Introduction to Computer Networks and the Internet COSC 264

Local Area Networks and Ethernet

Dr. Andreas Willig

Dept. of Computer Science and Software Engineering
University of Canterbury, Christchurch

UoC, 2020

Outline

1. LANs
   - LAN Standards
   - Physical Topologies
2. MAC Fundamentals
3. Orthogonal MAC Schemes: FDMA and TDMA
4. Random Access Protocols
5. Ethernet
   - Ethernet Frame Format
   - PHY
   - Half-Duplex Ethernet MAC Protocol
6. Bridges, Switches
   - Repeaters and Hubs
   - Bridges and Switches

Preliminaries

- The following slides are based mainly on [28], [25]
- The older, but still very good book [6] covers some related topics, book is available in pdf format here:

  http://web.mit.edu/dimitrib/www/datanets.html

Outline

Local Area Networks (LANs)

- LANs are packet-switched networks
  - Packets are often called **frames** in LAN context
- They have limited geographical extension, usually ≤ 1 km
- Often controlled by only one owner / administrative entity
- They offer:
  - A shared transmission medium to multiple stations
  - Low cost for station attachment
  - Higher rates than usually experienced in wide-area networks
- Some application areas:
  - Connect desktop computers to share files, emails, ...
  - Allow several computers to share printers, file servers, ...
  - Interactive video or telephony between local users
  - Providing Internet access

Outline

LAN Protocol Architecture

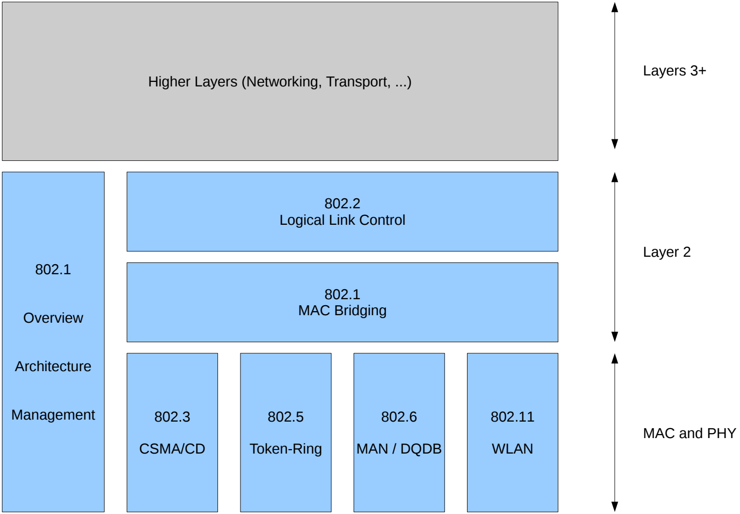
- LAN standards typically specify the following layers:
  - **Physical layer (PHY)**, specifying transmission media, network adapters, modulation schemes, data rates and network topologies
  - **Medium Access Control (MAC)** sublayer, specifying how stations share the transmission medium
  - Optional: **Link layer** (often called logical link control), providing error-control, flow-control, etc.
    - Error control: error detection, retransmissions, error-correction coding
    - Flow control: stopping a fast transmitter from overwhelming a slow receiver with more data than it can currently process

  Error-control coding often done in hardware and integrated in PHY
- This is the protocol architecture followed by the IEEE standards, which are the dominant LAN standards

The IEEE 802 Standards Series

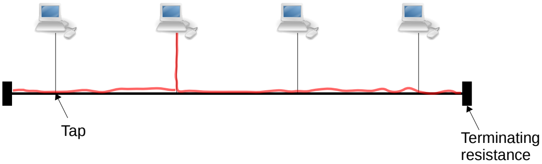
- IEEE = Institute of Electrical and Electronics Engineers
- IEEE is a professional association, not a standards body
- Nonetheless, ISO adopted several IEEE standards
- Some important standards (series):
  - IEEE 802.1: Overview, Bridging, Network Management,
  - IEEE 802.2: Logical Link Control (LLC) [23]
  - IEEE 802.3: Ethernet [14]
  - IEEE 802.11: Wireless LAN [16]
  - IEEE 802.15: Wireless Personal Area Network (WPAN), incl. Bluetooth [15], IEEE 802.15.4 [21], ...
- There are *many* more ...
- See `http://standards.ieee.org/getieee802`

The IEEE 802 Standards Series (2)



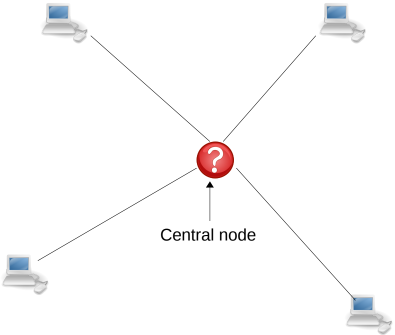
Outline

Bus Topology



- Stations are attached via tap line to bus
- Bus is a broadcast medium, signals are heard by all stations
- Parallel transmissions collide, all packets are garbled
- Frames include destination address field to indicate intended receiver
- Bus length usually limited to a few dozens / hundreds of m, e.g. to prevent excessive signal attenuation
- By cascading several buses (using branch points) more complex broadcast toplogogies can be built (e.g. trees)
- Examples: classical Ethernet, Token Bus (IEEE 802.4 [13])

Star Topology



- Stations are attached to a central unit, often with separate cables for transmit and receive directions
- Central unit can act either as a repeater or as a bridge/switch
- A repeater copies incoming signals to *all* other outputs
- A bridge/switch copies incoming frame only to output where destination is
- Discussed in more depth later

Wireless Topologies

- Wireless transmission media are much more prone to errors than wired media [26], [33], bit-error rates of 10^{-2} are not uncommon
- Wireless links are influenced by propagation environment
  - Doors, moving faces in the surrounding, walls, ...
- A station cannot necessarily hear **all** other stations

Important Property

Wireless transmission channels are time-varying, the links are volatile and unpredictable, there is usually no static wireless topology

Outline

Medium Access Control (MAC)

- MAC protocols are schemes which allow a number of users to coordinate the access to a common channel
- MAC protocols are a vast subject, some references (not even the tip of the iceberg!) are: [12], [27], [22], [8], [34], [29], [2], [18], [20], [9], [30], [17], [31], [32] [4], [5], [3], [10]
- The MAC layer is often regarded as a separate sub-layer between PHY and link-layer
- This view is supported by the fact that the MAC has a distinguished task not covered by any other layer
- MAC protocols are heavily influenced by the properties of the underlying transmission medium

MAC Definition

- We are given:
  - A number of users / stations wishing to communicate
  - A shared communications channel / resource that can only be used by one station at a time
  - No other means for information exchange between stations

Definition

MAC protocols are rules by which distributed stations coordinate access to a common channel to share it efficiently and in a manner satisfying given performance requirements

Example: 100 blind persons in a room – how to distribute right to talk?

Important Assumptions

- The shared channel is a broadcast medium, i.e. transmission of one station is heard by *all* other stations
  - Not necessarily true for wireless transmission media
- In case of parallel transmissions all contending transmissions are garbled, i.e. cannot be reliably decoded
  - Not necessarily true for wireless transmission media
  - Often not true for CDMA systems, also not in OFDMA

MAC Design Desiderata

- Small *medium access delay*: time between arrival of packet to empty station and start of successful transmission
  - Depends on overheads: collisions, waiting times, ...
  - For lightly loaded medium a small access delay is desirable
- Fairness and fair re-use of unused resources
- Efficiency: low overhead, high throughput
- Stability: increasing load should not decrease throughput

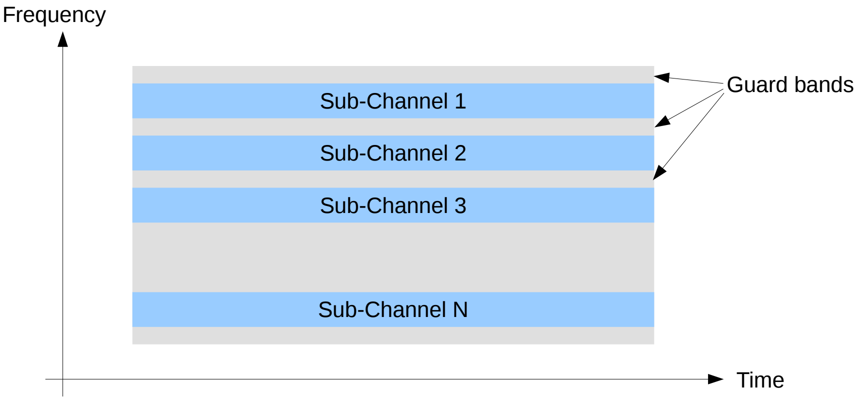
Note: you usually do not get all of these at the same time ...

Outline

Orthogonal Schemes

- In *orthogonal schemes* the behavior of one station does not influence the behavior / throughput / transmission success / . . . of other stations
- Orthogonal schemes allow for collision-free transmission
- The four main (mostly) orthogonal schemes are:
  - FDMA = Frequency Division Multiple Access
  - TDMA = Time Division Multiple Access
  - SDMA = Space Division Multiple Access
  - CDMA = Code Division Multiple Access
- We will not discuss SDMA and CDMA

Frequency Division Multiple Access (FDMA)



FDMA (2)

- The given channel bandwidth is subdivided into N *sub-channels*
- Between the sub-channels and at the fringe of the channel there are *guard bands*:
  - Reduction of adjacent-channel interference, robustness against imperfect frequency synchronization
- A sub-channel is *exclusively* assigned to a station i on a longer-term basis for transmission of data, **no other station is allowed to transmit on this channel**
- To receive data, a station must:
  - Either possess a separate receiver for each channel, or
  - Have a single tunable receiver that must be switched to a specific channel before data can be received on it
    - Problems: coordination/rendez-vous, tuning times

FDMA (3)

- If totally available bandwidth is B $\left[\frac{b}{s}\right]$, station i is assigned $\frac{1}{N}$ of B on a long-term basis (neglecting guard bands)
- Medium access delay for a new packet arriving to an empty station i is always zero, since i can start transmission immediately without risk of collision
- If a packet has size $\frac{B}{N}$ bits, its transmission takes one second:

$$E\left[\text{Transmission Delay}\right] = 1$$

- Its total completion time is the sum of transmission and access delay, which here is equal to the transmission delay

FDMA – Advantages

- N stations can transmit in parallel
- No need for time synchronization between the N transmitters

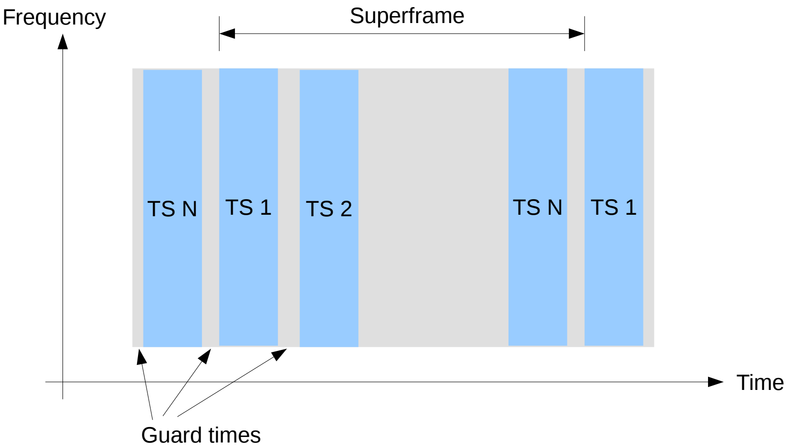
FDMA – Disadvantages

- Need for N receivers or tunable receivers increases complexity
- Frequency synchronization required
- No re-use: channel not used by owner can't be used by others
- Coordination and shared state required for allocating subchannels

Conclusion

FDMA is good for CBR but bad for VBR traffic

Time Division Multiple Access (TDMA)



TDMA (2)

- Each station uses the whole frequency band (except some guard bands at the fringe of the spectrum), but only at certain times:
    - Time is subdivided into *superframes* of duration T_{SF}
    - Each superframe is subdivided into N *time-slots*
    - There are short *guard times* between time slots
    - One or more time slots are assigned exclusively and on a longer-term basis to a station i for transmission
- Stations must be time-synchronized to avoid overlapping transmissions, guard times are required to compensate (small) synchronization errors

Completion Time in TDMA

- Neglecting guard times, each station having a slot gets the full channel bandwidth $B\ \left[\frac{b}{s}\right]$ for a fraction of $\frac{1}{N}$ of time
- Assume that:
  - station i owns one time slot
  - $T_{SF} = 1$ second
  - a time-slot suffices to transmit $\frac{B}{N}$ bits (we ignore guard times)
  - a packet of $\frac{B}{N}$ bits arrives at random time to empty station i
- Medium access delay = waiting time until station i's next slot starts

$$E\left[\text{Access Delay}\right] = \frac{T_{SF}}{2} = 0.5\ \ [s]$$

Completion Time in TDMA (2)

- The time to transmit the packet (transmission delay) is $\frac{1}{N}$ seconds
- Assuming no channel errors we have:

$$\begin{aligned} E\,[\text{Completion Time}] &= E\,[\text{Access Delay}] + E\,[\text{Transm. Delay}] \\ &= 0.5\ [s] + \frac{1}{N}\ [s] \leq 1\ [s] \end{aligned}$$

for $N > 2$ this is a true inequality

Conclusion

With TDMA we can start later and finish sooner than with FDMA!!

TDMA – Advantages and Disadvantages

- Advantages:
  - It is easier to achieve asymmetric bandwidth assignments in TDMA than in FDMA: using multiple time-slots is much simpler than transmitting on multiple frequencies in parallel
  - TDMA tends to have better completion times than FDMA
  - No tunable receivers needed
- Disadvantages:
  - Tight time-synchronization between stations required
  - High expected access delay even in otherwise idle systems
  - Not possible to re-use unused time slots
  - Coordination and shared state required for allocating time slots

Conclusion

TDMA is good for CBR but bad for VBR traffic

Outline

Random Access Protocols

- Random access protocols:
  - do not attempt to reserve channel resources for longer time
  - do not require a central station or (much) shared state
  - do not access the medium at predictable times
  - often have low complexity (e.g. only little signaling, if any)
  - typically involve some random element
- Random access protocols are used standalone and also as building blocks for more complex MAC protocols, e.g.:
  - In GSM a mobile uses slotted ALOHA to request call setup

Important Point

Random access protocols accept risk of collisions to save coordination overhead and have overall improved efficiency! How well this trade-off works depends for example on the offered traffic load.

ALOHA

- ALOHA [1] is one of the earliest MAC protocols, developed $\approx$ 1970 at the University of Hawaii
- Assumptions:
  - N uncoordinated transmitters
  - One receiver (e.g. a base station)
  - If two packets overlap at receiver, a *collision* occurs

The Pure ALOHA Protocol

- When a new packet arrives at an idle station:
  - a checksum is computed and appended to the frame
  - the frame is then **transmitted immediately**, there is no coordination with other stations
  - an *acknowledgement timer* is started
- The receiver sends an *immediate ack* upon successful reception of a packet – upon collisions or transmission errors it remains quiet
- If the transmitter receives an ack before the ack timeout, the frame is removed and the ack timer is canceled

The Pure ALOHA Protocol (2)

- When ack timer expires, transmitter enters **backoff mode**:
  - The transmitter chooses a random backoff time
  - It waits for this time without further action
  - At backoff timer expiry the frame is re-transmitted
  - The ack timer is set again, backoff mode is left
  - **Question**: why is the backoff time chosen randomly?
- When number of failed trials exceeds threshold, frame is dropped
- The precise choice of random distribution for backoff times is critical for delay, throughput and stability! [11], [19]
  - Often the random distribution depends on the number of subsequent collisions seen by the frame
  - An example backoff strategy will be discussed later!
- When a new packet arrives to backlogged station, it is stored in queue and served after all previous packets
- When transmission of a packet is completed and queue is not empty, then the next packet is transmitted after random backoff

UC UNIVERSITY OF CANTERBURY Te Whare Wānanga o Waitaha CHRISTCHURCH NEW ZEALAND

Advantages of Pure ALOHA

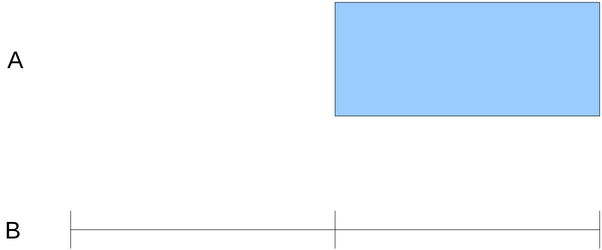
- Quite simple to implement
- If network load is small:
  - new frames are sent immediately $\Longrightarrow$ access delay is zero
  - they can use the full channel bandwidth
  - and the probability of collision at the receiver is low

Conclusion

For low network loads most packets can have the minimum possible completion time

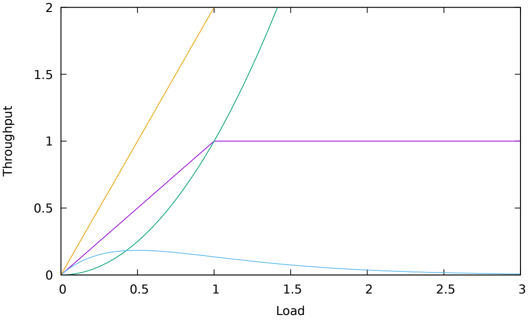
Disadvantages of Pure ALOHA

- Consider stations *A* and *B* sending frames of same length:



- When *B* starts its frame during the (two frame times long) *vulnerability period* of *A*'s frame, the frames collide
- When more stations are active the collision probability increases
- ALOHA cannot distinguish between collisions and channel errors destroying a frame

Throughput



- Consider a system with many transmitters with equal average load, each generating packets at random times
- Aggregate load is given, all packets have the same length, packet transmission time is τ
- Define load as the aggregate (average) number of packets generated during time τ, througput as the (average) number of successfully received packets during time τ in the absence of channel errors
- Which of these (idealized) curves is the throughput of ALOHA? And which one the throughput of FDMA? What about the other curves?

The CSMA Family of Protocols

- CSMA = Carrier Sense Multiple Access [17], [31]
- Common assumption: all stations can determine the state of the medium (almost) instantaneously:
  - **Busy**: at least one station is currently transmitting
  - **Idle**: no station is transmitting

  This operation is called **carrier-sensing** (CS) or **clear-channel assessment** (CCA)
- Common approach: **Listen-before-talk** (LBT)
  - Before station transmits a frame, it performs CS operation
  - If channel is busy, station defers transmission according to one of several possible strategies
  - The maximum number of deferrals (or **backoffs**) a station might experience for a frame is often bounded
- CSMA protocols do not eliminate collisions completely, but reduce their rate or their impact

The CSMA Family of Protocols (2)

- CSMA approach is especially useful when medium propagation time is small compared to packet length, since other stations notice transmission quickly after it started
  - Typically satisfied in LANs, propagation delay is small
  - Collisions can only occur when two stations start transmitting at almost same time (time difference smaller than propagation delay)
- When propagation time is large compared to packet length, the sender might have already stopped transmission when receiver senses busy carrier for first time
  - Example: multi-access satellite configurations
  - Here LBT is almost useless, ALOHA is reasonable

Nonpersistent CSMA

- After getting a new packet from higher layers a station first performs a carrier-sense operation
- If a station senses a busy medium, it:
  - draws a backoff time from a given random distribution
  - defers from channel activities during backoff time, and
  - after the backoff time it senses the medium again and starts over
- If station detects idle medium, it starts transmitting immediately
- In case of collision a backoff time is chosen, process starts over
  - **Question**: how to diagnose collisions?
- Performance problem: with high probability a medium is idle for some time after previous transmission has finished, this lowers utilization

p-persistent CSMA

- Be $p \in (0, 1)$ a parameter known to all stations
- If a station senses a busy medium, it defers until the end of the ongoing transmission, when medium becomes idle
- A station divides time on idle medium into small time slots
  - At the beginning of a time slot a station performs a random experiment: with probability p it starts transmission, with probability $1 - p$ it defers for one further slot
  - When station defers, it checks medium during remaining slot time: when another station started transmission, station waits for end of this transmission and starts over
  - Time slot just large enough to accommodate these activities
- In case of collision, process starts over
- **Question**: How would you choose p?
- Performance problem: again, medium will be idle for some time after previous transmission has finished

1-persistent CSMA or CSMA/CD

- CSMA/CD was chosen for classical Ethernet
- If station senses busy medium, it defers until end of transmission
- When medium is / becomes idle, station sends unconditionally
  - This avoids idle times after previous transmission
  - But if two or more stations start, we surely have collision and we need **collision resolution procedure**
- While transmitting, sender tests channel for collisions
- In case of a collision:
  - Transmission is aborted
  - A jamming signal is sent to inform all stations about collision
  - A collision resolution procedure is started, e.g.:
    - Backoff schemes (used in Ethernet and WLANs)
    - Tree algorithms [7]

Outline

Ethernet

- Ethernet is a packet-switched LAN technology, invented in 1973 by Metcalfe/Boggs at Xerox PARC
- Ethernet became the dominant wired LAN technology, early competitors like Token-Ring, Token-Bus vanished
- Standardized by IEEE ([14] and various amendments)
- Its name refers to the “Ether” that was believed to be the necessary medium for electromagnetic wave propagation
- It offers:
  - High data rates (10 Mbps, 100 Mbps, 1 Gbps, 10 Gbps, 100 Gbps)
  - Cheap and mature components
  - Large market penetration, many different vendors
- These slides are mainly based on [28, Chap. 16]

Outline

Frame format

7	1	6	6	2	46 - 1500	4
Preamble	SOF	DstAddr	SrcAddr	Length/ Type	Payload	FCS

- The original Ethernet had a slightly different frame format
- Minimum payload size is 46 bytes, smaller messages must be padded (filled up with zeros)
- Maximum payload size is 1500 bytes
- Preamble allows receiver to acquire symbol/bit synchronization
- SOF = Start of Frame
- FCS = Frame Check Sequence, it is a CRC checksum

Ethernet Addresses

- Address fields are 48 bits long
- Each Ethernet adapter has its own address, typically burned into adapter hardware
- Addresses are required to be **globally unique**
  - Each vendor gets own address range and assigns unique addresses from that range
  - Nowadays adapters with programmable address available
- Address representation as six colon-separated bytes in hexadecimal representation, e.g.:

  `00:0c:29:10:fb:f3`

- Special addresses and address ranges:
  - Broadcast address: `FF:FF:FF:FF:FF:FF`
  - Addresses with first bit set to `1` but different from broadcast address are multicast addresses
  - Addresses with first bit set to `0` are unicast addresses

The Length/Type Field

Type field	Protocol
0x0800	IPv4
0x0806	ARP
0x809B	AppleTalk
0x86DD	IPv6
0x8863	PPPoE Discovery
0x8864	PPPoE Session

- When the L/T field carries value $\geq$ `0x0600` it is interpreted as a type field, indicating the higher-layer protocol that is encapsulated in the Ethernet frame
- The type field therefore provides **protocol multiplexing**
- When the L/T field carries a value $\leq$ 1500, it indicates the length of the payload, then the type field is assumed to be in the first two bytes of the payload

Outline

Ethernet PHYs

- The Ethernet standard specifies several different physical layers, using different transmission media and adapters:
  - Coaxial cables
  - Twisted pair cables
  - Fiber cables
- The standard also specifies several transmission rates: 10 Mbps, 100 Mbps, 1 Gbps, 10 Gbps, 40 Gbps, 100 Gbps
- Ethernet supports fundamentally two types of topologies:
  - Broadcast topologies (almost disappeared nowadays)
  - Switched Ethernet

Broadcast Topologies

- All stations share capacity of the medium, MAC is needed
- Stations operate in half-duplex mode, i.e. they switch between transmitting and receiving / listening
- In Ethernet:
  - Bus topology (with coaxial cable)
  - Hub-based topology, using different types of cables
- Only used in the 10 Mbps PHYs
- Referred to as half-duplex Ethernet in the following

Switched Topologies

- Stations are attached to (possibly cascaded) switches via point-to-point links, no MAC needed on those links
  - The MAC is nonetheless “used”, since it is present anyway
- Stations operate in full-duplex mode, i.e. they can transmit and receive at the same time
- Parallel transmissions possible, contention occurs for resources in switches (e.g. buffer memory)
- Used for 100 Mbps and higher PHYs
- Referred to as switched Ethernet in the following

Outline

Half-duplex MAC Protocol

- Half-duplex Ethernet uses CSMA/CD
  - Carrier-Sense-Multiple-Access with Collision-Detection
- Major assumptions:
  - Parallel transmissions lead to collisions
  - Stations monitor the medium for collision while transmitting
    - Ethernet implements this by checking the voltage on the medium, a collision is inferred when this voltage exceeds the voltage applied by the transmitter alone

MAC Protocol

1. New packet arrives at the MAC of a station, set `coll` to zero
   - `coll` is a local counter, each station has its own
2. Station performs a carrier-sense operation
3. When the medium is idle, transmission starts immediately
4. When medium is busy:
   1. listen until channel becomes idle again
   2. start transmitting
5. While transmitting, check for collision
6. If collision is detected:
   1. Abort frame transmission, send a short jamming signal
   2. Increase counter `coll`, counting # of subsequent collisions
   3. If `coll` > 16 then drop frame, set `coll` to zero
   4. Wait for random time (the **backoff time**), then go to step 2
7. If no collision detected, transmit whole frame, set `coll` to zero

Computation of Backoff Time

- Draw a random integer number uniformly from the interval

$$\left[0, 1, \ldots, 2^{\min\{10, \texttt{coll}\}} - 1\right]$$

  which is called the **backoff window**

- The actual backoff time is computed by multiplying this integer with the pre-defined **slot time**
- Slot time is common parameter, just large enough to cover maximum round-trip time and small processing delays

Important Point

The backoff window size and therefore the average backoff time doubles after each collision, until 10 collisions have been observed! This is called the (truncated) binary exponential backoff algorithm!

Question: why this algorithm?

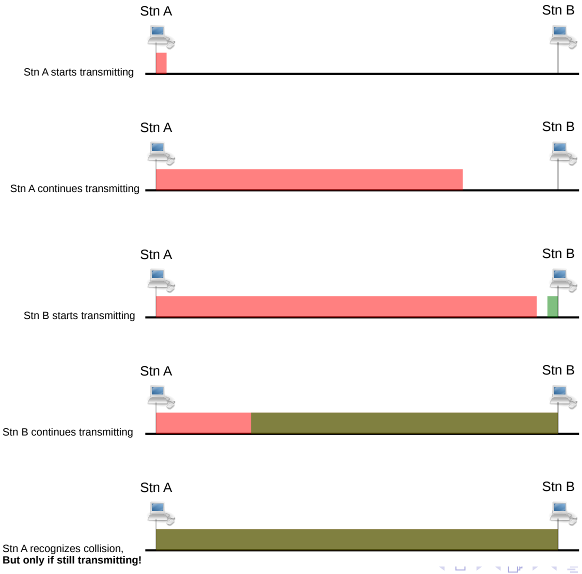
Minimum Frame Size / Slot Time

- Minimum frame size (64 bytes for 10 Mbps Ethernet) is chosen to ensure that transmitter can indeed detect collision on a cable of given length **while still transmitting**
- Rationale: a frame must be long enough to still being transmitted after the maximum round-trip delay plus small processing times introduced by repeaters / hubs
- Requirement for maximum round-trip delay can be understood from worst-case example (next slide)

Important Point

Smaller slot times / minimal frame sizes can be achieved by restricting the maximum length of an Ethernet segment!

Minimum Frame Size (2)



Half-duplex MAC Protocol – Important properties

- Very short medium access delays under light load
- Under heavy load and for many stations collision rate increases
  - Ethernet should not be operated beyond 50 - 60% load!

Outline

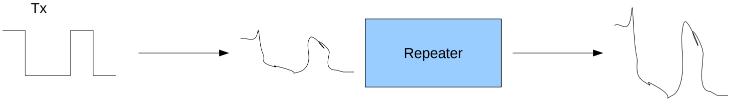
Coupling LANs

- It is often required to couple existing LANs, e.g. upon merging different departments
- Coupling requires special **coupling devices**
- Types of coupling devices:
  - PHY layer: repeaters, hubs
  - MAC layer: bridges, layer-2 switches
  - Network layer: router
  - Application layer: gateway
- See [24], [35]

Outline

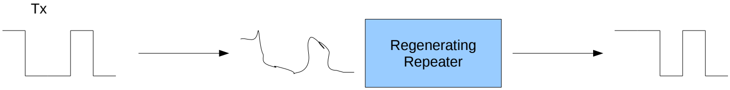
Repeaters

- A **repeater** amplifies a signal on the analog level
  - Any noise present in the signal is amplified as well
  - Repeaters add their own noise
  - Repeaters are agnostic to any protocol or modulation scheme
  - They can create slight delay (order of μs and less)

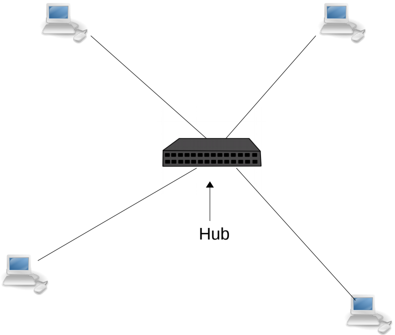


Regenerating Repeaters

- A **regenerating repeater** demodulates an incoming signal symbol-per-symbol and modulates it again
  - It does not look beyond one symbol at a time
  - No interpretation whatsoever of protocol fields is done
  - Especially, no error checking / error correction is done, regeneration can introduce errors



Hubs



- Hubs are centralized repeaters, they broadcast signals coming in on one port to all other ports
- No interpretation of the incoming frame is done, none of its fields is evaluated
- All stations are attached with one transmit and one receive line
- A hub creates a broadcast medium on a physical star
- Hubs can be cascaded
- It may be regenerative or not
- **Question**: Advantage over bus?

Outline

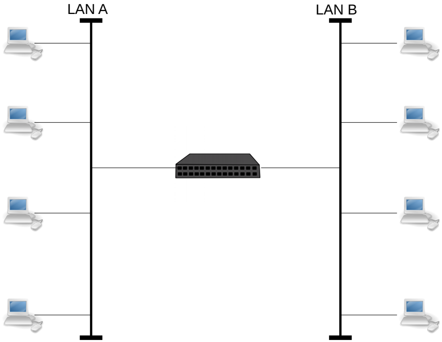
Bridges

- Bridges interconnect LANs on the MAC layer
- They mostly connect LANs of the same type (e.g. Ethernet), but bridges connecting LANs of different types **but the same MAC address structure** (e.g. Ethernet – Wireless LAN) also exist
- We focus on bridges interconnecting broadcast Ethernets
  - Important: Ethernet frames carry an Ethernet source address and an Ethernet destination address in their frame header
- A bridge can connect several LANs
- Bridges can be cascaded

Important Point

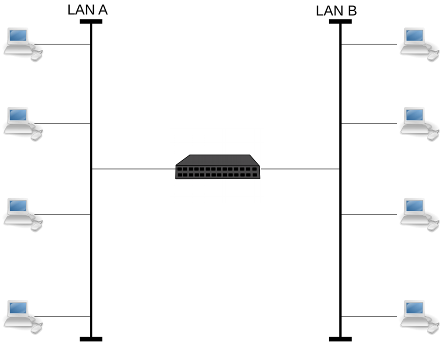
Bridges understand and interpret fields related to the MAC protocol (e.g. address fields), repeaters / hubs do not!

Basic Operation



- When bridge receives frame from LAN A, it checks for correctness, buffers it and checks MAC destination address (`dst`)
- `dst` on LAN A: bridge does nothing
- `dst` on LAN B or `dst` unknown: bridge transmits frame on LAN B, **following the rules of the MAC protocol!**
- Same in direction B $\rightarrow$ A
- Bridge does not modify any frame, nor does it encapsulate them
- Stations need not be aware of the presence of bridges (**transparency**)

Basic Operation (2)

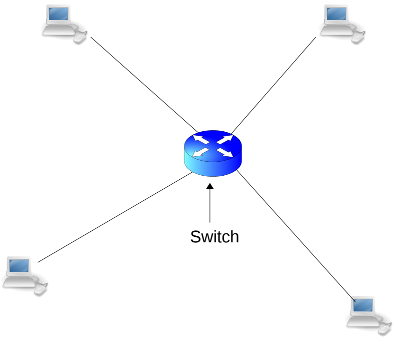


- How does bridge know which station is in which LAN?
- From reading a frames source address field (`src`) the bridge can learn on which bridge interface a source can be reached
- When a bridge receives a frame with `dst` not having been observed so far, it unconditionally re-transmits the frame on all interfaces except incoming one
- The latter approach is dangerous when several bridges are used and loops are present
- Additional mechanisms are needed to deal with loop scenarios

Some Reasons to Use Bridges

- **Reliability**: by keeping LANs separated and only interconnected by a bridge, failures in one LAN do not affect others
- **Performance**: by carefully evaluating addresses, bridges can confine traffic local to one LAN to that very LAN, enabling parallel local transmissions in different LANs
  - Repeaters / hubs cannot achieve this “traffic separation”!
- **Security**: similarly, traffic local to one LAN cannot be eavesdropped in the other LAN

Layer-2 Switches



- A switch is a centralized element, forwarding frames **only to the correct output port**
- Stations are attached to switch via point-to-point links with separate transmit/receive lines (full-duplex)
- No broadcast medium anymore!
- Switches can process frames to distinct destinations **in parallel**, switches can increase network capacity as compared to LANs with broadcast medium
- Frames arriving in parallel for the same destination are buffered (output buffering)
- Switches are transparent to stations
- Nowadays almost all Ethernet installations use switches

Layer-2 Switches (2)

- Difference to a hub:
  - A hub builds a broadcast medium, only one station can transmit at a time without collisions
  - A switch can accept up to N parallel transmissions, where N is the number of stations in the LAN
  - Each attached station can receive packets at full medium capacity

Important Point

Switches remove the “shared medium” assumption and the need for a MAC, but now the stations contend for the resources of the switch (switching capacity, buffer memory)!

[1] Norman Abramson.
Development of the ALOHANET.
IEEE Transactions on Information Theory, 31(2):119–123, March 1985.

[2] Norman Abramson, editor.
Multiple Access Communications – Foundations for Emerging Technologies.
IEEE Press, New York, 1993.

[3] Norman Abramson.
Multiple Access in Wireless Digital Networks.
Proceedings of the IEEE, 82(9):1360–1370, September 1994.

[4] Ian F. Akyildiz, Janise McNair, Loren Carrasco, and Ramon Puigjaner.
Medium access control protocols for multimedia traffic in wireless networks.
IEEE Network Magazine, 13(4):39–47, 1999.

[5] Guiseppe Anastasi, Luciano Lenzini, Enzo Mingozzi, Andreas Hettich, and Andreas Krämling.
Mac protocols for wideband wireless local access: Evolution towards wireless atm.
IEEE Personal Communications, 5(5):53–64, October 1998.

[6] D. Bertsekas and R. Gallager.
Data Networks.
Prentice Hall, Englewood Cliffs, New Jersey, 1987.

[7] J. I. Capetanakis.
Tree Algorithm for Packet Broadcast Channels.
IEEE Transactions on Information Theory, 25(5):505–515, September 1979.

[8] Lou Dellaverson and Wendy Dellaverson.
Distributed channel access on wireless atm links.
IEEE Communications Magazine, 35(11):110–113, November 1997.

[9] Andras Farago, Andrew D. Myers, Violet R. Syrotiuk, and Gergely V. Zaruba.
Meta-MAC Protocols: Automatic Combination of MAC Protocols to Optimize Performance for Unknown Conditions.
IEEE Journal on Selected Areas in Communications, 18(9):1670–1681, September 2000.

[10] Robert G. Gallager.
A Perspective on Multiaccess Channels.
IEEE Transactions on Information Theory, 31(2):124–142, March 1985.

[11] Jonathan Goodman, Albert G. Greenberg, Neal Madras, and Peter March.
Stability of binary exponential backoff.
Journal of the ACM, 35(3):579–602, 988.

[12] Ajay Chandra V. Gummalla and John O. Limb.
Wireless medium access control protocols.
IEEE Communications Surveys and Tutorials, 3(2):2–15, 2000.
http://www.comsoc.org/pubs/surveys.

[13] IEEE.
802.4 Token-passing Bus Access Method, 1985.

[14] IEEE Computer Society.
IEEE Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 3:

Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications, December 2005.

[15] IEEE Computer Society – Sponsored by the LAN/MAN Standards Committee.
IEEE Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 15.1: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for wireless personal area networks (WPANs), June 2005.

[16] IEEE Computer Society, sponsored by the LAN/MAN Standards Committee.
IEEE Standard for Information technology – Telecommunications and Information Exchange between Systems – Local and Metropolitan Area Networks – Specific Requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, 2007.

[17] Leonard Kleinrock and Fouad A. Tobagi.
Packet switching in radio channels: Part I carrier sense multiple access models and their throughput-/delay-characteristic.
IEEE Transactions on Communications, 23(12):1400–1416, 1975.

[18] J. F. Kurose, M. Schwartz, and Y. Yemini.
Multiple-access protocols and time-constrained communication.
ACM Computing Surveys, 16:43–70, March 1984.

[19] Byung-Jae Kwak, Nah-Oak Song, and Leonard E. Miller.
Performance Analysis of Exponential Backoff.
IEEE/ACM Transactions on Networking, 13(2):343–355, April 2005.

[20] S. S. Lam.
Multiaccess protocols in computer communications. volume I: Principles.
In W. Chon, editor, *Principles of Communication and Network Protocols*, pages 114–155. Prentice-Hall, Englewood Cliffs, NJ, 1983.

[21] LAN/MAN Standards Committee of the IEEE Computer Society.
IEEE Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low Rate Wireless Personal Area Networks (LR-WPANs), September 2006.
revision of 2006.

[22] Andrew D. Myers and Stefano Basagni.
Wireless media access control.
In Ivan Stojmenovic, editor, *Handbook of Wireless Networks and Mobile Computing*, pages 119–143. John Wiley & Sons, New York, 2002.

[23] The Editors of IEEE 802.
IEEE 802.2, ISO/IEC 8802-2: Local Area Networks: Logical Link Control, 1989.

[24] Radia Perlman.
Interconnections Second Edition – Bridges, Routers, Switches and Internetworking Protocols.
Addison-Wesley, Reading, Massachusetts, 1999.

[25] Larry L. Peterson and Bruce S. Davie.
Computer Networks – A Systems Approach.
Morgan Kaufmann, San Francisco, fourth edition, 2007.

[26] Theodore S. Rappaport.
Wireless Communications – Principles and Practice.
Prentice Hall, Upper Saddle River, NJ, USA, 2002.

[27] Izhak Rubin.
Multiple access methods for communications networks.
In Jerry D. Gibson, editor, *The Communications Handbook*, pages 622–649. CRC Press / IEEE Press, Boca Raton, Florida, 1996.

[28] William Stallings.
Data and Computer Communications.
Prentice Hall, Englewood Cliffs, New Jersey, fourth edition, 2006.

[29] Andrew S. Tanenbaum.
Computer Networks.
Prentice-Hall, Englewood Cliffs, New Jersey, third edition, 1997.

[30] Fouad A. Tobagi.
Multiaccess protocols in packet communications systems.
IEEE Transactions on Communications, 28:468–488, 1980.

[31] Fouad A. Tobagi and Leonard Kleinrock.
Packet switching in radio channels: Part II the hidden terminal problem in csma and busy-tone solutions.
IEEE Transactions on Communications, 23(12):1417–1433, 1975.

[32] Fouad A. Tobagi and Leonard Kleinrock.

Packet switching in radio channels: Part III – polling and (dynamic) split-channel reservation multiple access.
IEEE Transactions on Communications, 24(8):832–845, August 1976.

[33] David Tse and Pramod Viswanath.
Fundamentals of Wireless Communications.
Cambridge University Press, Cambridge, UK, 2005.

[34] Harmen R. van As.
Media access techniques: The evolution towards terabit/s LANs and MANs.
Computer Networks and ISDN Systems, 26:603–656, 1994.

[35] George Varghese and Radia Perlman.
Transparent Interconnection of Incompatible Local Area Networks Using Bridges.
IEEE Journal on Selected Areas in Communications, 8(1):1565–1575, January 1990.