EECS 369: Introduction to Sensor Networks

Instructors: Peter Scheuermann and Goce Trajcevski

Week2: Overview of Communication and Networking – PartII

Networking – Recap

- Traditional
  - Traditional local area network (LAN)
  - Traditional wide area network (WAN)
- Higher-speed
  - High-speed local area network (LAN)
  - Metropolitan area network (MAN)
  - High-speed wide area network (WAN)

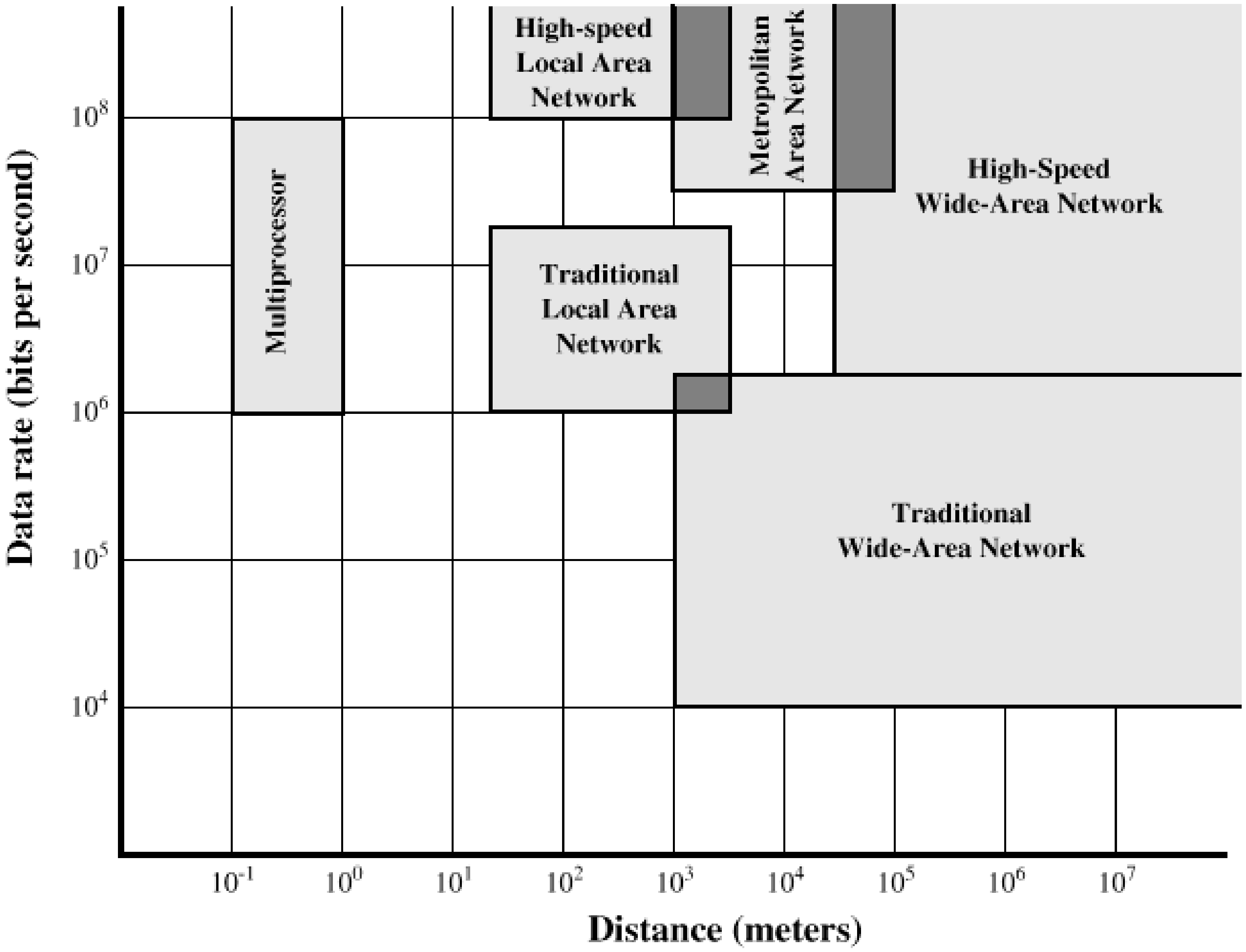


Figure 3.1 Comparison of Multiprocessor Systems, LANs, MANs, and WANs

Networking – Recap: Comparison

WAN

- Covers large geographical areas
- Circuits provided by a common carrier
- Consists of interconnected switching nodes
- Traditional WANs provide modest capacity
  - 64000 bps common
  - Business subscribers using T-1 service – 1.544 Mbps common
- Higher-speed WANs use optical fiber and transmission technique known as asynchronous transfer mode (ATM)
  - 10s and 100s of Mbps common
  - Network assets NOT owned by same organization.

LAN

- Like WAN, LAN interconnects a variety of devices and provides a means for information exchange among them
- Traditional LANs
  - Provide data rates of 1 to 20 Mbps
- High-speed LANS
  - Provide data rates of 100 Mbps to 1 Gbps (internal speed much higher than WAN).

The Need for MANs

- Traditional point-to-point and switched network techniques used in WANs are inadequate for growing needs of organizations
- Need for high capacity and low costs over large area
- MAN provides:
  - Service to customers in metropolitan areas
  - Required capacity
  - Lower cost and greater efficiency than equivalent service from telephone company

Networking – Recap

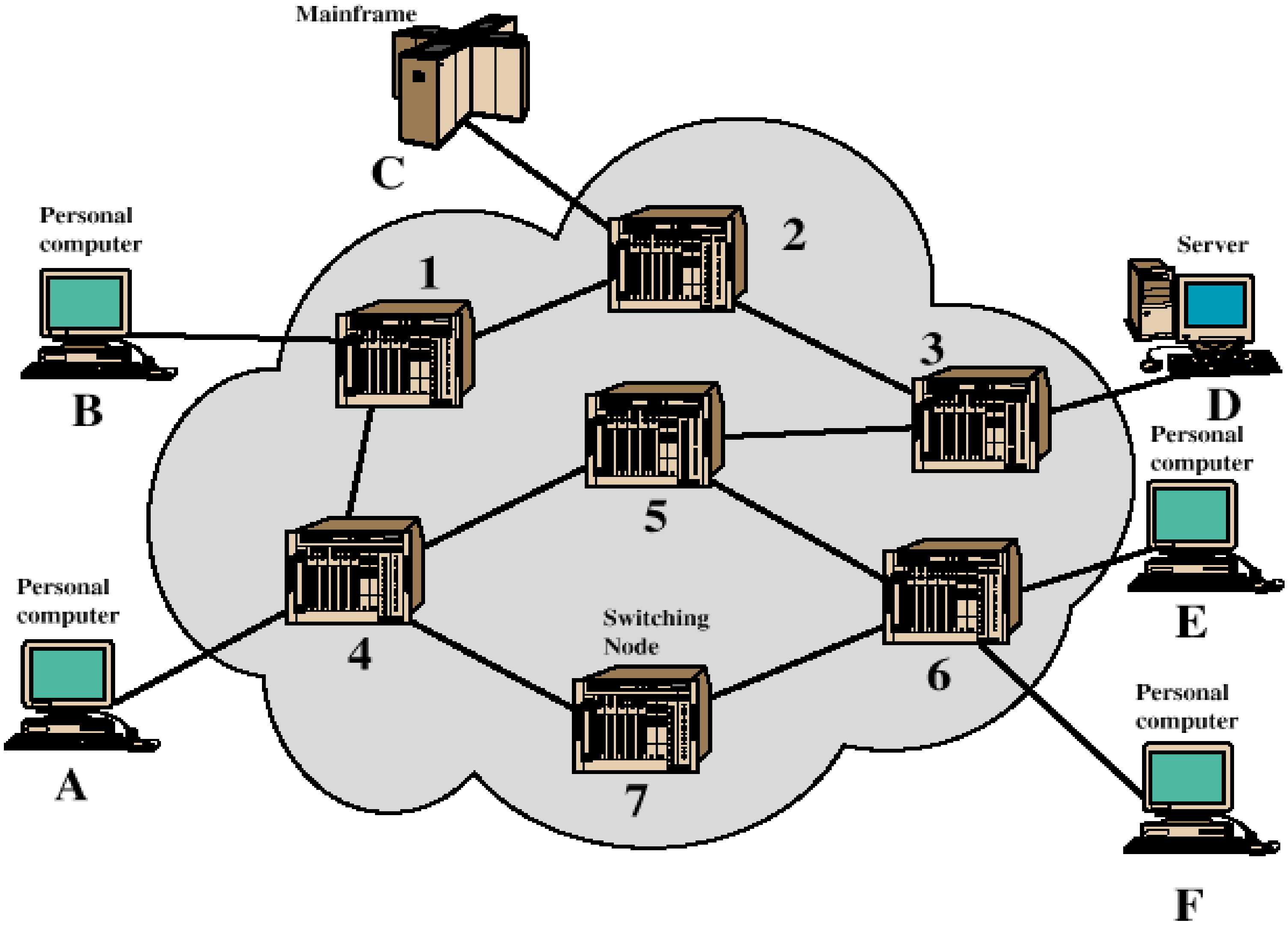


Figure 3.3 Simple Switching Network

Networking – Recap (Circuit Switching)

- Circuit establishment
  - An end to end circuit is established through switching nodes
- Information Transfer
  - Information transmitted through the network
  - Data may be analog voice, digitized voice, or binary data
- Circuit disconnect
  - Circuit is terminated
  - Each node deallocates dedicated resources

- Can be inefficient
  - Channel capacity dedicated for duration of connection
  - Utilization not 100%
  - Delay prior to signal transfer for establishment
- Once established, network is transparent to users
- Information transmitted at fixed data rate with only propagation delay

Networking – Recap (Packet Switching)

- Data is transmitted in blocks, called packets
- Before sending, the message is broken into a series of packets
  - Typical packet length is 1000 octets (bytes)
  - Packets consists of a portion of data plus a packet header that includes control information
- At each node en route, packet is received, stored briefly and passed to the next node

- Line efficiency is greater
  - Many packets over time can dynamically share the same node to node link
- Packet-switching networks can carry out data-rate conversion
  - Two stations with different data rates can exchange information
- Unlike circuit-switching networks that block calls when traffic is heavy, packet-switching still accepts packets, but with increased delivery delay
- Priorities can be used

Networking – Recap (Packet Switching)

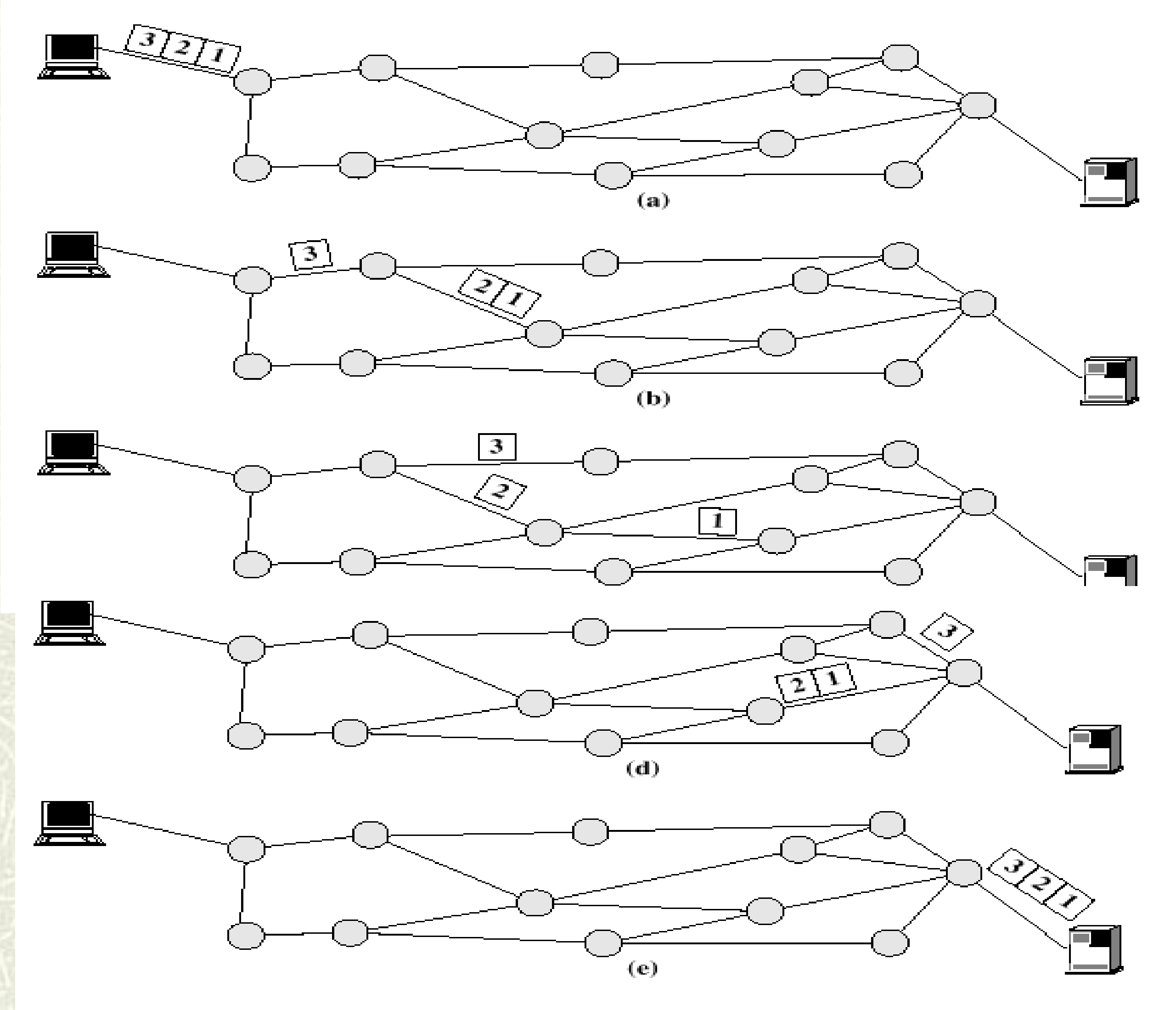


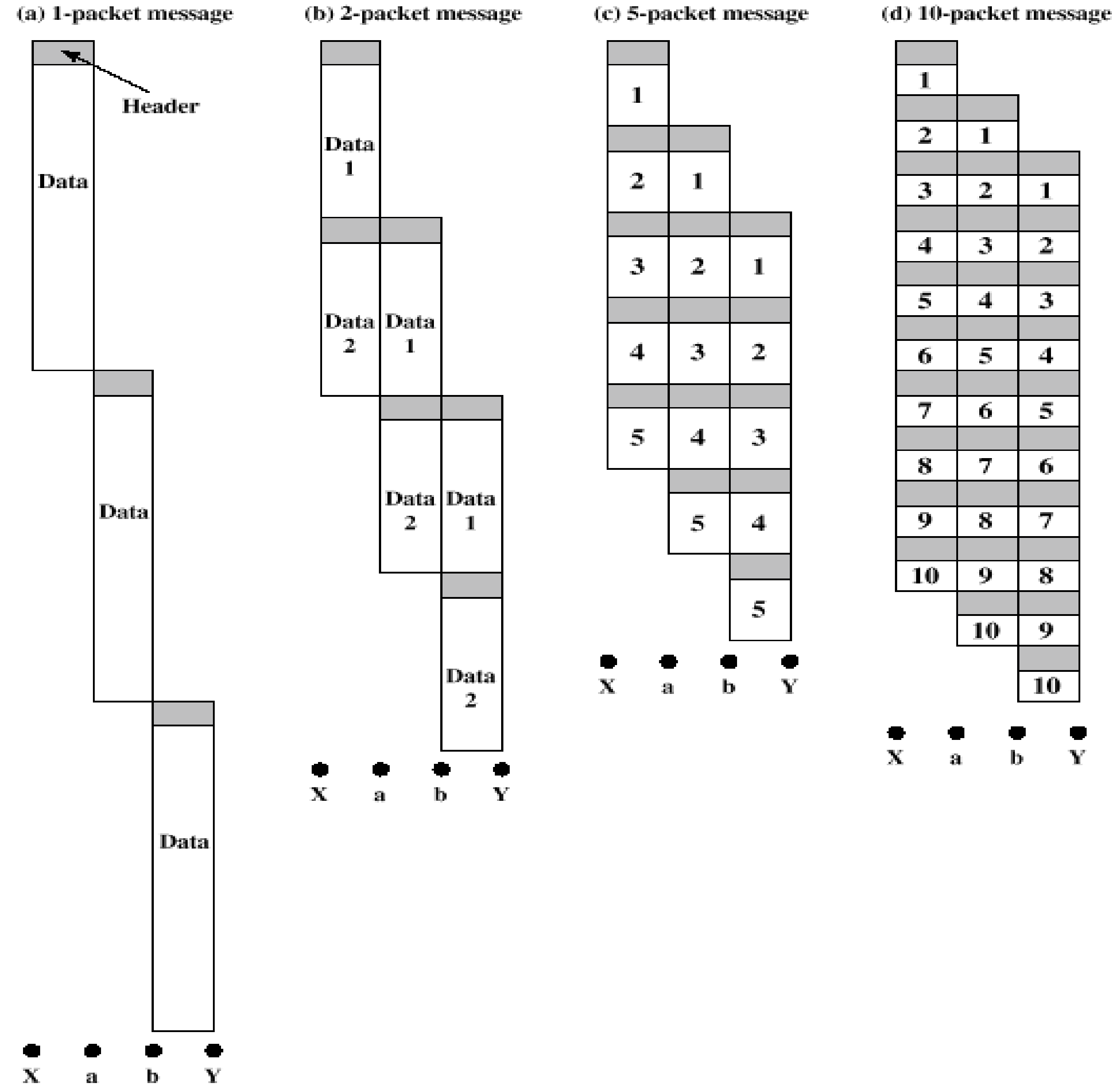
Figure 3.7 Packet Switching: Datagram Approach

Networking –Recap (Virtual Circuits)

- Preplanned route established before packets sent
- All packets between source and destination follow this route
- Routing decision not required by nodes for each packet
- Emulates a circuit in a circuit switching network but is not a dedicated path
  - Packets still buffered at each node and queued for output over a line

- Advantages:
  - Packets arrive in original order
  - Packets arrive correctly
  - Packets transmitted more rapidly without routing decisions made at each node

Networking – Recap (Transmission vs. packet-size)



Networking – Recap (ATM)

- Also known as cell relay
- Operates at high data rates
- Resembles packet switching
  - Involves transfer of data in discrete chunks, like packet switching
  - Allows multiple logical connections to be multiplexed over a single physical interface
- Minimal error and flow control capabilities reduces overhead processing and size
- Fixed-size cells simplify processing at ATM nodes

Real-time service

- Constant bit rate (CBR)

- Real-time variable bit rate (rt-VBR)

- Virtual channel connection (VCC)
  - Logical connection in ATM
  - Basic unit of switching in ATM network
  - Analogous to a virtual circuit in packet switching networks
  - Exchanges variable-rate, full-duplex flow of fixed-size cells
- Virtual path connection (VPC)
  - Bundle of VCCs that have the same end points

Non-real-time service

Non-real-time variable bit rate (nrt-VBR)
Available bit rate (ABR)
Unspecified bit rate (UBR

Networking – Recap (Protocols)

Key features:

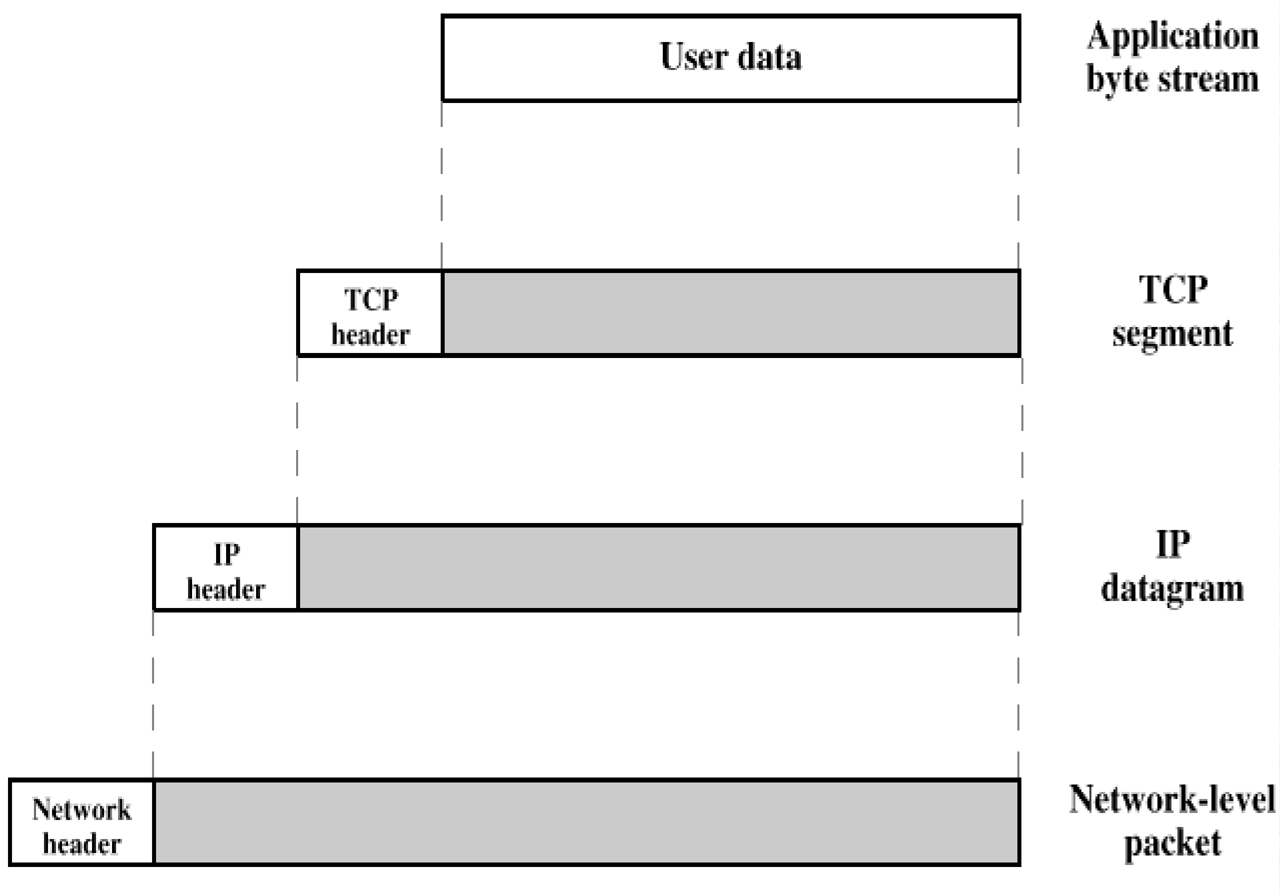
- Syntax
  - Concerns the format of the data blocks
- Semantics
  - Includes control information for coordination and error handling
- Timing
  - Includes speed matching and sequencing

Key agents:

- Applications
  - Exchange data between computers (e.g., electronic mail)
- Computers
  - Connected to networks
- Networks
  - Transfers data from one computer to another

Networking – Recap (TCP/IP layers)

- Physical layer
- Network access layer
- Internet layer
- Host-to-host, or transport layer
- Application layer



Networking – Recap (TCP/IP layers)

Physical Layer:

- Covers the physical interface between a data transmission device and a transmission medium or network
- Physical layer specifies:
  - Characteristics of the transmission medium
  - The nature of the signals
  - The data rate
  - Other related matters

Network Access Layer:

- Concerned with the exchange of data between an end system and the network to which it's attached
- Software used depends on type of network
  - Circuit switching
  - Packet switching (e.g., X.25)
  - LANs (e.g., Ethernet)
  - Others

Networking – Recap (TCP/IP layers)

Internet Layer

- Provides routing functions to allow data to traverse multiple interconnected networks
- Uses internet protocol (IP)
- Implemented in end systems *and* routers

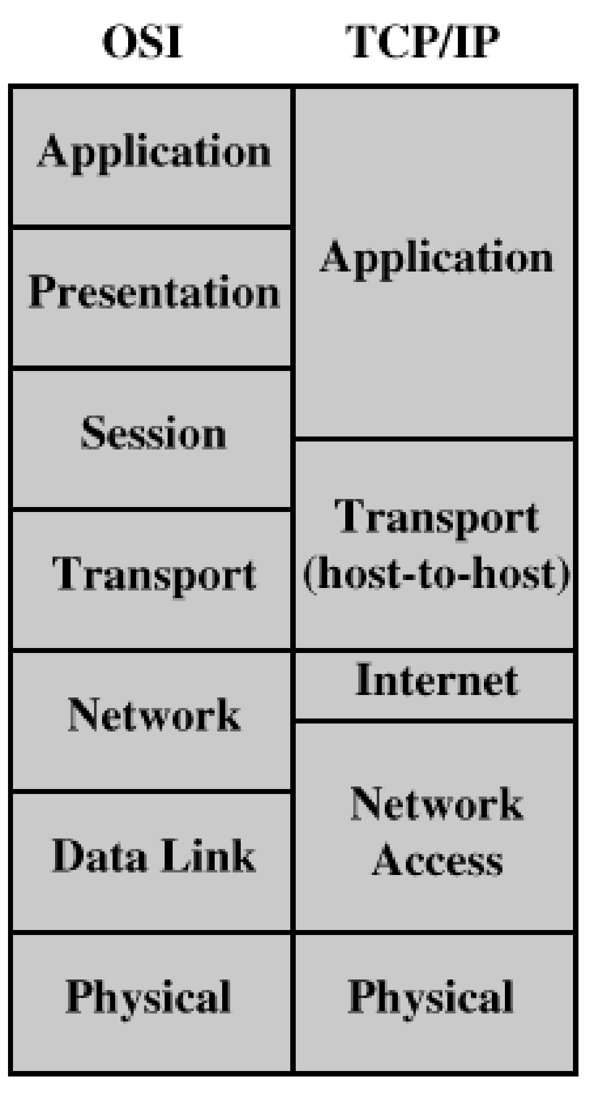
Transport Host-to-Host) Layer

- Commonly uses transmission control protocol (tcp)
- Provides reliability during data exchange
  - Completeness
  - Order

Application Layer

- Logic supports user applications
- Uses separate modules that are peculiar to each different type of application

Networking – Recap (OSI vs. TCP/IP)



OSI	TCP/IP
Application	Application
Presentation	
Session	
Transport	Transport (host-to-host)
Network	Internet
Data Link	Network Access
Physical	Physical

Networking – Recap (Mobile IP and Wireless)

- Enable computers to maintain Internet connectivity while moving from one Internet attachment point to another
- Mobile – user's point of attachment changes dynamically and all connections are automatically maintained despite the change
- Nomadic - user's Internet connection is terminated each time the user moves and a new connection is initiated when the user dials back in
  - New, temporary IP address is assigned

- Mobile node is assigned to a particular network – home network
- IP address on home network is static – home address
- Mobile node can move to another network – foreign network
- Mobile node registers with network node on foreign network – foreign agent
- Mobile node gives care-of address to agent on home network – home agent
  - Discovery – mobile node uses discovery procedure to identify prospective home and foreign agents
  - Registration – mobile node uses an authenticated registration procedure to inform home agent of its care-of address
  - Tunneling – used to forward IP datagrams between a home address and a care-of address

Networking Recap (Mobile IP and Wireless…)

Registration Process:

- Mobile node sends registration request to foreign agent requesting forwarding service
- Foreign agent relays request to home agent
- Home agent accepts or denies request and sends registration reply to foreign agent
- Foreign agent relays reply to mobile node

Authentication:

- Mobile-home – provides for authentication of registration messages between mobile node and home agent; must be present
- Mobile-foreign – may be present when a security association exists between mobile node and foreign agent
- Foreign-home – may be present when a security association exists between foreign agent and home agent

Networking – Recap (WAP…)

- Open standard providing mobile users of wireless terminals access to telephony and information services
  - Wireless terminals include wireless phones, pagers and personal digital assistants (PDAs)
  - Designed to work with all wireless network technologies such as GSM, CDMA, and TDMA
  - Based on existing Internet standards such as IP, XML, HTML, and HTTP
  - Includes security facilities

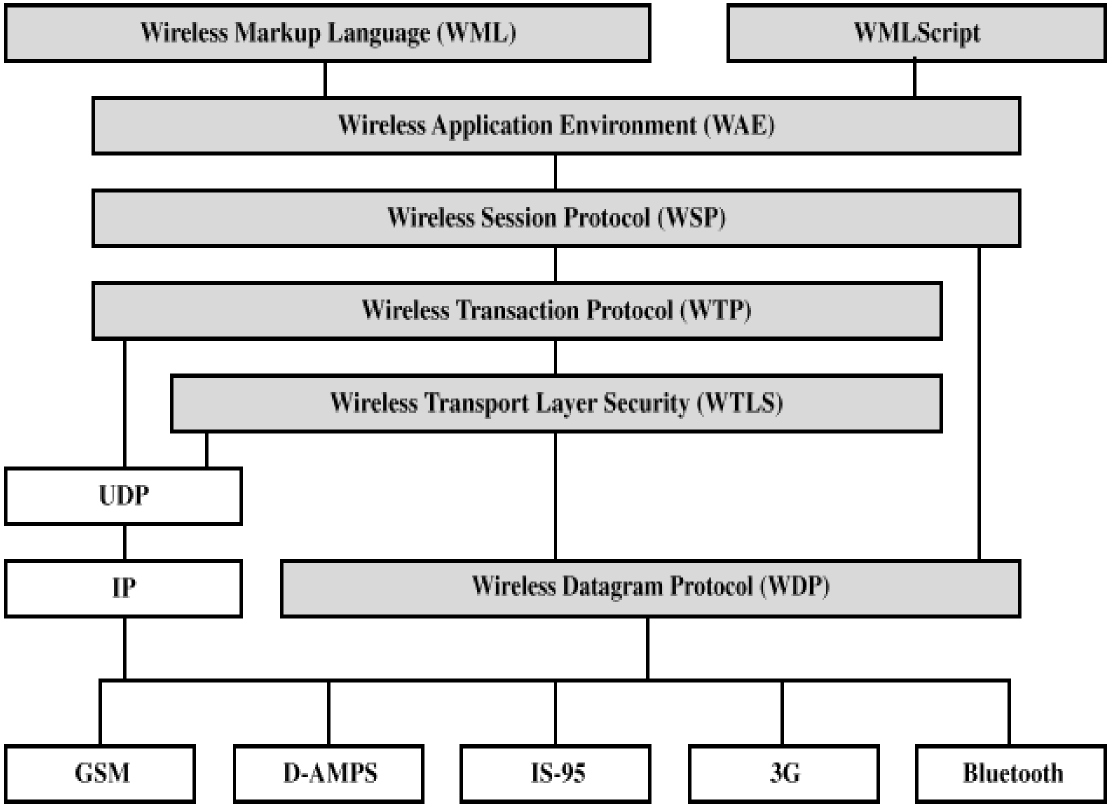

Wireless Markup Language (WML)
WMLScript
Wireless Application Environment (WAE)
Wireless Session Protocol (WSP)
Wireless Transaction Protocol (WTP)
Wireless Transport Layer Security (WTLS)
UDP
IP
Wireless Datagram Protocol (WDP)
GSM
D-AMPS
IS-95
3G
Bluetooth

Figure 12.8 WAP Protocol Stack

NORTHWESTERN
UNIVERSITY

Networking – Recap (WAP…)

WSP:

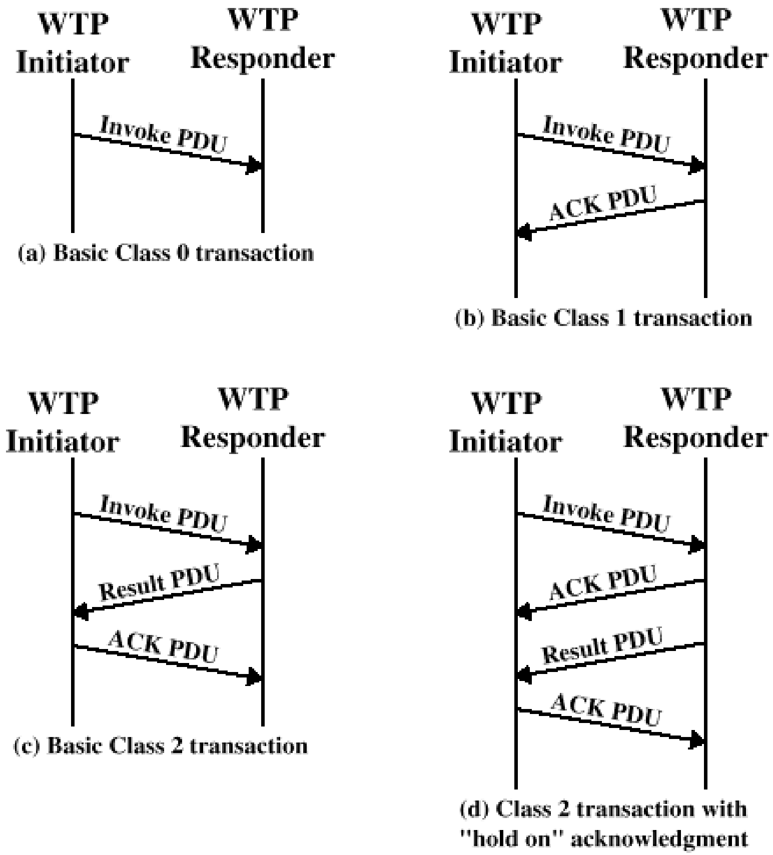
- Transaction-oriented protocol based on the concept of a request and a reply
- Provides applications with interface for two session services:
  - Connection-oriented session service – operates above reliable transport protocol WTP
  - Connectionless session service – operates above unreliable transport protocol WDP

WSP – Transaction Types:

- Session establishment – client WSP user requests session with server WSP user
- Session termination – client WSP user initiates termination
- Session suspend and resume – initiated with suspend and resume requests
- Transaction – exchange of data between a client and server
- Nonconfirmed data push – used to send unsolicited information from server to client
- Confirmed data push – server receives delivery confirmation from client

Networking – Recap (WTP)

- Lightweight protocol suitable for "thin" clients and over low-bandwidth wireless links
- WTP features
  - Three classes of transaction service
  - Optional user-to-user reliability: WTP user triggers confirmation of each received message
  - Optional out-of-band data on acknowledgments
  - PDU concatenation and delayed acknowledgment to reduce the number of messages sent
  - Asynchronous transactions



(a) Basic Class 0 transaction

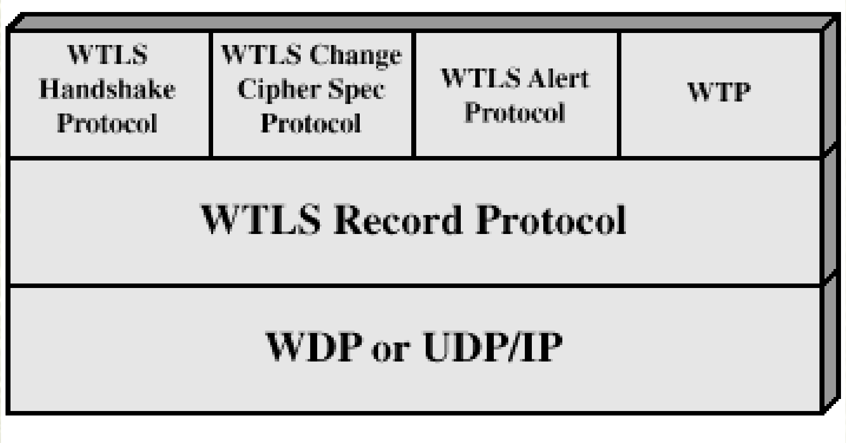
(b) Basic Class 1 transaction

(c) Basic Class 2 transaction

(d) Class 2 transaction with "hold on" acknowledgment

Figure 12.14 Examples of WTP Operation

Networking – Recap (MAC-role)



WTLS Handshake Protocol

WTLS Change Cipher Spec Protocol

WTLS Alert Protocol

WTP

WTLS Record Protocol

WDP or UDP/IP

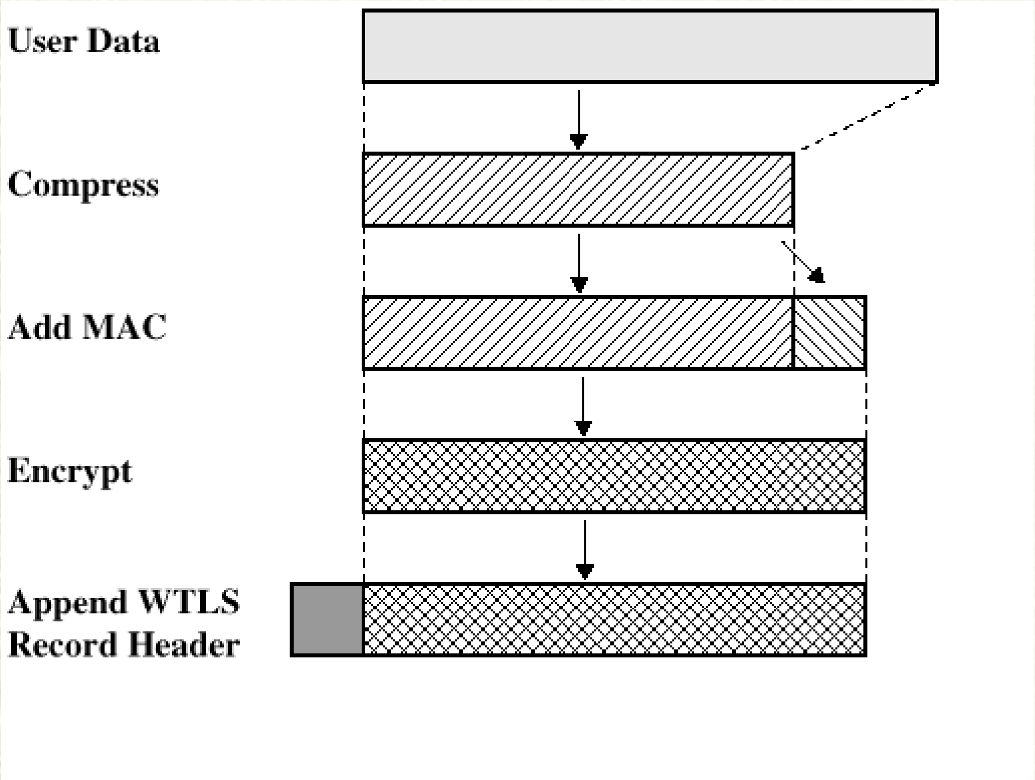
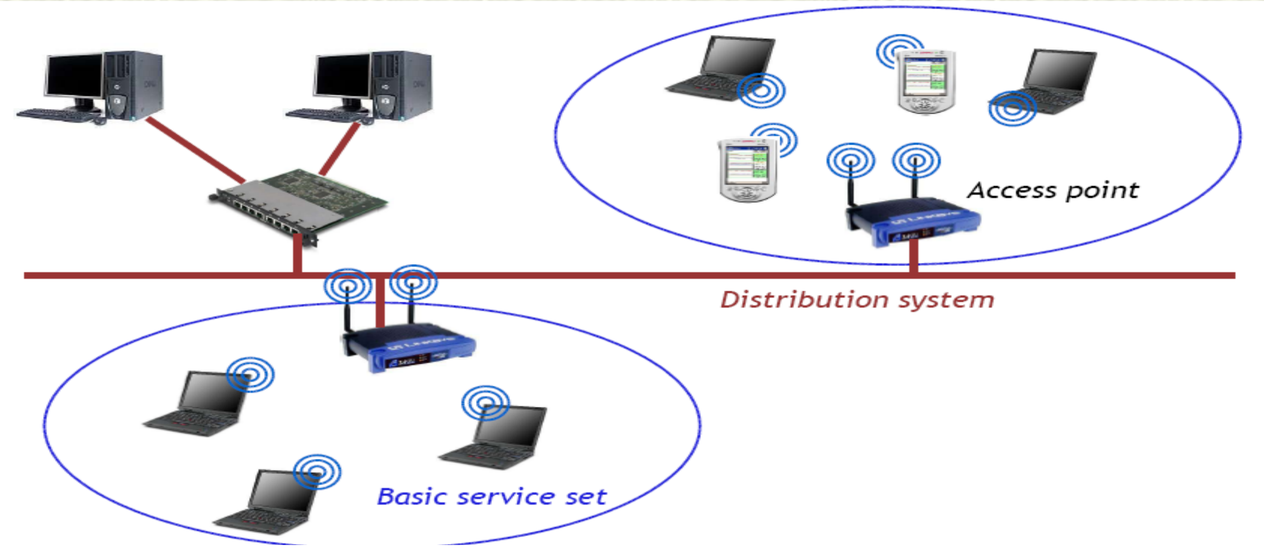
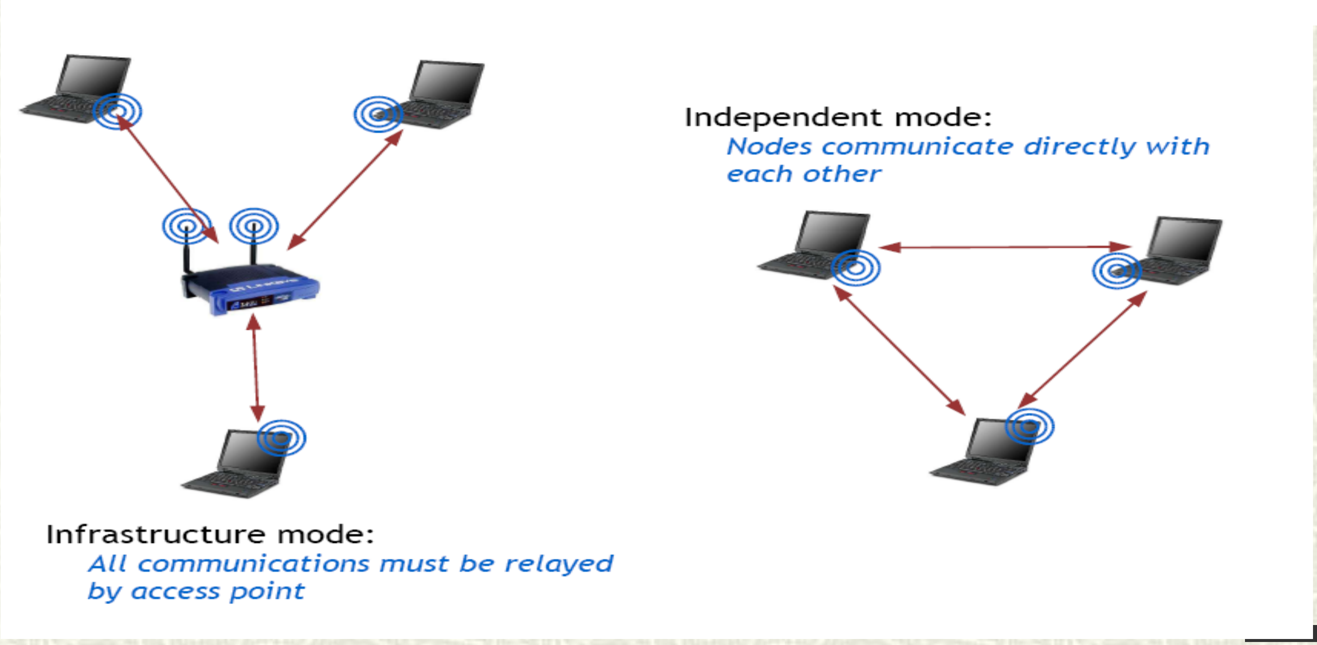


Figure 12.17 WTLS Record Protocol Operation

Wireless LAN and Ad-Hoc Networking




Independent mode:
Nodes communicate directly with each other

Infrastructure mode:
All communications must be relayed by access point

Wireless LAN and Ad-Hoc Networking

- Wireless link between LAN hub and mobile data terminal equipped with antenna
  - Laptop computer or notepad computer
- Uses:
  - Transfer data from portable computer to office server
  - Extended environment such as campus

- Temporary peer-to-peer network set up to meet immediate need
- Example:
  - Group of employees with laptops convene for a meeting; employees link computers in a temporary network for duration of meeting

Requirements/Expectations:

- Throughput
- Number of nodes
- Connection to backbone LAN
- Service area
- Battery power consumption
- Transmission robustness and security
- Collocated network operation
- License-free operation
- Handoff/roaming
- Dynamic configuration

Wireless LAN and Ad-Hoc Networking

Categories:

- Infrared (IR) LANs
- Spread spectrum LANs
- Narrowband microwave

PROs:

- Spectrum for infrared virtually unlimited
  - Possibility of high data rates
- Infrared spectrum unregulated
- Equipment inexpensive and simple
- Reflected by light-colored objects
  - Ceiling reflection for entire room coverage
- Doesn’t penetrate walls
  - More easily secured against eavesdropping
  - Less interference between different rooms

CONs:

- Indoor environments experience infrared background radiation
  - Sunlight and indoor lighting
  - Ambient radiation appears as noise in an infrared receiver
  - Transmitters of higher power required
    - Limited by concerns of eye safety and excessive power consumption
  - Limits range

Transmission Techniques:

- Directed Beam Infrared (range of few Km)
- Omnidirectional (LOS of all nodes; ceiling)
- Diffused (many IR, aim at ceiling->reflect)

Wireless LAN and Ad-Hoc Networking
IEEE 802.11 Standard

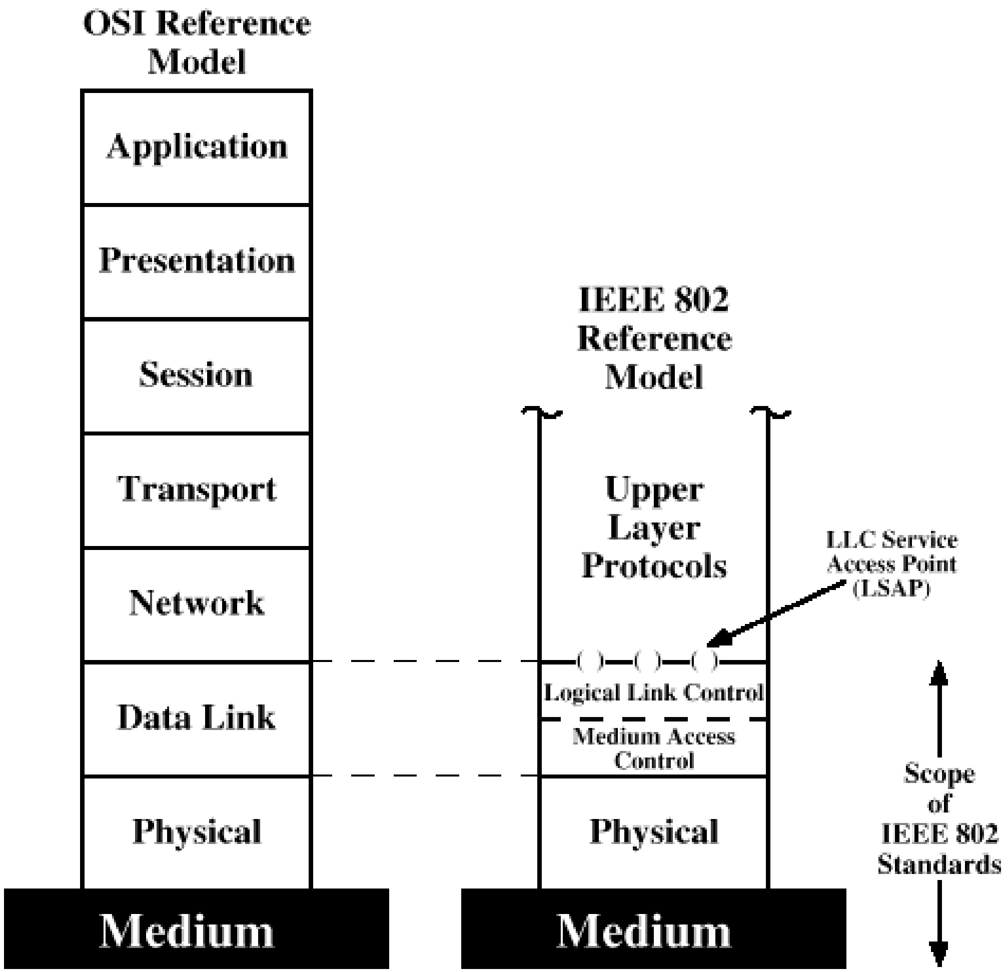


Figure 14.1 IEEE 802 Protocol Layers Compared to OSI Model

Wireless LAN - IEEE 802.11 Standard

- Functions of physical layer:
  - Encoding/decoding of signals
  - Preamble generation/removal (for synchronization)
  - Bit transmission/reception
  - Includes specification of the transmission medium
- Functions of medium access control (MAC) layer:
  - On transmission, assemble data into a frame with address and error detection fields
  - On reception, disassemble frame and perform address recognition and error detection
  - Govern access to the LAN transmission medium
- Functions of logical link control (LLC) Layer:
  - Provide an interface to higher layers and perform flow and error control

Wireless LAN - IEEE 802.11 Standard

Separation of LLC and MAC:

- The logic required to manage access to a shared-access medium not found in traditional layer 2 data link control
- For the same LLC, several MAC options may be provided

- MAC control
  - Contains Mac protocol information
- Destination MAC address
  - Destination physical attachment point
- Source MAC address
  - Source physical attachment point
- CRC
  - Cyclic redundancy check

- Characteristics of LLC not shared by other control protocols:
  - Must support multi-access, shared-medium nature of the link
  - Relieved of some details of link access by MAC layer

Services: Unacknowledged connectionless; Connection-mode; Acknowledged connectionless

Wireless LAN - IEEE 802.11 Standard

Architecture of 802.11…

- Distribution system (DS)
- Access point (AP)
- Basic service set (BSS)
- Stations competing for access to shared wireless medium
- Isolated or connected to backbone DS through AP
- Extended service set (ESS) (Two or more basic service sets interconnected by DS)

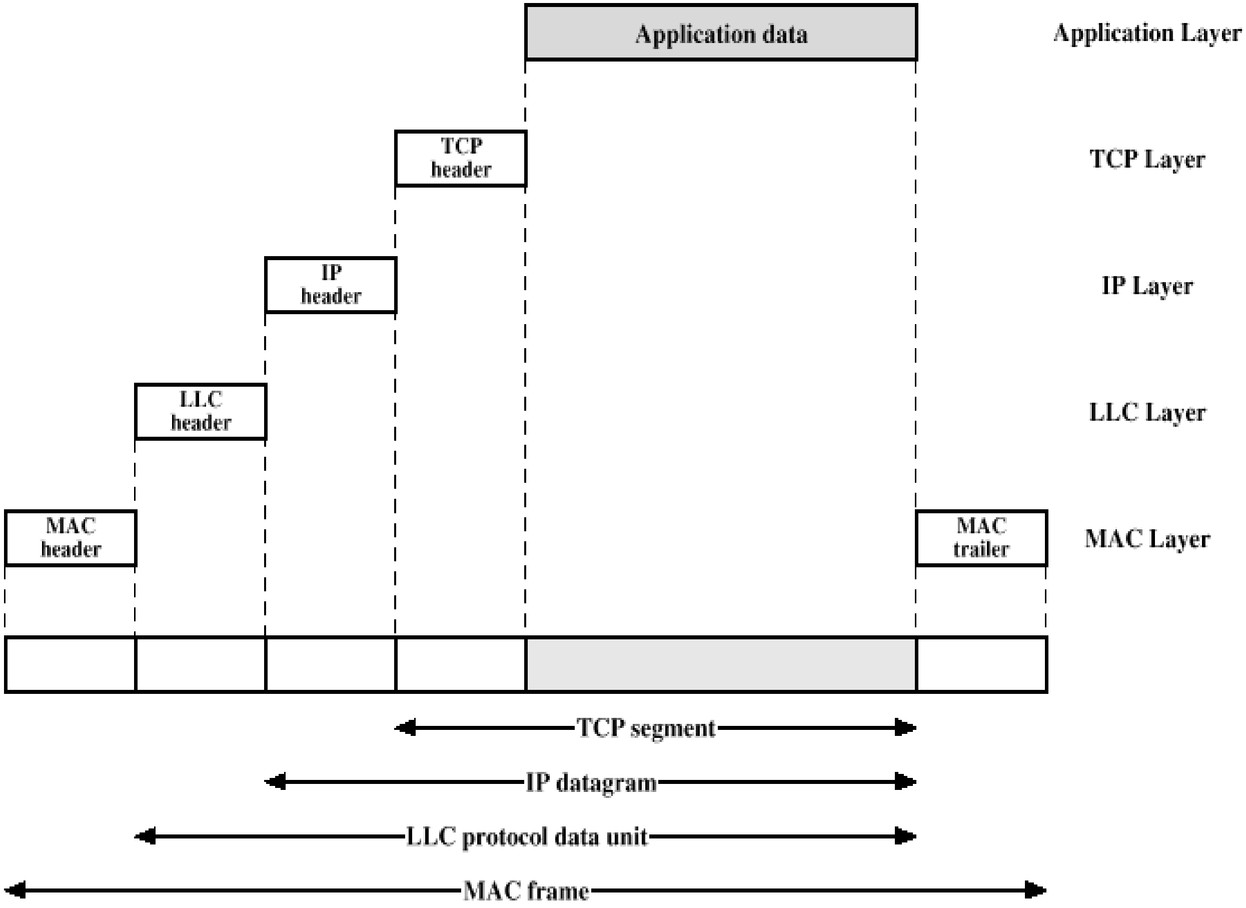


Figure 14.2 IEEE 802 Protocols in Context

Wireless LAN - IEEE 802.11 Standard

Distribution Service (DS):

- Exchanges MAC frames from station in one BSS to station in another BSS

Integration Service (IS):

- Transfer of data between station on IEEE 802.11 LAN and station on integrated IEEE 802.x LAN

- Association
  - Establishes initial association between station and AP
- Reassociation
  - Enables transfer of association from one AP to another, allowing station to move from one BSS to another
- Disassociation
  - Association termination notice from station or AP
- Authentication
  - Establishes identity of stations to each other
- Deauthentication
  - Invoked when existing authentication is terminated
- Privacy
  - Prevents message contents from being read by unintended recipient

Wireless LAN - IEEE 802.11 - MAC

- MAC layer covers three functional areas:
  - Reliable data delivery
  - Access control
  - Security

- More efficient to deal with errors at the MAC level than higher layer (such as TCP)
- Frame exchange protocol
  - Source station transmits data
  - Destination responds with acknowledgment (ACK)
  - If source doesn’t receive ACK, it retransmits frame
- Four frame exchange
  - Source issues request to send (RTS)
  - Destination responds with clear to send (CTS)
  - Source transmits data
  - Destination responds with ACK

Wireless LAN - IEEE 802.11 - MAC

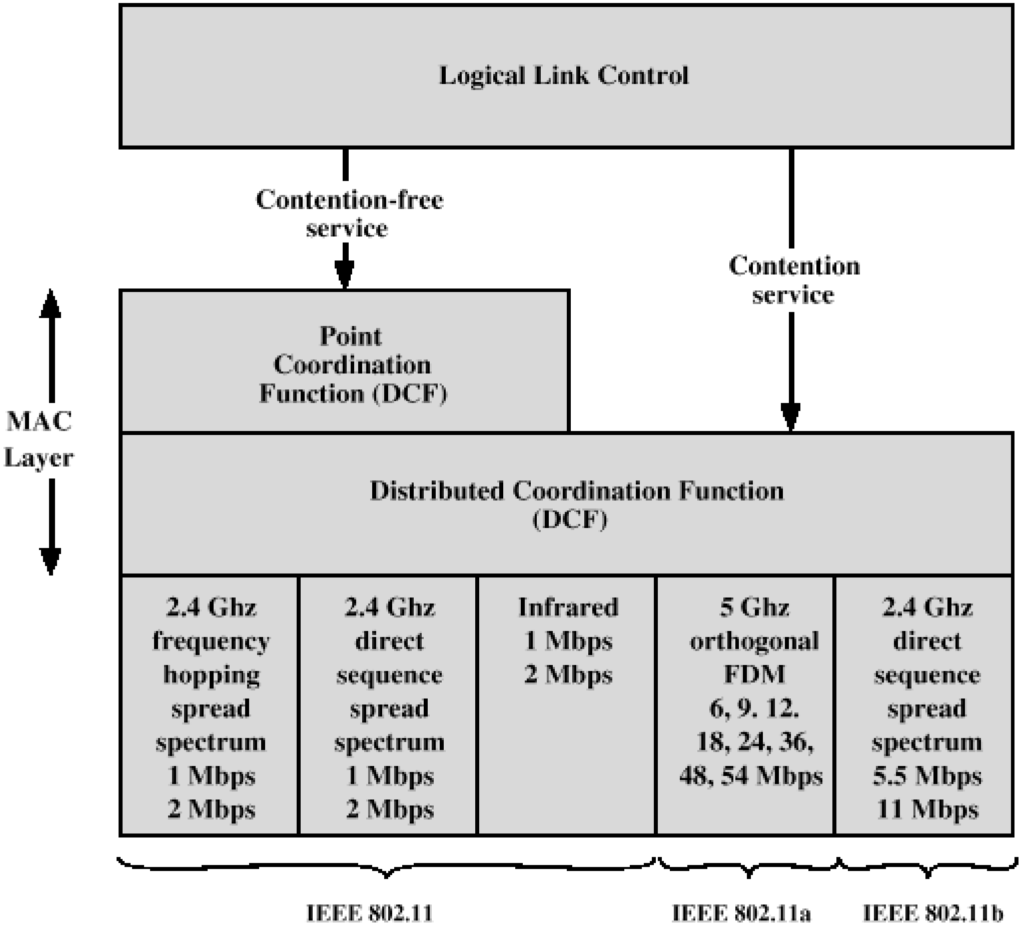

Logical Link Control
Contention-free service
Contention service
Point Coordination Function (DCF)
MAC Layer
Distributed Coordination Function (DCF)
2.4 Ghz frequency hopping spread spectrum 1 Mbps 2 Mbps
2.4 Ghz direct sequence spread spectrum 1 Mbps 2 Mbps
Infrared 1 Mbps 2 Mbps
5 Ghz orthogonal FDM 6, 9. 12. 18, 24, 36, 48, 54 Mbps
2.4 Ghz direct sequence spread spectrum 5.5 Mbps 11 Mbps
IEEE 802.11
IEEE 802.11a
IEEE 802.11b

Figure 14.5 IEEE 802.11 Protocol Architecture

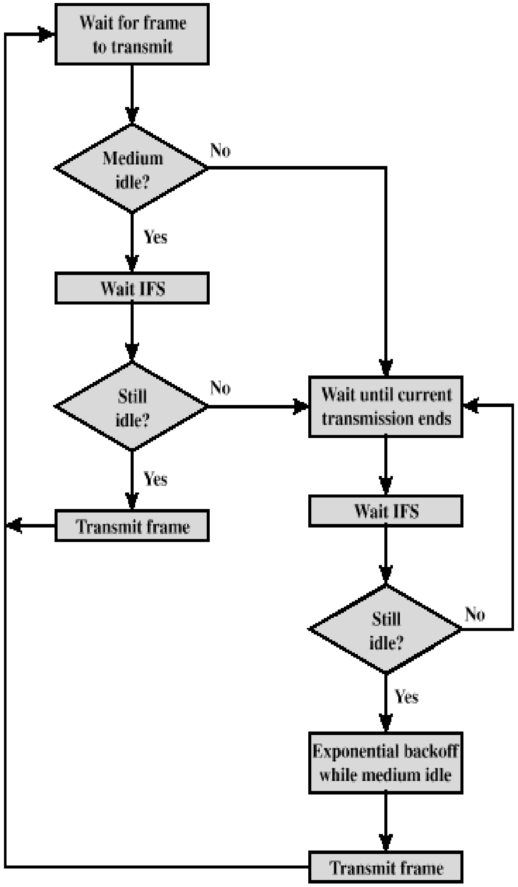

Wait for frame to transmit
Medium idle?
No
Yes
Wait IFS
Still idle?
No
Yes
Transmit frame
Wait until current transmission ends
Wait IFS
Still idle?
No
Yes
Exponential backoff while medium idle
Transmit frame

Figure 14.6 IEEE 802.11 Medium Access Control Logic

Wireless LAN - IEEE 802.11 - MAC

Basic Logic:

- A station with a frame to transmit senses the medium (channel).
- IF IDLE → waits to see if the channel remains idle for a time equal to IFS. If so, the station may transmit immediately.
- IF BUSY → (either because the station initially finds the channel busy or because the channel becomes busy during the IFS idle time), the station defers transmission and continues to monitor the channel until the current transmission is over.
- Once the current transmission is over, the station delays another IFS.
- If the medium remains idle for this period, the station backs off using a binary exponential backoff scheme and again keeps sensing the medium.
- The station picks up a random number of slots (the initial value of backoff counter) within a contention window to wait before transmitting its frame.

Networking of Sensors!!!

Specific Factors (v.s. typical Ad-Hoc Networks…)

A. Fault Tolerance (Reliability)

B. Scalability

C. Production Costs

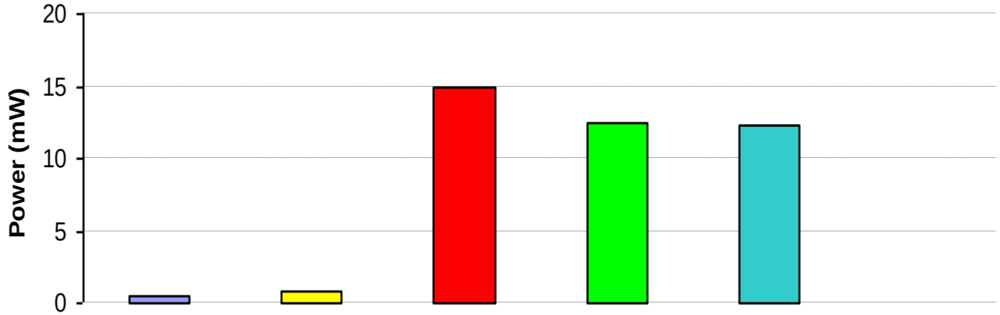
D. Hardware Constraints

E. Sensor Network Topology

F. Operating Environment (Applications)

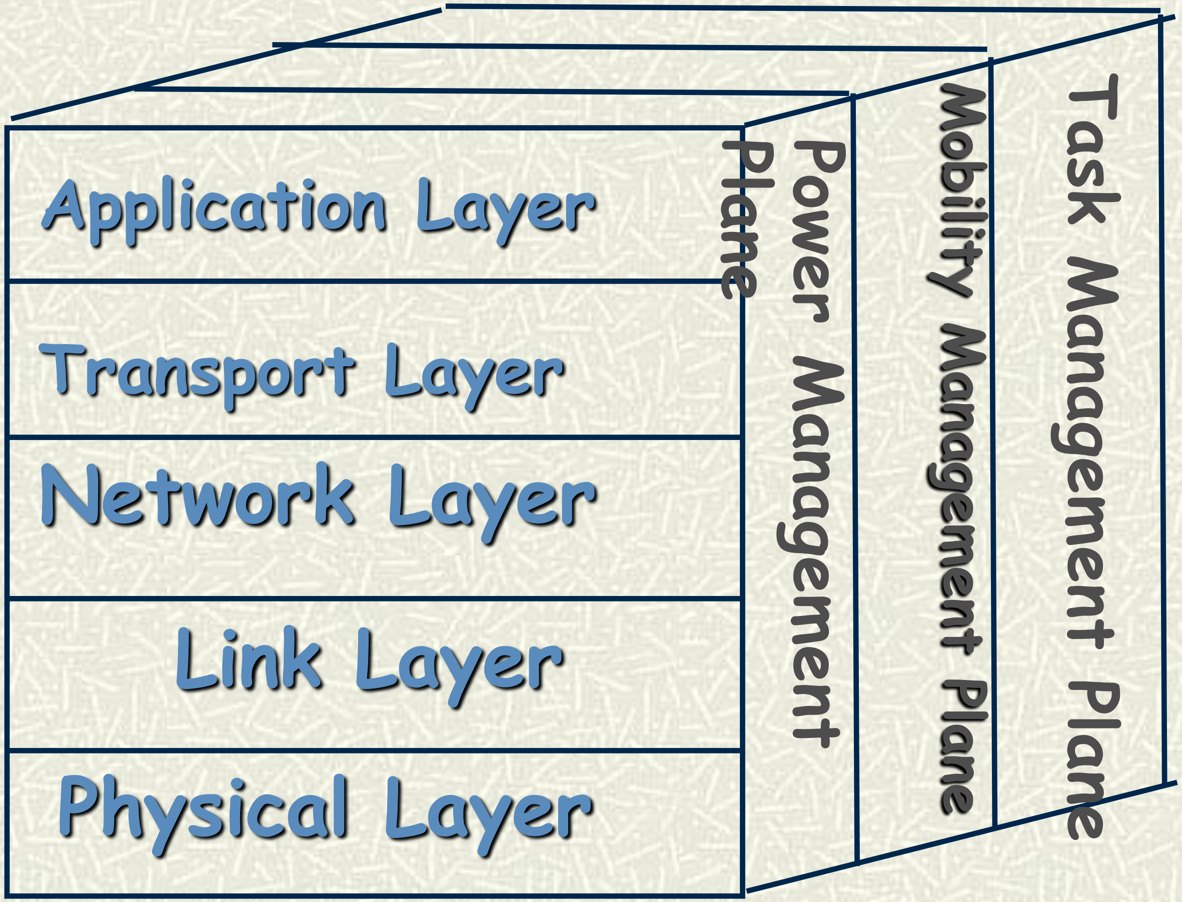
G. Transmission Media

H. Power Consumption (Lifetime)



Networking of Sensors

"Orthogonal Dimensions" of the Protocol…



Application Layer

Transport Layer

Network Layer

Link Layer

Physical Layer

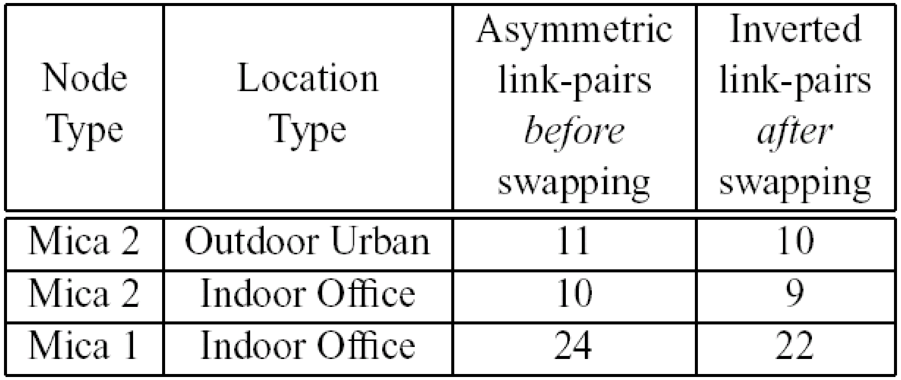
Power Management Plane

Mobility Management Plane

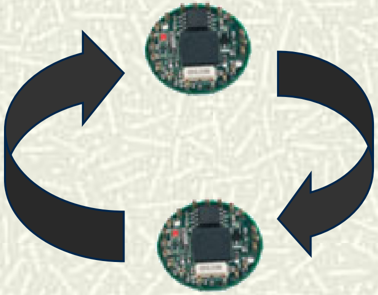
Task Management Plane

Networking of Sensors (Ex: Assymetry of Links)

- **Node A can transmit to Node B but Node B cannot transmit to Node A!!!**
- Why are asymmetric links a problem?
  - A thinks B is a neighbor and sends packet to B but never gets an ACK!
  - Existence of asymmetries requires careful identification of “good neighbors”
- Do the laws of physics allow for the existence of asymmetric links?
  - NO – transmitted signal strength, path loss, shadow fading, and multipath fading are all *symmetric* effects



Node Type	Location Type	Asymmetric link-pairs *before* swapping	Inverted link-pairs *after* swapping
Mica 2	Outdoor Urban	11	10
Mica 2	Indoor Office	10	9
Mica 1	Indoor Office	24	22



- When swapping the asymmetric links node pairs, the asymmetric links were inverted (91.1% ± 8.32)

- Link asymmetries are caused by differences in hardware calibration and not by the environment

Networking of Sensors (MAC-Issues)

WSN Architecture

- High density of nodes
- Increased collision probability
- Signaling overhead should be minimized to prevent further collisions
- Sophisticated and simple collision avoidance protocols required

Limits and Variability of Energy Resources

- Connectivity and the performance of the network is affected as nodes die
- Transmitting and receiving consumes almost same energy
- Frequent power up/down eats up energy
- Need very low power MAC protocols
- Minimize signaling overhead
- Avoid idle listening
- Prevent frequent radio state changes (active - sleep)

Networking of Sensors (MAC-Issues)

Cheap node requirement prevents sophisticated encoders/decoders to be implemented

- Cheap node requirement prevents expensive clock-crystals to be implemented
- Synchronization problems (TDMA-based schemes are not practical)
- Observed data depends on physical phenomenon (Spatial and temporal correlation in the physical)

-Complex algorithms cannot be implemented

-Conventional layered architecture may not be appropriate

-Centralized or local management is limited

- Simple scheduling algorithms required

-Cross-layer optimization required

-Self-configurable, distributed protocols required

Energy Waste

- Idle listening
  - E.g., in anticipation of a packet
- Collision
  - Collided packets are typically discarded (⇒ re-transmit)
- Overhearing/Overemitting
- Extra control-packets

Possible Solutions:

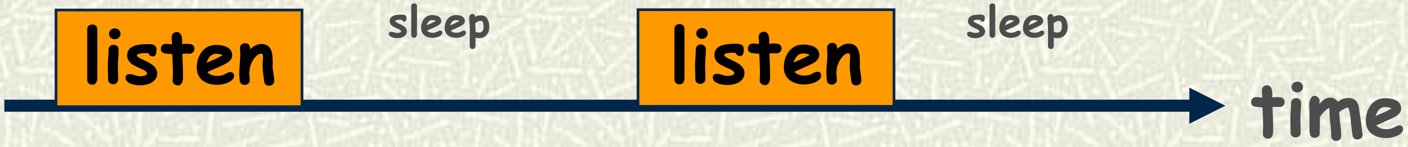
- Duty cycling (S-MAC; T-MAC)
- Energy-aware scheduling
- Scheduled Rendezvous
- Directed Antennae

Example: SLEEP MAC (S-MAC)

Problem: "Idle Listening" consumes significant energy

Example: in Mica2 motes: transmission costs 81mW; idle listening costs 30mW; ***Sleep "costs" 0.003 mW***

Solution: Periodic listen and sleep



- During sleeping, radio is turned off
- Reduce duty cycle to ~ 10% (Listen for 120ms and sleep for 2s)

Latency ☹ → ☺ **Energy**

S-MAC

- Each node goes into periodic sleep mode during which it switches the radio off and sets a timer to awake later

- When the timer expires it wakes up and listens to see if any other node wants to talk to it

- The duration of the sleep and listen cycles are application dependent and they are set the same for all nodes

* Requires a periodic synchronization among nodes to take care of any type of clock drift

- All nodes are free to choose their own listen/sleep schedules.

- To reduce control overhead, only neighboring nodes are synchronized together.

- They listen at the same time and go to sleep at the same time.

S-MAC: Synchronization

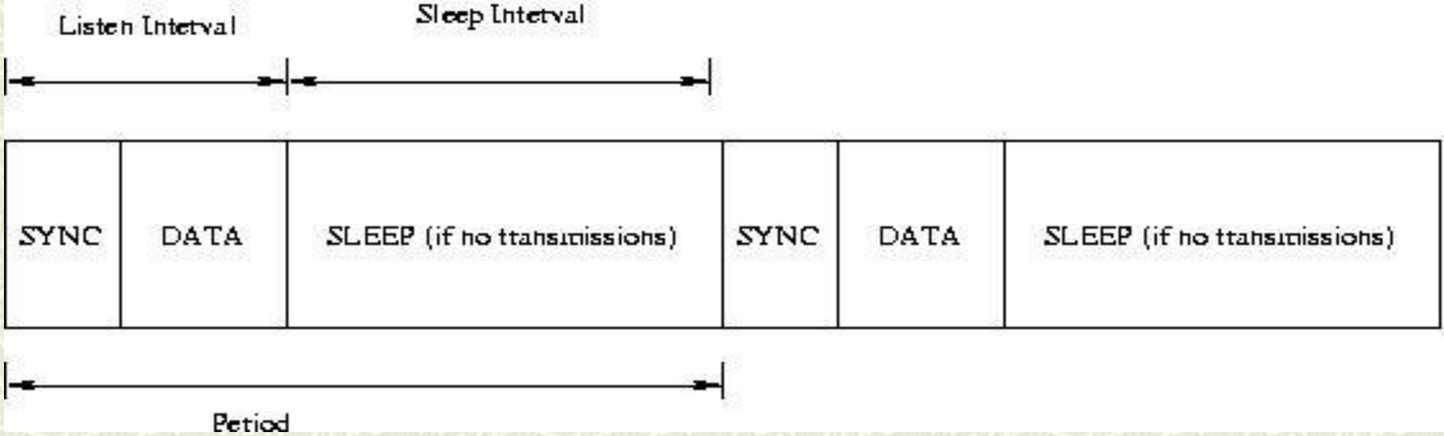
- SYNC packets are exchanged periodically to maintain schedule synchronization.

SYNC PACKET

Sender Node ID	Next Sleep Time

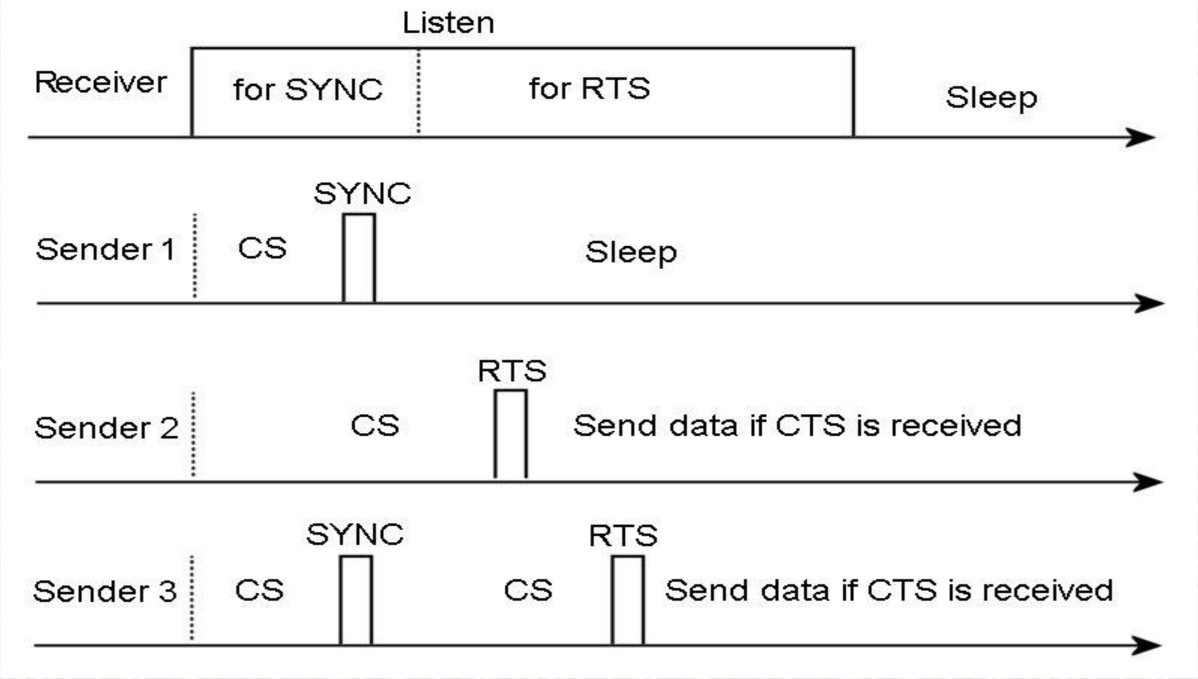
SYNCH

- Synchronization Period: Period for a node to send a SYNC packet.
- Receivers will adjust their timer counters immediately after they receive the SYNC packet



Maintaining Synchronization

Listen interval is divided into two parts: one for receiving SYNC packets and other for receiving RTS (Request To Send)



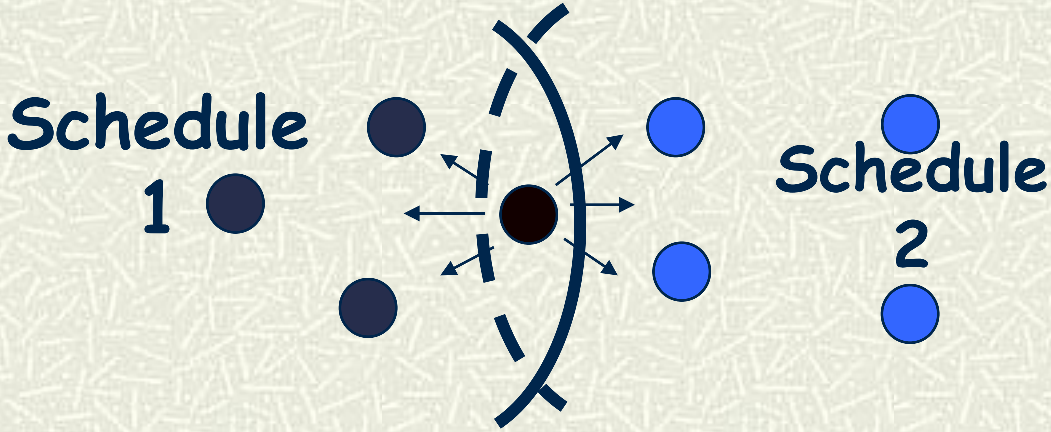
- If it does not hear a schedule from another node, it randomly chooses a schedule and broadcasts its schedule with a SYNC packet immediately
- This node is called a Synchronizer

- If a node receives a schedule from a neighbor before choosing its own schedule, it just follows this neighbor's schedule, i.e. becomes a Follower and it waits for a random delay and broadcasts its schedule

- Each node maintains a schedule table that stores schedules of all its known neighbors
- For initial schedule, DO:
  - A node first listens to the medium for a certain amount of time (at least the synchronization period)

Coordinated Sleeping

- In a large network, we cannot guarantee that all nodes follow the same schedule.
- The node on the border will follow both schedules.
- When it broadcasts a packet, it needs to do it twice, first for nodes on schedule 1 and then for those on schedule 2.



* Border nodes have less time to sleep and consume more energy than others.

OPTION: Let border node adopt only one schedule (say, whichever was received first).

Collision Avoidance

- S-MAC is based on contention, i.e., if multiple neighbors want to talk to a node at the same time, they will try to send when the node starts listening.

* Similar to IEEE802.11, i.e., perform carrier sense before initiating a transmission

* If a node fails to get the medium, it goes to sleep and wakes up when the receiver is free and listening again

* Broadcast packets are sent without using RTS/CTS.

* Unicast data packets follow the sequence of RTS/CTS/DATA/ACK between the sender and receiver

Collision Avoidance

Duration field in each transmitted packet indicates how long the remaining transmission will be so if a node receives a packet destined to another node, it knows how long it has to keep silent

* The node records this value in network allocation vector (NAV) and sets a timer for it

* When a node has data to send, it first looks at NAV.

* If this value is not zero, then medium is busy (virtual carrier sense)

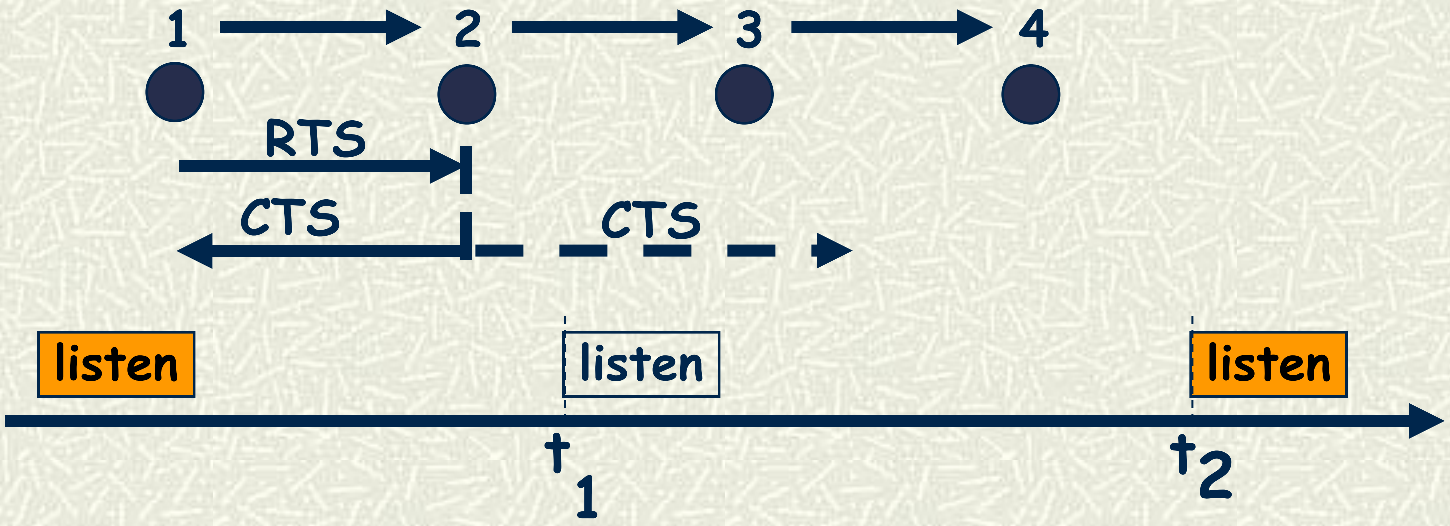
* The medium is determined as free if both virtual and physical carrier sense indicate the medium is free

* All immediate neighbors of both the sender and receiver should sleep after they hear RTS or CTS packet until the current transmission is over

Adaptive Listening in S-MAC

GOAL- Reduce multi-hop latency due to periodic sleep

BASIC IDEA: Let the node who overhears its neighbor’s transmission stay awake



- Both neighbors will learn about how long the transmission is from the duration field in the RTS and CTS packets.
- They are able to adaptively wake up when the transmission is over.
- Reduce latency by at least half
- (e.g., CTS of 2 is heard by 3 also ⇒ 3 remains awake!!)

Message Passing in S-MAC

- Long messages are broken down in to smaller packets and sent continuously once the channel is acquired by RTS/CTS handshake.

- Increases the sleep time, but leads to fairness problems.

Moral of the story…

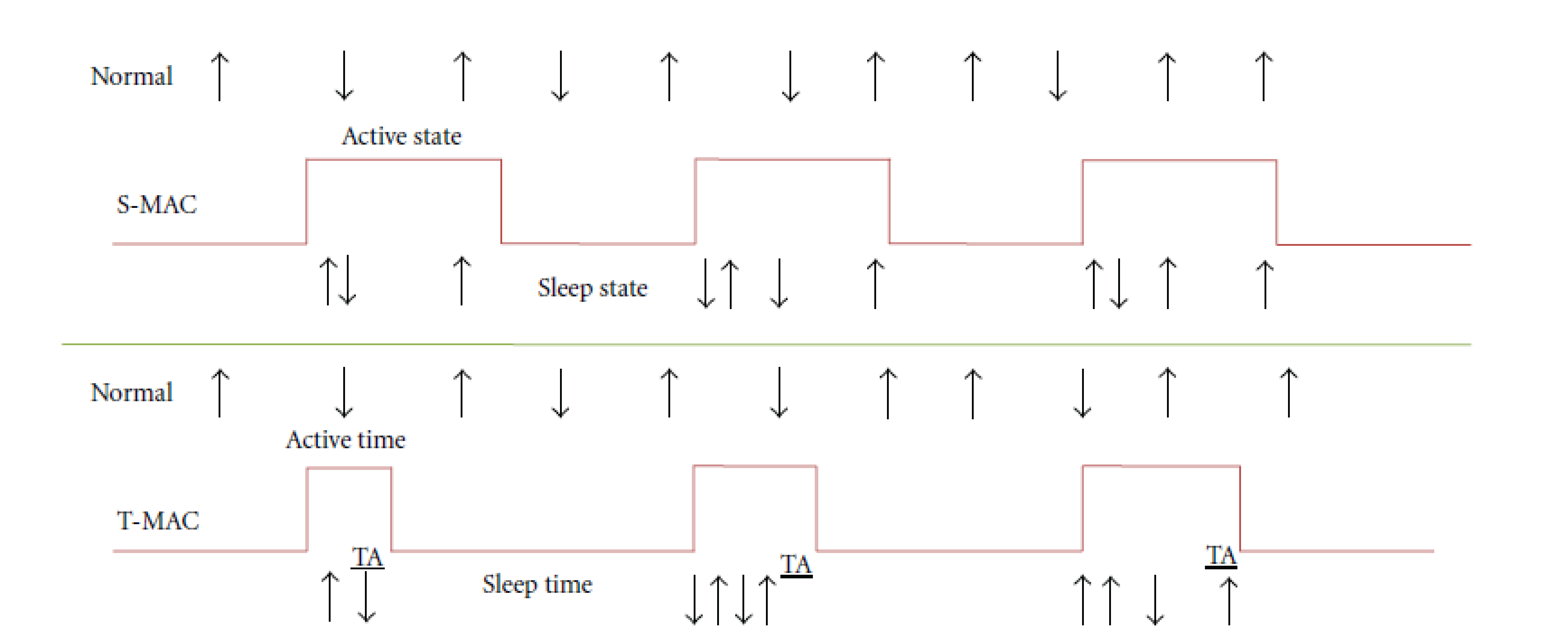
- S-MAC consumes much less energy than 802.11-like protocol without sleeping

- At heavy load, idle listening rarely happens, energy savings from sleeping is very limited. S-MAC achieves energy savings by avoiding overhearing and efficiently transmitting long messages.

* At light load, periodic sleeping plays the key role

Other MAC management

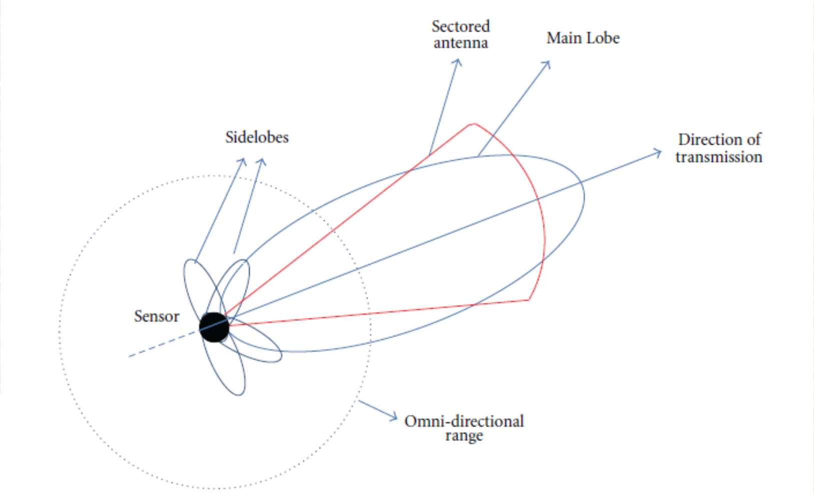
- T-MAC:
  - Adaptive improvement over duty-cycling
- Listening period ends when no event occurred for a time-period TA.
  - Plus: bursts of messages of variable lengths
  - Possible problem: early-sleep…

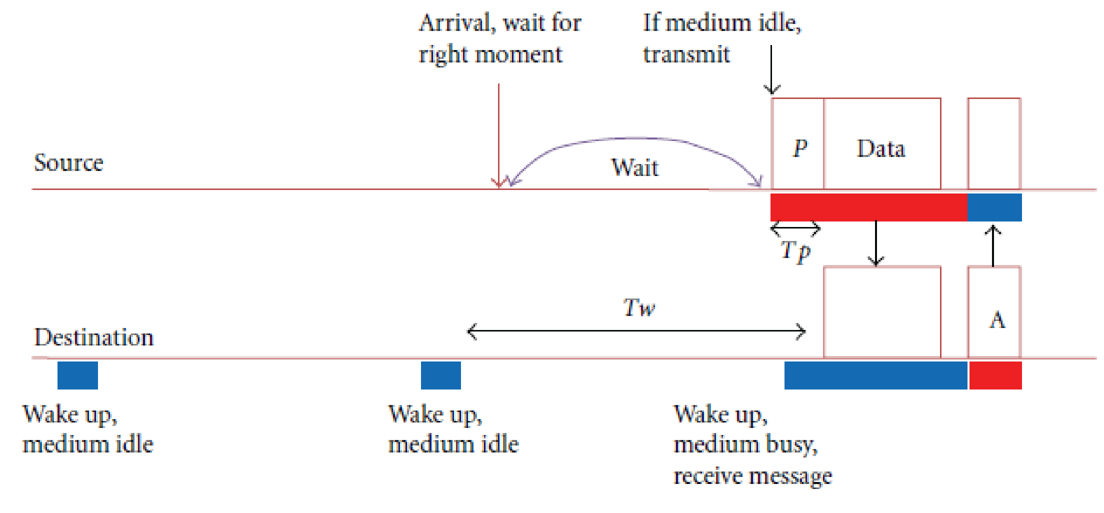


Other MAC management

- WiseMAC:
    - Synchronize the preamble-sampling (i.e., regularly sample the medium, and determine the length of the preamble)

Directional Antennae





“External Support” of MAC management

- Energy-Aware/Efficient Routing Algorithms
- Energy-Aware/Efficient Topology Control
- Data Aggregation

- **NOTE:**
  - There’ll always be trade-offs, e.g.,
    - Energy vs. Security;
    - Energy vs. Robustness/Multipath
    - Energy-expense vs. Lifetime (not trivial)

(Many, MANY MAC-related works)

Reading:

A SURVEY OF MAC PROTOCOLS FOR SENSOR NETWORKS
by Piyush Naik and Krishna M. Sivalingam (posted on the Blackboard)

Additional Readings:

J. Polastre, J. Hill, D. Culler, “Versatile Low Power Media Access for WSNs”, Proc. of ACM SenSys, Nov. 2004

S. Kumar, V. S. Raghavan and J. Deng, “Medium Access Control for Ad-Hoc Wireless Networks: a survey”, AdHoc Networks, 4(3), 2006.

I. Dietrich and F. Dressler, “On the Lifetime of Wireless Sensor Networks”, ACM Transactions on Sensor Networks, 5(1), 2009.