Outline

• Introduction to Networked Embedded Systems
  - Embedded systems ➔ Networked embedded systems ➔ Embedded Internet
  - Network properties

• Layered Network Architectures
  - OSI framework – descriptions of layers
  - Internet protocol stack

• Physical Layer Options
  - Guided transmission media
  - Wireless transmission media

• Data Link Layer Services and MAC Protocols

• Embedded System Communication Protocols
  - Wired protocols: Ethernet, CAN, TTP, BACnet
  - Wireless protocols: Wi-Fi, ZigBee, WirelessHART

• TCP/IP Stack and 6LoWPAN Stack

• Modeling and Analysis of Communication Protocols
NETWORKS FOR ALL SIZES AND SCALES

- **NoCs** – connecting processors inside MPSoCs
- **SPI, I2C, UART**… – connecting discrete components inside boards
- **USB, FireWire**… – connecting peripherals around a PC
- **Bluetooth, RFID, NFC**… – connecting peripherals or sensors in small areas (BANs, PANs ...)
- **CAN, fieldbuses**… – connecting sensors, actuators and controlling equipment in a monitoring or control system (DCS)
- **Zigbee, WirelessHART**… – connection of self-organized wireless sensors (WSNs)
- **Ethernet, WiFi**… – connection of PCs and equipment in local areas (LANs)
- **10G Ethernet, ATM**… – connection of large systems in large areas (MANs, WANs)
- **GSM, LTE, WiMax**… – wide area communications (MANs, WANs)
WHY NETWORKED AND DISTRIBUTED ARCHITECTURE

• Processing closer to data source / sink
  - Intelligent sensors and actuators
  - Reduce the computational overhead on the central processing node

• Dependability
  - Error-containment within nodes

• Composability
  - System composition by integrating components and subsystems

• Scalability
  - Easy addition of new nodes with new or replicated functionality
  - Especially for wireless

• Maintainability
  - Modularity and easy node replacement
  - Simplification of the cabling, especially for wireless
Distributed Embedded Systems

- System-centered (designed as a whole)
  - Confined in space (despite possibly large)
  - Normally fixed set of components
  - Preference for wired networks with fixed topology

- Most common non-functional requirements
  - Real-time
    - End-to-end constraints on response to stimuli
    - Jitter constraints on periodic activities
  - Dependability
    - Ultra high reliability and safety, high availability
  - Composability
  - Maintainability
Networked Embedded Systems

- Interconnected stand-alone equipment or systems for extra functionality (communication-centered)
  - Fuzzy notion of global system
  - Variable set of components
  - A combination of wireless/wired networks
    - Structured / Ad-hoc connections
    - Varying topology
    - Multi-hop communication

- Most common non-functional requirements
  - Scalability
  - Heterogeneity
  - Self-configuration
  - (Soft) real-time
NETWORK PROPERTIES

• Supported topologies
  - star, line, tree, mesh, bus, ring…

• Media access mechanisms
  - controlled access vs. uncontrolled access

• Network performance metrics
  - Bandwidth, throughput and goodput

• Network real-time performance
  - latency, jitter, coherent notion of time

• Network Security
  - Cryptosecurity, Emission, Transmission and Physical security
Outline

• Introduction to Networked Embedded Systems
  - Embedded systems ➔ Networked embedded systems ➔ Embedded Internet
  - Network properties

• Layered Network Architectures
  - OSI framework – descriptions of layers
  - Internet protocol stack

• Physical Layer Options
  - Guided transmission media
  - Wireless transmission media

• Data Link Layer Services and MAC Protocols

• Embedded System Communication Protocols
  - Wired protocols: Ethernet, CAN, TTP, BACnet
  - Wireless protocols: Wi-Fi, ZigBee, WirelessHART

• TCP/IP Stack and 6LoWPAN Stack

• Modeling and Analysis of Communication Protocols
Layer architecture simplifies the network design.
- Explicit structure allows identification, relationship of complex system’s pieces.
- Modularization eases maintenance, updating of system.
- Change of implementation of layer’s service transparent to rest of system.

It is easy to debug network applications with a layered architecture.

The network management is easier due to the layered architecture.

Network layers follow a set of rules, called protocol.

The protocol defines the format of the data being exchanged, and the control and timing for the handshake between layers.
Structured layering implies that the functions of each layer are carried out completely before the protocol data unit is passed to the next layer. This means that the optimization of each layer has to be done separately. Such ordering constraints are in conflict with efficient implementation of data manipulation functions.
ISO/OSI REFERENCE MODEL

- **Application**: Network processes to applications
  - FTP, SMTP, HTTP…
- **Presentation**: Data representation
  - encryption, compression, machine-specific conventions
- **Session**: Interhost communication
  - synchronization, checkpointing, recovery of data exchange
- **Transport**: End-to-end connections
  - TCP, UDP
- **Network**: Addressing and routing
  - IP, routing protocols
- **Link**: Access to media
  - Ethernet, 802.111 (WiFi), PPP
- **Physical**: bits “on the wire”
INTERNET PROTOCOL STACK

- Internet stack “missing” presentation and session layers.
  - These services, if needed, must be implemented in applications.

- **Application**: supporting network applications
  - FTP, SMTP, HTTP
- **Transport**: process data transfer
  - TCP, UDP
- **Network**: routing of datagrams from source to destination
  - IP, routing protocols
- **Link**: data transfer between neighboring network elements
  - Ethernet, 802.111 (WiFi), PPP
- **Physical**: bits “on the wire”
EMBEDDED / REAL-TIME PROTOCOL STACK

• The OSI 7 layers impose a considerable overhead
  - Time to execute the protocol stack
  - Time to transmit protocol control information
  - Memory requirements (for all intermediate protocol invocations)

• Many embedded / real-time networks
  - are dedicated to a well defined application
  - use single broadcast domain (no need for routing)
  - use short messages (no need to fragment/reassemble)

Figure from Dr. Luis Almeida
Outline

• Introduction to Networked Embedded Systems
  - Embedded systems ➔ Networked embedded systems ➔ Embedded Internet
  - Network properties

• Layered Network Architectures
  - OSI framework – descriptions of layers
  - Internet protocol stack

• Physical Layer Options
  - Guided transmission media
  - Wireless transmission media

• Data Link Layer Services and MAC Protocols

• Embedded System Communication Protocols
  - Wired protocols: Ethernet, CAN, TTP, BACnet
  - Wireless protocols: Wi-Fi, ZigBee, WirelessHART

• TCP/IP Stack and 6LoWPAN Stack

• Modeling and Analysis of Communication Protocols
GUIDED TRANSMISSION MEDIA

Magnetic Media

- HP Ultrium tape = 100GB. A box 60x60x60 holds 2000 tapes => 200 Tera bytes = 1600 Tbits.
- A box can be delivered in 24 hours anywhere in USA => throughput: 1600 Tbits/86400 sec = 19 Gbps!

Twisted Pair/ Unshielded TP (UTP)

- Classic telephone lines
  - Category 3 (a) – 16MHz
  - Category 5 (b) – 100 MHz
  - Category 6 – 250 MHz
  - Category 7 – 600 MHz

- Works up to 100m, afterwards repeaters needed.
GUIDED TRANSMISSION MEDIA (CONT.)

Coaxial Cable
- Bandwidth ~ 1 GHz (better shielding)
- Up to 200m

Fiber Optics
- Rather used at higher bandwidths
- Invulnerable to electric and electromagnetic signals
- Could be very long
- Hard to tamper with -> Security
- Usually simplex transmission
THE ELECTROMAGNETIC SPECTRUM

VLF = Very Low Frequency                   UHF = Ultra High Frequency
LF = Low Frequency SHF = Super High Frequency
MF = Medium Frequency EHF = Extra High Frequency
HF = High Frequency UV = Ultraviolet Light
VHF = Very High Frequency

- Frequency and wave length: $\lambda = c/f$, wave length $\lambda$, speed of light $c \approx 3 \times 10^8$ m/s, frequency $f$

- Radio spectrum is part of the electromagnetic spectrum from 1Hz to 3THz:
DATA LINK LAYER SERVICES

• Framing, link access:
  - encapsulate datagram into frame, adding header, tailer
  - channel access if shared medium
  - “MAC” addresses used in frame headers to identify source, destination

• Reliable delivery between adjacent nodes
  - Seldom used on low bit-error link (fiber, some twisted pair)
  - wireless links: high error rates

• Flow control:
  - Pacing between adjacent sending and receiving nodes

• Error detection:
  - Errors caused by signal attenuation, noise.
  - Receiver detects presence of errors: signals sender for retransmission or drops frame

• Error correction:
  - Receiver identifies and corrects bit error(s) without resorting to retransmission

• Half-duplex and full-duplex
  - with half duplex, nodes at both ends of link can transmit, but not at same time
MULTIPLE ACCESS PROTOCOLS

- Single shared broadcast channel
- Two or more simultaneous transmissions by nodes: interference
  - *Collision* if node receives two or more signals at the same time

Multiple Access Protocol

- distributed algorithm that determines how nodes share channel, i.e.,
  determine when node can transmit.
- communication about channel sharing must use channel itself.
  - no out-of-band channel for coordination
AN IDEAL MULTIPLE ACCESS PROTOCOL

given: broadcast channel of rate $R$ bps

desiderata:

1. when one node wants to transmit, it can send at rate $R$.
2. when $M$ nodes want to transmit, each can send at average rate $R/M$.
3. fully decentralized:
   - no special node to coordinate transmissions
   - no synchronization of clocks, slots
4. simple
MAC PROTOCOLS: TAXONOMY

Three broad classes:

• **Channel partitioning**
  - divide channel into smaller “pieces” (time slots, frequency, code)
  - allocate piece to node for exclusive use

• **Random access**
  - channel not divided, allow collisions
  - “recover” from collisions

• **“Taking turns”**
  - nodes take turns, but nodes with more to send can take longer turns
RANDOM ACCESS PROTOCOLS

• When node has packet to send:
  - Transmit at full channel data rate R.
  - No *a priori* coordination among nodes
  - Two or more transmitting nodes ➔ “collision”

• **Random access MAC protocol** specifies:
  - How to detect collisions
  - How to recover from collisions (e.g., via delayed retransmissions)

• Examples of random access MAC protocols:
  - Slotted ALOHA
  - ALOHA
  - CSMA, CSMA/CD, CSMA/CA
SLOTTED ALOHA

Pros:

• Single active node can continuously transmit at full rate of channel
• Highly decentralized: only slots in nodes need to be in sync
• Simple

Cons:

• Collisions, wasting slots
• Idle slots
• Nodes may be able to detect collision in less than time to transmit packet
• Clock synchronization
SLOTTED ALOHA: EFFICIENCY

**efficiency**: long-run fraction of successful slots (many nodes, all with many frames to send)

- Suppose: N nodes with many frames to send, each transmits in slot with probability p
- Prob that given node has success in a slot = p(1-p)^N-1
- Prob that any node has a success = Np(1-p)^N-1
- Max efficiency: find p* that maximizes Np(1-p)^N-1
- For many nodes, take limit of Np*(1-p*)^N-1 as N goes to infinity, gives:
  \[ \text{max efficiency} = \frac{1}{e} = 0.37 \]

At best: channel used for useful transmissions 37% of time!
PURE (UNSLOTTED) ALOHA

- Unslotted Aloha: simpler, no synchronization
- When frame first arrives:
  - transmit immediately
- Collision probability increases:
  - frame sent at $t_0$ collides with other frames sent in $[t_0-1, t_0+1]$
P(success by given node) = P(node transmits) \cdot 
\begin{align*}
P(\text{no other node transmits in } [t_0-1, t_0]) \cdot P(\text{no other node transmits in } [t_0, t_0+1]) \\
= p \cdot (1-p)^{N-1} \cdot (1-p)^{N-1} \\
= p \cdot (1-p)^{2(N-1)}
\end{align*}

\ldots \text{choosing optimum } p \text{ and then letting } n \to \infty \\
= 1/(2e) = .18

\text{even worse than slotted Aloha!}
CSMA (CARRIER SENSE MULTIPLE ACCESS)

**CSMA:** listen before transmit

- If channel sensed idle: transmit entire frame
- If channel sensed busy: defer transmission
- Human analogy: don’t interrupt others!
CSMA/CD (COLLISION DETECTION)

**CSMA/CD**: carrier sensing, deferral as in CSMA

- collisions detected within short time
- colliding transmissions aborted, reducing channel wastage

- Collision detection:
  - easy in wired media: measure signal strengths, compare transmitted, received signals
  - difficult in wireless media: received signal strength overwhelmed by local transmission strength

- Human analogy: the polite conversationalist
CSMA/CA (COLLISION AVOIDANCE)

- **CSMA/CA:**
  - Wireless MAC protocols often use collision avoidance techniques, in conjunction with a (physical or virtual) carrier sense mechanism.
  - To be discussed more in WiFi and ZigBee protocols.

- **Collision avoidance**
  - Nodes hearing RTS or CTS stay silent for the duration of the corresponding transmission.
  - Once channel becomes idle, the node waits for a randomly chosen duration before attempting to transmit.

- **Carrier sense**
  - Nodes stay silent when carrier sensed (physical/virtual)
  - Physical carrier sense: carrier sense threshold
  - Virtual carrier sense using Network Allocation Vector (NAV): NAV is updated based on overheard RTS/CTS/DATA/ACK packets.
“TAking Turns” MAC Protocols

Channel partitioning MAC protocols:

• Share channel *efficiently* and *fairly* at high load

• Inefficient at low load: delay in channel access, 1/N bandwidth allocated even if only 1 active node!

Random access MAC protocols

• Efficient at low load: single node can fully utilize channel

• High load: collision overhead

“taking turns” protocols

• Look for best of both worlds.
SUMMARY OF MAC PROTOCOLS

• Channel partitioning, by time, frequency or code
  - Time Division, Frequency Division

• Random access (dynamic)
  - ALOHA, S-ALOHA, CSMA, CSMA/CD
  - Carrier sensing: easy in some technologies (wire), hard in others (wireless)
  - CSMA/CD used in Ethernet
  - CSMA/CA used in 802.11

• Taking turns
  - Polling from central site, token passing
  - Bluetooth, FDDI, token ring
Outline

• Introduction to Networked Embedded Systems
  - Embedded systems ➔ Networked embedded systems ➔ Embedded Internet
  - Network properties

• Layered Network Architectures
  - OSI framework – descriptions of layers
  - Internet protocol stack

• Physical Layer Options
  - Guided transmission media
  - Wireless transmission media

• Data Link Layer Services and MAC Protocols

• Embedded System Communication Protocols
  - Wired protocols: Ethernet, CAN, TTP, BACnet
  - Wireless protocols: Wi-Fi, ZigBee, WirelessHART

• TCP/IP Stack and 6LoWPAN Stack

• Modeling and Analysis of Communication Protocols
EMBEDDED SYSTEM COMMUNICATION PROTOCOLS

Wired communication protocol examples:

• Ethernet (802.3)
• CAN
• TTP
• BACnet

Wireless communication protocol examples:

• Wi-Fi (802.11)
• ZigBee (based on 802.15.4 PHY and MAC)
• WirelessHART (Not discussed in this lecture)
INFRASTRUCTURE VS. AD-HOC NETWORKS

infrastructure network

AD-HOC NETWORK

AP: Access Point

wired network
802.11: INFRASTRUCTURE

- **Station (STA)**
  - terminal with access mechanisms to the wireless medium and radio contact to the access point

- **Access Point**
  - station integrated into the wireless LAN and the distribution system

- **Basic Service Set (BSS)**
  - group of stations using the same AP

- **Portal**
  - bridge to other (wired) networks

- **Distribution System**
  - interconnection network to form one logical network (EES: Extended Service Set) based on several BSS
802.11: AD HOC MODE

Direct communication within a limited range

- Station (STA): terminal with access mechanisms to the wireless medium
- Independent Basic Service Set (IBSS): group of stations using the same network
WLAN: IEEE 802.11B

• Data rate
  - 1, 2, 5.5, 11 Mbit/s, depending on SNR
  - User data rate max. approx. 6 Mbit/s

• Transmission range
  - 300m outdoor, 30m indoor
  - Max. data rate ~10m indoor

• Frequency
  - Free 2.4 GHz ISM-band

• Availability
  - Many products and vendors

• Quality of Service
  - Best effort, no guarantees (unless polling is used, limited support in products)

• Pros
  - Many installed systems and vendors
  - Available worldwide
  - Free ISM-band

• Cons
  - Heavy interference on ISM-band
  - No service guarantees
  - Relatively low data rate
### WLAN: IEEE 802.11A

#### Data rate
- 6, 9, 12, 18, 24, 36, 48, 54 Mbit/s, depending on SNR
- User throughput (1500 byte packets): 5.3 (6), 18 (24), 24 (36), 32 (54)
- 6, 12, 24 Mbit/s mandatory

#### Transmission range
- 100m outdoor, 10m indoor
- E.g., 54 Mbit/s up to 5 m, 48 up to 12 m, 36 up to 25 m, 24 up to 30m, 18 up to 40 m, 12 up to 60 m

#### Frequency
- Free 5.15-5.25, 5.25-5.35, 5.725-5.825 GHz ISM-band

#### Availability
- Some products, some vendors

#### Quality of Service
- Best effort, no guarantees (same as all 802.11 products)

#### Pros
- Fits into 802.x standards
- Free ISM-band
- Available, simple system
- Uses less crowded 5 GHz band
- Higher data rates

#### Cons
- Shorter range
WLAN: IEEE 802.11N

- **Data rate**
  - 7.2, 14.4, 21.7, 28.9, …, 72.2 Mbit/s, depending on SNR

- **Multiple input multiple output (MIMO)**

- **20MHz and 40MHz bands**

- **Transmission range**
  - Increase range by several factors due to MIMO

- **Frequency**
  - Free 2.4GHz ISM-band
  - Free 5.15-5.25, 5.25-5.35, 5.725-5.825 GHz ISM-band

- **Availability**
  - Some products, some vendors

- **Quality of Service**
  - Best effort, no guarantees (same as all 802.11 products)

- **Pros**
  - Fits into 802.x standards
  - Free ISM-band
  - Available, simple system
  - Uses dual band
  - Higher data rates

- **Cons**
  - Interference on ISM-band
Distributed and centralized access methods

- DCF CSMA/CA (mandatory)
  - Collision avoidance via randomized “back-off“ mechanism
  - Minimum distance between consecutive packets
  - ACK packet for acknowledgements (not for broadcasts)
- DCF w/ RTS/CTS (optional)
  - Distributed Foundation Wireless MAC
  - Avoids hidden terminal problem
- PCF (optional)
  - Access point polls terminals according to a list
Before a node transmits, it listens for activity on the network.

If medium is busy, node waits to transmit.

After medium is clear, don't immediately start transmitting...

Otherwise all nodes would start talking at the same time!

Instead, delay a random amount of time (random backoff).
Priorities defined through different inter frame spaces

- No guarantee, hard priorities
- SIFS (Short Inter Frame Spacing)
  - Highest priority, for ACK, CTS, polling response
- PIFS (PCF IFS)
  - Medium priority, for time-bounded service using PCF
- DIFS (DCF, Distributed Coordination Function IFS)
  - Lowest priority, for asynchronous data service
HIDDEN TERMINAL PROBLEM

- B can communicate with both A and C
- A and C cannot hear each other

**Problem**
- When A transmits to B, C cannot detect the transmission using the carrier sense mechanism
- If C transmits, collision will occur at node B

**Solution**
- Hidden sender C needs to defer
SOLUTION FOR HIDDEN TERMINAL PROBLEM: MACA

- When A wants to send a packet to B, A first sends a Request-to-Send (RTS) to B

- On receiving RTS, B responds by sending Clear-to-Send (CTS), provided that A is able to receive the packet

- When C overhears a CTS, it keeps quiet for the duration of the transfer
  - Transfer duration is included in both RTS and CTS
BACKOFF INTERVAL

- Collision avoidance
  - Backoff intervals used to reduce collision probability
- When transmitting a packet, choose a backoff interval in the range [0, CW]
  - CW is contention window
- Count down the backoff interval when medium is idle
  - Count-down is suspended if medium becomes busy
- Transmit when backoff interval reaches 0

B1 and B2 are backoff intervals at nodes 1 and 2

\[ cw = 31 \]
BACKOFF INTERVAL

- The time spent counting down backoff intervals is a part of MAC overhead
- Important to choose CW appropriately
  - large CW → large overhead
  - small CW → may lead to many collisions (when two nodes count down to 0 simultaneously)
- How to choose an appropriate CW?
### 802.11 - FRAME FORMAT

- **Types**
  - control frames, management frames, data frames
- **Sequence numbers**
  - important against duplicated frames due to lost ACKs
- **Addresses**
  - Sender, receiver, BSS identifier
- **Miscellaneous**
  - sending time, checksum, frame control, data

<table>
<thead>
<tr>
<th>bytes</th>
<th>Frame Control</th>
<th>Duration/ID</th>
<th>Address 1</th>
<th>Address 2</th>
<th>Address 3</th>
<th>Sequence Control</th>
<th>Address 4</th>
<th>Data</th>
<th>CRC</th>
</tr>
</thead>
<tbody>
<tr>
<td>bits</td>
<td>2</td>
<td>2</td>
<td>6</td>
<td>6</td>
<td>6</td>
<td>2</td>
<td>6</td>
<td>0-2312</td>
<td>4</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>bits</th>
<th>Protocol version</th>
<th>Type</th>
<th>Subtype</th>
<th>To DS</th>
<th>From DS</th>
<th>More Frag</th>
<th>Retry</th>
<th>Power Mgmt</th>
<th>More Data</th>
<th>WEP</th>
<th>Order</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Protocol version</td>
<td>Type</td>
<td>Subtype</td>
<td>To DS</td>
<td>From DS</td>
<td>More Frag</td>
<td>Retry</td>
<td>Power Mgmt</td>
<td>More Data</td>
<td>WEP</td>
<td>Order</td>
</tr>
</tbody>
</table>
802.15.4 ARCHITECTURE

- IEEE 802.15.4 MAC
- IEEE 802.15.4 Service Specific Convergence Sub Layer (SSCS)
- IEEE 802.2 LLC, Type I
- IEEE 802.15.4 868/915 MHz PHY
- IEEE 802.15.4 2400 MHz PHY
DEVICE ADDRESSING

• Two or more devices communicating on the same physical channel constitute a WPAN which includes at least one FFD (PAN coordinator).

• Each independent PAN will select a unique PAN identifier.

• All devices operating on a network shall have unique 64-bit extended address. This address can be used for direct communication in the PAN.

• An associated device can use a 16-bit short address, which is allocated by the PAN coordinator when the device associates.
IEEE 802.15.4 SUPPORTED TOPOLOGIES

• MAC supports 2 topologies: star and peer-to-peer
• Star topology supports beacon and no-beacon structure
  - All communication done through PAN coordinator
PHYSICAL FREQUENCIES AND CHANNELS

868MHz / 915MHz

**PHY**

Channel 0

868.3 MHz

Channels 1-10

902 MHz - 928 MHz

2 MHz

2.4 GHz

**PHY**

Channels 11-26

2.4835 GHz

5 MHz
IEEE 802.15.4 MAC OVERVIEW

- Star networks: devices are associated with coordinators
  - Forming a PAN, identified by a PAN identifier
- Coordinator
  - Bookkeeping of devices, address assignment, generate beacons
  - Talks to devices and peer coordinators
- Beacon-mode superframe structure
  - GTS assigned to devices upon request
IEEE 802.15.4 GENERAL FRAME STRUCTURE

Four Types of MAC Frames:

- Data Frame
- Beacon Frame
- Acknowledgment Frame
- MAC Command Frame
EMBEDDED SYSTEM COMMUNICATION PROTOCOLS

Wired communication protocol examples:
• Ethernet (802.3)
• CAN
• TTP
• BACnet

Wireless communication protocol examples:
• Wi-Fi (802.11)
• ZigBee (based on 802.15.4 PHY and MAC)
• WirelessHART (Not discussed in this lecture)
“dominant” wired LAN technology:

- cheap $20 for NIC
- first widely used LAN technology
- simpler, cheaper than token LANs and ATM
- kept up with speed race: 10 Mbps – 10 Gbps

An example avionics communication network: AFDX network (Avionics Full Duplex Ethernet)

(Figure from Airbus, more details can be found at: http://www.artist-embedded.org/docs/Events/2007/IMA/Slides/ARTIST2IMA_1tier.pdf)
ETHERNET: PHYSICAL TOPOLOGY

• **Bus**: traditional topology
  - All workstations are connected on a single cable.
  - All transmissions go to all the connected workstation.

• **Star**: the most common solution today
  - Active **switch** in center
  - Each “spoke” runs a (separate) Ethernet protocol

---

**bus**: coaxial cable

**star**

**TTEthernet**
ETHERNET FRAME STRUCTURE

Sending adapter encapsulates IP datagram (or other network layer protocol packet) in **Ethernet frame**

![Ethernet frame structure diagram]

**Preamble:**
- 7 bytes with pattern 10101010 followed by one byte with pattern 10101011
- Used to synchronize receiver, sender clock rates
ETHERNET: UNRELIABLE, CONNECTIONLESS

- **Connectionless**: no handshaking between sending and receiving NICs
- **Unreliable**: receiving NIC doesn’t send ACKs or NACKs to sending NIC
  - data in dropped frames recovered only if initial sender uses higher layer reliable data transfer (e.g., TCP), otherwise dropped data lost
- Ethernet’s MAC protocol: unslotted **CSMA/CD with binary backoff**
Many different Ethernet standards

- Common MAC protocol and frame format
- Different speeds: 2 Mbps, 10 Mbps, 100 Mbps, 1Gbps, 10G bps
- Different physical layer media: fiber, cable

https://en.wikipedia.org/wiki/Ethernet_physical_layer