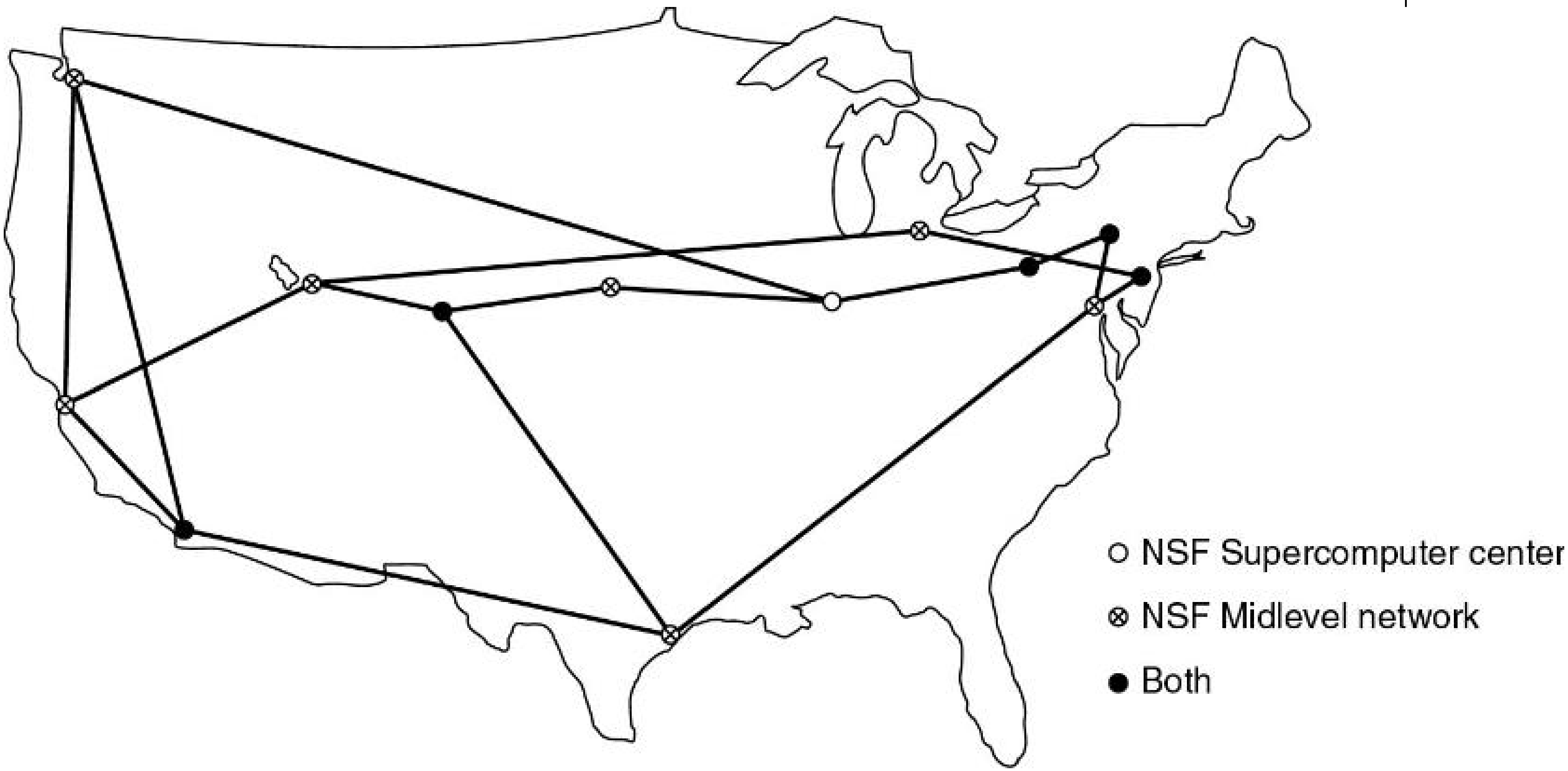


NAP (Network Access Point).



Growth of the ARPANET (a) December 1969. (b) July 1970. (c) March 1971. (d) April 1972. (e) September 1972.

NSFNET



The NSFNET backbone in 1988.

NSFNET

- Late 1970s - Many other folks wanted to get on the net, but Arpanet was essentially limited to military contractors.   NSF set up another network to handle this need. Started at 448 Kbps and by 80's upgraded to 1.5 Mbps.
- 1990 Formed ANS (Advanced Networks and Services) - MERIT, MCI, IBM took over from the government running at 45 Mbps.
- 1995 ANSNET sold to AOL, who now runs it.

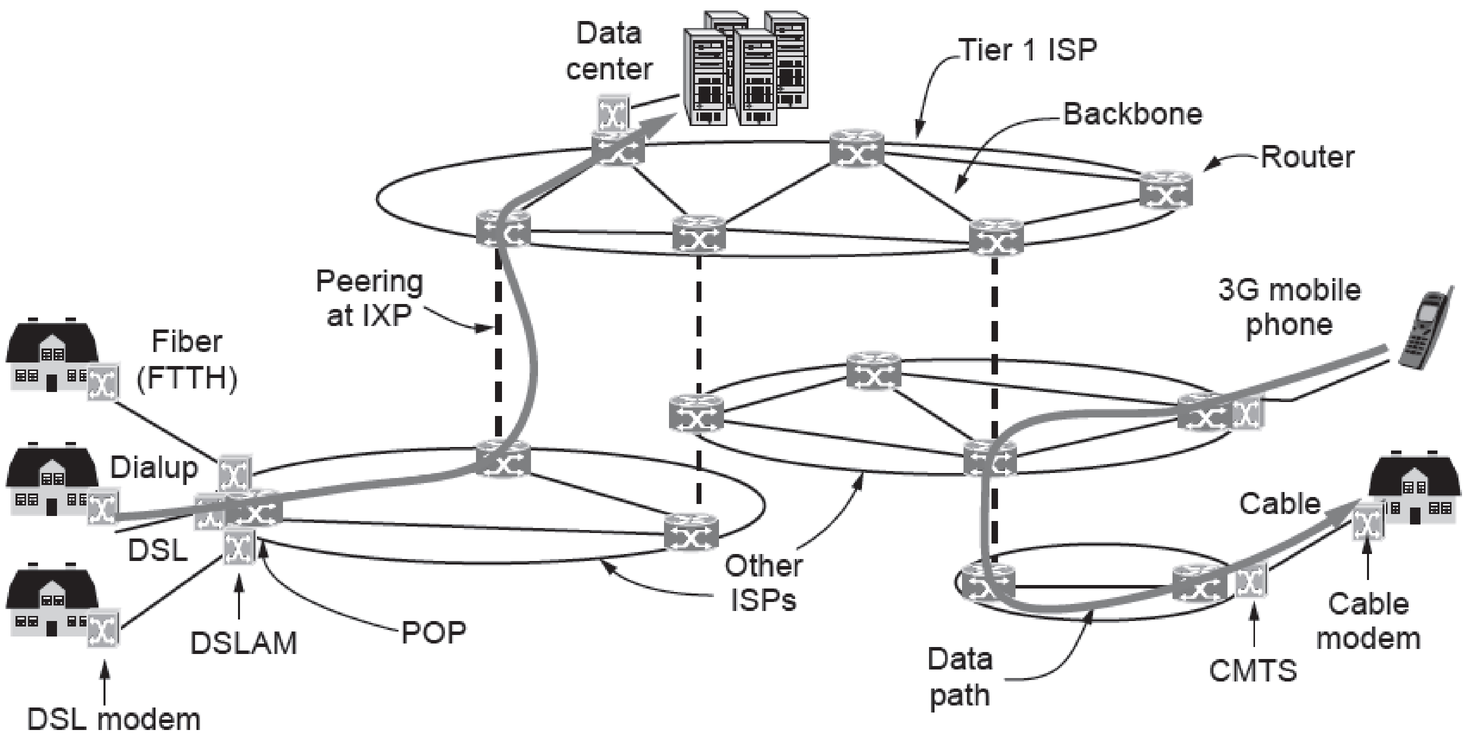
Internet Usage

- Growing exponentially.
- All nodes run TCP/IP. Means that all nodes have an IP address by which they can be contacted.
- Traditional applications (1970 – 1990)
  - E-mail
  - News
  - Remote login
  - File transfer

Internet Usage

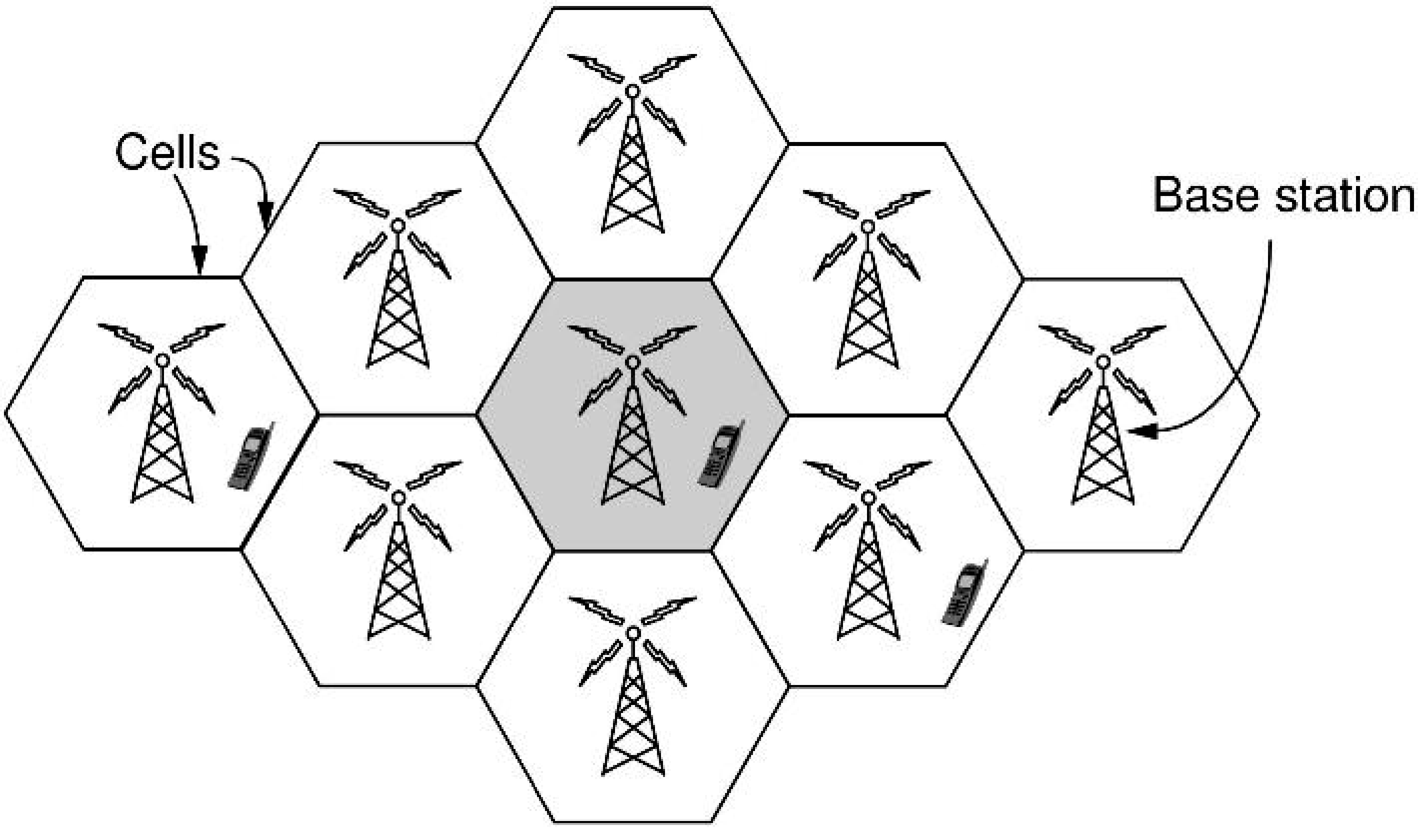
- **1990s :**
  - **the WWW (World Wide Web)**
    - invented by CERN physicist Tim Berners-Lee
  - **Together with the Mosaic browser**
    - Written by Marc Andreessen at the National Center for Supercomputer Applications in Urbana, Illinois
  - **ISPs (Internet Service Providers)**
    - Offer individual users at home the ability to call up one of their machines and connect to the Internet

Architecture of the Internet



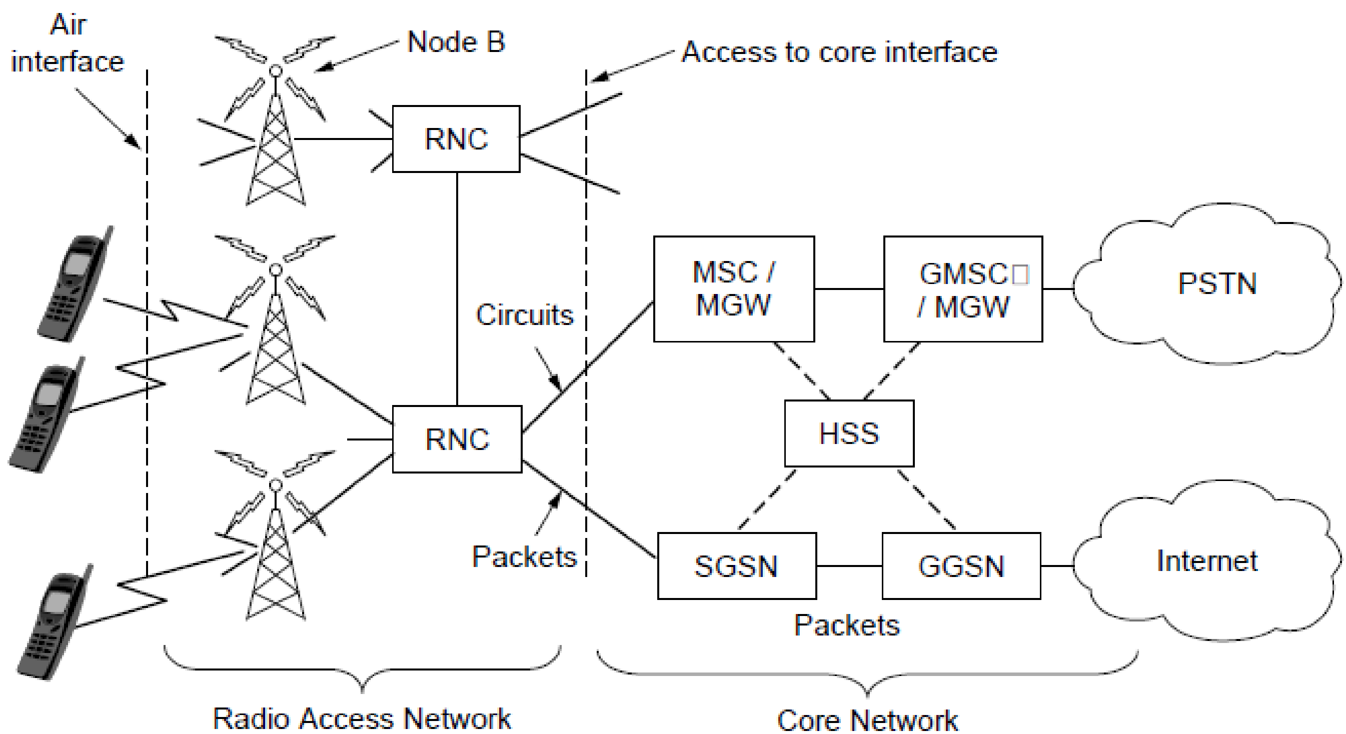
Overview of the Internet architecture

3G Mobile Phone Networks



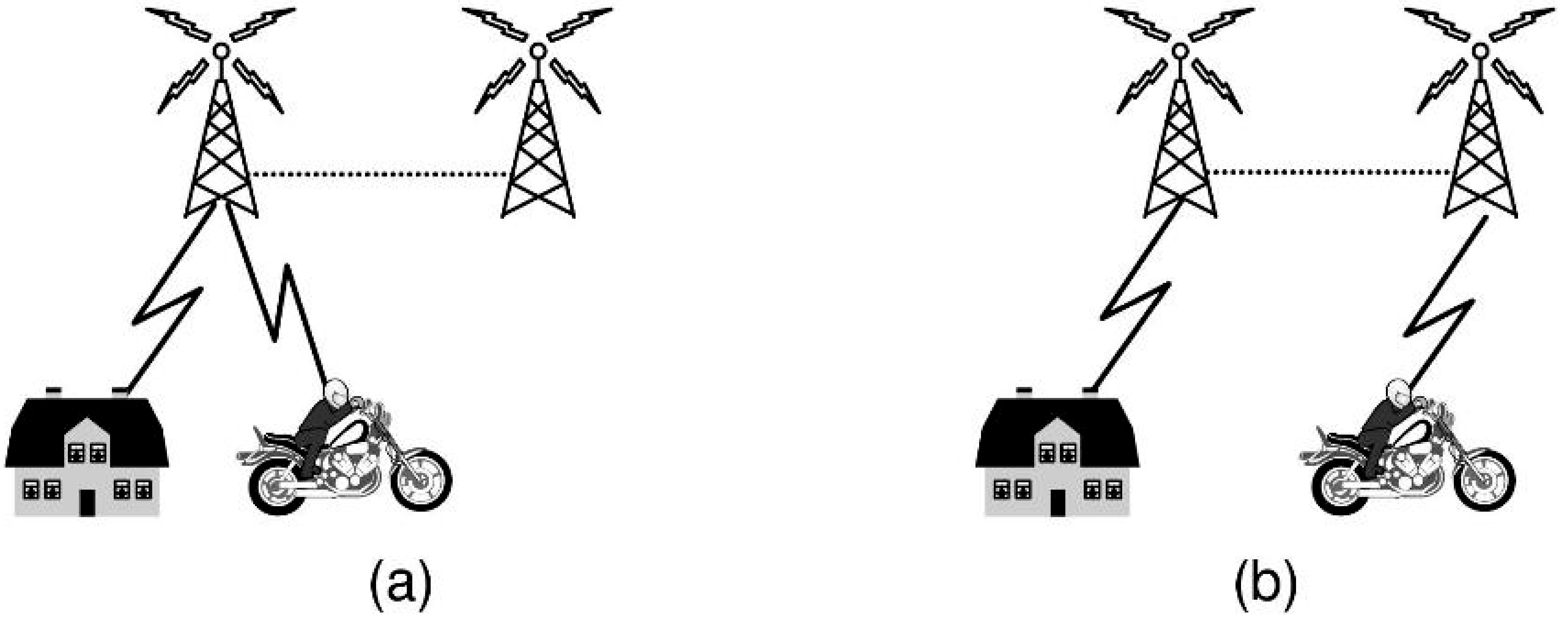
Cellular design of mobile phone networks

3G Mobile Phone Networks



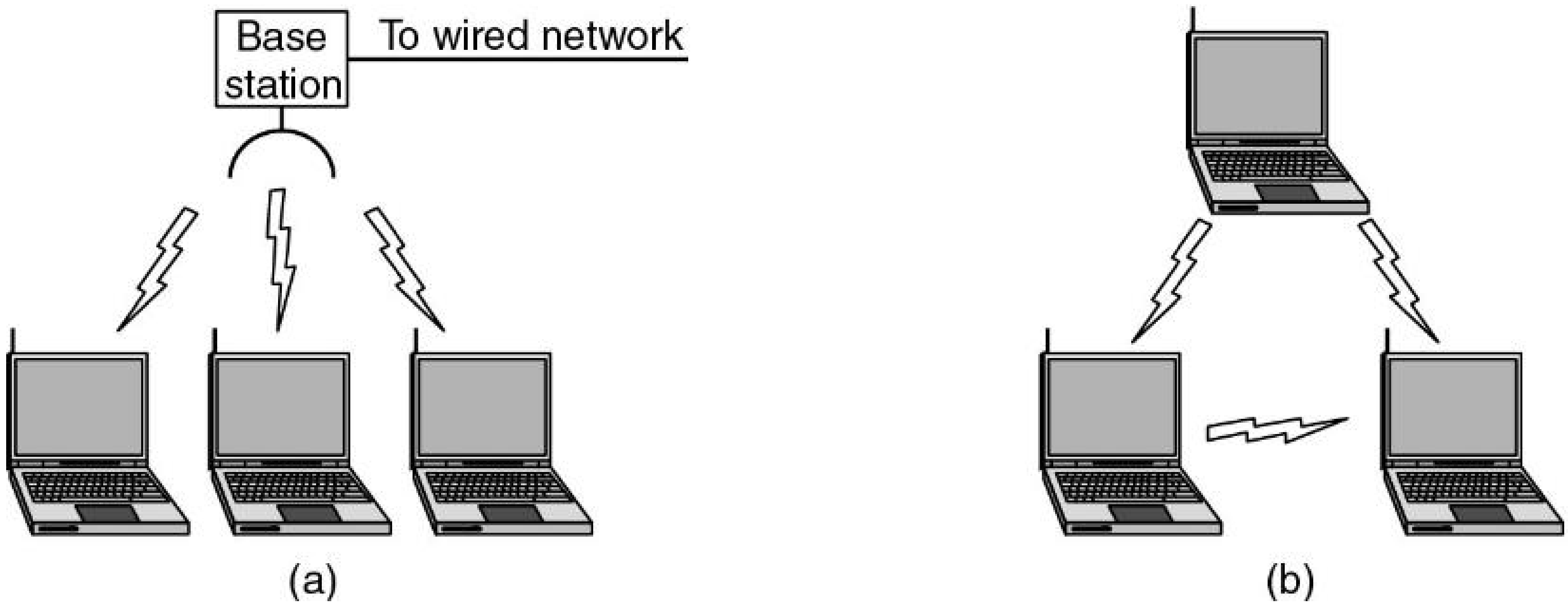
Architecture of the UMTS 3G mobile phone network.

3G Mobile Phone Networks



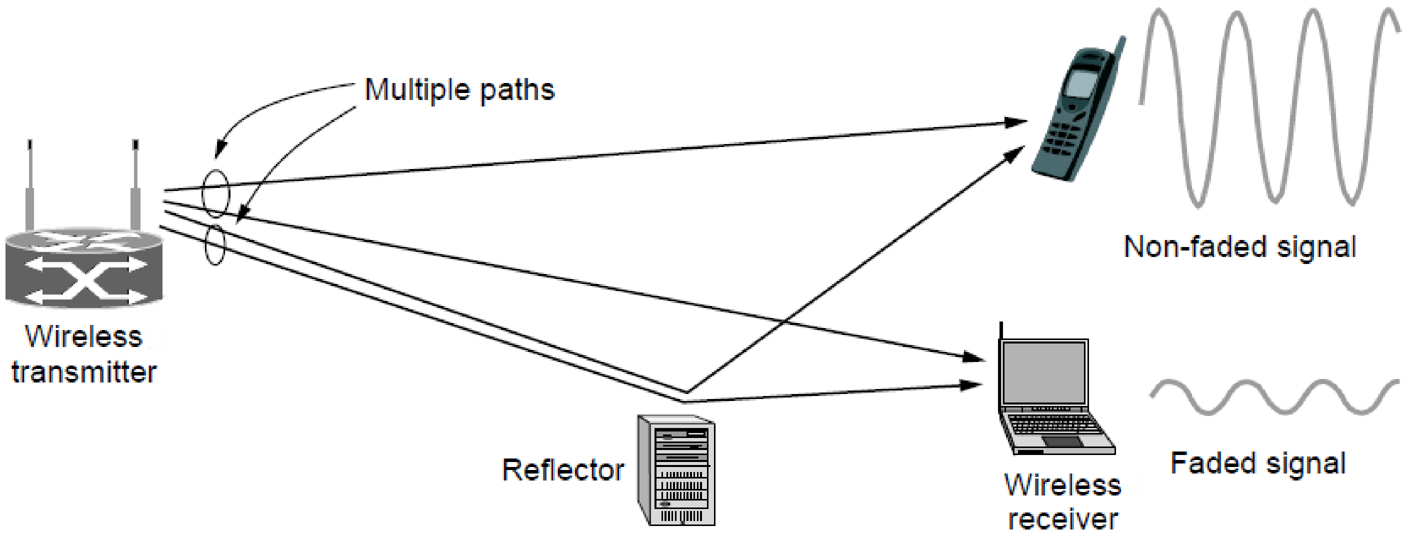
Mobile phone handover (a) before, (b) after.

Wireless LANs - WiFi (802.11)



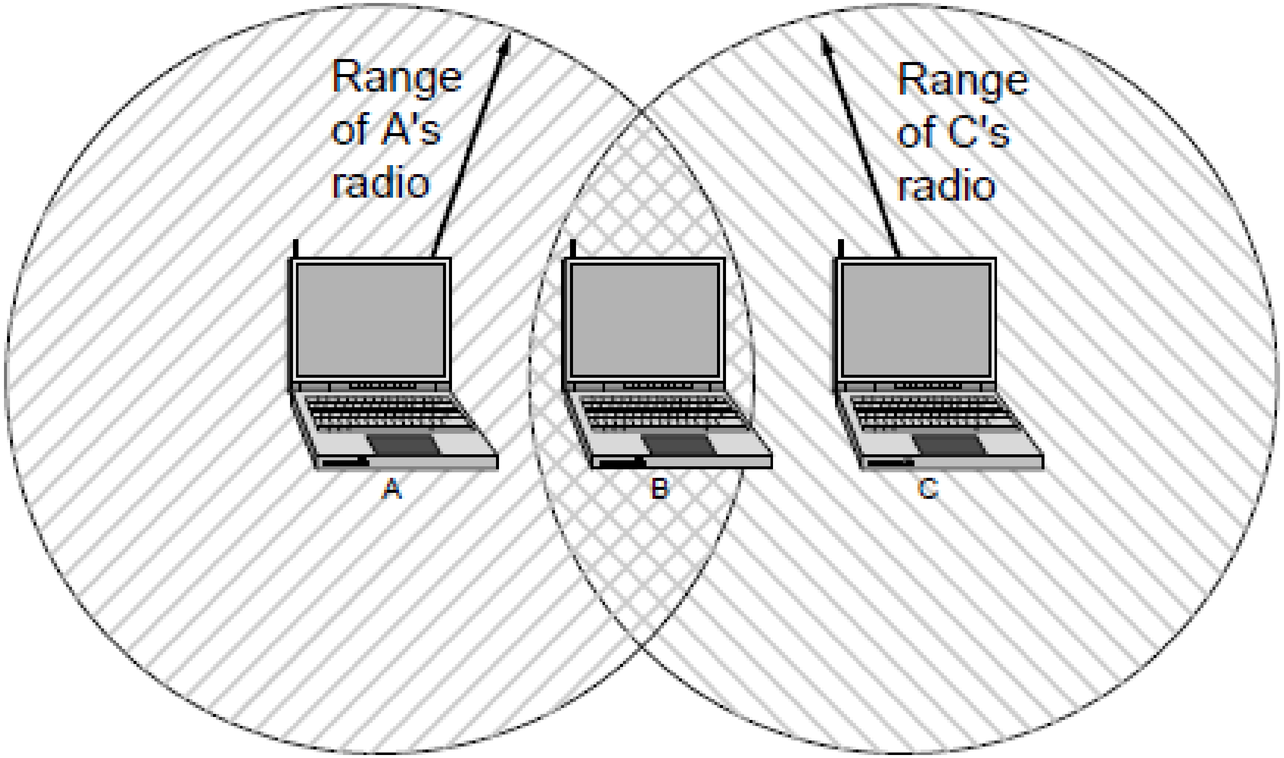
(a) Wireless networking with a base station.
(b) Ad hoc networking.

Wireless LANs: 802.11



Multipath fading

Wireless LANs: 802.11

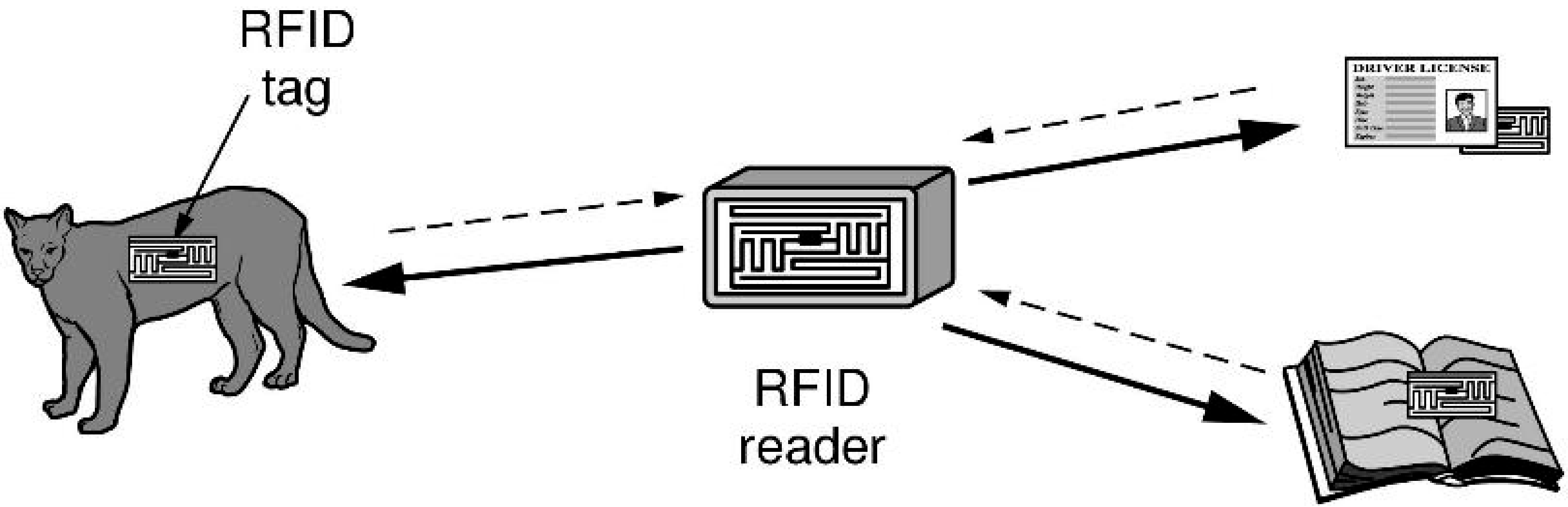


The range of a single radio may not cover the entire system.

Wireless LANs standards

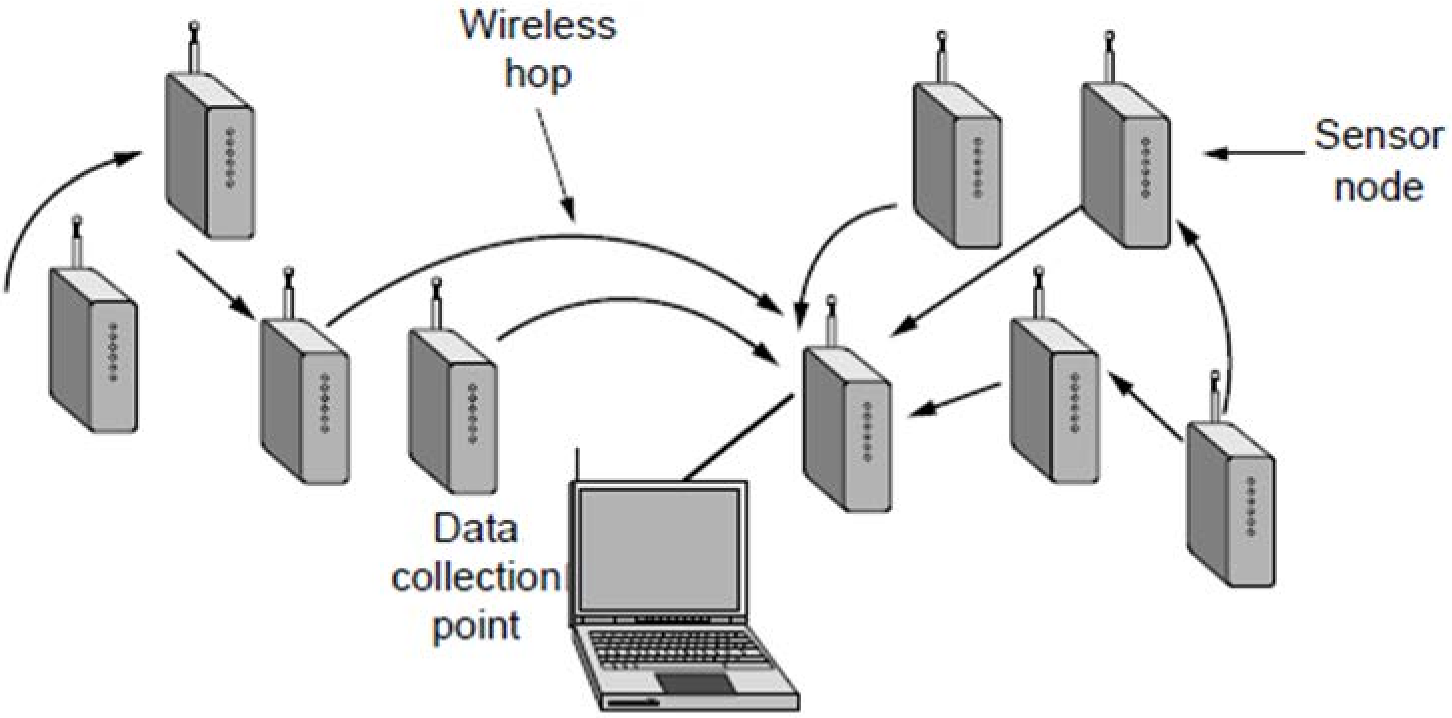
- The development of the standard
  - 802.11-1997: 1Mbps, 2Mbps (2.4 GHz)
  - 802.11a-1999: 54Mbps (5 GHz band)
  - 802.11b-1999:11Mbps(2.4 GHz)
  - 802.11g-2003: 54Mbps (2.4 GHz)
  - 802.11n-2009:upto 600Mbps (operates on both the 2.4 GHz and the lesser used 5 GHz bands)
  - 802.11ac-2012:upto 1Gbps(5GHz)

RFID and Sensor Networks



RFID used to network everyday objects.

RFID and Sensor Networks



Multihop topology of a sensor network

1.6 Network Standardization

- Who's Who in the Telecommunications World
- Who's Who in the International Standards World
- Who's Who in the Internet Standards World

De facto and De jure

ITU
(International Telecommunication Union)

- Main sectors
  - ITU-R: Radio communications
  - ITU-T: Telecommunications Standardization
  - ITU-D: Development
- Classes of Members
  - National governments
  - Sector members
  - Associate members
  - Regulatory agencies

Network Standardization

- ISO (International Standards Organization)
- ANSI (American National Standards Institute)
- NIST (National Institute of Standards and Technology)
- IEEE (Institute of Electrical and Electronics Engineering**)**

IEEE 802 Standards

Number	Topic
802.1	Overview and architecture of LANs
802.2 ↓	Logical link control
802.3 *	Ethernet
802.4 ↓	Token bus (was briefly used in manufacturing plants)
802.5	Token ring (IBM's entry into the LAN world)
802.6 ↓	Dual queue dual bus (early metropolitan area network)
802.7 ↓	Technical advisory group on broadband technologies
802.8 †	Technical advisory group on fiber optic technologies
802.9 ↓	Isochronous LANs (for real-time applications)
802.10 ↓	Virtual LANs and security
802.11 *	Wireless LANs (WiFi)
802.12 ↓	Demand priority (Hewlett-Packard's AnyLAN)

The 802 working groups. The important ones are marked with *. The ones marked with ↓ are hibernating. The one marked with † gave up and disbanded itself.

IEEE 802 Standards

802.13	Unlucky number; nobody wanted it
802.14 ↓	Cable modems (defunct: an industry consortium got there first)
802.15 *	Personal area networks (Bluetooth, Zigbee)
802.16 *	Broadband wireless (WiMAX)
802.17	Resilient packet ring
802.18	Technical advisory group on radio regulatory issues
802.19	Technical advisory group on coexistence of all these standards
802.20	Mobile broadband wireless (similar to 802.16e)
802.21	Media independent handoff (for roaming over technologies)
802.22	Wireless regional area network

http://standards.ieee.org/about/get/802/802.html

Internet standards

- Internet Architecture Board.
  - IETF: Internet Engineering Task Force
    - RFC: Request for comments

      http://www.ietf.org/rfc
  - IRTF (Internet Research Task Force)
- **Internet Society**
  - http://www.isoc.org

END OF CH-1